Info Sheet

Implementing GDPR In An Identity Management Framework

Increase success of your GDPR strategy with these simple guidelines.

Highlights

- GDPR Defined
- Customer Impact
- Data Centralization
- Authentication Centralization and Data Mapping
- IAM and GDPR Success

The General Data Protection Regulation (GDPR) is the European Union's (EU) strengthened data protection rule covering all citizens of the EU. It gives control of their personal data back to the individual as well as restricting it's transfer outside of the EU. The GDPR unifies the regulations across Europe and is applicable without any action by individual countries. Violations can result in fines of 20 million Euros or 4 percent of worldwide revenue, whichever is greater, so the regulations have gotten the attention of businesses. It replaces the old Data Protection Directive and goes into effect on May 25, 2018.

How does GDPR impact Optimal IdM and its customers?

Optimal IdM only utilizes state-of-the-art datacenters, operated by internationally recognized providers. The datacenters we utilize are configured with the highest possible security and are audited annually, keeping us GDPR compliant. Our software acts a broker between identity providers and relying parties. We do not store or maintain personal information in our software. The amount of encrypted information passed during this authentication exchange is a function of the relying provider request. For our on-premise clients and installations, all the transactions and data are controlled internally by the client and Optimal IdM does not add any vulnerabilities, additional data stores, or outside processing. For cloud services customers, it is a little more complex. The Internet operates without regards to international borders, so an EU citizen's authentication request may transverse the EU boundary, depending on locations. Our cloud customers will need to consider that potential in their data mapping and risk assessment processes.

Data Centralization

An identity access management (IAM) solution can reduce headaches by centralizing all the identities and personal information you manage to fewer locations. Personal information does not need to be stored in numerous applications and databases across your company. Reducing your identity stores will make user management easier and more efficient while lowering inappropriate disclosure risks. With our software acting as a middleman, access to a data store is restricted only to our software. And for consumer

identities, you no longer need to maintain your own repository of personal identity information.

Authentication Centralization and Data Mapping

Having an IAM solution in place can simplify your data mapping process by providing a roadmap for your data flows. An IAM serves as a centralized control point for authentication and access to systems throughout your company. The sources of identity data used in your company are specified in the IAM software. Likewise, all parties relying on that identity data are also specified in the IAM software. Therefore, an IAM solution can be your internal source to understand where data goes. If a web app requests access to your customer database, you now know you must pursue that path to see is if the data is stored elsewhere. By centralizing identity management to one application, it eliminates pathways that allow access to other locations.

Identity and Access Management (IAM) and GDPR Success

When IAM is done right, the chances for GDPR success are greatly enhanced. Here are a few areas to manage closely:

- Authentication/MFA - Multi-factor authentication (MFA), or sometimes two-factor authentication, is a form of cyber security that requires two methods of authentication: a password and some other requirement unique to the user. This type of protection makes it exponentially harder for a hacker to impersonate you and steal your data.
- Authorization - Authorization is the process of verifying that you have access to something. Gaining access to a resource (e.g. directory on a hard disk) because the permissions configured on it allow you access.
- Administration - These critical activities manage user authentication and authorization. Subtle, yet very significant, differences in management levels may leave vulnerabilities to access control. When the in-line business managers are responsible for determining and attesting to access levels, mistakes are less likely to happen and GDPR compliance is more likely.
- Audit - GDPR requires organizations to periodically – as well as on-demand - prove that authentication, authorization and administration are happening in a way that does not place personal data at risk or was not the culprit in the event of a breach.

For more information on GDPR, visit our website at www.optimalidm.com/gdpr.