2021

MARKETERS GUIDE TO DATA PRIVACY

10 ACTIONABLE STEPS FOR MARKETERS TO DEVELOP A PRIVACY STRATEGY NOW

Adzapier

Marketers Guide to Data Privacy

Most marketers understand the value of actionable data. It helps us reach the right customers at the right time, measure the effectiveness of our efforts using analytics, and develop targeting and propensity models. With data, we can reach better quality prospects and leads, offer them a personalized experience at the right time, and with the right offer; all within our marketing budget.

There are 2 major shifts that will affect data-driven marketing practices:

- The eventual end of 3rd party cookies.
- Data privacy regulations.

Now and in the future, any organization that tracks user behaviors for analytics, advertising, subscriptions, or for any other reason, will need consent. Some companies have already incurred fines for contacting data subjects without their consent. With more privacy regulations on the horizon, the challenge of tracking consent and other privacy rights will only become increasingly difficult. Consent records are becoming increasingly more important for businesses to show a track record of consent if, or when, audited.

Here are 10 actionable steps to develop your privacy strategy now:

1. Assign internal ownership of data privacy strategy.

Is it the job of IT Department, Marketing Department, Legal or Operations? With such new concepts of data privacy and regulations, it's no wonder that most organizations have not considered who should bear the responsibility, and why most organizations have not already implemented a data privacy standard and practice.

Many marketers will start the conversations and will feel the effects first, as their ability to use data to offer personalized experiences for their customers will become increasingly difficult. Marketers who make it a priority now will have an advantage leading to 2023 and before more state or federal mandates affect your privacy strategy. Since marketers use data insights and analytics to target their marketing initiatives and demographics, we are starting here.

Marketers often speak on using actionable data and metrics to improve consumer engagement, customer acquisition, and of course, return on investment. But how is that data collected, consented, stored, and managed? In this endeavor, we propose the marketing department assume responsibility for the data that they collect.

2. Determine what laws apply to you.

New privacy regulations continue to develop across the world. GDPR (General Data Protection Regulation) in the EU, which by some standards is considered the most stringent regulation with privacy by design and by default. GDPR requires a prompt to ask users for consent before collecting any online audience members data.

In comparison, California's CCPA is all about privacy via transparency. CCPA does not require websites to prompt for consent first, but users must be presented with transparent and effortless ways to opt-in or opt-out.

With both CCPA & GDPR, brands are required to honor and manage data subject access requests (DSAR) and give people a straightforward way to request information being collected and stored about them, where the data is stored, how that data is being used, and who its shared with or sold to. Data requests may include updating incorrect data, availability to delete user data, or the access to opt-out of future data collection, the option to "be forgotten" and request their data be deleted from all systems and the vendors whom the site owner shares data with.

Start by asking the following questions. Where are you based? Where are your website audience members based? Do you collect Personal identified Information (PII) from your users such as email addresses, IP addresses, phone numbers, etc.
Depending on location review the following privacy laws for compliance requirements:

- GDPR - Europe
- PIPEDA - Canada
- LGPD - Brazil
- CCPA and CPRA - California
- CoPA - Colorado
- VaCDPA – Virginia
- PDPA - Thailand
- PIPL - China

More regulations are getting passed around the world and consumers are expecting the organizations they work with to have safe and transparent data collection and usage. Plus, we predict it is just a matter of time until a Federal Data Privacy Act is passed in the United States. Because of this, we advocate for marketers to develop a privacy strategy now, regardless of where you and your consumers are located.

3. Update your privacy policy, terms and conditions and make it easy to create Data Subject Access Requests (DSAR's) on your website.

If you own a website or app, then you most likely are processing user data. You are processing user data if you use sign-up forms, newsletters, or third-party services such as Google Analytics, social media widgets, CRMs, or have login buttons... Even IP addresses are considered personal data!

A Privacy Policy is a statement or a legal document that states how a company or website collects, stores, processes, and maintains data of its online visitors.

If you have a website that involves client interaction to download a product, buy goods or services, communicate with other users, play a game, etc., then your homepage should include a link to your site's Terms of Service. This is contractual language that legally protects your company by notifying customers, clients, subscribers, or other users about the dos and don'ts of how they can utilize the site.

