Solving the *personalization puzzle.*

How the financial services industry uses data in a compliant manner.

When it comes to financial matters, it's personal. Customers don't want to be just another account number—they want to feel that their financial institutions know them. For a customer who just paid off their auto loan, this might mean receiving an invitation to open a high-interest savings account for their freed-up cash. For others, it may mean being encouraged to bundle car insurance with their home insurance after a new car purchase.

However financial institutions choose to engage with their customers, making the experience personal is crucial. Creating a valuable customer experience with real-time personalization was highlighted as the most exciting prospect for differentiation in the coming five years in a recent report on digital trends for financial services released by Econsultancy and Adobe.

Yet in a highly regulated industry like financial services, creating personalized experiences that rely on data takes a considered approach. With recent high-profile privacy breaches, including HSBC and Equifax, consumers are increasingly concerned with how financial services companies are using and protecting their data. In a report from the Clearing House, 56 percent of banking users and 59 percent of fintech users say they hold these institutions accountable for the security of their data.

Regulators are also continuing to enact regulations—like GDPR, GDPL, and CCPA, among others—that limit data capture and empower consumers to determine how their data is used. These regulations, coupled with the Dodd-Frank and the Credit Card Act, which protects consumers from discriminatory lending practices, make it more challenging for the financial services industry compared to other industries to ensure data compliance.

But consumers still strongly indicate that they want to receive a personalized experience. So much so that 83 percent say they are willing to share their data to make it happen, according to Accenture. This is good news for the financial services industry, but it also begs the question: how can a highly regulated industry deliver personalization in a compliant manner?

As we see it, any compliant personalization strategy must include a number of components, from how data is captured all the way to how the organization governs its teams that use the data. In this article, we'll unpack what's involved with each of these components and show how you can achieve personalization at scale while remaining in regulatory compliance.

97% of financial services leaders say they will focus on building offerings that better meet customer needs as a way to differentiate themselves.

Source: Econsultancy and Adobe

1. Pinpoint your personalization *use cases*

Robust personalization requires companies to deeply understand their customers—their needs, wants, attitudes, past purchases, and behaviors—as well as the context in which they are interacting with the company at that moment. However, too frequently, companies capture data without a strategy behind how they want to use it. Instead, they hold onto data that is no longer of value while missing key data points necessary for personalization use cases.

As you begin your personalization journey, think first about the customer journey and use cases you are looking to fill—whether that's cross-selling auto insurance customers with home insurance or targeting prospective customers with a new credit card offering. From there, you can determine the data sources necessary to enable that use case.

For instance, an auto insurance company who wants to cross-sell homeowners insurance to customers would begin by looking at what data they need to achieve this objective—like an address change or inquiries about home loans that could indicate they are planning to or have purchased a home. The company should then think about the best way to capture this data.

Because first-party data—which includes site traffic and behavior, product preferences from quotes, and offer click-through-rates—is the most controlled and easiest to activate, it is usually the most logical place to begin data capture efforts. Based on this data, which would include the ability to see when an account address changes, the insurance company could determine if a customer is likely to need new homeowner insurance.

The insurance company can use third-party data to increase their audience reach beyond their first-party data. However, due to ITP and other measures limiting the capture and use of cookie-level data, third-party data is increasingly difficult to gather and trust. Instead, most advanced companies use second-party data partnerships to expand their pool of prospects and enrich their data about current customers. In the case of the insurance company, they could partner with home-buying sites, like Zillow, to find customers who are currently interested in buying a home and will likely need home insurance in the near future.

Understanding your data options

First-party data: This is data you own. It includes data gathered online through your website, app, email, and other digital channels, as well as data from your offline sources, such as branches, ATMs, and agents.

Second-party data: This is another company's first-party data. For example, a retail bank might receive customer data from a partner airline who co-issues a travel rewards credit card.

Third-party data: This is data you can purchase. This data often incorporates customers' intent, demographics, and significant purchases.

