Grazitti Interactive®
Marketing for Digital Natives

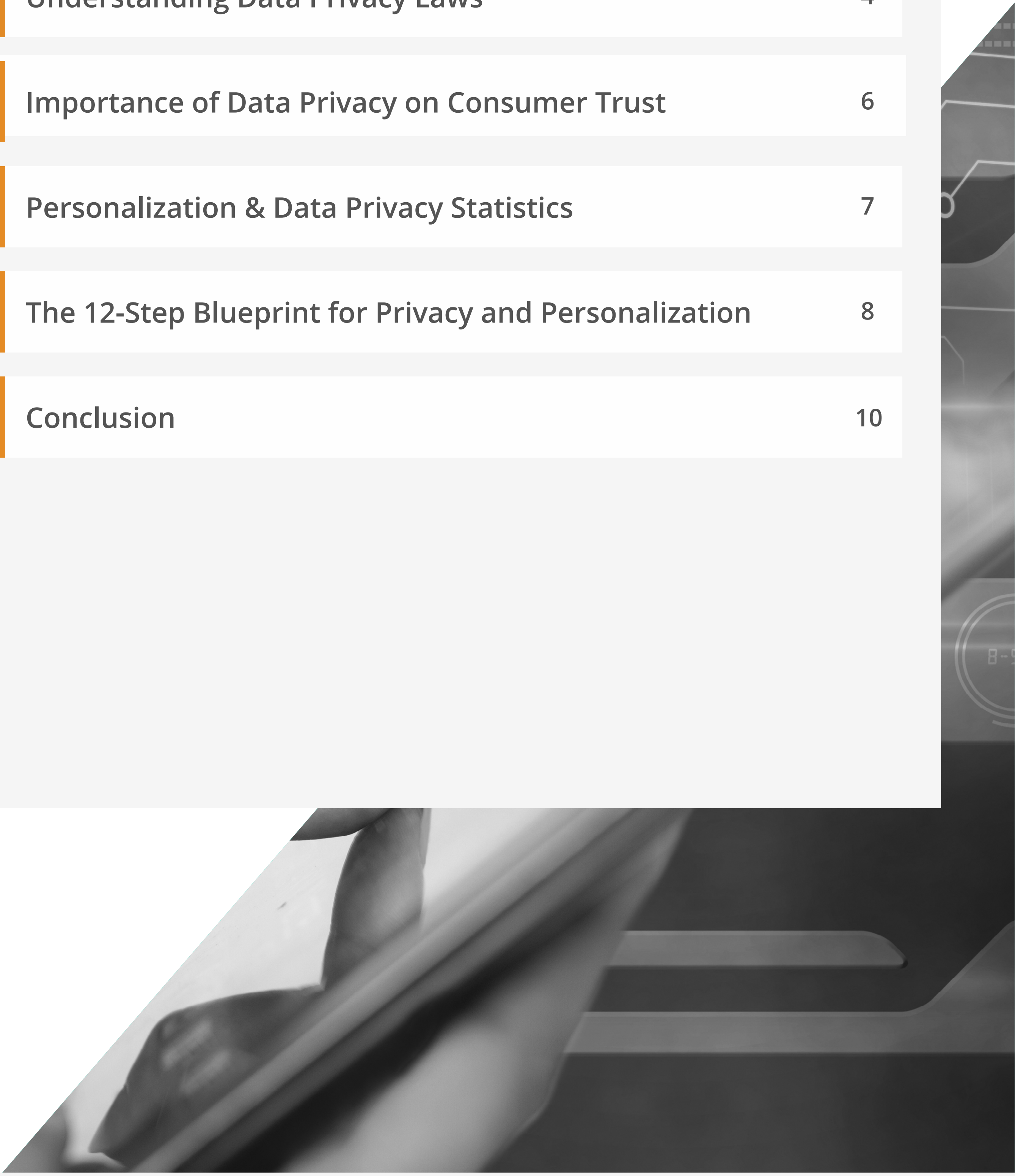
EBOOK

The 12-Step Blueprint to Privacy and Personalization

A Publication of Grazitti Interactive

www.grazitti.com

Table of Contents



Introduction

Data privacy became an oxymoron after the world first witnessed data breaches and ransomware attacks. Up until the recent past, the right to privacy was invisible and intangible to end users. People have been checking "I Agree" without reading the privacy policy and now, they've realized the implications of their casual approach in allowing companies to collect, store, use, and sell their personal data.

