

ZENDESK INSIGHTS

# The IT dilemma: balancing data privacy and personalisation in customer experience



# Competing priorities: IT leaders balance data privacy with CX personalisation initiatives

Customer relationships are built on trust. But with the data privacy and security landscape evolving quickly, trust can be difficult to maintain. Facing rising cybersecurity threats and increasing regulation, IT leaders are moving to ensure customer data stays private and secure. But this focus on privacy is at odds with customer expectations around personalisation, which is shown to create better customer experiences and drive loyalty – a key investment for IT leaders.

Zendesk uncovered these conflicting priorities of privacy and personalisation in the 2023 [Zendesk IT report](#). In fact, 63% of IT leaders

reported strengthening cybersecurity and data privacy measures was of high importance in the next twelve months, while 60% said the same for enhancing customer experience. Zendesk also found that 88% of IT leaders plan to increase the budget on cybersecurity over the next twelve months.

The difficulty of managing these conflicting priorities lies in protecting and handling the data used to create personalised customer experiences. Adding to the challenge, data privacy regulations are changing faster than ever before, and keeping up with the latest regulatory standards can feel like a never-ending game of cat and mouse.

# 85%

of IT leaders say creating more personalised customer experiences is a high priority over the next year



# Why resolving this conflict is critical for IT leaders

Given the urgency of these priorities, IT leaders without a strategy to deliver on both CX data privacy and personalisation are in for a difficult year. In order to protect their business and drive its growth, IT leaders need to resolve how they will both ensure customer data stays private and leverage that data to drive CX personalisation for better business outcomes.

In this report, we outline three actions that IT leaders can take to resolve these conflicting priorities and deliver personalised customer experiences that inspire trust.

# 66%

of surveyed IT leaders cite data privacy and protection regulations as limiting their personalisation efforts significantly

# 86%

of IT leaders believe that customer service data is valuable and should be leveraged more within the organisation

# 79%

of IT leaders say that their CX software could do more to address cybersecurity risks.



# How IT leaders can deliver trusted and secure CX without sacrificing personalisation

## Evaluate your encryption strategy

To establish a strong data security foundation, evaluate your encryption strategy. Data encryption protects sensitive information like customer data from being accessed by bad actors by translating the data to ciphertext. However, there are a variety of encryption models to consider, and not every model may be right for every business.

For many companies, Bring Your Own Key (BYOK) encryption has become the new standard to promote a higher level of data security. Some CX providers, however, require that encryption keys be stored on providers' platforms, resulting in the provider and any regulatory body auditing that provider losing control of keys.

To gain more control over data security, IT leaders should consider more advanced encryption methods, including the ability to store encryption keys outside of a CX provider platform in a dedicated key management service (KMS). Zendesk's own advanced

encryption capabilities offer a form of BYOK encryption that gives businesses greater control by allowing them to manage and store their keys in a KMS outside of Zendesk.

### **Deep dive: What is BYOK?**

With Bring Your Own Key (BYOK) encryption, companies can generate and retain control over the encryption keys used to protect data stored in third-party applications. This way, they can limit the risk of data exposure by retaining control of encryption keys including the ability to rotate and revoke them.



# Ensure flexible data privacy policies

Flexible data privacy policies supported by customisable tools can help businesses build on a strong data security foundation by giving them the control they need to meet their unique privacy compliance obligations while still leveraging customer data for personalisation.

In particular, flexible data privacy policies enable businesses to control customer data access and retention to ensure that data privacy is respected without preventing CX agents from accessing the data they need to personalise service. Below are specific steps IT leaders can take to strike this balance.

“We’ve been able to leverage Zendesk security and privacy to support our business at every level, reflecting our customers’ understanding and priority of data security”.

Dean Macris, Chief Information Security Officer (CISO), Indigov



## **Redact personal data that isn't needed for service**

Keeping a clear record of customer conversations is key to delivering personalised service. However, these conversations often include customers sharing sensitive personal information that's either already stored within customer records or simply not necessary to serve the customer.

For example, a customer might share contact information with an agent that is already stored within their customer profile. Businesses should see that this unnecessary information is redacted from agent conversations. Data redaction tools make this possible by enabling organisations to recognise and remove unnecessary personal data from agent conversations.

While data redaction policies might be in place, the process can be onerous if it's not automated and at scale. Zendesk's advanced

redaction capabilities, for example, enable efficient redaction through AI-powered detection and automation.

## **Ensure data retention policies are customisable**

Even when personal data is necessary to service, businesses should keep it for only so long. IT leaders need flexible tools for enforcing data retention policies that delete the CX data they don't need while retaining the data they do. This is especially critical for businesses in industries and regions where personal data are required to be deleted when a business no longer has a legitimate purpose to hold it.

With data retention policies, businesses can accomplish this by deleting and keeping specific customer data on a regular schedule. Zendesk's advanced data retention policies enable businesses to do this in a targeted manner by specifying exactly what data should be deleted and retained based on chosen parameters.

## **Deep dive: The complexities of delivering personalised CX**

In order to provide personalised customer service, agents need access to personal customer information. However, not all agents need the same level of access. According to the privacy principle of least privilege, agents should only have access to information they need to do their jobs effectively. For example, if one group of agents relies on specific personal data to service customers while a second group does not, only the first group should have access to that data. IT leaders should ensure agent access to personal customer data is limited based on the needs of their role via data masking and similar capabilities, while also rotating and revoking them.

# Develop continuous data access monitoring

IT leaders need a way to know who is searching for and accessing personal data so that they can quickly identify privacy risks and respond in a timely manner. That's why it's crucial to establish visibility and continuous monitoring.

Monitoring change logs is simply not enough, because this may not catch every breach. For example, bad actors may not be changing data – they may simply be viewing it. That's why it's imperative to know who is searching for and accessing personal data. Teams that need this level of visibility need access log capabilities.

## Establish visibility with access logs

Access logs provide this capability by giving businesses a detailed record of access, including which agents searched for and

viewed CX data, and when and where they accessed it. These logs help identify suspicious behaviour such as repeated searches for sensitive information (like card details or access to data from unexpected locations). Maintaining a record of data access can be critical to demonstrating compliance with certain data protection and privacy laws.

Businesses can use access logs to proactively strengthen data privacy and protection. Reviewing agents' data access to understand what information is required to do their job can help businesses separate necessary data from unnecessary data, allowing them to update data retention and access policies accordingly.

Balancing data privacy and personalisation can be complex. However, with the right strategies and tools in place, IT leaders can enable personalised CX while protecting their business and their customers.

## Deep dive: The value of access logs

Zendesk's own access log capabilities allow businesses to view a 90 day record of what data agents have viewed, including tickets and users, and which searches they have made. Based on this record, a business can proactively identify risks and optimise security and privacy policies including agent roles and permissions.







## Learn more about Advanced Data Privacy and Protection

The Zendesk platform provides strong data privacy and security including threat management and monitoring, identity and access management, auditability and more.

For businesses that need the highest level of data privacy and protection, Zendesk offers Advanced Data Privacy and Protection—a set of customisable capabilities for encryption with self-managed keys, access logging and data minimisation including tools for masking, redaction and deletion.

## About Zendesk

Deliver the best customer experiences in a world of constant change.

Only Zendesk delivers the unique blend of best in class experiences and the flexibility needed to adapt to evolving technology and customer expectations. It's a powerful combination that ensures businesses can take advantage of new opportunities and handle constant change. Zendesk delivers cost efficient scalability and agility, without making customers sacrifice service or innovation.

Visit [Zendesk.co.uk](https://www.zendesk.co.uk)



**zendesk**