It is not a requirement of online privacy laws, but it's the best way to avoid risks and protect your site/ app (or e-commerce) from potential liabilities.

DSAR – With both CCPA & GDPR, brands are required to honor and manage data subject access requests (DSAR) and give people a straightforward way to request information being collected and stored about them, where the data is stored, how that data is being used, and who its shared with or sold to.

4. Know what cookies you have on your website and categorize them.

Marketers have become reliant on cookies to deliver personalized messaging to their audiences. As 3rd party cookies depreciate sometime in 2023, 1st party cookies will still have a significant role beyond 2023.

First-party cookies are directly created and managed by the organization that manages a website while 3rd party cookies are generated by other organizations (a 3rd party) different from the website owner/manager.

Both 1st party and 3rd party cookies help marketers keep track of user activity, preferences, and visits.

A few functions of cookies:

1. Session management. Cookies recognize users and store their individual login information and preferences, such as news versus fashion.
2. Personalization. Customized advertising is the predominate way cookies are used to personalize your sessions. As users surf their ways through the web, cookies use this data to help build personalized and targeted ads.
3. Tracking. Shopping sites use cookies to track items users previously viewed, allowing the sites to suggest other goods they might like and keep items in shopping carts while they continue shopping.
4. Analytics. Marketers use cookies to develop attribution and propensity models.

To ask for permission to use 1st or 3rd party cookies with website visitors, you need to know what cookies are on your website and be clear about what they are used for. You can create a list of all the cookies on your website and categorize them manually or use **Adzapier Free Cookie Scanner** technology to discover and categorize analytical, essential, functional, advertising, social, etc. cookies.

To be compliant with both GDPR or CCPA it is necessary that your Consent Management Platform (CMP) can block codes or offer cookie blocking if no consent or an opt-out is given. Organizations should know the difference and manage both implicant vs. explicit cookie consent.

For GDPR compliance, your cookie banner must be visible when users first enter your website and offer clear information- whether active consent, implied consent, or soft opt in- that if the user continues to use your website this constitutes active/implied consent.

5. Implement a cookie banner on your website(s).

Besides knowing what cookies are on your website before asking users for cookie consent, having a cookie banner makes it easy for them to know and understand which cookies you are asking consent for, what they are used for and what vendors you share that data with.

- GDPR requires that you collect users' informed consent before storing non-technical cookies (e.g., tracking cookies) on your users' device.
- CCPA requires you to make it easy for users to opt out or request “do not sell data”. A cookie banner makes it easy and transparent.
- If you are a publisher and have advertising on your website, you should choose a CMP that supports the IAB – TCF 2.0 framework .

6. Develop your first-party data strategy.

A first-party data strategy is the best way to counter third-party cookie depreciation.

Safari and Firefox have already stopped allowing 3rd party browser cookies. With 56% of browser market share, Google has announced they will be ending 3rd party cookies in 2023. This disruption will affect targeting, measurement, and attribution. Strategizing and implementing a comprehensive approach to privacy that follows the entire lifecycle of collecting, managing, and utilizing data and data requests is integral. It can help companies build their intelligence on behavior patterns among consumers who use their products or services.

To successfully collect first-party data, you must create a data transaction that provides value for the customer and ensures trust by communicating transparency of use and responsible data governance. To responsibly collect 1st party data, you must collect consent.

7. Know what vendors you share data with, and how you can distribute consumer opt-in and opt-out simultaneously to all your vendors.

Most marketers share data across their platforms and tech stacks. For example, email subscription management, CRMs, mar-tech, social platforms, programmatic ad platforms... It is important for marketers to know where their audience data is being stored, shared, and used. If a consumer opts out or opts in, that privacy choice needs to be passed down the line to the vendors you share data with.

8. Develop a DSAR strategy.

The Data Subject Access Request (DSAR) is a specific request that an individual consumer or online audience members may send to an organization whose data has been collected and/ or stored.

A survey from 2019 found 62% of London enterprises experienced a surge in DSARs over the first year of GDPR kicking in. Now new research claims substantial costs are involved to manage these requests. “Companies with more than 5,000 employees can spend as much as $2,136,065 on responding to data subject access requests”, according to research commissioned by Guardum, a data-security firm. “75% of data protection officers polled say they struggle to meet data compliance obligations whilst working remotely” Guardum continued.