The increasing frequency of high-profile data breaches gave rise to strict data protection laws and regulations such as:

California Consumer Privacy Act (CCPA)

EU's General Data Protection Regulation (GDPR)

Customers love unique and personalized experiences, they consider personalization an important factor when engaging with any brand. The Association of National Advertisers named "**Personalization**" their Word of the Year in 2019 highlighting its popularity and importance for brands' advertising today. Today's customers expect privacy and tailored personalized experiences simultaneously. But marketers can't create personalized experiences that customers love without customer-specific data which has become more difficult to get to. As marketers strive to find the right balance between providing personalized experiences, protecting data privacy, and building consumer trust, they're stuck in a catch-22.

In this eBook, we'll break down this privacy paradox for you and you'll learn more about how you can strike the balance between customers' desires for personalized interactions and data privacy. Let's get started then.

Understanding Data Privacy Laws

Until now, the average consumer was likely unaware about how many businesses or 3rd parties have access to their data, what data is it, and how do they use it?

Those days are over with data privacy laws like GDPR and CCPA. With GDPR and the CCPA now in effect, organizations must protect the customer's data and privacy.

GDPR came into effect starting May 25th, 2018. Based on GDPR, businesses need to include the following rights:

- Right to Access Data
- Right to Deletion
- Right to Restriction
- Right to Portability
- Right to Object
- Right to be Informed
- Right to Withdraw

Key elements of GDPR for businesses :

- Privacy by Design
- Assign a Data Protection Officer
- Conduct Data Protection Impact Assessment
- Regular Training

Non-compliance to GDPR could result in penalties up to €10 million, 2% annual global turnover or €20 million, or 4% annual global turnover, whichever is higher.

The purpose for CCPA is to give consumers "**the right to know and the right to say no**".

The California data privacy law got into effect on January 1, 2020. However, businesses have been given a grace period to meet the requirements until July 1, 2020 to comply with CCPA.

Rights of the consumers under CCPA are:

- Right to Request Information
- Right to Portability
- Right of Deletion of Personal Information
- Right to Opt-Out

Key elements of CCPA for businesses are:

- Privacy Policy
- Website Policy
- Record-Keeping Training
- Verifications

Failure to comply with CCPA can result in a fine of $7,500 per violation.

52% of respondents said they felt they had more control of their personal data as a result of GDPR. Compliance with these regulations brings a competitive advantage of data privacy and transparency to businesses, and with it, you can build customer trust and drive loyalty.

Now that we are all clear with data privacy laws, let's understand how data privacy impacts consumers' trust.

Importance of Data Privacy on Consumer Trust

48% customers indicated they'd switch companies or providers because of their data policies/data sharing practices. **86%** of consumers are concerned about their data privacy and are skeptical about how their data is being used.

Data isn't going anywhere, in fact, it's only growing and so is data privacy. Companies must comprehend data privacy into their processes and marketing strategies. **35%** find it invasive when they get ads on social sites for items they've browsed on a brand's website. Brands need to show that they respect the customer's privacy and actively participate in a two-way exchange, that is, give customers something of value in exchange for the data they share with you. This concept of a "value exchange" means that in exchange for their participation, customers should receive something of value, like:

Personalized offers and recommendations

Exclusive and/or targeted content

Free trials

Exclusive early access to new products/features

Discounts or coupons

In a survey, Accenture found out that **83%** of consumers are willing to share their data in exchange for a personalized experience only if a business is transparent about how they use data which is why every data-driven business should comprehend on:

- What are the best practices to follow that can build customer trust?
- How can they have quality data while reducing security and privacy risks?
- How can they ensure inherent concern for security throughout the organization?

To truly build customer trust as your competitive edge, your organization must first establish a reputation for protecting customer data and privacy.

