NP digital

The Data Breakdown for a GDPR & CCPA Conscious Brand

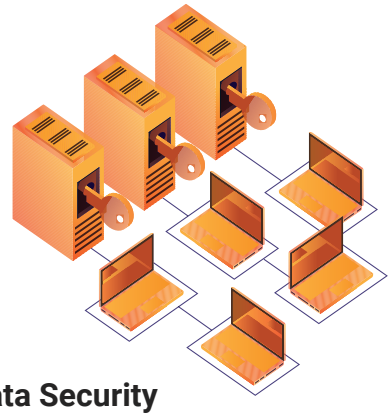
PRIVACY VS. SECURITY

Privacy vs. Security

Data Privacy and Data Security are often confused or used interchangeably. Although they are associated, they are not synonymous. For brands, it's essential to understand the difference.

Data Privacy

Data privacy is controlling the flow of one's personal information, and the right to control how that information is shared with others through digital channels.



Data Security

Data security is how that data is handled once collected, and what that brand does to protect that information.

GDPR SETTING THE PRECEDENCE

GDPR Setting the Precedence

The EU General Data Protection Regulation (GDPR) is legislation passed to grant users the transparency, access, rectification, and erasure of their own data profile. Passed in 2018, GDPR began the wave of legislation focused on data privacy and consumer protection, designed to harmonize data privacy laws across Europe and protect EU citizens from privacy and security breaches. By 2021, similar regulations are expected to be instated on the US Federal level.

ARE YOU COMPLIANT?

GDPR also applies to non-EU companies that offer goods or services or monitor an individual's behavior in the EU. Among other things, it requires increased transparency, access, rectification and erasure.

Failure to comply can cost companies up to 20 million Euros or 4% of their annual global revenue, whichever is greater.

CCPA & Brands

Companies that qualify within the below are required to provide California residents with access to the types & sources of personal information collected about them, specific pieces of personal information collected about them, access to the categories of personal information about them that has been sold or disclosed, types of entities with which the personal information was shared, and the ability to delete consumer's personal information and to opt out of future data sales and sharing.

CCPA applies to companies that meet one of the following requirements:

>$25 MILLION

Have annual gross revenue of more than $25M.

50,000 CALIFORNIANS

Have annually bought or received for commercial purposes personal information on at least 50,000 California residents.

50% REVENUE

Have derived 50% or more of their revenue from selling consumer information

IS YOUR BRAND PREPARED?

Are you GDPR compliant? Do you qualify for CCPA regulations? If it's yes to both, being GDPR compliant does not mean you're CCPA compliant. Blanketed regulations are coming, but it's best to get ahead of the game and ensure you're CCPA compliant, as well as GDPR.

Consumer Expectations

Ever-connected consumers now expect brands to know them across every touch point and to deliver relevant messaging along the way. Simultaneously, the majority of internet users worldwide say that they are concerned about their privacy. This may seem contradictory, but the transparency required by GDPR and CCPA can help brands find the balance of the two.

In fact, more than 70% of marketers say their investments are driven by customer expectations of more personalized and relevant brand interactions.

KEY IMPLICATIONS

Key Implications

The expansion of regulations and legislation surrounding American data policy have many implications for consumers. The key implications address the concerns and wishes of many consumers:

Monetary Fines

Monetary Fines for failing to comply, but also for data breaches and hacks. Data hygiene and security should be at the utmost forethought of marketers, not only how you're collecting and storing it, but what you're collecting.

Brand Sentiment & Trust Could Waver

According to cybersecurity firm Symantec, 83% of internet users polled worldwide said they were concerned about their privacy.

Personalized Messaging, Increased Engagement

Although the data collected may have fewer touch points, they're more valuable. This is leading to the ability to personalize your marketing to consumers, ultimately driving a higher brand engagement.

NP DIGITAL RECOMMENDATION

NP Digital Recommendations

1. **Don't bog consumers down with "legalese."**
2. **Put a consumer-first foundation down.**
3. **T&Cs should be in layman's terms, easy to navigate and digest.**
4. **What are you collecting? How are you using it? Are you sharing it?**

For marketers, ensuring you're GDPR compliant isn't enough. Put focus on less of a "legalese" catch all approach, and more of a consumer first foundation. Most consumers are confused on what they're agreeing to, and that's the exact opposite of the intention of these regulations. We anticipate a crack down on bogging down users with a very detailed "cover our butts" legal speak T&Cs when they are opting in, when these GDPR regulations make it to the US Federal level. Consider the consumer's point of view, and spell it out plainly what you're collecting, how you're using it, and who you are sharing that data with. It may ultimately drive a higher opt out rate at first, but that proprietary data will only get more relevant and smarter – doing more for your brand than the incomplete, broad, less relevant data profiles you have now.

This article was last updated in December of 2019.

NP digital