

DROP FOR DATA BROKERS

Getting ready for deletion request processing



DROP

California Privacy Protection Agency · June 2026

privacy.ca.gov/data-brokers

Agenda

01 Introduction to DROP

02 Data broker obligations

03 Deletion request processing

04 Implementation overview

05 Resources

06 Q&A

The information presented in this webinar is for informational purposes only, and should not be construed as providing legal advice or as comprehensively covering all data brokers' obligations under the Delete Act.

SECTION 01

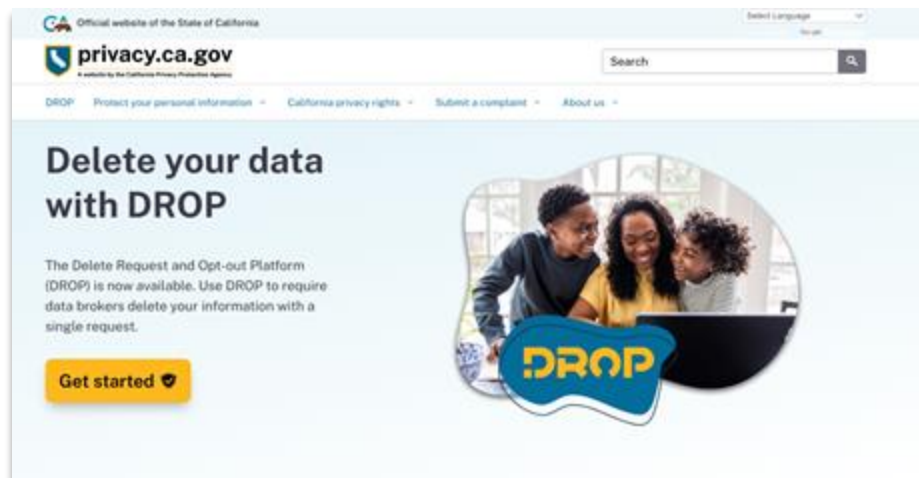
Introduction to DROP

Intro to DROP

Delete Request and Opt-Out Platform

- California's "accessible deletion mechanism" required by the Delete Act (SB 362)
- One consumer request covers all 590+ active data brokers simultaneously
- Consumers verify identity via California Identity Gateway
 - no account created, no raw consumer data is retained by DROP
- All consumer identifiers are SHA-256 hashed — data brokers match records without seeing raw personal data
- Free for consumers to use

Civil Code section 1798.99.80 et seq.



Submitting a DROP request - verify residency



To be eligible to submit a deletion request, the person must be a California resident.

To verify residency, consumers may use personal information or sign in using Login.gov.

Residency is verified via the California Department of Technology's CA Identity Gateway.



Verify you're a California resident

DROP status

Exit DROP

Check eligibility Fill out request Submit request

You can use DROP if you're a [California resident](#)

Verify you're a California resident using personal information ?
or through using Login.gov ?

Once verified, you'll be directed back to DROP.

!

Each time you use DROP, you must use the same method to verify you're a California resident. Example: If you used Login.gov, then you must always use Login.gov.

Use personal information

Use Login.gov

Already submitted a request? [Check DROP Status.](#)

[Exit DROP](#)

Submitting a DROP request – Enter info



Consumers enter information into their profile.

Consumers may enter multiples of all identifiers except for date of birth.

Protect your privacy
Submit a request to delete your data

Check eligibility Create profile Submit request

Start by entering some information about yourself. The more information you provide, the more likely your personal data will be deleted. This information is only used to find and delete your data.

[What will be deleted?](#)
[Submitting a request for someone else?](#)

Basic information

Name

First name Last name

Names must include both a first and last name.

+ Add another name for the same person

Example legal names, maiden name, other variations, etc.

Date of birth

Month / Day / Year

ZIP/postal code

Only the initial five characters of the ZIP/postal code are used.

+ Add another ZIP code

Email address

We'll send you an email to make sure the number is correct.

+ Add another email address

Phone number

We'll call or text to make sure it's you.

☒ Text me ☐ Call me

+ Add another phone number

Mobile advertising ID (MAID)

+ Add another MAID

Connected TV ID

+ Add another TV ID

Vehicle identification number (VIN)

+ Add another VIN

☐ Check this if you're submitting this information for someone else.

Confirmation email

Enter the email address where we should send a confirmation email with your DROP ID. It's important to save your DROP ID, so you can check your status in the future.

Email address for confirmation

☐ Same as primary email.

All current and future data brokers who register with our Agency are included in your deletion request. If you would like specific data brokers to keep your data, you can remove them in the [data broker list](#).

Submitting a DROP request – Submit



Consumers submit their request and get an 8 digit DROP ID.

Consumers can use this DROP ID to check their request status.

