GDPR and IAM Automation

elevateHR®
Taking Talent to the Top

Elevate HR, Inc.

Published: September 2018

Microsoft Partner
Microsoft
Gold Enterprise Resource Planning
Microsoft Dynamics 365
Certified

www.elevate-hr.com

GDPR and Active Directory Integration in Microsoft Dynamics 365 and AX 2012

GDPR and IAM Automation

for Microsoft Dynamics 365 and AX 2012

You've heard the numbers: penalties for GDPR violations are a staggering $11 million, minimum, and as high as 4% of a company's global revenue for serious infringements. You've already acted to comply with GDPR, maybe by appointing your own Data Protection Officer or by revamping your Consent and Privacy Policies. But have you looked at your internal security protocols? Have you evaluated your Identity and Access Management (IAM) tools and processes from a GDPR perspective?

This white paper details how to ensure GDPR compliance through Identity and Access Management (IAM) automation. The IAM underpinning of your data management practices can make the difference between GDPR compliance or costly – and avoidable – GDPR penalties.

Pulling apart the acronyms

The **General Data Protection Regulation**, or **GDPR**, is a significant European Union statute that went fully into effect on 25 May 2018. It guarantees protection of sensitive personal information as stored, managed, and utilized by commercial enterprises. Since GDPR applies to all EU citizens, no matter where they reside, and to all companies that touch EU citizens' data, it has global reach and affects most companies. According to the Sierra-Cedar 2018–2019 HR Systems Survey, only 23% of companies affected by GDPR are extremely prepared to adhere to the regulation. It is critical to understand that, while DGPR is today's most visible data protection regulation, it represents a growing global trend. Over 120 countries currently have data privacy regulations and 34 countries have specific legislation for Data Localization or Sovereignty standards. Certain U.S. states are also evaluating GDPR "Lite" legislation; for example, the California Consumer Privacy Act of 2018 grants California residents similar privacy rights to those offered by GDPR.

Identity and Access Management, or **IAM**, is broadly defined as "the security discipline that enables the right individuals to access the right resources at the right times for the right reasons" (Gartner), and more narrowly as "the process used in businesses and organizations to grant or deny employees and others authorization to secure systems" (Technopedia). Various tools have been used by companies to operationalize their IAM, but the most frequently used tool is Microsoft's ubiquitous Active Directory (AD), and Azure Active Directory (AAD).

IAM Automation is the mechanism by which day-to-day business processes in your CRM or ERP drive the creation, continuous maintenance, and disablement of Active Directory user accounts, and automatically apply the corresponding security roles within your CRM or ERP, *without manual intervention.* "Day-to-day business processes," for instance, include onboarding a customer in *Microsoft Dynamics 365 Customer Engagement* (CRM), setup of a Resource in *Dynamics 365 Field Service*, creation of a supplier in *Dynamics 365 for Finance and Operations* (ERP), or hiring an employee in either *Dynamics 365 for Talent* or *Finance and Operations (F&O)*. IAM Automation also includes record maintenance and offboarding or termination processes. Proper IAM Automation operates bi-directionally, to update and synchronize security profiles in both Active Directory and your CRM and ERP platforms.

GDPR provisions relevant to IAM

Two critical provisions of GDPR stand out as most relevant for IAM:

1. **Protect against data breaches**

Companies must properly protect personal data from unauthorized or unlawful processing, access, loss, or modification, and such protection begins with the accuracy of their network access controls. Proper system security, of course, goes well beyond GDPR: according to IBM's 2018 Cost of a Data Breach study, the average cost to companies for a data breach event is $3.9 million—this is in *addition* to any fines levied by European Union authorities.

2. **Identify what data you share, and with whom you share it**

It is common, in our connected world, for Personally Identifiable Information to be shared with vendors, customers, and employees, all for important and lawful business purposes. The most powerful way to ensure you comply with this provision is to codify your data access business rules within your IAM processes.

Manual IAM

Active Directory is most often maintained manually. Procedures are put in place to standardize who gets access to what network resources; while such standards are an important foundation for automation, they are far from actual automation. One typical procedure is for managers to fill out an online form to authorize specific system access for a new employee. Another procedure is for a security clerk to follow a pre-established decision tree to identify what kind of system access is appropriate for a new employee. The next step in both procedures is for a system administrator to manually create an Active Directory account based on the authorization they have received. Finally, most such procedural approaches include a final audit step to ensure that the network access was correctly requested, and

correctly administered. Such procedures are time consuming, error prone, and expensive. These processes must be repeated for each job change an employee experiences throughout their career, and again when they leave the company. Often, changes of manager, personal information, title, role or department are processed late or, in fact, go unreported. Manual IAM quickly erodes the quality of your Active Directory data, and exposes your company to compliance lapses.

Benefits of IAM Automation

IAM automation leads to many benefits, including increased efficiency, data accuracy, enriched Active Directory utilization, optimization of network resources and simplification of software licensing and subscriptions (more on this subject in a subsequent white paper). From a GDPR perspective, the highest-value features of Automated IAM are:

1. *Direct tie-in to your company's business processes*
   System access maintenance is not a separate, ad hoc, procedural (and therefore error-prone) activity, but is the direct outcome a business operation. System access can be immediately—and automatically—disabled when a user leaves the company or their role
2. *Policy-driven business rules*
   The business rules that determine what employees (or customers or vendors) have access to are built into the Automated IAM process
3. *Documented profile exceptions*
   Any policy exceptions are easily identifiable
4. *Significantly reduced error rate*
   No manual intervention means fewer errors and reduced audit overhead
5. *Finally, Happy…* HR, Sales, and Finance departments
   Happier… Network Administrators
   Happiest… GDPR Data Protection Officers

Sound simple? In concept, perhaps, but GDPR compliance requirements are complex, and the mechanisms needed to fully automate IAM are demanding. The effort to stay current in the ever-evolving landscape of network administration can be daunting. Best not to automate your IAM from scratch, but to deploy a packaged solution such as **elevateAD®**. elevateAD is built specifically to address the Microsoft Dynamics market need for IAM Automation.

Conclusion

The European Union isn't kidding around: Global Data Protection Regulation is here, and here to stay. The GDPR requirements and penalties are clear, but do not include a clear strategy to ensure compliance. IAM automation with elevateAD® facilitates GDPR compliance and reduces the headache, overhead, expense, errors, and risks inherent in manual Active Directory and Azure Active Directory administrative procedures.

About elevateAD®

Elevate HR's on-premise and cloud (Azure) AD integration tool (elevateAD®) automates the exchange of information between your Microsoft Dynamics modules and Active Directory, so all updates between AD and your CRM or ERP become an automatic extension and outcome of natural business process.

Users configure policy- and date-driven parameters so anytime you enter a contact, onboard a vendor, or hire an employee, elevateAD triggers the creation and activation of each corresponding AD user account, and automatically assigns security groups in AD and security roles in Dynamics by policy/position. Seamless bidirectional synchronization provides your company's employees, customers, or vendors the access they need, when they need it, without delay or manual intervention. Terminate an employee or end a contract, and elevateAD automatically disables AD user accounts and cancels access to all systems. elevateAD respects AD account security options, including Kerberos DES encryption types, smart card interactive logins, and sensitive accounts.

About Elevate HR

Elevate HR is the original developer of the HCM component in Microsoft Dynamics. We've attained Microsoft's two highest standards of partner achievement: we are a Microsoft Gold Certified Partner, and all our solutions are CfMD (Certified for Microsoft Dynamics). You can view more information about elevateAD® and our other Microsoft Dynamics ERP product modules through the Solutions and Resources sections of our website (www.elevate-hr.com).