

# osano





# Universal Consent: Building Beyond Cookie Consent

Tuesday, 26 March

10:00-11:00 PST

13:00-14:00 EST

18:00-19:00 CET



# Presented by



**Brian Herr**

Chief Product Officer

Osano



**Anna Covert**

Principal of Covert  
Communication / Forbes  
Author

# Agenda

- Poll
- The Transition to First- and Zero-Party Data
- What Is Universal Consent and How It Helps
- How Universal Consent Aligns Privacy and Marketing
- How to Operationalize Universal Consent
- Universal Consent Use Cases
- Q&A

## Poll

Which of these statements best reflects your organization's perspective on the transition away from third-party cookies and toward first- and zero-party data?

01

My organization uses third-party cookies, and we're seeking a way to regain access to consumer data with first- and zero-party data.

02

My organization already relies on first- and zero-party data, but we are not experts. We need to learn more and do better.

03

My organization is well prepared for the transition away from third-party cookies and toward first- and zero-party data.

04

My organization has not prepared for the transition away from third-party cookies and/or doesn't realize there's a need to do so.

05

I'm not familiar with how my organization manages consumer data collection; I'm just here to get informed.



## Why Universal Consent Matters for Both Marketing and Privacy

# The Transition From Third- to First-/Zero-Party Data

Before diving into universal consent, we need to understand:

- The transition from third-party data to first- and zero-party data.
- How marketing teams rely on consumer data of all categories.
- How universal consent aligns marketing and privacy.



## Quick Recap

# Third-, First-, and Zero-Party Data

### Third-Party Data

- Collected by another domain/server, such as an ad tech vendor
- Tracks user activity across participating websites
- Slowly being phased out by major browsers

### First-Party Data

- Collected by your server and systems from the user

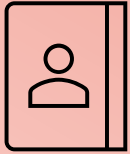
### Zero-Party Data

- Provided by the user directly (also known as solicited data)

# It All Comes Down to Trust

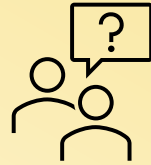
Is the data actionable? Can you trust the data? Do your consumers trust you with actionable data?

## Third-party data



- Third-party data is old and collected in ways that are **implied** vs **explicit**.
- This results in wasteful marketing spend.

## First-party data



- First-party data **infer** consumer intentions, preferences, and attitudes from their behaviours. But these inferences are not very accurate.
- Many of these opt-ins are also no longer allowed based on the new FCC ruling of 1-to-1 opt-in.

## Zero-party data



- Zero-party data is trustworthy because the individual has shared it with the company directly.
- Less overall data, but MUCH higher quality.
- Allows for personalization of messaging that the user wants.
- The data is accurate and actionable.



# Risks vs ~~Rewards~~

How to persuade your marketing teams on the value of consent.



## Risk 1: Sending Emails to Users Who Didn't Opt In

- Over 0.1% SPAM can damage your domain and block the ability to send emails to users who do consent to email marketing.
- **Reward for Keeping Clean Data:** Reduced costs for mail programs—i.e. MailChimp, Constant Contact, etc.



## Risk 2: Sending SMS to Users Who Didn't Opt In

- Over 0.1% blocked replies or bad numbers can result in flagging carriers placing a SPAM notice on business phone numbers and stopping all active text campaigns to users who do consent to text marketing reminders and offers.
- **Reward for Keeping Clean Data:** Reduced cost for SMS programs + higher delivery rate on all campaigns.



## Risk 3: Calling Customers Who Didn't Opt In

- Putting consumers on the DNC list incorrectly reduces ability to contact them from ANY channel in the future.
- **Reward for Keeping Clean Data:** Reduced air time and costs to use dialers & rotate numbers.

# Is Our Marketing Working?

- Businesses must answer fundamental questions as they relate to spend and results.
- Answering those questions requires consumer data.
- But the answers don't have to come at the cost of consumer data privacy—and will, in fact, be clearer when respecting consumer data privacy rights.

?

## Cost to Acquire and Keep Customers

Just because customers bought before, doesn't mean they will in the future. What can your business afford in terms of customer acquisition/retention costs?

?