The screenshot shows the DROP website interface. On the left is a dark blue sidebar with the DROP logo and navigation links: "My data profile", "Edit request", "Data broker list", and "Exit DROP". The main content area has a dark blue header with the text "Deletion request submitted". Below this, a light gray box contains the message "You successfully submitted a request to delete your data." followed by "Your DROP ID is 1234ABCD". A sub-message states: "You can use this ID to check your [DROP status](#). Be sure to keep this number." Below this is a button labeled "Download or print". Further down, a section titled "What's next?" provides information about processing timelines and next steps, including a list of bullet points and a link to the DROP website.

Deletion request submitted

You successfully submitted a request to delete your data.

Your DROP ID is 1234ABCD

You can use this ID to check your [DROP status](#). Be sure to keep this number.

[Download or print](#)

What's next?

Beginning August 1, 2026, data brokers will start processing your deletion request.

After you submit your request:

- You can check your DROP status to see if your data was deleted.
- It may take up to 90 days before you notice updates to your data.
- You can add more information about yourself anytime. New data can take up to 90 days to process.
- You can review the [DROP website](#) for resources.

SECTION 02

Data broker obligations

Delete Act - Core Obligations for Data Brokers



Register Annually

Create a DROP account. Register with CalPrivacy by January 31 each year and pay the annual registration fee. *If you are newly operating in 2026, pay required access fee when accessing DROP, and register in January of following year.*



Publish Consumer Request Metrics

By July 1 of each year, update Privacy Policy to include consumer privacy request metrics from the previous year.



Audit

Beginning January 1, 2028: undergo independent third-party compliance audit every 3 years.



Access DROP and Process Deletion Requests

Delete all non-exempt personal information, including inferences, for the consumer.



Report Status Back

Report the status of each request (Deleted, Opted-out, Exempt, Not Found) within 45 days of download.



Screen incoming data

Maintain a list of identifiers needed to ensure ongoing compliance for both matched and unmatched records. Some refer to this as a "suppression list."

Penalties & Enforcement



Failure to Register

\$200 per day

Fine for each day after January 31 that data broker is not registered plus registration fee and CalPrivacy's costs of investigation and administrative action



Failure to Process Deletion Requests

\$200 per day, per consumer

Fine for each day a data broker fails to delete information as required under Delete Act plus CalPrivacy's costs of investigation and administrative action

Your DROP account



Create Account

Create a DROP account. Enter contact and business information and complete required forms and payment.



Manage Account

From your account dashboard, select your consumer deletion list(s). Upload and download lists.



Review Technical Docs

Technical docs are available on our website and accessible via your DROP account.



Use the Sandbox

Test on synthetic data in the DROP Sandbox environment (Optional). Sandbox will remain live after August 1st.



Contact Us

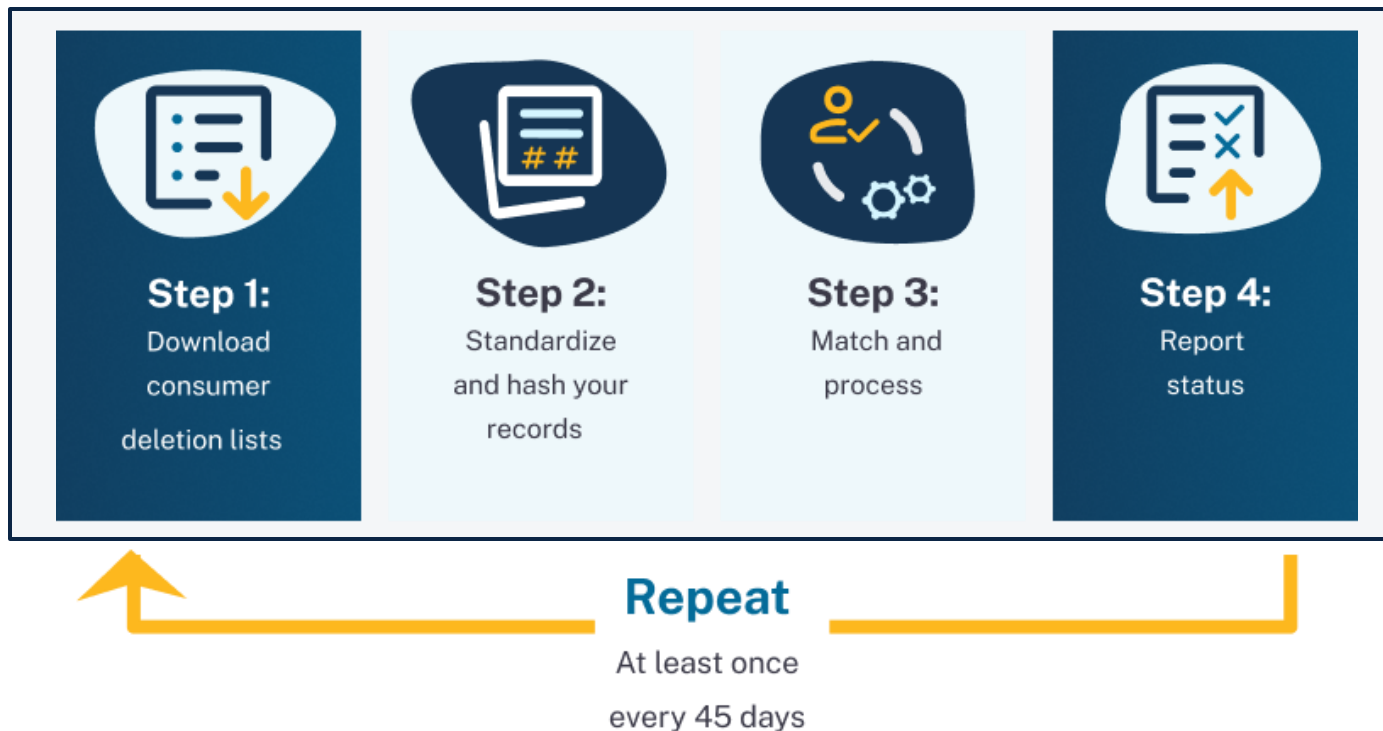
Questions? Use the Contact Us form in DROP to email us at any time. The DROP Support team is available to respond M-F 9am-5pm PST.