Matt Lock of Varonis says fake DSARs are a real problem as well now. More companies became aware of it after an Oxford-based researcher obtained a vast amount of personal information via impersonated DSAR requests for his fiancée last year (with her permission).

DSAR trends reflect that DSARs will be growing in 2022. The European Data Protection Board recently issued guidance that companies can expect a significant increase in DSAR over the next few years due to the increased awareness of the rights created by GDPR. Now is the time to create a strategic approach for DSAR requests in America.

DSAR workflows allow companies to manage the number of requests they receive, how they prioritize them and ensure that employees are clear on who is responsible for processing each request.

Fake data requests can quickly become a big problem. Why? Companies now must deal with these situations because of GDPR, which states that if a company doesn't verify the DSAR request is from the correct person, it's not allowed to comply. You must find the individual requesting the data and let them know that they're complying. If you don't, you can face a huge financial penalty.

DSAR forms help companies manage the number of requests they receive, how they prioritize them and ensure that employees are clear on who is responsible for processing each request. DSAR templates help companies ensure best practices are being taken so that each request is dealt with correctly.

Finally, DSAR automation tools help website owners by eliminating manual efforts that can easily be done by bots. Make sure you train your employees on best practices when it comes to data subject access requests. A CMP helps to manage DSAR timelines by automating the process as much as possible.

Companies need to be able to manage their DSARs not only from a volume perspective but also from a risk perspective.

Therefore, it's important to have the right tools in place that can help you manage your company's DSARs.

9. Develop a Consent Preference Management strategy with a single point of truth.

As you collect user consent and their consent preferences, it's important to keep detailed records along with all the data around those consent preferences. For example, complete and detailed records of consent preferences associated with each consent agreement, consent revocation, or consent withdrawal.

Your consent preference management solution should maintain a single version of truth for all individual consent preferences within your company – the ultimate source of truth for consent preference data. For example, you must keep track of every piece of personal data that you process under each consent agreement as well as what third parties you share it with and how long you store it for. In addition, if the record shows that an end-user changes their mind about sharing this information after agreeing to it at some point in time, then there must be an easy process and way to un-share the data with vendors.

10. Implement a CDP and other tech depending on your needs.

Customer Data Platforms or Customer Intelligence Platforms allow marketers to collect, unify and analyze customer data. CDPs allow companies to turn customer data into a 360-degree view of each individual customer to make better business decisions.

CDPs with consented data generally offer at least four benefits:
1) Helps give marketers an understanding of what is working well and not working in terms of marketing efforts by allowing them to track and compare everything they do across all channels.
2) Enable much greater visibility into the customer journey.
3) Provide insights into both online and offline audiences.
4) Can be extended across other areas like loyalty or CRM programs that further enhance the CDP's data and insights.

CDPs not only enables marketers to gather customer data but also unify it across all channels, which is important since customers are no longer using one channel for brand interactions (i.e., email). Rather, they are using many channels (i.e., Facebook, SMS, Amazon, Foursquare, CVS). CDPs allow companies to aggregate information from all those sources into one place and then analyze that data.

The CDP has quickly become the latest buzzword in the industry with CMOs and CIOs alike scrambling to find a CDP for their business. Most recently, Forbes Magazine reported CDPs as a CMO Must-Have, and Gartner has named CDP as one of its Top 10 Strategic Technology Trends for 2022.

Action Plan

While it may be tempting to put off planning for data privacy, there are plenty of reasons why you should get started now. We've outlined 10 actionable steps that will help you develop your Data Privacy Strategy today. The sooner you act the faster and more efficiently you can ramp up your efforts in this area.

If all these step's sound like too much work or if they seem overwhelming, we offer a FREE consultation and product demo of how **Adzapier CMP** can help!

Our platform is designed to automate many aspects and best practices of data compliance so that organizations can focus on what matters most – their core business activities.

CLICK HERE

FOR A FREE CONSULTATION WITH AN PRIVACY EXPERT!

Relevant Content: