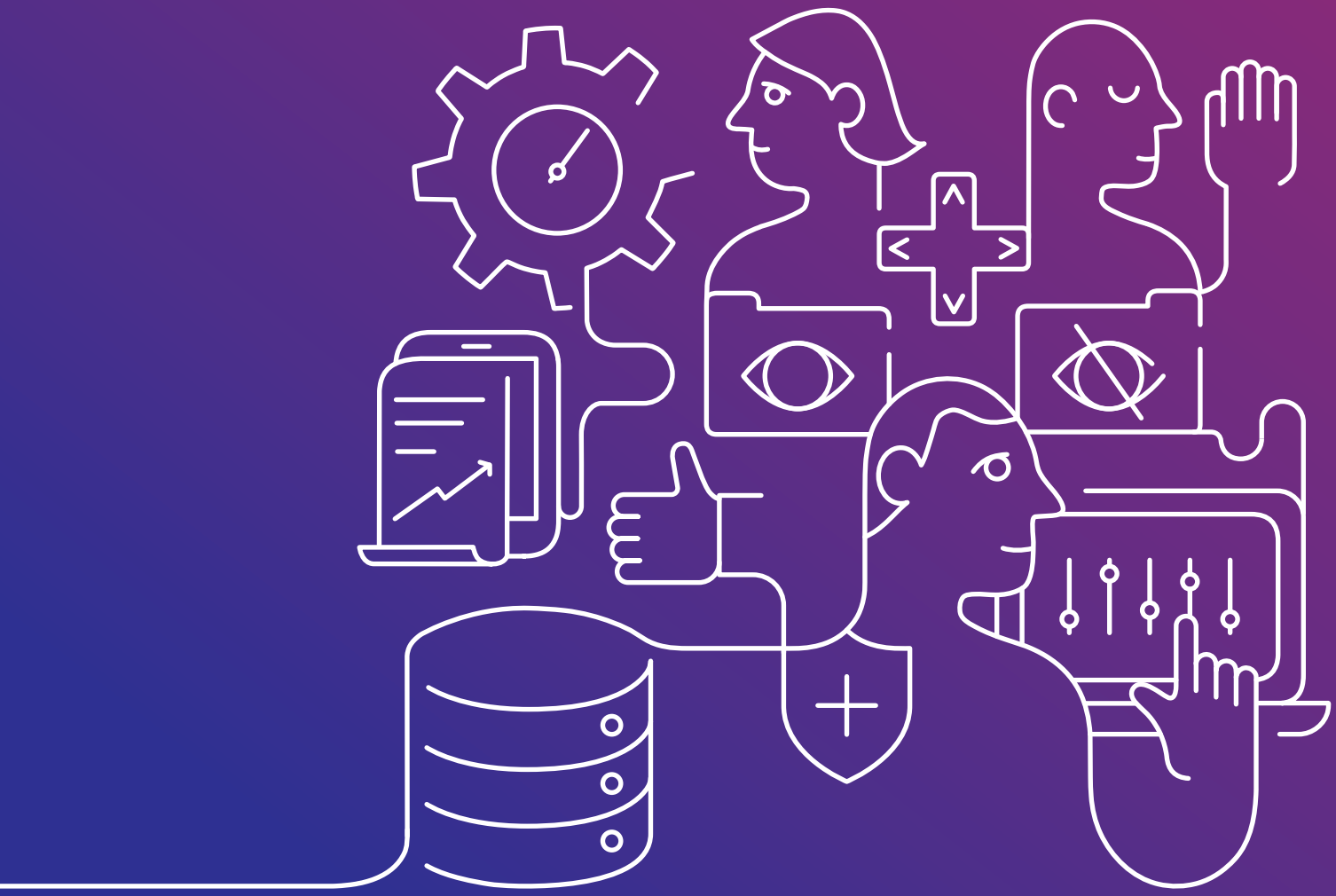
PRIVITAR

Retail and Data Privacy

The Need to Leverage Customer Data is Increasing for Retailers Worldwide



www.privitar.com

From traditional brick-and-mortar to e-commerce, retailers have become increasingly aware of how crucial customer data is when creating a personalized experience and achieving higher conversion rates. Increasingly, consumers are shifting their buying habits to those organizations that can provide a tailored and efficient shopping experience. Consumer behavioral data is compelling:

> 91% are likely to shop with brands that provide personalized marketing and communications.[1]

> 79% are willing to share personal information in exchange for some benefit, such as price reductions.[2]

> 71% have expressed frustration when their experience isn't personalized.[3]

> 49% have purchased a product they didn't initially intend to buy after receiving a personalized recommendation.[4]

Increases in Data Breaches, Privacy Regulations and Customer Expectations Create Urgency for Data Privacy

In the midst of increased demand for a personalized customer experience comes regulations and trends that seem in direct conflict with these goals. While customers want a retail experience tailored to their needs and interests, they are also sensitive to their personal data being collected, and how it may be used. From 2016-2018, the volume of records reported as breached increased twelve-fold. Customer concerns about how and when their data is being used has risen as a result.