databroker.drop.privacy.ca.gov

SECTION 03

Deletion request processing

Deletion request processing – overview



Access DROP



API ACCESS

Automated, programmatic

- Generate API Key in DROP portal
- Integrate with DROP API
- Pull consumer deletion lists automatically
- Upload responses automatically



MANUAL UPLOAD / DOWNLOAD

Browser-based, no code

- Log in to the DROP portal
- Download consumer deletion lists manually
- Upload response manually
- No API integration required

If connection via API fails for any reason the manual option is available — processing deadlines still apply.

Step 1: Download consumer deletion lists



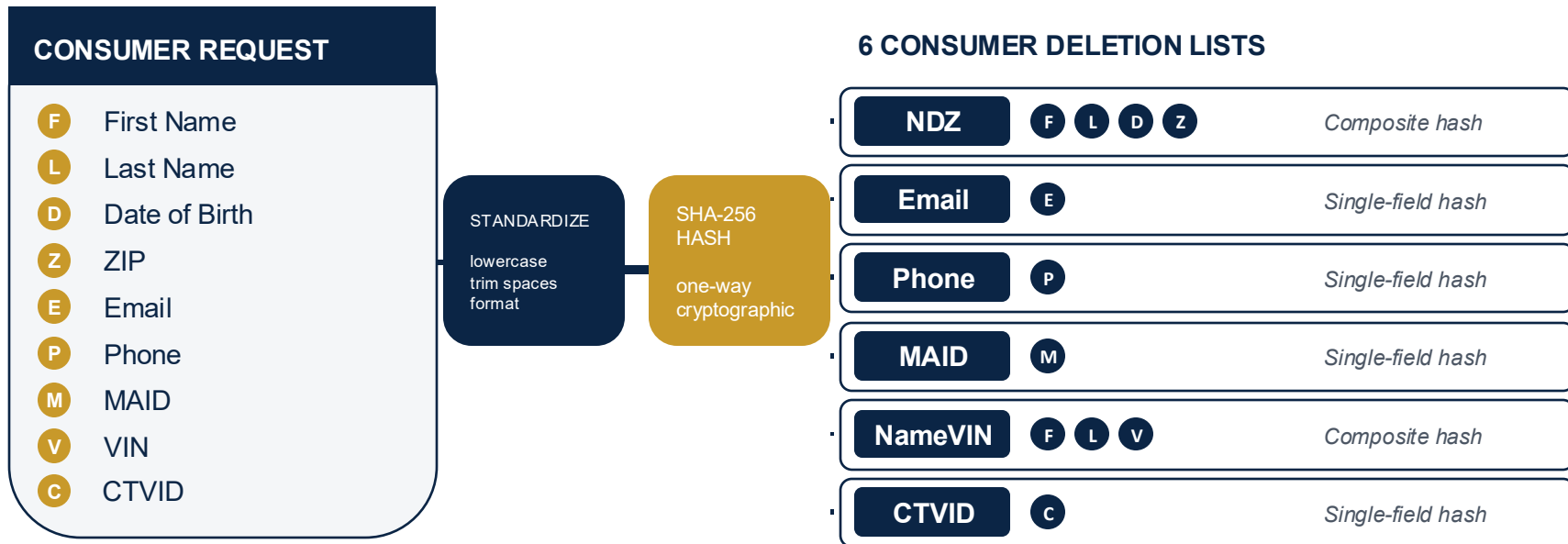
There are currently 6 consumer deletion lists, and each list includes one or more consumer identifiers, all provided in hashed format.

