Ping Identity

GDPR OPPORTUNITIES: BUILDING CUSTOMER TRUST AND LOYALTY

HOW CUSTOMER IDENTITY & ACCESS MANAGEMENT SOLVES COMPLIANCE CHALLENGES AND INCREASES ENGAGEMENT

WHITE PAPER

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The General Data Protection Regulation (GDPR) is one of the most significant worldwide pieces of data privacy legislation in more than 20 years. By establishing strict controls on how organizations handle personal and sensitive information, GDPR ups the ante on data protection. The EU regulation imposes a series of technical and other requirements on any organization that sells or markets to EU citizens, even non-EU entities, and the consequences for non-compliance are steep.

Leading organizations see much of GDPR compliance as an extension of their existing employee management, customer experience or "know your customer" initiatives. This approach has the significant advantage of moving beyond compliance to improved trust and engagement with your organization's most valuable asset–your customers–and toward transparency for your workforce regarding the use of employee private information.

A holistic identity and access management setup plays a vital role in complying with GDPR requirements for both employees and customers.

Customer identity and access management (CIAM) solutions provide key capabilities that help you not only comply with GDPR but fundamentally transform how you see your customers. CIAM helps you turn the challenges of adhering to GDPR, such as consent capture and management, data access governance and application security, into a unique opportunity to build customer trust during your digital transformation journey.

INTRODUCTION

BACKGROUND

The EU parliament approved GDPR after four years of intense study, debate and preparation. The previous legislation, the Data Protection Directive 95/46/EC, regulated the processing of personal data in the EU, but was widely seen as no longer sufficient for protecting personally identifiable information (PII) in today's digital environment.[1]

GDPR promises to make privacy requirements much more enforceable and uniform. Requirements on new categories of data, expanded territorial scope and data access and erasure rights are just some of the areas that have been bolstered.

IMPLICATIONS

What does all this mean for your organization?

No matter where your enterprise is located, if you market or sell to EU individuals, or if you collect or process EU citizen data, your organization must comply with GDPR or risk facing hefty fines: up to 4 percent of your global annual revenue or €20 million, whichever is greater.

And keep in mind that personal data is defined very broadly. For instance, even if an EU citizen does nothing more than browse your website, that browsing data may be considered personal data and therefore require user consent.

Clearly, GDPR has significant enterprise-wide implications; it is not merely a business issue or an IT issue. In this paper, we focus on some key technical requirements, the challenges they present and solutions for meeting those challenges—all while ensuring a smooth customer experience.

[1] *"Comparison of General Data Protection Regulation and Data Protection Directive," The Centre for Internet & Society, accessed February 2, 2018, https://cis-india.org/internet-governance/blog/comparison-of-general-data-protection-regulation-and-data-protection-directive*

KEY TECHNICAL REQUIREMENTS OF GDPR

GDPR requirements are spelled out in the legislation's articles, and many of these articles relate to how data is collected, stored, accessed, modified, transported, secured and erased. These requirements are very broad and enterprises must address them through process, organizational and technical changes. This paper highlights some of the more prevalent technical requirements that our customers find challenging.

CONSENT

Articles 7, 8 and 9 govern how individuals give consent and can be summed up thus *(NOTE: all article descriptions included here are Ping summaries)*:

> **The controller needs to seek and record consent from the data subject for collection, storage and use of personal data.** An organization must obtain unambiguous consent from the data subject prior to collection; this includes unbundled consent of data fields along with consent for use cases. This consent must be stored in an auditable, secure way. You must also give your customers the right to withdraw their consent at any time, in a way that is not more complex than the one used to collect their consent originally.

DATA ACCESS & RECTIFICATION

Articles 15 and 16 cover the ability of the individual to access data and correct inaccuracies:

> **The data subject can access the personal data that was collected and make corrections and updates.** In addition, the individual can access details about the data's collection purpose, storage period and recipients.

ERASURE

Article 17 handles data erasure:

> **The data subject has the right to ask the controller to "forget" or erase all personal data.** Other regulations requiring record retention, however, can take precedence over erasure.

DATA PORTABILITY

Article 20 instructs controllers on how data is structured and transferred:

> **The data subject has the right to receive any personal data received by a controller.** The data must be structured in a commonly used, machine-readable format, and the individual may request that data be transferred directly to a third party.