## Attribution and Tracking

What marketing efforts were responsible? How many ads, emails, events, etc. were needed to move customers down the funnel?





?

## Efficacy and Waste Reduction

- Do different types of data (e.g. first-, zero-party) yield better results relative to others (e.g. third-party data).
- Does purging customer data (in accordance with the “right to be forgotten”) improve results and decrease cost?
- Is the critical mass of messaging frequency being achieved and delivered to the right audience in the purchase funnel?

# How Marketers Use Data Today

## Common ways marketing team use data to reach new users today

-  • **Look-A-Like Targeting** -> Using first-party data, marketers try and match users who behave similarly on their website.
  - Very hard to do, especially with multiple users on the same IP with different behaviors or devices.
  - Ineffective and cannot build up critical mass impression share.
-  • **Customer Match** -> Using second-party or first-party data, marketers try to match users' emails to enter them into a marketing pool, which is a pipedream at best.
-  • **List Acquisition** -> Purchasing data and then sending those users texts, email, or cold calling them.
  - Unwanted outreach that can permanently damage your brand.
  - Direct mail can also be utilized which is the least invasive but harder to track and expensive with printing, sorting and mailing fees making it ineffective (around 0.5% conversion rate with 3x mail to the same user).
-  • **Programmatic & AI** -> Effective to increase reach and scale new users based on contextual browsing and other signals.
  - The goal should be to generate real traffic and then remarket to the users who opt into messaging using full-funnel remarketing.

# Third-Party Cookies Are Falling Out of Favor...

## ... But a Major Challenge Remains

- Existing consent management platforms are well designed for capturing cookie consent.
- First- and zero-party data can be collected via cookies as well as many other mechanisms.
- Not all consent management solutions are currently equipped to collect, store, and manage consent for personal data processing across different systems and devices.

### Third-party transfers via CDP

- The CCPA/CPRA requires you to provide users with the option of opting out of the sale or share of their personal data, with all transfers ceasing within 15 days of request receipt.
- If a user submits a Do-Not-Sell request, how do you stop your CDP from transferring their data automatically?

### Communication consent & preferences

- A user may signal their consent to be contacted via email, for certain types of content, and/or at a certain frequency
- How do you operationalize those communication preferences?
- How do you coordinate preferences across email clients (e.g., MailChimp + HubSpot)?

### Consent across channels, systems, & devices

- If a user consents or does not consent to certain types of data collection, how do you retain those consent preferences across devices and experiences?



# Why Does This Matter?

## Poor User Experience

- With all these different points of personal data collection throughout the customer journey, it's easy to ask for redundant consent or to miss key moments.

## Non-Compliance

- The more points of consent collection, the easier it is to make a mistake that could put you out of compliance with the GDPR, CAN-SPAM Act, CPRA, and others.
- This especially true if you operate across jurisdictions.

## Tangled Audit Trail

- If you ever need to answer a question about user consent or demonstrate compliance, it gets difficult to track down consent records across all systems and interactions

## Technical Complexity

- Securing and storing consent from all of these different possible systems and interactions requires a technical solution.
- An inefficient approach would involve a bespoke solution for each channel and interaction.