Data brokers must select **every** list containing a consumer identifier corresponding to personal information within the data broker's records.

A data broker may select fewer lists if the consumer identifiers used across multiple lists would lead to matches with the exact same set of consumers in the data broker's records.

Code	Identifier	Type
NDZ	First Name + Last Name + Date of Birth + ZIP	Composite hash
Email	Email address	Single-field hash
Phone	Phone number	Single-field hash
MAID	Mobile advertising ID	Single-field hash
NameVIN	First Name + Last Name + VIN	Composite hash
CTVID	Connected TV identifier	Single-field hash

How Identifiers Map to Deletion Lists



Step 2: Standardize and hash your records



All consumer identifiers in DROP are hashed.

In order to compare the identifiers in the DROP consumer deletion requests to your records, you must standardize and hash your data.

Standardization Overview

Identifier	Standardize First
Email	Lowercase
Name	Lowercase, remove special characters
Date of Birth	Format: YYYYMMDD
Phone	10 digits, no dashes/country code
ZIP Code	First 5 digits only, remove leading zeros
MAID / VIN / CTVID	Lowercase

Refer to the Technical Documentation for additional information on standardization and hashing.

Step 3: Match and process requests



Once standardized and hashed, compare your records to the hashed identifiers in the consumer deletion list(s) you download via DROP.



If you find a match:

- Delete all non-exempt personal information, including inferences, for the consumer
- Direct all service providers and contractors to delete matching records



If you find a match and multiple consumers are associated with a single matched identifier:

- Opt all associated consumers out of sale and sharing
- Direct all service providers and contractors to opt-out accordingly



If you don't find a match:

- Save and maintain a list of all consumers who submitted a deletion request via DROP to screen any newly collected records before they are sold or shared to ensure the deletion request is maintained on an on-going basis

Step 4: Report status



2

Exempted

Match found, but all personal information is exempt.

Example: Data is exempt because all of it is subject to GLBA.

3

Deleted

Match found. All non-exempt personal information deleted.

Example: Exact match on email address hash.

4

Opted Out

Multiple consumers are linked to the same identifier and all are opted out of sale and sharing.

Example: A hashed phone number matches multiple consumers — all matching consumers opted out.

5

Not Found

No match found after completing the matching process.

Example: No records in the data broker's records match the hashed consumer identifiers provided.

What consumers see in DROP



My data profile

My data profile

Edit request

Data broker list

Exit DROP

DROP ID 1234ABCD

Below is the data used in your current deletion request. Your data looks like this to protect you. When we collect your data, we securely store it in a format the is difficult to understand in the unlikely event of a breach.

You can add more data and submit an updated request anytime. Updates can only be processed every 45 days.

Status

Last request submitted: 11/11/2025

581

Total data brokers

Deletion status ⓘ

Updated as of: 08/11/2026

Deleted: 40/200

Opted-out: 40/200

Exempted: 40/200

Record not found: 40/200

Pending: 40/200

[See full list by data broker](#)

All current and future data brokers who register with our agency are included in your deletion request. If you would like specific data brokers to keep your data, you can remove them in the [data broker list](#).

Name

FOOO OOOOOO

Date of birth

##/##/##

ZIP/postal code

#####

Email address

#####

Phone number

###-###-####

MAID ⓘ

XXXXXXXXXX-XXXX-XXXX-XXXXXXXXXX

TV ID ⓘ

VIN ⓘ

###-###-###-###

[Edit request](#)



Data broker list

DROP status

My Data Profile

Data Broker List

Exit DROP

Here's a list of all currently active data brokers and your deletion request status for each broker. Data brokers are added to this list as soon as they create an account and register with CalPrivacy or newly begin processing deletion requests, whichever occurs first. Note that the status for all data brokers is likely to remain as "pending" until they begin processing deletion requests after August 1, 2026. If you are visiting this page prior to January 31, 2026, please check back later as the data broker registration process runs from January 1st to January 31st of each year.

If you want specific data brokers to **keep** your data, you can remove them by unchecking their box in the Delete data column and selecting Update list. If you're only updating the data broker list, you'll still need to submit a request on your profile for it to take effect.

☒ [Select/Deselect all](#)

Delete data	Data broker ▼	Request status ▼	Date updated ▼
☒	Intelytica, Inc.	☐ N/A	N/A
☒	01Advertistine Inc.	☐ N/A	N/A
☒	33 Mile Radius LLC	☐ N/A	N/A
☒	33Across, Inc.	☐ N/A	N/A
☒	5x5 US, LLC	☐ N/A	N/A
☒	Bazaar Insights, Inc.	☐ N/A	N/A
☒	A Project Marketing, Inc.	☐ N/A	N/A
☒	Above Data, Inc.	☐ N/A	N/A
☒	Accudata Integrated Marketing, LLC	☐ N/A	N/A
☒	Accurate Append Inc.	☐ N/A	N/A

☒ Include future data brokers

< Previous

12345...