DATA PROTECTION BY DESIGN

Article 25 describes how data systems are to be designed:

> **The controller must design systems to protect personal data integrity based on risk**. This encompasses a range of data protection techniques, such as storage, backup, restoration, retrieval and minimal collection, whereby enterprises collect only needed data.

Notable GDPR Definitions*

Controller: The natural or legal person, public authority, agency or other body which determines the purposes and means of the processing of personal data.

Data Subject: An identifiable natural person who can be identified by an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to that natural person.

Personal Data: Any information relating to a data subject.

Consent: Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

**excerpted from the General Data Protection Regulation*

DATA SECURITY

Article 32 establishes guidelines for securing personally identifiable information:

> **The controller must design systems to secure personal data by adopting appropriate technical and organizational measures.** In a concept known as pseudonymization, data should be stored or accessible in a format that would make the data unrecognizable to an individual. Encryption is one of the techniques used to satisfy this requirement. Organizations are also responsible for ensuring ongoing confidentiality, integrity and availability of their data processings. Regular tests should be carried out to satisfy the requirement of a timely restoring of availability and access to data in case of an incident.

CHALLENGES GDPR CREATES FOR THE ENTERPRISE

CHALLENGE 1: INADEQUATE CONSENT

The baseline level of consent in the past is no longer sufficient under GDPR. Instead of implicit or opt-out consent allowed in some cases, your customers must give unambiguous consent via a statement or clear action, such as marking an online checkbox or filling in an online form. As a data controller, the organization is required to demonstrate that the request for consent has been presented in a clear and intelligible manner.

An even higher standard of explicit consent is required if you collect special categories of data. In addition, consent is required in a wider range of scenarios than ever before. For example, user browser data is considered personal data, necessitating explicit agreement for data capture. If your enterprise does not yet support such activity, you will need to update your environment.

CHALLENGE 2: SILOS OF DATA

Consider a customer who is shopping via your business website. Your company may be storing browsing data in an analytics system, other lead data in your e-commerce system, purchase history in an order management system, and credentials and other identity data in yet another system. This siloed data makes adhering to GDPR requirements such as data access and portability much harder to carry out. Also, it is unlikely that all these disparate systems adhere to the data protection and security by design requirements.

CHALLENGE 3: LACK OF GOVERNANCE

Not only is it a good business practice to limit application access to customer identity and profile data needed for the app to function, but GDPR essentially requires that enterprises create specific policies to limit applications' access to any unnecessary customer data. Enterprises that have not done so already must adapt and enforce data access processes on an app-by-app basis via centralized data access governance policies that take consent, privacy preferences and corporate requirements into consideration.

CHALLENGE 4: WEAK APPLICATION SECURITY

Organizations have been facing tough security challenges long before GDPR, but now the bar has been raised even higher. Customer identifiable information that is fragmented and not secured at the data layer is vulnerable to breach, lowering your application security profile and your ability to comply with the legislation's requirement that systems must secure personal data by design.

CHALLENGE 5: LIMITED SELF-SERVICE ACCESS

Are your customers able to self-manage their profiles and preferences? Are these preferences consistently enforced across all devices and channels?

Does your organization have the ability to easily store and retrieve different types of preference data, both structured and unstructured? If your organization answers "no" to any of these questions, you will find yourself having to beef up customer self-service access to comply with GDPR.

HOW CIAM HELPS SOLVE GDPR COMPLIANCE

The aforementioned challenges may be daunting, but they are surmountable. CIAM not only helps your organization solve many of the challenges that GDPR presents, it goes beyond the requirements to yield secure, convenient and personalized customer experiences across all channels and devices.

SECURITY + COMPLIANCE + EXPERIENCE = SUCCESS

Most organizations find that holistic customer solutions create more value for their enterprises and are more likely to stand the test of time. When you start with a complete view of your customer journey and use that for a compliance framework, it can yield a better compliance solution, providing significant value to your organization.

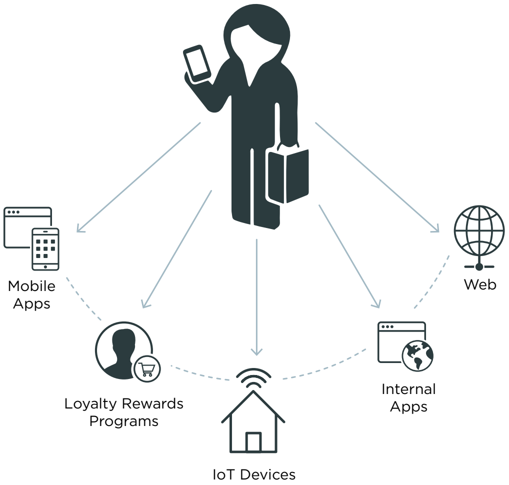
Let's take a quick look at some of the key stages in a typical customer journey and see how GDPR compliance applies in each.

Research
A customer in this stage may actually be just an anonymous prospect, but if you use cookies or gather personal browsing data, and unless you can rely on another lawful basis for processing, a requirement for consent applies. If there is any data attributable to an IP address or any other personally identifiable information, it is your responsibility to gather consent.

Purchase
As both guests and registered users make purchases, consent for use of personal data is required. It is at this point that, depending on how the data is used, it is critical that the data is secured and protected—and for registered customers, that you have account management capabilities in place. In addition, the process of collecting consent and progressively adding details to a customer profile must be simple and seamless to users. Such requirements apply as using clear and plain language and the request for consent being clearly distinguishable from other contents of the given communication.

Registration
Another point at which personal data is collected is during the conversion from an anonymous user to a registered customer. Consent may be required and the underlying data must be secure and protected. The sharing of such profile data with any third parties, such as sub-processors, is governed by GDPR as well.

Account Management
Registered users need access to manage and update profile data, which would include features supporting data access and rectification. This is typically also where users need the ability to request a copy of their data (data portability) and potentially the deletion of their account and personal data (right to erasure or "right to be forgotten").



Streamlining each of the above stages is imperative, as poorly implemented GDPR functionality could adversely affect the customer journey.

A CIAM solution is designed to improve security, privacy and the ability for an organization to effectively engage with customers. Ping Identity's CIAM solution can turn GDPR compliance into an opportunity to rise above the competition, fostering trust and brand equity.

SYNCED AND CONSOLIDATED CUSTOMER DATA

The ability to sync and consolidate customer data is critical to creating unified customer profiles, but if you're like many organizations, identity silos contribute to a complex landscape that is challenging to manage under GDPR. Fortunately, CIAM is up for the challenge.

A comprehensive CIAM solution consolidates identity silos through tools such as real-time or scheduled bi-directional sync, the ability to map data schemas, support for multiple connection methods/protocols and built-in redundancy, fail-over and load-balancing. Syncing and consolidating customer data is a great strategy not only for complying with GDPR but also for helping your organization go above and beyond by enhancing the customer experience.

EASY CONSENT CAPTURE & MANAGEMENT

By its very nature, a comprehensive CIAM system is tailor-made for seamlessly capturing and managing customer consent. CIAM simplifies consent capture across multiple channels and enables you to drill down to consent capture for specific attributes. It allows you to enforce consent choices based on centralized policies that can reflect geographic regulations such as GDPR, as well as corporate policies, industry regulations and customer consent for sharing data with groups like internal teams or external partners.

In addition, many CIAM systems enable transaction consent and approval, an important multi-factor authentication (MFA) use case. Lastly, CIAM systems allow the customer to revoke consent at any time, satisfying a vital GDPR tenet.

SELF-MANAGED CUSTOMER PROFILES

As part of compliance with GDPR, your customers should able to access and manage three key types of personal profile information: profile data, personal preferences and consent. This is another area where robust CIAM systems shine, thanks to pre-built user interfaces and APIs that allow individuals to self-manage their profiles.

Via CIAM, customers can see and make edits to their data or request those changes to be made. End users also can access personal preferences, and these preferences are enforced consistently across various channels. As for consent, your customers can see consent records that give details about when they consented, to what they consented, with whom they consented that information be shared, and more.

DATA ACCESS GOVERNANCE

Data access governance has long been a key component of a solid CIAM strategy. Giving applications unrestricted access to customer data is a recipe for disaster in the forms of increased risk of breach and lost customer trust. Instead, you can maximize the value of your data with CIAM.

CIAM enables centralized data access governance policies with fine-grained, attribute-by-attribute control so that internal and external applications are allowed access to only the particular subset of identity attributes necessary. You get the benefit of governing and auditing customer data access from one system while adhering to GDPR and a host of applicable governmental, industry and other regulations.