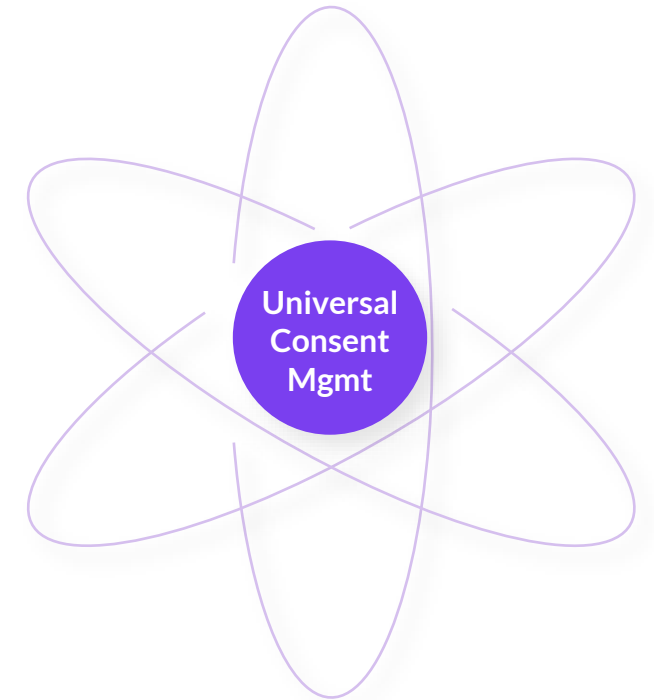
# Enter Universal Consent

## Universal consent systems:

- Serve as a way to operationalize consent collection across devices and experiences.
- Act as a unified system of record.
- Enable organizations to:
  - Comply with regulations like the GDPR, CAN-SPAM Act, and others.
  - Prove customer interactions.
  - Simplify the implementation and management of consent collection.

## Universal consent is different from cookie consent. It can be used for:

- Non-cookie-based targeted advertising.
- Internet of Things (IoT) device data collection.
- Consent to be texted, called, emailed, or otherwise communicated with.
- Consent to terms of service or other legally binding documents.
- Opting into or out of the use of sensitive data.
- And more.



# How Does Universal Consent Address These Challenges?

## Consistent User Experience

- Consent preferences can be remembered across systems, devices, and platforms.
- Users can set consent preferences in a centralized hub.

## Compliance

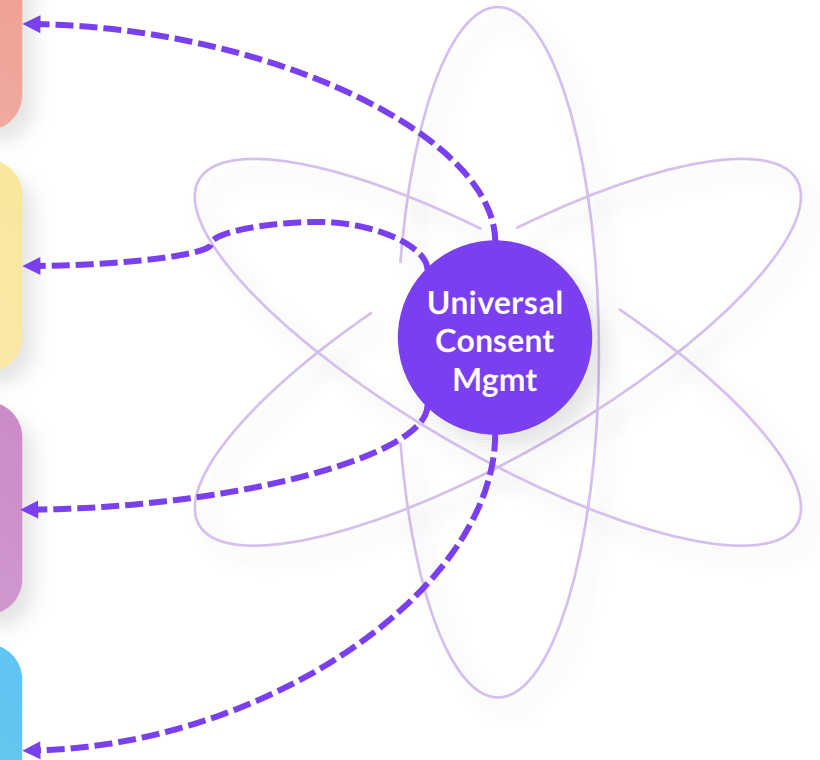
- Consent can be managed for devices, experiences, etc. across jurisdictions.
- Centralized consent management minimizes the chances of human or technical errors.

## Clear Audit Trail

- Universal consent solutions provide a reliable system of record for any inquiries you need to make into individual data subjects' consent preferences or your organization's overall consent management history.