60

Next >

Update list

Return

Deletion request processing - key dates

Ongoing Obligation

At least once every 45 days: access DROP and download deletion lists. **Within 45 days of each download:** upload response with status codes. *This cycle repeats indefinitely.*



Example processing timelines

Download Date	October 1	October 1	October 1
Upload Date	November 1	November 15	November 16
Uploaded within 45 days?	Yes	Yes	No



The date you download, in this example October 1st, is counted as Day 0. **You must upload within 45 days of your download date.**

Ongoing obligations

Maintain consumer deletion lists

Data brokers should maintain a list of identifiers needed to ensure ongoing compliance for both matched and unmatched records.

Some people refer to this as a “suppression list.” Compare this list against any newly collected records before new personal information is sold or shared.

For this list, you do not have to use our identifiers. Use the identifiers you need to maintain compliance.

Prepare for audit

Beginning January 1, 2028, independent third-party compliance audits will be required every 3 years.

Consider how to demonstrate compliance for auditing purposes, such as maintaining logs.

For example you may want to maintain:

- List download details (timestamps, record counts, etc)
- Processing and status reporting outcomes
- Upload details (uploads, amendments, etc)

SECTION 04

Implementation overview

Prepare for implementation

Account	Confirm account setup <i>Ensure relevant staff can access DROP Data Broker Portal.</i>	✓
Account	Verify account information. <i>Confirm contact email addresses are correct and up to date.</i>	✓
Integration	Review Technical Documentation <i>Review Technical Docs and API requirements, if relevant.</i>	✓
Integration	Test in the DROP Sandbox <i>Testing is optional but highly recommended.</i>	✓
Integration	Develop your integration (if applicable) <i>Prepare and develop your integration if using API</i>	✓
Operations	Define your workflow <i>Confirm your internal processing operations, schedules and workflow requirements.</i>	✓
Audit	Determine reporting needs <i>Maintain records needed to demonstrate compliance for audits.</i>	✓

DROP Technical Docs



Review the docs

Review the technical documentation before you prepare your workflow and implementation processes.

The screenshot shows the official website of the State of California's Privacy Protection Agency. The header includes the agency's name, logo, and a search bar. A navigation menu lists: DROP, Protect your personal information, California privacy rights, Submit a complaint, and About us. The main content area is titled 'Technical specifications' and features a sidebar with a list of links: Account creation and registration, Technical specifications (highlighted), Getting started, Integration workflow, Working with the data, API operations, Reference, Processing DROP requests, and Help with DROP. The main content area displays the title 'DROP Technical and API Reference Documentation', the last update date 'June 3, 2026', and the version '1.1.0'. It provides an overview of the documentation's purpose and includes a 'Download API Specification (OpenAPI YAML)' button. A note at the bottom states that data brokers are required to access DROP for deletion requests starting on August 1, 2026, and provides a link to contact the agency for questions.

Official website of the State of California

privacy.ca.gov

A website by the California Privacy Protection Agency

Search

DROP Protect your personal information California privacy rights Submit a complaint About us

Technical specifications

< DROP for data brokers

- Account creation and registration
- Technical specifications**
- Getting started
- Integration workflow
- Working with the data
- API operations
- Reference
- Processing DROP requests
- Help with DROP

DROP Technical and API Reference Documentation

Last updated: June 3, 2026

Version 1.1.0

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

Please be aware that this information 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 cippa.ca.gov/regulations.

[Download API Specification \(OpenAPI YAML\)](#)

① 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.

privacy.ca.gov/drop-for-data-brokers/technical-specifications/

What the documentation covers

01



Getting Started

Account setup,
authentication,
API key generation,
quick start

02



Integration Workflow

Download → process
→ upload cycle +
validation, retries

03



Working with the Data

List types, file
schemas,
standardization,
hashing

04



API Operations

Endpoints, request
examples,
error handling, rate
limits

05



Reference

Glossary, status codes,
file naming, support

Setup and authentication (if you elect to use API)

Prepare your:



DROP account setup

Complete registration (when applicable) and pay required fees



API key (if using)

Generated in DROP account after selecting consumer deletion lists.



HTTPS client

GET + POST over TLS 1.2+ (curl, PowerShell, any HTTP library)



CSV handling

Read and write CSVs, maintain naming convention (recommended)



Secret storage

Env variable or secrets manager for your API key



Logging

Log request timestamps and upload/download outcomes

Authentication

All API requests require an API key in the X-API-KEY header:

```
X-API-KEY: your-api-key-here
```

Environments

Production

<https://api.drop.privacy.ca.gov>

Sandbox

<https://api.drop.privacy.ca.gov/sandbox>

Regenerate your key if compromised or if list selection changes.