GLOBAL NAMESPACE CONTROL

CIAM systems have a variety of underlying capabilities that satisfy the notion of managing a global namespace. One, you can achieve "data residency" by routing data to the appropriate place with a proxy server. Two, you can set up partial data synchronizations and maintain partial copies of your data where appropriate. And three, as mentioned earlier, you can govern the data that applications can receive on an attribute-by-attribute level, based on geographic, corporate, industry or other policies. Doing this helps you comply with GDPR's regulations on data portability, along with regulations on data security and protection by design.

SECURE CUSTOMER DATA

Of course, a managed global namespace doesn't in and of itself guarantee security. An extremely important aspect of securing customer identities is to secure them at the data layer. This centralized approach ensures that strong security is present across applications instead of being fragmented and weaker in some areas.

A self-respecting CIAM system contains a slew of centralized, data-layer security features including data encryption in every state (at rest, in motion and in use), record limit access, tamper-evident logging, active and passive alerts, integration with third-party monitoring tools and much more. This centralized, secure environment helps satisfy GDPR's requirements for data security.

CIAM Function	GDPR Articles address
Synced and Consolidated Customer Data	Articles 15, 16, 17, 20, 25
Easy Consent Capture & Management	Articles 7, 8, 9
Self-Managed Customer Profiles	Articles 15, 16
Data Access Governance	Article 32
Global Namespace Control	Article 25
Secure Customer Data	Article 32

APPROACHES TO IMPLEMENTING CIAM FOR GDPR

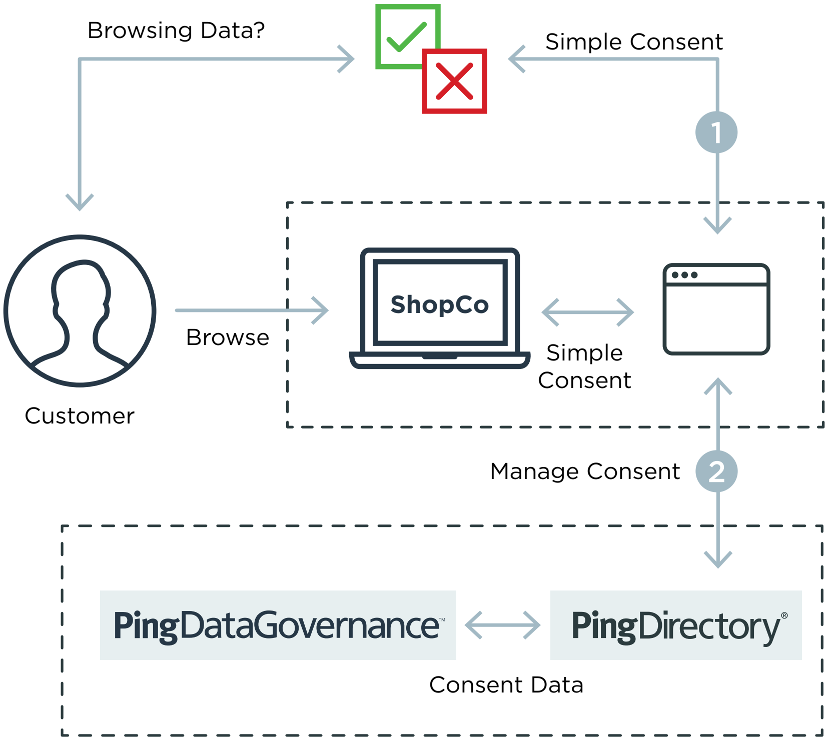
CIAM PROVIDES KEY BUILDING BLOCKS

Many components of CIAM provide building blocks that are the key to a GDPR solution that goes beyond compliance. It is also true that solutions driven by digital transformation provide greater longer term value and return on investment than compliance-only stopgaps. For instance, consider what happens when new regulations come into play or there are changes to existing ones. Compliance-only solutions typically won't support these types of changes, but a broader business solution like CIAM can and should be architected for flexibility and extensibility to support new or updated requirements.

Let's take a closer look at how CIAM components come together to solve some common GDPR use cases.