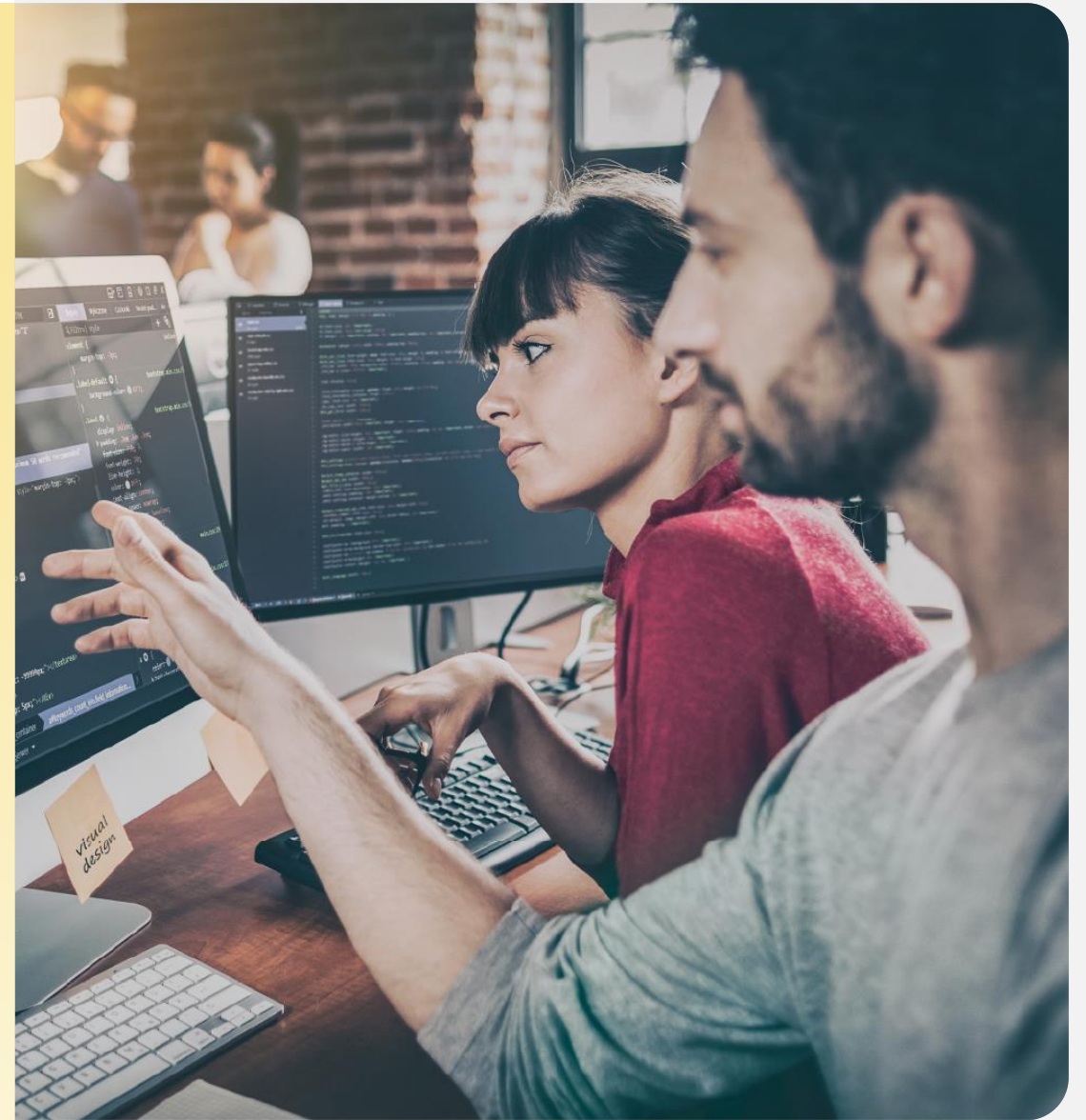
## Simplified Technical Mgmt

- Universal consent solutions simplify implementation and maintenance of consent collection mechanisms.
- Enable you to update consent configurations in one place rather than many when regulations require change.



## How Universal Consent Aligns Privacy and Marketing

- Privacy pros want compliant, ethical treatment of consumer data; marketers want actionable data to inform their efforts.
- Both parties can have their cake and eat it too through universal consent.
- Universal consent helps businesses keep consumers informed and in control, while ensuring that marketers gain access to clean data from the audience cohort most likely to engage.