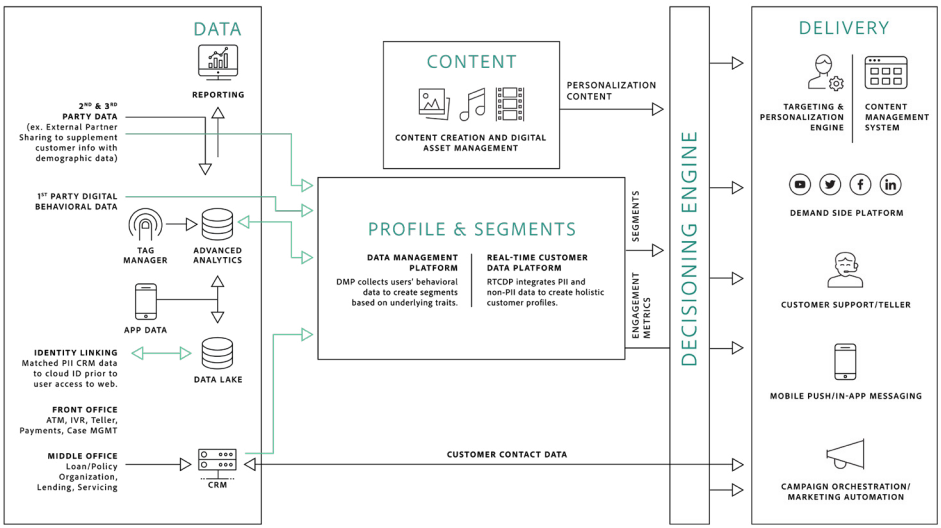
2. Manage your data *compliantly*

Once you've gathered each type of data you intend to use, you need to be able to translate the data into a usable format for your personalization efforts. The ideal process is to have your data sources flow into a centralized location where you can manage and structure your profile data for use, such as a data management platform (DMP) or a real-time customer data platform (CDP). Which data platform you use will depend on your overall objective. Both platforms support the use of data for personalization, but CDPs allow for the combination of personally identifiable information (PII) data with non-PII anonymous data while DMPs focus solely on non-PII data.

After capturing data, it's critical to match and resolve inconsistent customer identities. The simplest way to achieve this goal is through natural matching, where once the customer logs into your site, the device used is automatically linked to their account.

Additionally, as you bring data into your data platform, you need to ensure you have a combination of batched and real-time ingestion, or data at rest and data in motion. Data at rest often houses critical information, such as CRM data and propensity scores, while data in motion allows for real-time personalization with your digital properties. For example, if a customer clicks on "savings accounts," the site would draw on data at rest, using third -party CRM data to understand who the customer is. Then, as the customer takes action by clicking on certain links or pages within the website, using data in motion, the site would immediately populate relevant offers for opening a savings account.

Unify data for activation in one central location



Finally, to ensure you're meeting compliance standards throughout this process, you need to properly label your data upon ingestion. This can include identifying if data is sensitive, requires regulatory compliance, or is personably identifiable information. You also need to develop usage policies for how each piece of data can be viewed and used, and that address factors such as activation channels, content type, and consent.

Labeling your data in Adobe Experience Platform

In Adobe Experience Platform there are four labels to categorize your data:

1. **Contractual:** Contractual obligations of second and third-party data
2. **Identity:** Data that can be used to directly or indirectly identify a specific person
3. **Sensitive:** Potentially sensitive information, like zip code for loan offers
4. **GDPR:** Data governance related to GDPR and other similar regulations, taking factors such as consent into consideration

3. Develop *a holistic audience strategy*

Once you've captured and organized your data sources, the next step toward personalization is audience segmentation. Segmentation often takes on different meanings throughout an organization. For the purpose of this discussion, there are three types of segments we think you need:

- **Strategic:** These segments are the personas that your company is driving toward, often reported to investors, like "mass affluent."

- **Go-to-market:** These segments align to audiences that each line of business is targeting as part of their marketing strategy, like "young family."
- **Micro-behavioral:** These segments are activated upon in personalization and optimization efforts, like "visited 'credit dard page.'"

While each segment serves a different purpose, it's critical for them to map to one another so that the strategic personas inform all communications and the findings.

Using audience segments in a holistic and strategic manner isn't always easy. But the payoff is well worth it. One electronics manufacturer we interviewed described struggling to create actionable segments from their personas. To combat this, they developed a process where they break those personas down into testable segments. Then, once they launch content for a segment, they test both the effectiveness of the message and the accuracy of the audience, refining as they go.

4. Use predictive *modeling*

At the end of a given campaign, the data science team also tests the significance of the audience attributes to tracked KPIs and feeds those insights back to the strategic team. While most of the time the insights gathered require only small changes to the segment's attributes, about 5 percent of the time they discover that the entire segment was wrong (e.g., targeting young families when in fact the product resonates best with millennials). This holistic testing-oriented approach now touches 26 percent of their site traffic. Moreover, for that group, they've seen a **390 percent increase in CTR and 300 percent increase in conversion.**

Predictive modeling uses data and statistics to predict outcomes within Predictive modeling uses data and statistics to predict outcomes within data models—and can be highly valuable as a way to not only improve, but scale personalization. There are many applications for predictive modeling, including mitigating risk, improving operational efficiency, and encouraging revenue-driving behavior.

It's likely that your personalization efforts are most concerned with encouraging revenue-driving behavior, which includes two primary models to help predict what the next best action should be:

- **Look-alike modeling:** Identifies attributes of high-value customer segments to find new audiences.
- **Propensity modeling:** Predicts the future actions of your customers to encourage desirable behavior.

