POSSIBLENOW™

Preferences, Consent, Insights, Compliance

TRUST
Be Human

ZERO-PARTY DATA, CONSENT, AND PRIVACY MANAGEMENT

By Jeff Jarvis, Senior Vice President of Strategy & Consulting

We empower the individual's voice, so trust is built, and relationships are enriched.

WHAT'S INSIDE

Introduction

In the past, corporate compliance was an effort to align with applicable laws and regulations. This effort was influenced by what the company sold, where they sold it, and the various uses of their goods after sale.

Today, in an increasingly digitized and virtualized global marketplace, other factors matter as much or more than the physical circumstances of the transaction. Chief among them is the person with whom the enterprise hopes to do business. In order to engage with this person and share information, enterprises must collect customer third-, first-, and zero-party data, store it, and utilize it to create meaningful interactions.

This process, essential to survival in an age of limitless virtualized information, is fraught with danger for enterprise corporations. Why? We entered an era of permission, privacy, and data protection, the emergence of the empowered consumer as an actor in what used to be an enterprise-only communications flow.

For evidence of this shift, consider the EU's recently implemented General Data Protection Regulation (GDPR) and its ePrivacy regulation to follow. This paper explores both measures, explains their impact on multinational enterprises affected by them and concludes with specific recommendations for compliance and consumer engagement in an environment of increasing regulation and consumer protection.

The Global Trend Towards Privacy and Data Protection Rights

In a 2017 PriceWaterhouseCoopers report, *Consumer Intelligence Series: Protect Me,* 87% of consumers say they'll take their business elsewhere if they don't trust how a company handles their data. Accordingly, a recent Accenture study of 25,000 global consumers found that when they decided to switch companies, 46% did so because they lost trust in the company.

The facts are evident: companies need an approach that builds customer trust, showing transparency while providing value to consumers. Trusting relationships require two-way communication, establishing a positive cycle of reciprocity. That leads to deep customer insights by allowing consumers to provide direct input about their preferences, consent, feedback, and insights.

In response to the current wave of consumer wariness, regulators and legislators around the globe are moving quickly to enhance privacy protections and address widespread consumer concerns about data and identity theft, unwanted engagement, and behavior tracking.

Here in the US, acceleration of this trend can be seen in the raft of guidelines implemented by states and standard-setting organizations. In 2016, the Office of the Attorney General for California established that companies doing business in California must, at a minimum, adopt 20 specific security controls established by the Center for Internet Security in order to demonstrate "reasonable" security practices. New York's first-in-the-nation cybersecurity regulations, just implemented in March 2017, requires banks and insurers to scrutinize security at third-party vendors that provide them goods and services.

At the federal level, the U.S. Department of Commerce issued a request for public comment on the benefits, challenges, and potential government roles for regulating the Internet of Things (IoT), the clearest signal to date that privacy rules will govern virtual assistants, exercise monitors, smarthome features and appliances, and more.

Worldwide, this trend is best evidenced in the EU rulemaking that forms the basis for this paper – GDPR and ePrivacy. What is critical for US enterprise business leaders to recognize is A) their almost certain vulnerability to these regulations and B) that GDPR and ePrivacy represent a long-term global trend that shows no signs of slowing, including in the United States.

> "What is critical for US enterprise business leaders to recognize is A) their almost certain vulnerability to these regulations and B) that GDPR and ePrivacy represent a long-term global trend that shows no signs of slowing, even in the United States."

The Current Wave: GDPR

The GDPR, an EU privacy and data protection measure, went into effect in May 2018 and sent companies around the world scrambling to comply. Adopted to strengthen data protection for individuals within EU countries, GDPR is designed to give people more control over their personal data, protect data from the risk of loss and unify regulatory privacy and data requirements within the EU.

Understanding GDPR begins with a very simple premise: it standardizes certain regulations across all member nations. That's a good thing given all the competing languages and rules that exist today. From there, it gets a little scarier for companies that need to comply. Central to the regulation is a high standard for consent and fines as great as 20 million euros or four percent of total worldwide annual revenue, whichever is larger.

> GDPR requires that:
> - All identifiable personal information, regardless of where it is used, must be protected and proof of protection must be verified.
> - Companies ensure that they have the right to communicate based on conditions such as:
>   - Performance of a contract with the data subject
>   - Maintaining compliance with a legal obligation
>   - Having a legitimate interest with the data subject
>   - Obtaining explicit consent from the data subject

The regulation goes so far as to state that the protection of personal data is a fundamental right of natural persons.

Moving forward, natural persons in the EU will also hold the "right to be forgotten." In certain circumstances, consumers will be able to request that companies destroy all records related to them. Having done so, the burden of proof will lie on the company in any instances where records must be stored or maintained to comply with other, superseding regulation.

In another fundamental shift, GDPR doesn't just limit the rights of companies. It empowers consumers to hold greater leverage against the companies that collect and use their personal data. GDPR will enable natural persons in the EU to request explanations from companies about the personal data they have, the uses they intend for it, how long they plan to keep it, and more.