Personalization & Data Privacy Statistics

80% of consumer respondents of a recent survey stated that they're more likely to buy from a business if they regularly receive "personalized experiences". However, another survey states that **32%** don't like personalized messages from brands because they feel like an invasion of privacy. And **28%** of people said that they don't like it when companies collect their information without them providing it.

This is where it gets tricky for marketers as consumers want personalized offers that are relevant to them but in order to execute personalization, companies must have data on consumers.

To get it right, businesses must leverage the right efforts, like the 'value exchange' concept we discussed before which promotes a two-way exchange. These stats justify the concept:

- **90%** of consumers are willing to share their data to receive discounts on products they like.
- **87%** stated they'd share if their issues are resolved quickly and in a hassle-free manner.

54% of respondents are highly likely to walk away from a business that requires them to provide highly personal data, in order to conduct business with them. That is because consumers want to share data in a non-invasive way. Additionally, any information that a customer shares willingly will be of better quality and will help marketers get insights about what products their customers desire, what they look for in a service, and what motivates them to purchase.

Privacy and personalization can work hand-in-hand if businesses support data privacy with integrity, transparency, and roll out marketing campaigns that are compliant with privacy laws.

To initiate trust, organizations must provide consumers with visibility into how their personal data is being collected and used. So, let's understand how it's done.

The 12-Step Blueprint for Privacy and Personalization

Businesses need to start being transparent and practice some restraint when collecting personal data and only seek absolutely necessary information that will help them build personalized messages for customers. It is possible to include both privacy and personalization in your operations, if you balance them right. Here's how you can balance the scales of privacy and personalization:

1 Use trust badges on your website to assure customers that their information will be stored carefully and securely. **82%** of organizations see privacy certifications such as ***ISO 27701*** and ***Privacy Shield*** very important when they select a product or vendor.

2 Include only specific individual data that aligns with the customer experience, preferences, and interests. Communicate with your audience as to what they'll get in exchange for providing information – better products, amplified experience, etc. For instance, Netflix shares that their recommendation engine can work better if consumers provide data about their preferences.

3 You can include progressive forms when someone signs up for your service or downloads a piece of content. Keep forms short and conversational. This will help gather essential information to build better buyer personas over time. As a result, you can craft nurture campaigns with targeted content based on job role, industry, company size, and more to move lead closer to purchase decisions.

4 Ensure that all data collection methods are CCPA/GDPR compliant such as landing pages, forms, etc. You can customize your forms and landing pages which should include checkboxes for opt-in consent.

5 Use double opt-ins to improve the quality of your leads. This way, you'll stay compliant with data privacy regulations while increasing email open rates and filtering out bot clicks.

6 Check your third-party data sources whether they comply with CCPA/GDPR requirements to ensure data security.

7 Communicate with your customers about your updated policies that align with CCPA/ GDPR regulations.

8 Place mechanisms that allow consumers to exercise their rights to obtain and delete their information and manage opt-outs.

9 Give customers control over communication. The apt way to do this is through an ***Email Preference Centre*** — a form that allows your subscribers to control when, how, and what they'd like to hear about from you. This way you can tailor your messages according to the desires of the customers while being responsible for privacy.

10 Give customers flexibility over the type of data they are comfortable with sharing. This makes it far more likely that they will offer up at least some personal information which you can use for personalization.

11 Ensure proper compliance documentation. Map your data and its sources. Compliance plans and processes should be properly documented. A variety of content management systems such as Enterprise Content Management in SharePoint, OneDrive for Business, OnBase, etc, are available to house and track all documents, reports, and records.

12 Provide proof of compliance with clearly verifiable and readily accessible through reports and documentation.

Privacy and personalization can co-exist if consumers are engaged and receive something in return for their attention and data.

Conclusion

Consumers are increasingly skeptical of whether or not they can trust brands with their personal data. But they're willing to trust brands who use their data in a responsible way to deliver personalized experiences. It's up to marketers to focus on building relationships by providing consistent, valuable communication which is transparent, secure, and protective towards consumers' personal data while creating marketing strategies.

Are you ready to balance the scales of Privacy & Personalization? Talk to us!

To learn more about our commitment to security and privacy, feel free to drop us a line at info@grazitti.com and we'll take it from there.