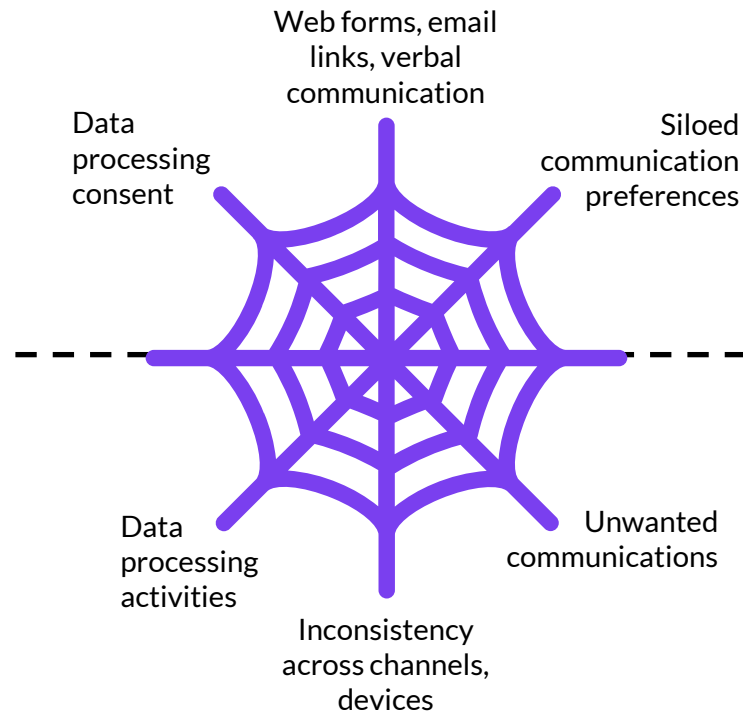
# Operationalizing Universal Consent

## How Do You Actually Make UC Work?



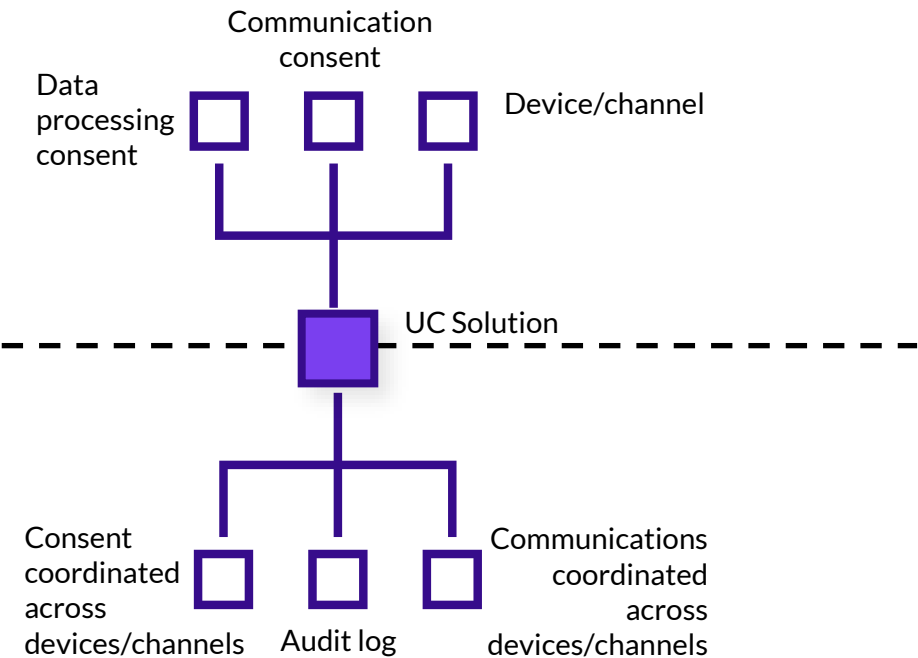
### Homegrown

- Many-to-many



### With a Dedicated UC Solution

- Many-to-one; one-to-many



# Operationalizing Universal Consent

## How Do You Actually Make UC Work?



### Homegrown



- Fully customizable to unique and/or niche tech stacks and systems.
- Feasible for organizations with very simple tech stacks/systems who do not anticipate future changes.



- Labor intensive and expensive in terms of implementation and maintenance.
- Requires regulatory expertise.
- Easy to make mistakes and increases risk exposure.