Consumer deletion lists: file naming + schema details



Downloaded CSV files follow a standard naming convention.

If you upload multiple response files for the same downloaded list, add a suffix to the file name using an underscore followed by up to 10 alphanumeric characters.

`<YYYYMMDD>_<DataBrokerId>_<DataType>[=<OptionalSuffix>].csv`

Example file names:

20260312_4821_NDZ.csv
20260312_4821_Email.csv
20260312_4821_Email_part01.csv
20260312_4821_NameVIN.csv
20260312_4821_Removed.csv

Consumer deletion lists: what's inside

20260312_4821_NDZ.csv

Id	Hash
7fa12c9d44	k92n4F1bq7dH1pNwV2sBf8G5xT0yR3uPoq1Zc7Qk2nE=
c28f9b11de	Abc19XyZpQfL0mTn3oR9sW2vH4kJ8dS6tUeP1rA0lCg=
9eab42cf10	zL8r1PwQh7NfE2tSd5uBv3kJy9mXc0aR4oTg6hQpLsY=
e2f17cd9a0	B7dP4m2KsZ1cUv9lHt3Qw8rAe6oF0gYxNqW5sJlCv8=

20260312_4821_Removed.csv

Id	Hash	List Type
f2c784b1493	Yt9Qk5uPj3vF8rLm0aB2wXyC7dS6eT1oHn4cR9lZs0E=	NDZ
1bb0e8f227d	Qx1nVf8yT0zKp3cLr9bH2mS4uD6eJ7aW5tP0oF1gNqU=	Phone

Code	Hash Type	Identifier(s)
NDZ	Composite	First Name + Last Name + Date of Birth + ZIP
Email	Single-field	Email address
Phone	Single-field	Phone number
MAID	Single-field	Mobile Advertising ID
NameVIN	Composite	First Name + Last Name + VIN
CTVID	Single-field	Connected TV identifier

How DROP handles combinations for composite hashes

Consumer provided			
First Name	Last Name	DOB	ZIP
Jane	Doe	7/22/1990	94103-3857
Jane-Ann	Doe		92101

DROP combinations	
1.	hash(jane) + hash(doe) + hash(19900722) + hash(94103)
2.	hash(janeann) + hash(doe) + hash(19900722) + hash(94103)
3.	hash(jane) + hash(doe) + hash(19900722) + hash(92101)
4.	hash(janeann) + hash(doe) + hash(19900722) + hash(92101)

Standardization and hashing examples



Composite lists (NDZ, NameVIN): hash each field individually → concatenate hashes → hash again. Output is Base64

Examples

	Raw input	Standardize	Hash SHA-2 6 → Base6 (-characters)
Single-field hash (email)	Jane.Doe@Email.com	→ jane.doe@email.com	→ KA18MT/ph6IHjzT9zwETySDQyvSh87YuoSBpOQtkhE=

	Raw input	Standardize	Hash SHA-2 6 → Base6 (-characters)
Composite hash (NDZ)	First Name: Jane	→ jane	→ gfj23eiDZfOSh5bseqU/colLBtuGZPX+dqfrE+JFRql=
	Last Name: Doe	→ doe	→ eZ75KhGvkY4/t0HfQpNPO1aO0tk6wd908bjUGieTKm8=
	DOB: 7/22/1990	→ 19900722	→ 0oJHwSqomfyhaatmj6yKGJfv+q7SrChsjxL7siNkmM4=
	ZIP: 94103-3857	→ 94103	→ kdwlGeqYxQAs8gkeahK3cur9zp3KYY5ibX07gnU2F4k=
	Concatenate hashes (First Name + Last Name + DOB + ZIP)		
	gfj23eiDZfOSh5bseqU/colLBtuGZPX+dqfrE+JFRql=eZ75KhGvkY4/t0HfQpNPO1aO0tk6wd908bjUGieTKm8=0oJHwSqomfyhaatmj6yKGJfv+q7SrChsjxL7siNkmM4=kdwlGeqYxQAs8gkeahK3cur9zp3KYY5ibX07gnU2F4k=		→ X7qUgPCyldidyYW0lpVyXUQ1nfrZdsb3LDH02zC0rfQ=

Status codes and API operations

2 Exempted

Match found; all personal information exempt

3 Deleted

Match found; non-exempt personal information deleted

4 Opted out

Multiple consumers linked to the same identifier; all opted out of sale/sharing

5 Not found

No match found after completing the matching process

API endpoints

GET

/data/download

Request current ZIP archive. Returns ZIP if ready, or JSON to retry later.

POST

/data/upload

Upload new status response files. Returns accepted/rejected JSON.

POST

/data/amend

Correct or update previously submitted status responses.