GDPR ANONYMOUS CONSENT ARCHITECTURE

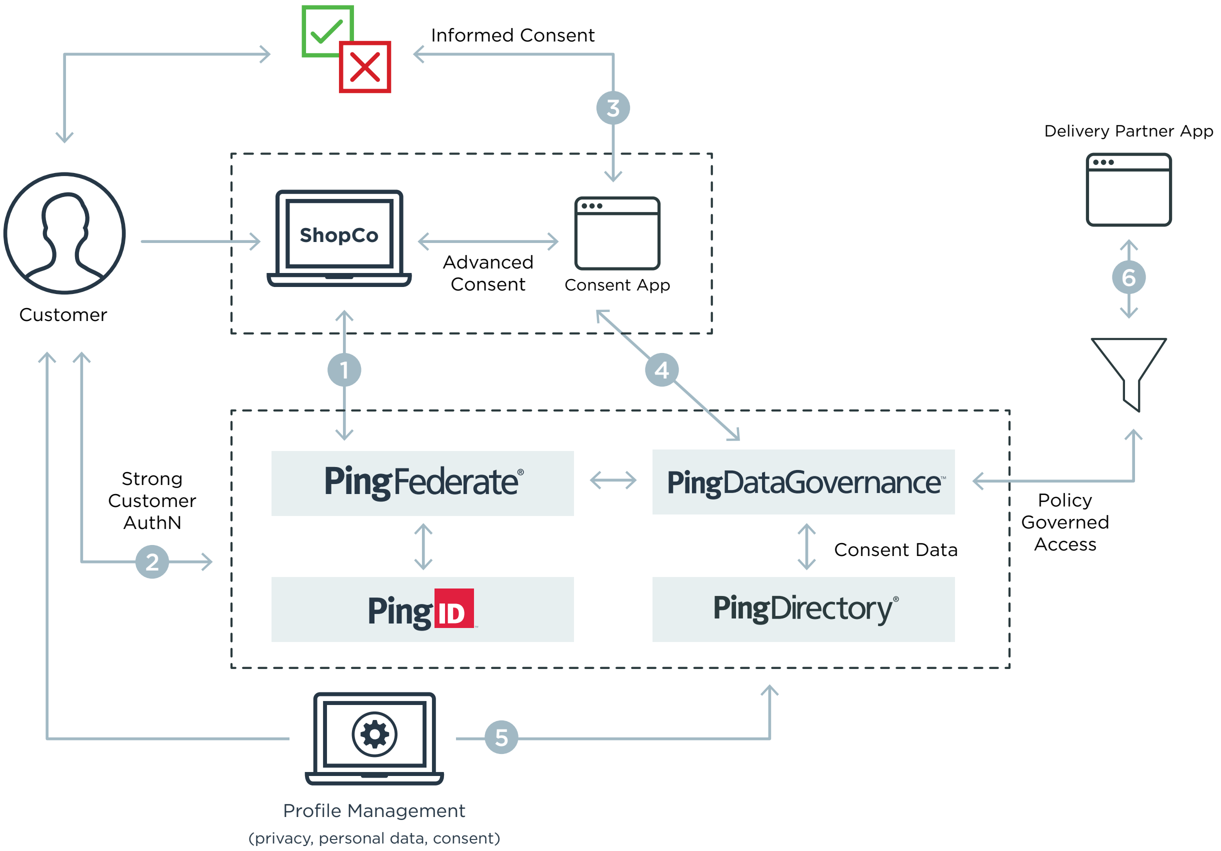
Collecting consent begins with anonymous customers browsing your site. As you gather IP addresses and other personal information and store that data in cookies, you must begin managing that consent. The diagram below shows a basic solution architecture for gathering anonymous customer consent.



