Jotform

# HOW TO MANAGE CUSTOMER DATA IN AN ERA OF PRIVACY CONCERNS

# How to manage customer data in an era of privacy concerns

The world runs on customer data. In fact, many thought leaders *call data "the new oil" because of its value and potential.* But customer data management comes with a growing number of risks and challenges.

*As data breaches become more common,* worried consumers are more discerning about who they share their information with. McKinsey research *suggests 87 percent of consumers won't conduct business with an organization* if they have concerns about its data privacy management. Many consumers are also *switching to privacy-first browsers and search engines like DuckDuckGo and Brave.*

They're not alone in their worries: Grassroots and nonprofit privacy rights organizations are raising awareness and lobbying governments for better protection. Legacy social justice organizations like the *American Civil Liberties Union* are also focusing on consumer data as it *emerges as a civil rights issue.*

Europe once *stood alone as a leader in enforcing data protection policies*, but now *Australia* and *other countries* have stepped up their efforts. The U.S. is primarily *taking action at the state level*, and policymakers in California *continue to refine* their regulations.

To reduce risk and increase trust, you need a comprehensive, three-pronged approach to data: educate employees about regional and global laws, create a technology and data management strategy, and foster a customer-first mentality. Over the next few chapters, we'll provide an overview of how to do this and share best practices for implementing technology to make the most of the data you collect.

# The current landscape of data privacy

Some nations are relatively new to tackling data privacy, while others are pioneers. *Sweden passed a data act in 1973*, criminalizing computer and digital information theft and giving data subjects the right to access their records. The U.S. didn't have policies pertaining strictly to data rights until the *Children's Online Privacy Protection Act (COPPA) in 1998*.

Now, data privacy regulations differ around the world, creating an uneven landscape for organizations to navigate in an increasingly global economy. Plus, rules change based on industry or the type of information being collected. Some national laws even extend protections to residents regardless of where an organization is based.

Currently, the European Union has some of the strongest and most comprehensive data protections in the world. The Council of the European Union and European Parliament began enforcing the *General Data Protection Regulation* (GDPR) in 2018, two years after its approval. The rules limit the amount of data organizations can collect to what's necessary to conduct business and grants individuals the power to request all of their data. In some instances, consumers may even request that their information be erased.

In contrast, the U.S. has no one law governing data protection — but individual privacy regulations, such as the *Health Insurance Portability and Accountability Act (HIPAA)*, the *Family Educational Rights and Privacy Act (FERPA)*, the *Gramm-Leach-Bliley Act (GLBA)*, and the previously mentioned COPPA combine to create a *patchwork of federal oversight.*

Some states have their own data privacy laws, and more are joining them. The 2018 *California Consumer Privacy Act (CCPA)* gave residents some of the same rights and

protections as the GDPR. Organizations must disclose how they use and share customer data and give customers the opportunity to prevent the sale of their data or delete it altogether.

In March 2022, Utah became the *fifth state to sign a consumer privacy act into law,* joining California, Nevada, Virginia, and Colorado. Michigan, New Jersey, Ohio, and Pennsylvania *have introduced similar laws.*

Some influential organizations are forming their own data protection policies to stay ahead of the curve. In 2021, Apple released a *series of privacy enhancements* requiring developers to ask users for permission before tracking their activity in third-party apps and websites and to explain what information their apps collect and how it's used. More recently, Google announced it's *offering more protections around sensitive healthcare information*, with more organizations expected to follow suit.

**Global cybercrime costs are expected to reach $10.5 trillion USD annually by 2025.**

As data privacy management concerns mount among both consumers and legislators, it's imperative that organizations be proactive about their data collection and management policies. Cybersecurity Ventures, a leading researcher of the global cyber economy, expects global cybercrime costs to grow to *$10.5 trillion annually by 2025*. In spite of these risks, a *World Economic Forum survey* found that 59 percent of organizations may find it challenging to manage cybersecurity incidents because of a shortage of technical skills on staff.

# How to future-proof your organization's customer data

Most organizations already have policies and solutions to safely store, report on, and erase customer data in compliance with regulations. But since regulations constantly evolve, you need a strategy to mitigate future risks.