Key retry rules

429 Too Many Requests → wait 30s · 202 Preparing → call GET /data/download again · 409 Conflict → no outstanding records; download new batch

Upload validation: file level and record level

DROP validates every upload (API or Manual) in two stages. File-level errors block the upload immediately.

FILE-LEVEL VALIDATION

API key

Must be present and valid (if uploading via API)

File type

Only CSV files accepted

CSV header

Must be exactly: Id,Status

File name

No duplicate names within the same batch

Encoding

File must be readable as UTF-8



API or UI immediately returns a message with files accepted or rejected for processing

RECORD-LEVEL VALIDATION

ID present

Each row must include a work item ID

ID valid

ID must match a record previously delivered

Status code

Must be 2, 3, 4, or 5

No duplicates

Each ID may appear only once per upload



Email sent to primary and secondary contacts with processing outcome, including any errors that need to be corrected

Download behavior: cycle 1 vs. cycle 2+

CYCLE 1 — First download

Full list contents

Every identifier from every consumer who has submitted a DROP request for your selected list types. Provided as ZIP file.

One CSV per list

e.g. 20260801_4821_Email.csv, 20260801_4821_NDZ.csv

CYCLE 2+ — Incremental

New identifiers only

Only consumers who submitted requests since your last download — not the full list again.

Removed file may appear

20260914_4821_Removed.csv — identifiers to remove from suppression list. No response required.

Empty CSVs still included

A list CSV with headers only means no new requests for that list type. No response required.

Processing times

Time to download may vary based on batch size. File sizes expected to be larger for initial download. Plan accordingly.

Correcting submissions: the amend workflow

Use *amend* when you need to correct a status you submitted already, in your current or previous batch. Same file format as *upload* — different intent.

When to use /upload vs /amend



POST /data/upload — New responses

Use for: records from the current download batch that have not been submitted yet.

You may upload in parts — submit remaining records later with a suffix on the filename.



POST /data/amend — Corrections

Use for: correcting a status you already submitted — e.g. you reported Status 5 (not found) but later discovered a match and need to update to Status 3 (deleted).

How amend works

1

Create correction CSV

Same format: Id,Status. Include only the records you are correcting — not the full batch.

2

POST to /data/amend

Same request structure as /data/upload. Field name: files. One or more CSVs per call. You may also upload manually using the Amend button.

3

Await email confirmation

Amend submissions go through the same record-level validation. Errors trigger the same email notification flow.

4

No deadline reset

Amending a record does not restart the 45-day clock. Maintain your processing schedule.

Troubleshooting potential issues

Examples of potential integration and/or operational issues.

403 Forbidden

Potential causes: Registration incomplete and/or required fees unpaid · No consumer deletion list(s) selected · Account not in eligible status

Action: Log in to the Data Broker Portal → confirm account status.

409 Conflict on download

Potential causes: You have outstanding unsubmitted records from the previous download · You already uploaded responses for all records in the current batch

Action: Upload responses for all records in the current batch first. Then call GET /data/download to receive the next incremental batch.

202 on download attempt

Potential causes: ZIP is still being prepared by DROP · High-volume processing period — system is still generating the file for download

Action: Wait and retry. 202 means your request was received and the download is being prepared.

Hashes not matching

Potential causes: Standardization implemented incorrectly · Wrong encoding (not UTF-8) ·

Action: Test in sandbox with the synthetic dataset. Verify your output. Check standardization order: normalize → encode UTF-8 → SHA-256 → Base64.

Upload accepted but no email

Potential causes: Record-level processing still queued · Email address on account is incorrect · Accepted ≠ processed — validation continues asynchronously

Action: Wait for async processing to complete. Confirm primary and secondary contact emails are correct.

Record-level error email

Potential causes: Invalid ID · Status code not 2, 3, 4, or 5 · Duplicate ID in the same upload

Action: Review the error details in the email. Address errors and try upload again.

Testing in the DROP Sandbox



Testing in the sandbox environment is optional.

Sandbox testing steps

- 1 Select consumer deletion list(s) and generate API key
- 2 Point integration to sandbox endpoint:
<https://api.drop.privacy.ca.gov/sandbox> (if using API)
- 3 Download the synthetic dataset
- 4 Download consumer deletion list(s)
- 5 Standardize and hash synthetic data
- 6 Match, process and upload response
- 7 Confirm match outcomes

The screenshot shows the DROP Sandbox Environment interface. On the left is a dark blue sidebar with the DROP logo and navigation links: Home, Registration, Payments, Sandbox Environment (highlighted), Technical Docs, and Exit DROP. The main content area is titled 'Standardization and hashing tool' and includes a description: 'This tool allows you to test your standardization and hashing. Type a value to generate standardized output and hash values. Composite values appear when all required fields are present.' Below this is a table with three columns: INPUT, NORMALIZED, and SHA-256 (BASE64). The table contains three rows of data for First name, Last name, and Email.