Regulatory bodies have responded firmly. Over 100 countries now have data protection las in place, focusing on safeguarding personal information.

Personal information can include data ranging from address and bank account number to lesser known regulated data, such as demographic data you collect or buy, or browsing or sales history that can be used to positively or reasonably infer demographic information about a customer.

Regulatory bodies have increasing power to investigate potential violations and issue fines as well as other enforcement actions. Newer pieces of legislation, like CCPA, also include protections called the Private Right of Action. Consumers are given the right to pursue damages against a company when the consumer feels legally aggrieved. These damages can be significant. In the case of CCPA, individuals can claim damages of $100-$750 per person for distress alone. Damages for actual harm are uncapped.

With this increasing risk and regulation, sensitive customer data must be protected to ensure your organization is minimizing exposure and maintaining hard-won customer trust and brand integrity. Retailers must adapt and standardize on a centralized data privacy solution that consistently mitigates risks and optimizes data utility to safely enhance the customer experience.

Data Privacy Must be an Integral Part of Data Management for Retailers

Retailers must protect customer data to minimize the impact of data leaks, ensure regulatory compliance, and preserve brand integrity. Yet they must maintain their ability to use that personal information to create a customer experience that increases sales, customer satisfaction, and customer lifetime value. Failing to ensure privacy while refining insights significantly limits the type of tailored customer experience that allows retailers to remain competitive.

1. Accenture. "Making it Personal: Why brands must move from communication to conversation for greater personalization." 2018.
2. Katz, Chemi. "How Data Privacy Will Reshape the Future of E-Commerce." TotalRetail.com. 2019.
3. Petro, Greg. "Retailers Walking a Tightrope Between Data Privacy and Personalization." Forbes.com. 2019.
4. Katz, Chemi. "How Data Privacy Will Reshape the Future of E-Commerce." TotalRetail.com. 2019.

Leading retailers typically have many different data users with many distinct and simultaneous goals: increasing conversion rates with targeted promotions, evaluating the customer journey to enhance upselling and cross-selling opportunities, predicting and avoiding customer churn, and personalizing every part of the omni-channel experience. The sheer volume and scope of data analyzed using Machine Learning and Artificial Intelligence can yield critical insights for retailers that make full use of the data in an increasingly competitive environment. Shoppers linked to email addresses, home addresses or phone numbers may not even need to be a registered shopper on a website in order to have their buying behavior analyzed. Every additional purchase can provide more context and insight to retailers, allowing them to infer relationships between shoppers, or determine statistics like gender, income, age, profession, and political positions:

> Targeted marketing using Machine Learning models can use anonymized buying history to predict the next best purchasing action; for example, a shopper who begins buying larger quantities of things like unscented lotion and prenatal vitamins will be inferred to be female, pregnant and likely in her first trimester based on buying habits of other individuals' buying habits. Ads and upsell options can be placed accordingly.

> Dynamic Clustering can leverage demographic data to identify trends for retail locations across different regions, socioeconomic status and more. For example, identifying trends that might be similar across the United States' northeast region but very different from the US Southwest will allow more focused and relevant suggestions to increase basket size in each region according to trend.