Responding to changes as they come up will be more time-consuming than staying ahead of them. Ensuring your customer data privacy system is future-proof saves time and money and makes it easier to navigate the changing data landscape. But revamping your existing policy, or building a new one from scratch, requires careful research and planning.

# What do future-proof customer data management policies look like?

Many organizations have already overcome the strategy hurdles that defined the early days of customer data governance, including identifying what information they need, how to get it, and how to store it. Next, organizations focused on improving accuracy and eliminating data silos and storage of unnecessary information to maximize and streamline the use of customer data. Now, compliance with data privacy regulations and consumer trust are becoming issues that impact profitability.

Here's what a future-proof policy looks like.

### Designed for global standards

Even if your organization operates in a limited market, you should design your policy to match the highest standards in the world. Many municipalities look to others for guidance on how to draft their own data privacy legislation, so the laws of one land could soon become the laws of yours.

Failure to adopt a global mindset could also hinder your organizational growth. You may decide to expand into a new market or additional regions. If those new areas are governed by data privacy regulations you neglected to incorporate into your policy, your organization will have to start from square one.

### All-encompassing

A modern data management policy needs more than input from legal and IT — it also needs to engage stakeholders and unify departments to enforce compliance. Customer data can end up in the hands of marketing, sales, customer service, accounting, and other departments. Sharing data between these departments helps provide a better customer experience, but it also creates more risks. With data privacy policies increasingly influencing consumer behavior, organizations need to treat their responsibility for data protection as a revenue-enabler rather than an expense.

### Uniform

A future-proof data management policy is the same for each department and employee. Uniformity streamlines training. If an employee moves from one department to another, they won't have to learn a new set of data privacy policies to function in their new role. Having one universal policy may even allow you to create organization-wide data management training.

### Transparent

Consumers want to know exactly what information an organization collects and why. A future-proof customer

data management policy details exactly when and how to share this information with customers. Transparency is not a one-time action but an ongoing practice that needs to be enshrined in protocol.

**Flexible and scalable**

A future-proof customer data management policy adapts to changing regulations, as well as the needs of a growing organization. Every aspect of the policy is expandable without making drastic, structural changes, even when new laws go into effect. You can update your data management policy seamlessly when it's powered by the right software.

## Developing a future-proof data management policy

The guidelines above clarify the goals of your customer data management policy, but putting them into action is a different matter.

Developing a new policy begins with researching current data privacy laws. Find the laws that govern your market and the regulations influencing the global business community. Search government web pages for the full texts of their compliance rules or other resources that simplify the language. The European Union has a *checklist for how to establish GDPR compliance*.

Organizations like *Digital Impact* offer toolkits to help nonprofits improve their data privacy compliance.

The next step is auditing your organization's current policy to identify how it fails to comply with global standards. List everything you need to change and how you'll update it.

This audit is also an opportunity for stakeholders to flag any potential challenges of enforcing global standards. Get input on drafts of the policy from experts in the department involved in customer data management. They will have more insight into challenges than IT or legal. Partnering with them early in the process will improve buy-in and aid rollout and implementation.

Finally, train all employees who handle sensitive customer data on your organization's new policy. This training should educate employees on the following:

- The protocols they should follow to comply with the new policy. Highlight the changes from your previous policy.
- The dangers of data breaches. Mention fines that result from non-compliance and the impact data leaks could have on customers.

Create an internal chain of command that outlines who enforces the customer data management policy, as well as who will amend it as regulations evolve. Establish a line of communication for employees who may have questions after training.

Throughout this process, leverage data privacy consultants, lawyers, or other experts to ensure your policy is compliant and easy to update. No organization has to handle this challenge alone.

## The importance of a scalable customer data management system

Customer data management policies are useless unless enforced. A customer data management system or platform serves as a dashboard for all your customer information and the central tool of privacy policy enforcement. This technology needs to be as scalable and future-proof as your policy.

A data management system should enable your organization to follow whatever privacy policy you want. Beyond your policy, the management platform you choose needs to follow specific compliance protocols on the backend. For example, even if you draft a policy that doesn't fully comply with GDPR, your platform should comply with it in case you want to expand into Europe later. Otherwise, you will have to find a new technology solution in addition to updating your policy.