INPUT	NORMALIZED	SHA-256 (BASE64)
First name Mary	mary	aRV3G+HFqgyIaHC2LRsD1+r8Eh/qDcCl6o+
Last name Jones	jones	lwaYfWM+BaDSkxwhEIs36MeQVwB1rEFElQAx
Email hello@test.com	hello@test.com	BqQY9GehThYxoxexB1SKEDnSbxLqRTAasU52

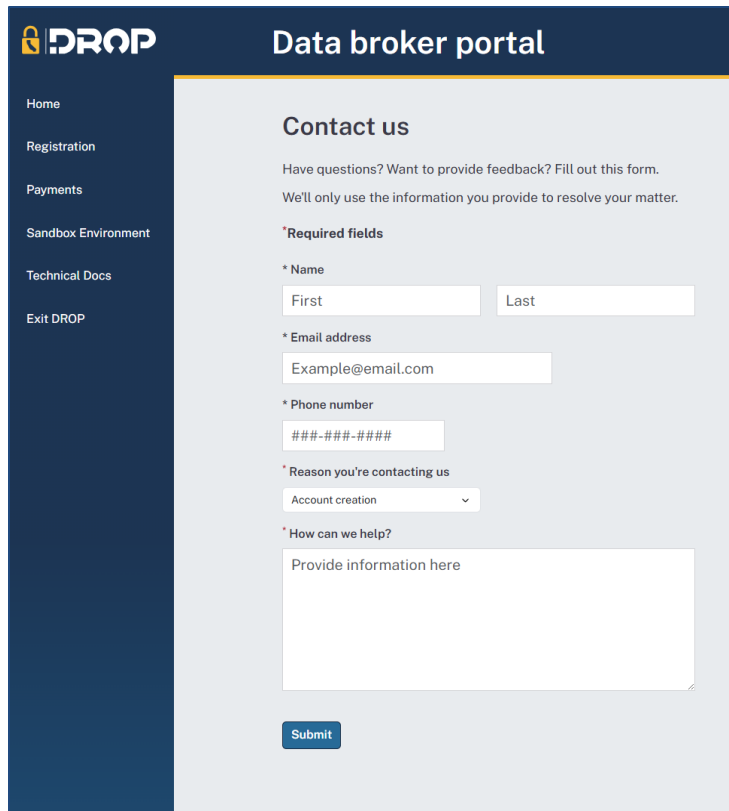
SECTION 05

Resources

Contact and support

- Automated connection failure: notify CalPrivacy in writing via DROP account within 45 days of last access
- Send us a message at any time using the contact form in your DROP account for technical issues or other account-related questions
- DROP Support Team is available to respond M-F 9am-5pm PT

If connection via API fails for any reason: Brokers must use the manual upload/download option — processing deadlines still apply.



The screenshot shows the 'Data broker portal' interface. On the left is a dark blue sidebar with a vertical list of links: Home, Registration, Payments, Sandbox Environment, Technical Docs, and Exit DROP. The main content area has a dark blue header with the DROP logo and the title 'Data broker portal'. Below the header, the section is titled 'Contact us'. It includes a brief instruction: 'Have questions? Want to provide feedback? Fill out this form. We'll only use the information you provide to resolve your matter.' The form contains several fields, each preceded by an asterisk indicating they are required: 'Name' (split into 'First' and 'Last' text boxes), 'Email address' (a single text box with 'Example@email.com' as a placeholder), 'Phone number' (a text box with a '###-###-####' placeholder), and 'Reason you're contacting us' (a dropdown menu currently showing 'Account creation'). There is also a 'How can we help?' section with a large text area labeled 'Provide information here'. A blue 'Submit' button is located at the bottom right of the form area.

Key Resources for Data Brokers



DROP Data Broker Site

General information about DROP

privacy.ca.gov/drop/data-brokers



DROP Sandbox

Test environment; synthetic data

api.drop.privacy.ca.gov/sandbox



DROP Data Broker Portal

Your account, list selection, API key generation

databroker.drop.privacy.ca.gov



California Data Broker Registry

List of registered data brokers

cppa.ca.gov/data_broker_registry/



Technical Documentation

Endpoints, schema, hashing rules, status codes

privacy.ca.gov/data-brokers



Contact / Support

Send us a message using the Contact form

databroker.drop.privacy.ca.gov/contact

SECTION 06

Q&A

Questions

We don't collect any of the identifiers in the 6 current lists. Which lists should we select?

What do consumers see? Do they understand the processing timelines?

How does a consumer cancel their request? What happens?

Are all deletion requests from consumers coming through DROP now?

Can we download previous batches of requests?

Do IDs per identifier map across lists?

This information is provided for guidance only. You are responsible for ensuring your own compliance and accuracy.

Thank You

Questions? Send us a message using the Contact Form in your DROP account.



DROP