California Consumer Privacy Act (CCPA)

Table of Contents

Acqueon – an Introduction

Acqueon's AI-driven conversational engagement software enables sales, marketing and service organizations to engage in meaningful, emotionally connected, open dialogs with customers that yield much greater results.

Your organization will maximize the potential of every conversation by utilizing next-best-action intelligence across every communication channel to increase sales, improve collections and rescue otherwise-defecting customers.

Acqueon's multichannel campaign orchestration and analytics solutions empower forward-thinking enterprises to shift from being reactive to becoming proactive in how they engage with customers. Acqueon is trusted by 100s of clients across the globe, including premier brands such as AIG, Cigna, Coca-Cola, Consumer Cellular, Costco and Roche.

Key Highlights

- 18 countries across 5 continents
- Over 50,000+ empowered customer service agents
- Trusted by over 200+ clients across 6 vertical lines-of-business
- Over 3.5 billion proactive interactions annually
- Triple digit YoY growth
- 40+ partners

What is CCPA?

California Consumer Privacy Act. The California constitution grants a right of privacy to every citizen residing in California. Existing law provides for the confidentiality of personal information in various contexts and requires a business or person (that suffers a breach of security of computerized data that includes personal information, as defined) to disclose that breach, as specified.

Beginning January 1, 2020, the law will grant citizens residing within California the right to request a business to disclose all personally identifiable information (PII) it has on them, the sources of that information, the business purpose for collecting and selling that information, and who it has been sold to and/or shared with. CCPA will impact all business sectors, and perhaps most notably, contact centers which collect data and interact with its customer base.

How does CCPA impact Enterprises?

Information that can be utilized or sold to identify a person, their place of residence or their personal choices are categorized as 'Personally Identifiable Information' (PII). All service providers to every enterprise must provide the enterprise with the ability to identify PII stored in the application database and provide it to the consumer when requested under the provision of CCPA.

Acqueon provides outbound dialing to enterprises through Acqueon Engagement, List and Campaign management and U-Nexsys. These applications require uploading phone numbers to the campaign management application. Phone numbers are classified as PII, therefore requests can be submitted by the consumer to disclose those details. In addition to the phone numbers, although not mandated by the application, an enterprise may also choose to upload other PII information such as first name, last name, address, zip code, account number, customer ID, email ID, etc. These details are stored under respective business fields.

All Acqueon's Compliance-Ready Solutions Will Support the CCPA effective January 1, 2020

Acqueon will provide redact APIs' for all its Campaign management solutions which will allow the enterprises to extract stored information and share with the end consumers. The API will return phone number, name, address, mobile number, email or any other identifiable information stored in the business fields and will return a list of all that match the search criteria. Search criterion can be a unique identifier such as an email ID or a phone number, and the returned list can contain zero records, a single record, or many records.

APIs' from Acqueon

Acqueon's software does not store any PII other than the phone numbers uploaded by the enterprise and any corresponding business fields in respective campaigns. Thus, the applicable regulations include:

- **Right to access**: A consumer should be able to request a copy of all data that the enterprise holds about the consumer. Acqueon Engagement will support the enterprise per a consumer's request for a copy of all data including:
  - Consumer PII that is stored in Acqueon database (such as phone number, first name, last name, email, etc.)
  - Export consumer information to a PDF or CSV file

- **Right to erasure**: A consumer should be able to request that all data the enterprise holds about the consumer be deleted. CCPA also enables enterprises to pseudonymize the data instead of deleting them. Acqueon Engagement will enable enterprises to:

    o Search and download consumer PII that is stored in Acqueon database (such as phone number, first name, last name etc.)
    o Single click ability to pseudonymize PII for search criterion

Acqueon will make redact APIs' available for both stipulations, which can be consumed by enterprises to extract a list of details corresponding to a unique identifier. This list can further be exported and sent to the requesting consumer.

Deployment Process

Acqueon will offer its CCPA solution in a phased approach:

In Phase 1, to comply with 'Right to access', Acqueon will develop new APIs' to display PII residing in Acqueon Engagement databases against a unique identifier (phone number or email ID) and release this API for use by the enterprise.