Using globally compliant technology right off the bat reduces the risk of compliance gaps and helps your organization align with your industry's highest standards. This lays the foundation for trust with your community, customers, and prospects, as we'll cover in the next chapter.

**Trust is the #2 most important factor in the decision to buy from a new brand.**

***Source : Edelman***

## TRUST SECOND ONLY TO PRICE FOR PURCHASE AND LOYALTY

Percent who say they focus most on each brand attribute

| Brand attributes that are most top of mind when deciding whether to... | buy a new brand | become a loyal customer |
|---|---|---|
| Its price and affordability | 64 | 63 |
| Whether you trust the company that owns the brand *or* brand that makes the product | 53 | 49 |
| The reputation of the brand | 48 | 42 |
| Whether you trust the product to perform well and do everything you need it to do | 43 | 45 |
| How well they it treats its customers | 41 | 42 |
| How easy it is to find and buy the brand | 38 | 39 |
| How well it treats the environment | 37 | 37 |
| If they get the ingredients and materials they use locally, sustainably and ethically | 31 | 29 |
| How well it treats its employees | 27 | 29 |
| How the brand has responded in the face of the COVID-19 pandemic | 25 | 24 |

*Source : Edelman*

# How to take ownership of customer data

In many ways, new data privacy regulations are forming at the perfect time. Organizations have never been more vulnerable to data leaks. Tightening regulations and organizational compliance is the perfect way to protect customers, restore trust, and safeguard the future of the digital economy.

However, more complex privacy policies also put organizations at higher risk of compliance breaches — a major liability, even if it doesn't result in a data leak. Compliance breaches have three primary causes:

- **Human error.** Sometimes, employees entrusted with sensitive customer information make mistakes that result in a breach, exposing your organization to fines. Examples include storing information incorrectly or accidentally sharing information with unauthorized parties.
- **Remote/hybrid work.** *Data breaches increased by 17 percent in 2021* because of the increase in remote work. Remote employees could expose information to hackers if they don't follow proper security protocols — especially if they connect to

open Wi-Fi networks at coffee shops or cafés. Plus, remote work has actually *raised the cost of data breaches*.

- **Using non-compliant,** third-party software. To be more productive, many workers use third-party software to manage information. If your employee uploads sensitive customer data to an unsafe app or software, your organization is liable for the risk, even if it's not sanctioned by your organization.

Workers need to know the difference between compliant and non-compliant third-party apps, and your organization needs to educate them on the difference.

## Taking a proactive approach to customer data management

Without proper guidance or support, your employees will inevitably do something to put customer data at risk. Facing this reality is the only way to protect your organization and your customers.

Educate employees about data privacy compliance, and support them with compliant third-party solutions. A comprehensive data management strategy also improves their customer experience delivery.
*Deloitte's 2022 Global Marketing Trends* report overwhelmingly promotes one message: Put your customers first. With access to so many apps and digital services, consumers are used to a highly personalized customer experience and expect it from any organization. Marrying customer experience with a data management policy is the perfect way to put customers first.
But doing so requires full control of your organization's data

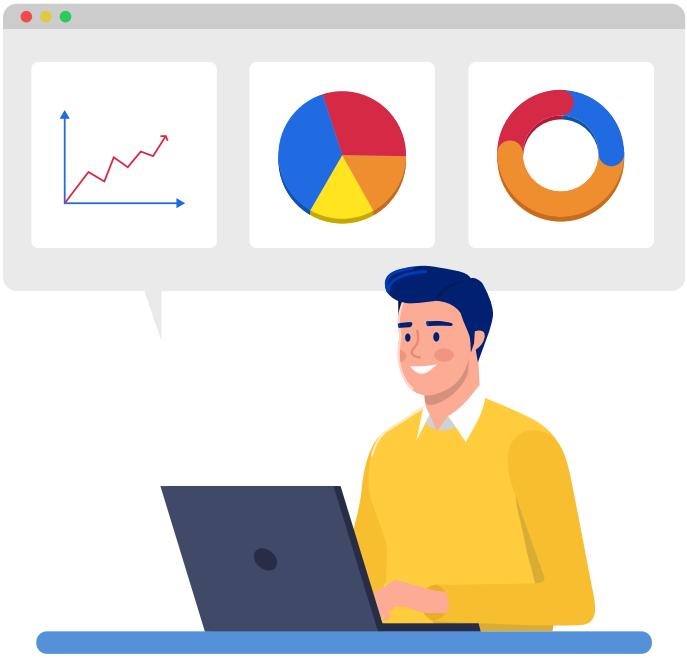
## Becoming a first-party data organization