### With a Dedicated UC Solution

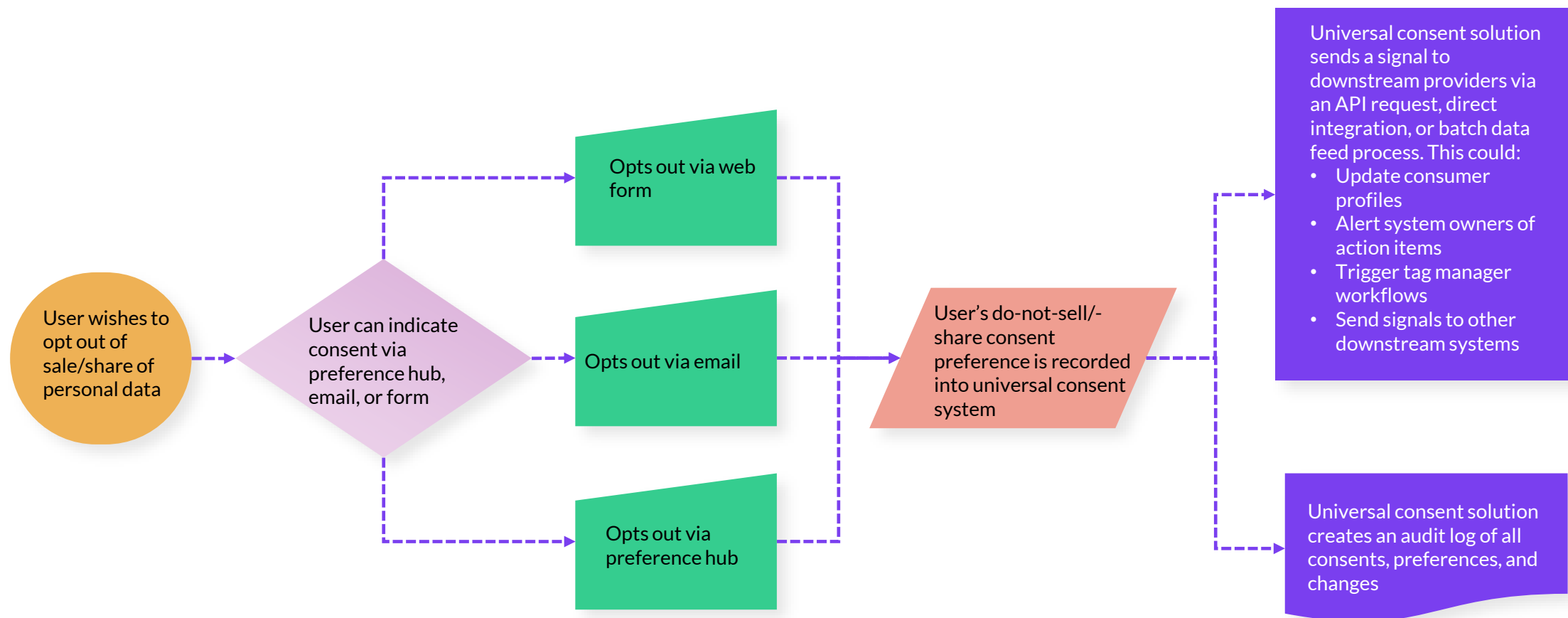


- Easier and ultimately cheaper than building in-house (depending on selected solution).
- Reduces risk exposure.
- Easy to scale.