Acqueon will also offer a simple GUI within the application that will enable enterprises to extract all information against the provided identifier and export it as a PDF or CSV file to be shared with the consumer.

Similarly, in Phase 1, to comply with 'Right to erasure', Acqueon will develop a new redact API that allows the enterprise to pseudonymize all consumer PII. Acqueon will also offer a GUI navigation within Acqueon Engagement that authorized personnel can use to pseudonymize PII for requesting consumers as required.

Acqueon will offer the ability to manage the new CCPA-relevant GUI available within the product by roles, and only designated personnel will be granted access or allowed to make changes.

In Phase 2, Acqueon will offer CCPA-specific agent desktop widgets that will enable enterprises to record and submit consumer requests, set periodic reminders to act on the submitted requests and ability to access the CCPA APIs' from external systems such as Salesforce, ServiceNow, etc.

Consumer Request Ingress Points

Under CCPA, enterprises must provide at least two ingress points to consumers to submit their requests – one of the channels must be a toll-free number and the other can be a website, an email ID, or anything else that the enterprise deems fit. Once a request is placed, the enterprise must establish the consumer's credentials and confirm consumer identity. Enterprises will have up to 45 days to respond to a consumer's query from the day it was submitted by the consumer. The enterprise must conclude all the above steps independently and must discuss with internal Process and Information teams to setup the right process.

Later, during Phase 2, a CCPA-specific desktop widget will enable enterprises to capture requests received during an inbound call, or as part of an outbound campaign, to be submitted (processed) by the agent within the agent desktop. This will then trigger an email to respective stakeholders to take a specific action. Periodic reminders will also be sent to remind the stakeholders of any pending action(s). This new widget will also be able to be turned off for campaigns that target consumers outside of California.

Affected Products

1. **Acqueon Engagement**: These APIs' will be released as software patches and will be available post release. Acqueon will provide pre-release notification before GA release.
2. **LCM**: Acqueon Engagement APIs' will be assessable in LCM as is and will be made available for enterprise usage.
3. **Unexsys**: These APIs' will be available for Unexsys, too; however, all Unexsys customers must upgrade to the latest version of Unexsys (Version 4.2) to be able to utilize these APIs'.

API – Expected delivery

This is part of Acqueon's Q3 (FY 19-20 Oct – Dec) product roadmap. First phase of the APIs' will be available before the last week of Dec, to enable enterprises to be able to deploy it before January 1, when the new law goes into effect.

Work on phase II will begin in Q4 (FY 19-20 Jan – Mar) and will be made available to enterprises as part of regular product patch releases before end of Q4 (March 2020).

Addl. Consumer Responsibilities

To stay compliant with CCPA, enterprises must also take into consideration the following:

1. **Purging data** – CCPA allows consumers to request information predating up to 1 year. Therefore, no database (including Acqueon Engagement) can be purged to remove these details for the period of 12 months.

2. **Right to opt-out** – If a consumer requests data deletion, but doesn't exercise the right to opt out, that customer record can be uploaded to Acqueon Engagement again as a new contact and can be contacted (dialed out). If the consumer has requested for opt out as well, enterprise must externally scrub their contact list(s) outside of Acqueon Engagement to remove such contacts.

3. **Right to portability** – CCPA allows consumers to submit requests to move data from one data center to another. Such requests can be turned down by enterprises under the following conditions:

   a. Request being unreasonable and overly complex

   b. Request being expensive to execute while having adequate security in place to safeguard data

   c. Absence of infrastructure in the requested location

   d. Request cannot be addressed due to legally binding circumstances such as ongoing criminal cases

4. Enterprises can also inform the consumer of any nominal fee that it will charge if the enterprise is willing to undertake such a task under Right to portability.

5. **Prior consent of minors** – Enterprises must scrub/validate their contact list externally outside of Acqueon Engagement to ensure the contact list doesn't contain phone numbers of minors under the age of 16, whose parents or legal guardians haven't provided written consent.

6. These clauses are not applicable if the phone number is collected and stored with the consumer's consent, such as due to medical/health insurance purposes.