Both of these models can be used to scale personalization—by either finding new audiences that can be targeted or by helping you predict what the next best offer should be. At Adobe, we analyze all customers' interactions, behaviors, and demographics to generate 1.5 billion predictive scores daily. This allows us to "score" customers' probability of taking different actions along the customer journey. For example, a customer's churn score has proven to be an accurate predictor of behavior, with customers in the top 10 percent of churn scores four times more likely to stop using our products than the average user. So, as a customer's churn score increases, we make an active effort to reengage the customer with our products.

For instance, when we notice a customer has reduced their use of an Adobe application, we know that it means they're more likely to cancel their subscription, which can increase their churn score. Seeing the increased risk for churn, we can then trigger a popup notification through the Adobe application to draw the customer's attention towards great features they might not have tried.

While predictive modeling can open many exciting new doors to personalization, it's also important to keep in mind that predictive models must meet regulatory standards. One Canadian retail bank we interviewed uses predictive modeling to monitor its customers for mortgage-like withdrawals and then target them with relevant mortgage refinancing offers. However, because it's critical throughout the process that any data streaming into the models meets regulatory standards, they use credit score ranges rather than exact numbers.

Understanding look-alike modeling

Look-alike modeling identifies traits of your highly valuable customers and uses those to find new prospects. The process includes these steps:

1. **Selecting a baseline audience** that is a small but highly desirable subset of your visitors.
2. **Modeling the difference between the baseline and general population** to determine the reach of every possible trait combination.
3. **Determining how you want to balance accuracy and reach,** by deciding how closely your audience must align with your baseline versus how large an audience you want to reach.

5. Establish strong *audience governance*

The last piece of the personalization puzzle is audience governance, which includes identifying who is responsible for audience creation, strategy, and governance. Typically, audience users and creators are scattered throughout an organization, with marketing teams owning personalization and business units separately governing channel and product strategies. This model often causes disjointed customer experiences, like a customer receiving multiple emails in one day from the same company but from different business units.

However, leaders are beginning to shift toward an audience center of excellence (COE) that manages audience creation and use. Having an audience COE can help eliminate organizational silos and ensure a smoother customer experience.

Here's an example of what this might look like in real life. One retail bank we spoke with developed a three-pronged team that handles all audiences and personalization. The analytics team ensures that the necessary data is being captured, the insights team extracts key insights from that data, and the personalization team develops and executes upon segments. To maintain coordination with the larger organization, they disseminate weekly reports to each business unit of how their segments are tracking against KPIs. This model helps keep everyone informed and avoids the audience silos that can lead to a disjointed customer experience.

As part of ensuring audience governance, it's also critical to establish review processes that enable strong marketing and compliance collaboration. There are three options for compliance reviews:

1. **Separate compliance:** Compliance acts as a distinct group that's consulted for each marketing ask. This requires standardized processes that limit the frequency of requests.

2. **Embedded compliance:** Each business unit has a designated compliance representative that acts as the liaison to legal, who must be educated about the marketing teams' needs to accurately communicate with legal.

3. **Accountable executive:** Legal advises an executive in each business unit on the request but the executive is responsible for the final decision.

An example of how this might work comes from a member services company we interviewed. To establish their personalization initiative, they created a traffic light system in partnership with their compliance team. Red activities were never allowed, green activities were always allowed, and yellow activities were sometimes allowed. This system allowed the marketers to know what they can and can't do upfront, making it easier to scale their initiatives and revise the system itself as the complexity of tactics increases.

The new data steward

Who: The single person responsible for an organization's data governance.

What: They need to understand all data sources, destinations, and what can and can't be done with the data.

Their counterparts: Data engineers in IT and privacy experts in compliance.

Your path to compliant personalization

Personalization is critical to increasing customer engagement through meaningful interactions and outcomes. It is also an important tool for gaining the competitive advantage. And it can be done compliantly and successfully when you follow both personalization and compliance best practices covered in this paper.

Here's a brief review of what those are:

1. Align on prioritized journeys and begin to integrate second- and third-party data sources to augment first party data.

2. Unify data sources into single location and allow for real-time ingestion and activation where needed.
3. Develop ways to connect your strategic personas to micro-behavioral segments.
4. Prioritize predictive modeling use cases, beginning with a few models

Adobe can help.

Learn how Adobe can help as you compliantly scale your personalization efforts.

Learn more

Sources

"2019 Digital Trends: Financial Services in Focus," Econsultancy and Adobe, 2019.

"Embracing a Customer-Centric Business Transformation," Adobe, 2019.

"FinTech Apps and Data Privacy: New Insights from Consumer Research," The Clearing House, August, 2018.

"Personalization Pulse Check," Accenture, 2018.

Personal interviews with financial services and insurance customers and industry experts, conducted by Kasey Haas and Michelle White, 2019.