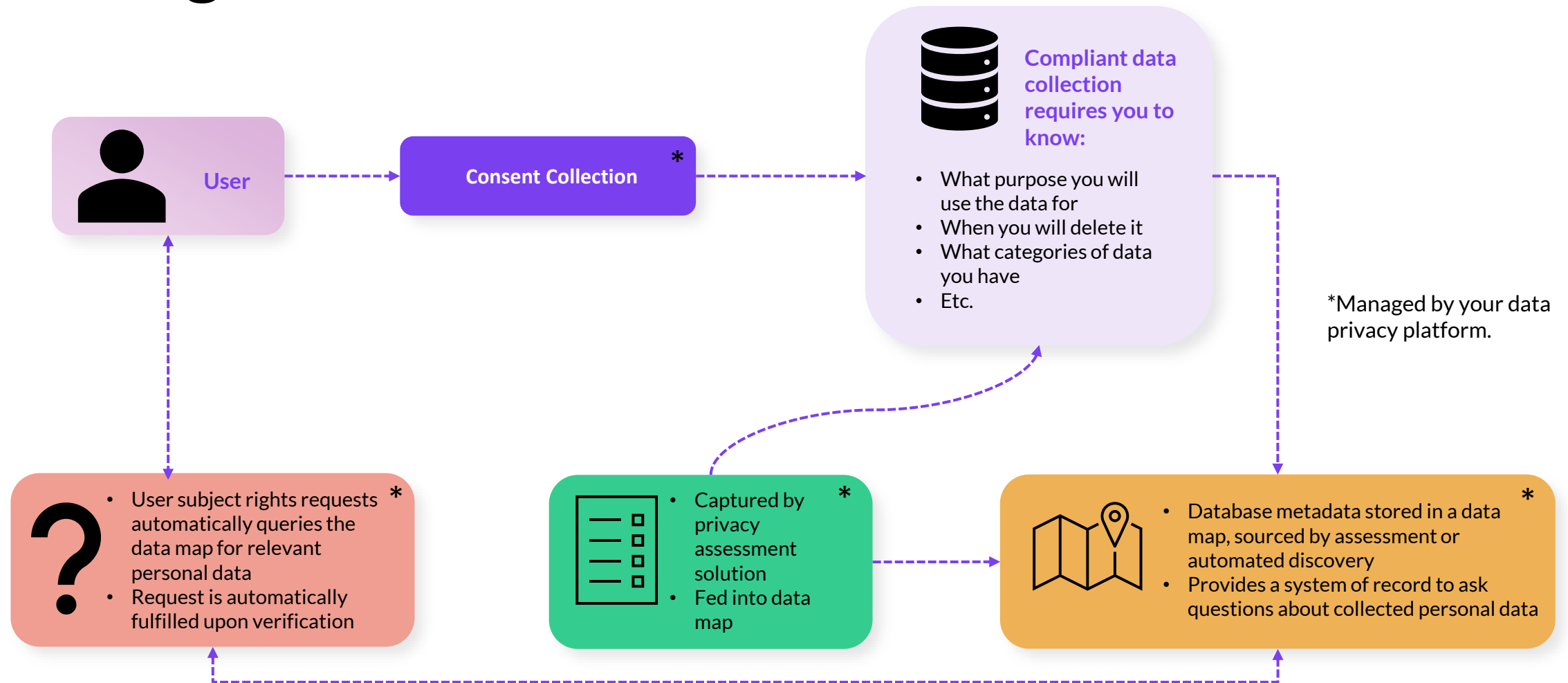


- May face internal resistance due to perceived cost.
- Lack of control over the solution's design/capabilities.

# Universal Consent Use Case: Do Not Sell/Share

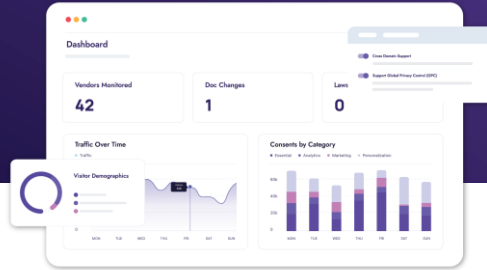


# How Universal Consent Fits Into Your Privacy Program





# Stay In Touch and Learn More!



[Schedule a Demo!](#)



[Check out the Osano Blog](#)



Pre-order *The Covert Code* at  
[theconvercode.com](https://theconvercode.com)



# Q&A

Ask your most pressing universal consent questions.



# Thank You!

A collection of decorative geometric shapes in the bottom-left corner, including a large pink-to-orange gradient arc, a white hexagon outline, and several smaller orange, purple, and pink circles and polygons.

**osano**

# 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 to take the survey](#)

Thank you in advance!

For more information: [www.iapp.org](http://www.iapp.org)



### **Attention IAPP Certified Privacy Professionals:**

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your 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 will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting 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  
or to obtain a copy of the slide presentation please  
contact:

[livewebconteam@iapp.org](mailto:livewebconteam@iapp.org)