IAM’s Role in GDPR

The General Data Protection Regulation (GDPR) will change how organizations 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 organizations ensure that only the right people have access to customer personal data.

<table>
<thead>
<tr>
<th>Segregation of Duties</th>
<th>Employ an IAM solution to enforce segregation of duties (SoD), requiring more than one user to complete tasks around customer personal data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Monitoring</td>
<td>Monitor users’ sessions when dealing with consumers’ personal data to allow for concrete analysis in the event of an incident.</td>
</tr>
<tr>
<td>Least Privilege</td>
<td>Utilize the concept of least privilege so that the organization knows exactly what access each user has, and when and where access is granted.</td>
</tr>
<tr>
<td>Access Recertification</td>
<td>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.</td>
</tr>
<tr>
<td>Privileged Account Management</td>
<td>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.</td>
</tr>
<tr>
<td>Authentication</td>
<td>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.</td>
</tr>
<tr>
<td>Lifecycle Management</td>
<td>Ensure proper lifecycle management of customer personal data, including collection, distribution and termination of attributes.</td>
</tr>
</tbody>
</table>
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 organizations 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.

- **Centralized Customer Data**
  CIAM solutions consolidate consumer personal data through the use of tools such as real-time syncs, built-in redundancy and support of multiple connection protocols to allow organizations to know exactly where customer personal data resides.

- **Customer-Managed Profiles**
  Through CIAM, consumers can see and edit personal data points that have previously been collected.

- **Storage of Personal Data**
  CIAM streamlines storage of customer personal data, as well as creates a backup of personal data points where applicable.

- **Simplified Personal Data Consent**
  CIAM simplifies the collection, consent and management of customers’ personal data, allows for consent to be managed by individual data points, and enables customers to revoke consent at any time.

- **Data Access Governance**
  CIAM governs customer personal data attributes individually, allowing applications access only to necessary data points.

- **Personal Data Encryption**
  Through multiple security features, CIAM encrypts personal data at all times and incorporates monitoring tools to ensure safekeeping of personal data.

- **Customer-Managed Profiles**

- **Storage of Personal Data**

- **Centralized Customer Data**

- **Simplified Personal Data Consent**

- **Data Access Governance**

- **Personal Data Encryption**