

GDPR and Identity and Access Management

IAM's Role in GDPR

The General Data Protection Regulation (GDPR) will change how organisations collect and store personal data about their consumers. Under this new regulation, companies have to be more transparent about how consumers' personal data is collected, stored and used. Because customer identities are at the forefront of this new regulation, GDPR is directly tied with identity and access management (IAM). *An effective IAM program will ensure that only the right people have access to personal data, including employee and customer identities.*

How IAM Helps Solve GDPR Compliance

The following IAM components will help organisations ensure that only the right people have access to customer personal data.

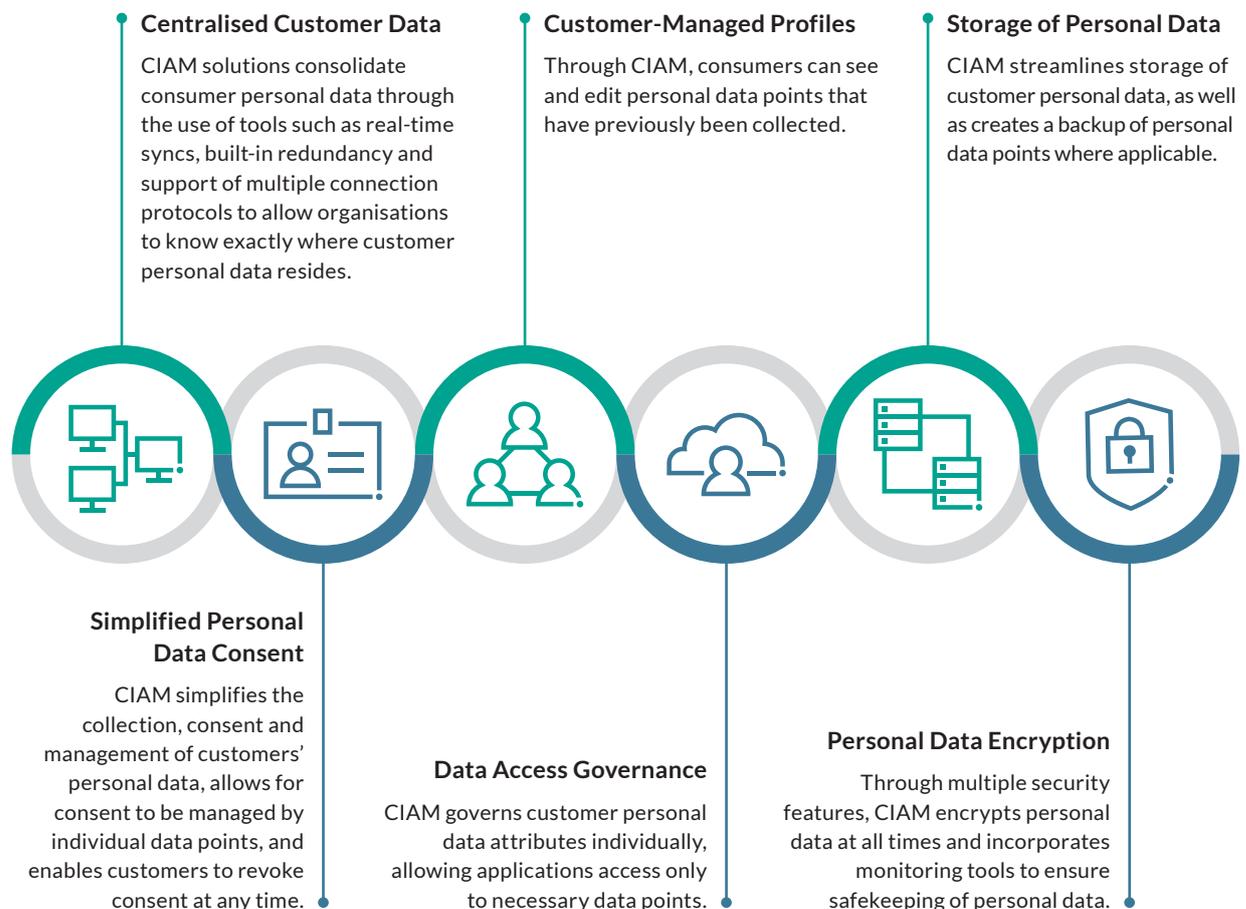
	Segregation of Duties	Employ an IAM solution to enforce segregation of duties (SoD), requiring more than one user to complete tasks around customer personal data.
	Session Monitoring	Monitor users' sessions when dealing with consumers' personal data to allow for concrete analysis in the event of an incident.
	Least Privilege	Utilise the concept of least privilege so that the organisation knows exactly what access each user has, and when and where access is granted.
	Access Recertification	Regularly recertify users' access to consumer personal data to ensure that users have the correct level of access, and remove access to users who no longer need it.
	Privileged Account Management	Tightly control users who have administrative or root access to customers' personal data to mitigate accidental or deliberate misuse of access around consumer personal data.
	Authentication	To keep customers' personal data safe, promote strong authentication techniques – including, but not limited to, multifactor authentication – to ensure that users can prove who they are.
	Lifecycle Management	Ensure proper lifecycle management of customer personal data, including collection, distribution and termination of attributes.

The GDPR Requirement

On May 25, 2018, GDPR was implemented as law, allowing European Union (EU) customers to have more control over their private information across all digital forms. The scope of the new regulation has been extended to all organisations collecting and processing personal data of individuals residing in the EU, regardless of the company's physical location. The key driver for this change is increased risk of exposing customer data through increased use of mobile devices, adoption of big data analytics, and increased volumes of personal data being digitally generated, processed and shared across the globe.

How CIAM Helps Solve GDPR Compliance

Customer relationship management (CRM) provides an avenue for companies to engage with customers. However, without an effective customer identity and access management (CIAM) platform in place that works to secure customer personal data, relationships with customers could falter.



Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 75 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.