Companies will face 30-day deadlines to comply with such requests and if they want to file an extension, they should be prepared to demonstrate very convincing reasons for needing more time.

To many marketers, these requirements seem to signal a swift end for their customer engagement initiatives. After all, marketers depend on technology and systems to anticipate customers' needs before they realize they have them, and where scrutiny on the return for the dollars marketers are spending is increasing.

On the Horizon: ePrivacy

Savvy EU data security and privacy wonks may be wondering how a legal framework that dates back to 2002 could be "on the horizon." That's because ePrivacy, the renowned "cookie law," is finally due for an overhaul.

As GDPR is now in effect, an ePrivacy update is inching closer to realization. EU residents and visitors will recognize the policy from its most visible effect: pop-up messages on websites asking for consent to collect cookies (thus the nickname). In reality, ePrivacy covers much more than just browsing data.

In its updated form, experts expect the new ePrivacy Regulation to complement and extend GDPR while cleaning up privacy and security policy discrepancies between EU member nations. Broadly speaking, the regulation will govern "electronic communications," an umbrella that covers the Internet, telephone, instant messaging, and much more. Given the breadth of its charter, the possible impacts on marketing and customer service communications are significant. Published as a proposal text in January 2017, the ePrivacy update includes a few critical changes:

Privacy: Online communications providers will be placed under the same requirements as traditional telecommunications providers. That means the Facebooks and Gmails of the world will have to enhance security and face an elevated threshold for customer data safety.

Cookies: Websites will be expected to obtain consent before cookies are placed on users' computers, and a separate consent is expected for each type of cookie. Website owners will need to be able to show consent was collected and will be accountable for managing consent for third-party tracking on their sites.

Consent: Prior consent to communicate will be broadened yet again, this time to each individual email or mobile account holder for texts or emails and there is no concept of legitimate interest. This change, along with strengthened penalties via GDPR, will make consent acquisition and management an essential capability for any company hoping to do business with EU citizens.

Finally, it's important to note a key difference in the implementation process: where the existing framework is a Directive, the update will be introduced as a Regulation. This means that once it is introduced, the ePrivacy update is self-executing and legally binding across the EU and to any party communicating with EU citizens, employees, vendors or partners.

Governing Engagement Through Privacy and Permission

To some, enhanced consumer protection rules are a bad thing that will hamper marketing efforts and lead to increased overhead, liability, and hassle. To others, it is merely further confirmation of a broad and positive trend towards opt-in relationships between companies and consumers.

Research overwhelmingly confirms that relationship marketing informed by explicit, self-reported consumer insights and zero-party data is exponentially more effective than the spray-and-pray model of the interruption marketing past. With that in mind, companies that have used regulatory changes as an opportunity to pivot towards interactive models of customer data management and persistent consent have not only enhanced risk mitigation but also increased marketing ROI.

By framing the consent and insights collection process as a progressive conversation, enterprises are better able to understand and plan for customer engagement in the era of GDPR and ePrivacy. Customers reveal zero-party data in iterative steps related to their evolving interest in what a business has to offer and their perception of what the business will do with the information that is disclosed.

> "Research demonstrates that customers are much more willing to provide zero-party data, including their feedback and insights, when the request is:
>
> A) Presented in context,
> B) Offers a clear benefit to them (i.e. protects privacy, saves time, saves money, etc.), and
> C) Is easy to understand and an easy task to complete."

In many ways, the collection of customer zero-party data (including their consent and myriad insights) lies at the intersection of a customer's interests and the interests of the company hoping to serve them. Seen in that context, it is clear that the interaction can be compromised when one party's interests outweigh the interests of the other party.

For example, a lengthy and complicated registration page can act as a barrier to a trial software download because the customer's interest in the product is not significant enough to justify the time required to fill out the form. The company over-emphasized its own interests at the expense of the customer and as a result, lost a valuable prospect.

When trust is not established slowly between the customer and the company, the customer is more likely to question how the information being collected about them will be used. In fact, according to recent research from Oracle Eloqua, mean conversion drops significantly when more than six fields are on a form.

It's also worth noting that customers view companies as one entity, not as individual business units or discrete functional groups (e.g. sales, customer support, and so forth). In order to maintain compliance and support customers' expectations, consent and insights collection should take place across the full spectrum of prospect and customer engagement. Enterprise-level businesses engage in complex interactions that include an expanding set of personal and virtual interactions. It's essential to collect and react to information from all touchpoints such as call centers, social media, and mobile devices, not just the easy or inexpensive ones (e.g. email or websites).

It is also imperative that once consent and zero-party data is collected at a given touchpoint that they are passed seamlessly across the organization. A customer dialing in to a call center will expect to have the ability to change their consent or insights information for all communication channels as part of that transaction. Enterprises should take advantage of every customer interaction to learn more about the customer in order to establish deeper relationships, understanding and ultimately better servicing their customers' needs.