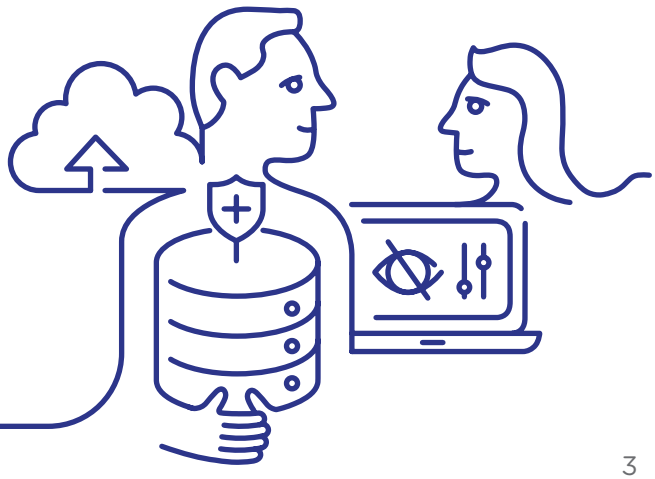
> Focused demographic trends leveraging anonymized data can allow the best strategic marketing approach for each. For example, Millennials are often more fiscally responsible, spending less on entertainment and often prefer generic brands[5], whereas Baby Boomers want the trust and longevity of a relationship with a retailer or brand and are less concerned about price. This demographic data can best help tailor the customer experience and present the right mix of products and promotions to each shopper.

As these insights sharpen, retailers can more accurately target life milestones, current events or issues that can better drive purchasing decisions. With this huge increase in data, however, comes more urgency to protect this data from breach or misuse. Simply protecting insights with security measures like Access Control does not sufficiently allow sharing the information across channels and keeps data siloed. Data Privacy is crucial in ensuring enterprises are maximizing data utility while minimizing the threat of data leakage and regulatory non-compliance, and its resulting restrictions and fines.

A Customizable Approach to Protecting Data is the Only Way to Ensure the Widest Range of Use Cases can be Met

> Protect all personal information. All sensitive customer data you collect and store must be de-identified for analysis. Only unless strictly necessary in catering to a personalized campaign intended to craft the customer experience should data be re-identified, to minimize risk and exposure. A wide range of de-identification techniques allows for the most comprehensive privacy coverage while permitting the best use of customer data.

> Controlled Reversibility. Data should only be re-identified by approved individuals, and not in every case. Ensuring control over when and how de-identified data can be re-identified and acted upon is critical in protecting customer privacy while leveraging the information to increase customer lifetime value.



5. Lexington Law. "45 Statistics on Millennial Spending Habits in 2020". 2020.

- Controlled Linkability. De-identified data must still allow for the discovery of trends and insights. As more data becomes available, it should be consistent to enrich existing de-identified data models and provide additional customer insights. In parallel, data must be tightly controlled to ensure that any unintended enrichment or linkability is prevented.
- Scalability. As Machine Learning and Artificial Intelligence process ever-growing volumes of valuable data, it is critical that the ability to de-identify and leverage that data is able to keep up with the demands of a retailer's system.
- Compatibility with Modern Data Architectures. Ensuring data privacy should not negatively impact an organization by requiring a shift to a new technology stack, nor should it require a significant shift in process to become effective.
- Traceability. Make sure that the reason for data collection and transmission is tracked, as well as who has access to it and when.

The Privitar Data Privacy Platform™: Safely Use Sensitive Data to Achieve the Promise of Relationship Retailing

Using customer data gives organizations a competitive advantage and helps foster and solidify relationships with their customers. Maximizing data utility while adhering to consumer privacy laws, the Privitar Platform offers functionality that assists in automating, centralizing and precisely managing the different requirements that allow the best use of sensitive information.

- De-identification. Privitar provides the full range of techniques to anonymize data while maximizing utility and insights. You can control the degree of anonymization according to what level of information is appropriate and when.
- Controlled Linkability. Privitar's Protected Data Domains™ allow a centralized method to control what data can be linked. Within each one, referential integrity of the data is protected, but between them linkage is prevented, allowing each retailer to control which sets of data are linked and how.
- Controlled Reversibility. Privitar also enables you to control reversibility so that you can re-identify anonymized data after analysis, if required.
- Scalability & Automation. Privitar includes a comprehensive set of RESTful APIs that enable organizations to automate and orchestrate their data de-identification and provisioning processes. Programmatically configure policies that ensure personalized campaigns and online re-optimization are adhering to the appropriate privacy policies at scale.
- Architecture Compatibility. The Privitar Platform supports on-premise, hybrid and cloud environments. It accommodates a wide range of technology platforms and data processing models, allowing it to fit seamlessly into existing technology stacks.
- Traceability. Privitar Watermarks™ are unique technology that enable end-to-end traceability of sensitive data. Watermarks allow tracking and management of when a dataset was generated, who it was generated for, when it should be deleted and where it can be used.

Contact us:

e: info@privitar.com
t: UK +44 203 282 7136 / US +1 857 347 4456
w: www.privitar.com

PRIVITAR

@PrivitarGlobal
www.privitar.com