For the past few decades, organizations have learned about their customers through cookies that track people across websites and social platforms. But in the wake of scandals like *Cambridge Analytica*, consumers are increasingly wary of companies tracking their web activities. Companies like *Google are phasing out cookies entirely*, while the GDPR demands that *users grant tracking permission to websites that use cookies.*

In a cookie-less world, organizations will become increasingly responsible for gathering customer data themselves. Organizations that use first-party data can customize exactly what data is collected — and the channels it's gathered through — to solidify data privacy compliance.

Surprisingly, business leaders are finding that switching to first-party data is a major driver of growth. In fact, *61 percent of brands in a high-growth phase are moving to first-party data,* compared to only 40 percent of shrinking companies. Organizations need a scalable, open API solution to do this effectively and continue growing.

## Customer data management systems to the rescue



The right *customer data management system* is essential to using first-party data as it can help optimize your use of high volumes of data. So, what are the benefits of a comprehensive data management system?

### Deeper analytics

Go beyond merely storing data to actually parsing it for a deeper understanding of customer relationships. Analysts can leverage data for actionable insight into improving customer experience, offering more personalization and launching new products or features.

### Dedicated storage for proprietary data

Without cookies, organizations need more storage space for the information they collect. Having a dedicated system and server unifies information to create a single, secure source of truth for all of your customer data.

### Integration with first-party apps

A central database makes it easier to create first-party apps. You can design the interface to be compatible with your data management platform, with fewer chances of API or other compatibility issues that arise when using multiple solutions.

### Higher security with third-party apps

Just as data management platforms improve compliance, they also improve security with third- party apps they integrate with — including Single Sign-On (SSO) integration capabilities and *SOC 2* compliance. Many platforms provide higher visibility into what customer data is being shared with each app, with options to limit sharing. They can also detect and alert users when a third-party app seems dangerous to integrate with.

**61 percent of high-growth brands are switching to first-party data, compared to only 40 percent of brands on decline.**

Source : *Deloitte*

# What to look for in a customer data management system

Finding a comprehensive customer data management system is vital to building a future-proof privacy policy. But data privacy compliance is just one trait to look at when evaluating different options. Here are other parameters and features to consider.

### Maintainability

Organizations should prioritize long-term growth over speed when choosing a solution. In fact, an estimated *55 percent of firms will inflate their tech debt if they prioritize speed over maintainability*, which could hinder future tech investments.

### Security

How safe is the platform from hacks and cybersecurity attacks? Does it meet industry and global security standards for data storage, encryption, or other protections? How customizable and robust are data-sharing and restriction capabilities?

### Customizable

How much can users personalize the platform? Can you tailor the experience to match your brand? Does the platform improve customer experience with conditional logic or prefilled text? Is it possible to remove unnecessary data silos so different departments, like marketing and customer service, can work together more effectively? Can you improve shareability without increasing the risk of compliance breaches?

### No code

Employees should be able to use and customize the platform without any coding skills. *No-code solutions* maximize user experience, both on the backend and the front end.

### Mobile/cloud-based

In a hybrid workplace, employees need to connect to customer data wherever they are without sacrificing security or compliance.

### Plug and play

The ideal solution should be ready to go without a complex installation process. Previous generations of office software sometimes required weeks or months for the seller to customize it. Modern data management systems walk users through installation.

### End-to-end

The platform should be completely end-to-end, directly enabling the collection, use, and portability of data. Consider solutions that let users survey customers, analyze and share data, and generate external reports. These platforms should also automate communications and management workflows to minimize administrative tasks.

No-Code by the numbers:

41% of organizations used low- or no-code tools in 2019 and 2020, up from
34% previous years.