Only by embracing a culture of thoughtful, progressive relationship-building will enterprises be able to engage in meaningful dialogue that is in alignment with GDPR and ePrivacy. The mere installation of consent or zero-party data collection without commensurate internal process and policy will simply result in delayed exposure to regulatory risk as consent expires, customer feedback changes, and new rules are implemented.

Best Practices for Customer Engagement Compliance

1. Ask for Less: Trusted customer relationships are established over time. As technology, social media, and other marketing tactics replace the traditional face-to-face relationship developed in a store, by a salesperson, or through a call center agent, it is important to determine the right moments within the customer journey to collect customer zero-party data, ask for consent to engage and use that personal information correctly once collected.

Structuring the ask from the customer's perspective, at moments that matter, improves the odds of receiving permission to collect, store and use customer data at a later time. The collection of self-reported zero-party data enables mutually beneficial engagement over the lifespan of the customer relationship. Asking the customer for their feedback, opinions, and insights is an essential key to maintaining permission. Identifying all potential customer data that will improve the customer relationship and breaking the collection up over time is an effective strategy. Resist the temptation to ask for as much as possible during an initial interaction.

A good rule of thumb – one that aligns compliance with customer experience – is to understand why you are asking for customer information in the first place. This simple exercise of identifying the why behind the collection assists in overall decision-making regarding the governance and logical right time to collect customer data.

2. Store in One Place: Marketing technologies have grown exponentially over the last five years. With the introduction of each new technology comes a separate ability to capture and store customer data – a potential compliance risk. Disparate data in siloed systems is one of the greatest risks to running an effective and compliant marketing infrastructure. The correct approach is one where data is stored and maintained in a distributed and centralized manner.

Only through a neutral, centralized, fully auditable system, a system that is built with compliance-by-design (not a bolted-on afterthought) can organizations ensure compliance to GDPR and future changes in compliance. GDPR and ePrivacy firmly place the responsibility on the party collecting customer data to understand and disclose how data will be used, how long it is needed, and provide an easy way to respond to customer inquiries. Not only that, the regulation requires alleged violators to deliver proof of consent within days of the inquiry – an impossible challenge for companies without a system of record to maintain enterprise-wide consent.

The marketing benefit of this centralization? Disparate knowledge collected about customers across the enterprise is brought together to provide a complete picture of the customer. This comprehensive picture of the customer leads to more effective and meaningful outreach, providing better customer experiences across the customer journey. The requirement for centralization stems the introduction of unapproved marketing technology by rogue marketing groups that ends up negatively impacting the marketing organization as a whole.

3. Use Judiciously: Implementing a governance structure that includes all individuals responsible for managing and using customer data for outbound communications was nice to have in a pre-GDPR environment. In a post-GDPR environment, it is a requirement.

Governance forces an across-organization view of all outbound engagement to a customer group and encourages communication within the company about strategies, tactics, and identification of overlap of use of customer data. This can only be achieved through a combination of technology and oversight.

The fewer times your organization reaches out to a customer, the more strategic those touches become. This enables a better understanding of the customer and helps mitigate the greatest source of GDPR risk – customer complaints.

4. Anticipate Change: Take advantage of built-in capabilities within marketing technology systems to anticipate customer concerns around use of data. Prepare for consent expiration, pay attention to customer engagement with outbound communications ,and make sure you are closely tracking negative marketing events such as unsubscribes. GDPR specifically protects consumers' right to revoke consent. Any delay in compliance with such a request or worse yet, continued engagement, will result in costly violations.

The proactive management of customer data is key to adhering to GDPR/ePrivacy requirements and ensures customers' feeling that they are receiving an ideal experience. Anticipating that a customer may unsubscribe by paying attention to the number of times they open (or don't open) a certain correspondence and proactively offering a digest or decrease in frequency is an effective approach. Pausing all customer engagement based on an event (visit to an unsubscribe page, completion of a purchase) is also an effective way to preserve the customer relationship and stem customer complaints.

Your organization should ensure that all departments have access to the latest and most up-to-date information about your customers. Enabling only the digital channels that are customer-facing but keeping your customer care or front line representatives in the dark regarding customer data and use of that data is a recipe for running afoul of GDPR and ePrivacy guidelines.

PossibleNOW's technology, processes, and services enable relevant, trusted, and compliant interactions between businesses and the people they serve. We gain customer insights through qualitative Voice-of-Customer research to understand the expectations and emotions influencing customer behavior. We leverage that understanding when deploying MyPreferences to collect and utilize zero-party data such as customer insights, preferences, and consent across the enterprise, resulting in highly relevant and personalized experiences.
DNCSolution addresses Do Not Contact regulations such as TCPA, CAN-SPAM and CASL, allowing companies to adhere to DNC requirements, backed by our 100% compliance guarantee.

PossibleNOW's strategic consultants take a holistic approach leveraging years of experience when creating strategic roadmaps, planning technology deployments, and designing customer interfaces.

PossibleNOW is purpose-built to help large, complex organizations improve customer experiences and loyalty while mitigating compliance risk.

CONTACT

Contact Us

(800) 585-4888 or (770) 255-1020

email | info@possiblenow.com

visit | www.possiblenow.com