GDPR CUSTOMER CONSENT AND DATA ACCESS ARCHITECTURE

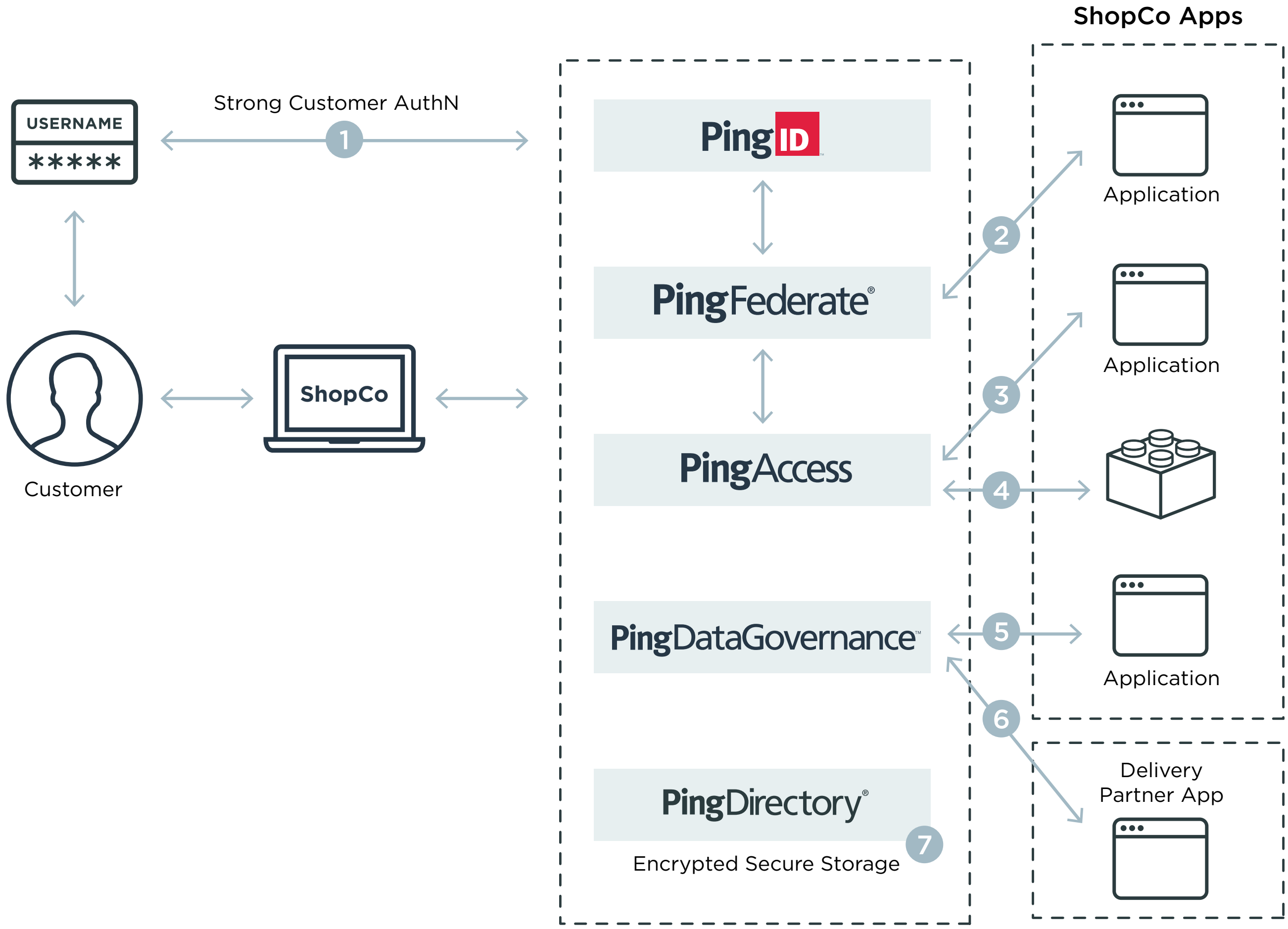
Site visitors who have accounts require another level of capabilities from your solution. Strong customer authentication, compulsory within the financial environment and considered good practice beyond this sector, must ensure that only the right customers have access to their own accounts and that the user experience is secure.

In addition, consent requires ongoing management. The profile management interface should provide customers with full data access, allowing them to maintain and update their personal information as they desire. Finally, governing access to this data for other applications and partners is also critical.



GDPR DATA PROTECTION AND SECURITY ARCHITECTURE

Recognizing all of the capabilities that secure and protect personal data is paramount. This starts with authentication, but also includes data access controls to applications and APIs, along with data storage security.



CONCLUSION

Robust CIAM solutions offer key capabilities including data consolidation, consent capture and management, data access governance and end-to-end security that will help your enterprise meet GDPR requirements. In addition, CIAM best practices help make GDPR compliance efficient and cost-effective through consolidation of data, improved control and governance of your data, while improving security and streamlining experience.

But the organizations whose goals exceed mere compliance will be the real winners as they deliver secure, seamless experiences across all channels and devices, resulting in increased customer trust, engagement and loyalty.

The Ping Identity Platform is designed to provide key capabilities that help meet GDPR technical requirements out of the box. Our leading CIAM solution can transform a GDPR compliance challenge into an opportunity to get closer to your customers, building trust, loyalty and engagement along the way.

To learn more about how Ping Identity's CIAM solutions can help your organization, please visit www.pingidentity.com/GDPR.