Source: *Venture Beat*

70% of new applications developed by organizations will use low-code or no-code technologies by 2025.
Source : *Gartner*

48.6% of enterprises surveyed are purchasing low-code or no-code platforms to move innovation in-house.

Source: *IDC*

95% of new digital workloads are estimated to be deployed on cloud-native platforms by 2025, compared just 30% in 2021.

Source : *Gartner*

Nearly 60% of all custom apps are built by individuals outside the IT department. 30% of those apps are built by employees with little to no technical development skills.

Source: *451 Research and Filemaker*

# How to become a customer-first organization

With a scalable platform, you have the tools to improve customer experience — including protecting customers' sensitive data. Gartner predicts that in 2023, *more than 60 percent of the world's population will be able to exercise their privacy rights.*

Consumers are *more likely* to trust companies that limit the use of personal data and respond quickly to security breaches. Any organization that doesn't offer transparency about the kind of data it collects could lose their competitive edge.

## The risks of neglecting customer data security

Adopting a customer-centric approach to data management isn't just a way to maintain market share — it's necessary to navigate data privacy changes.

Regulators are becoming more stringent about levying fines for violations, and the fines are becoming larger. In 2021, the Luxembourg Data Protection Authority *fined Amazon $887 million* for GDPR violations. The same year, WhatsApp was fined *$266 million* by the Irish Data Protection Commission for similar breaches.

In 2021, the *average cost of data breaches was $4.24 million*, but only a fraction of this goes to fines and remediation. Lost business and revenue *accounts for one third of the cost,* making it the most expensive aspect of any breach. After a major data breach, a tarnished reputation can haunt an organization for years, slowing recovery.

# Becoming a customer-centric organization

Using data to improve customer experience begins with a strategy to get more first-party information. This strategy should cover how you gather information, what employees do with it, and how you show customers that you're listening to their feedback.

Begin by initiating conversation with your customers. ***Develop surveys*** and rating systems to collect customer feedback to start building your first-party database. Consider rewarding participation with discounts or other promotions.

Use your customer data management platform to record the feedback, and analyze the data to develop new features, products, services, or customization options. Many organizations already do this to boost revenue, productivity, and customer loyalty.

Trader Joe's is known to ***implement customer feedback*** to optimize inventory and hours, helping it achieve an astounding ***$1,750 in sales per square foot***. Salesforce famously turned its customer feedback forum into an online community called ***IdeaExchange***. Originally started to gather suggestions from customers, it quickly evolved into a way for business owners to connect.

Transparency is another key to improving customer experience — and complying with emerging data privacy regulations. Your organization should explain the reason for gathering or tracking data, highlight the value of doing so, and offer an opportunity to opt out of data collection. Have these messages come from actual leaders at your company. For example, frame an email announcing new data privacy features as a message from the head of your IT department.

Providing more insight into your organization's culture, leadership processes, and decision-making can dramatically improve customer engagement as well — with benefits to the bottom line. When consumers understand an organizations' purpose, they're ***four times more likely to purchase from the company.***

Take your customer-centric approach deeper by forming an advisory board for your organization's most loyal followers. This

rewards them with the opportunity to influence decision-making and product development, while helping you learn what they want. Analyze customer data to identify who they are and invite them to participate.

The most important element of becoming a customer-centric organization is to meet customers where they are: online, through digital experiences. A no-code data management platform will create touchpoints with each of your customers while streamlining collaboration as well as data compilation and storage.

**Forrester Research predicts that the most innovative leaders in tech will move beyond digital transformation to focus on human-centered transformation that merges customer and employee experience.**

**Source: *Forrester***

# Putting data privacy concerns to rest

Customer-centric has been a buzzword for the past decade, but organizations must take the concept to heart as they safeguard the valuable information they've been entrusted with. Fortunately, in their efforts to ***improve security*** and compliance and overhaul IT infrastructure, organizations can become radically transparent and build a new type of relationship with their customers. When organizations choose an ***end-to-end enterprise solution***, they have the resources they need to remain compliant with international data privacy laws, as well as scale in larger markets. With a customizable, no-code enterprise solution, your organization has the ultimate resource for success in customer data management and your respective market.