Omada

SOLUTION BRIEF

Achieving GDPR Compliance with Omada

The General Data Protection Regulation (GDPR) is a global game-changer, introducing new data privacy regulations that puts the power of privacy back into the hands of consumers. Any organization, that collects, processes, and stores EU citizens' privacy data, such as names, titles, email addresses, IP addresses, financial information, or health records, will be affected and needs to be in compliance.

The GDPR is European legislation, yet it affects all companies handling privacy data of EU citizens, which extends to essentially any global company. This can create some confusion as to who needs to comply, and in what capacity. This landmark legislation also uplevels data privacy to a boardroom discussion, with executives now forced to be aware of what data they store, and where.

According to a new global study a staggering 70% of employees have unauthorized access to confidential business data and in most organizations, the required access governance processes for compliance are not implemented. In terms of the GDPR, this lack of governance oversight could have significant ramifications.

Consequences of non-compliance:

- Hefty fines reaching up to 4% of global revenue
- Risk of reputational damage.
- Exposure to lawsuits.
- Loss of prospective business partners

Access Governance is the Cornerstone in GDPR Access Compliance

Organizations are realizing that solid access governance is a vital prerequisite for GDPR compliance. Two GDPR articles highlight where access governance is vital.

1) Article 5 which states that personal data must be processed lawfully, fairly, and transparently, that data is only collected for specific purposes and limited to adequate scope, that personal data is kept up to date and only kept for the appropriate period of time, and that it is processed in a manner that ensures security and protection against unlawful processing, accidental loss, or damage.

2) Article 24 which takes into account the types of data that is processed, and how the controller must implement appropriate technical and organizational measures to demonstrate that they are compliant.

Not only do organizations need to have efficient and effective access governance in place, but they also need to be able to clearly demonstrate compliance.

Avoid Fines, Image Loss and Lawsuits

GDPR means organizations have to take several actions:

- Ensure that data collected is business-essential, and only kept for time required
- Assign a Data Protection Officer*
- Conduct security awareness training
- Document the process for notification of any data breach to authorities and individuals
- Prepare for Privacy by Design and Privacy by Default requirements
- Prepare for Privacy Impact Assessment requirements
- Review and update Data Processor agreements

** Does not apply to all organizations*

The Future-proof Solution for GDPR Compliance

With Omada, organizations can quickly implement a full-featured Identity Governance and Administration (IGA) solution to help enforce least privilege and prove GDPR compliance. Our approach allows our customers to be up and running within 12 weeks, supporting a fast track to get in control of data and demonstrate compliance with easy-to-use, easy-to-manage processes and dashboards.

The Omada Compliance Dashboard

At the heart of the solution is an interactive Compliance Dashboard, that provides a complete overview of all systems that contain critical data, with actionable workflow-based remediation functions. Built-in analysis and reporting features deliver identity intelligence and provide an overview of 'who has access to what', 'who approved that access,' and for what reason.

The Compliance Dashboard renders compelling insights about systems and protected data, indicating the compliance level for each application and system. It provides a high level overview with approvals indicators (see figure 1) and the ability to drill down into detailed access data. With a single click it is possible to instantly execute remediation activities for critical findings. Teams also save huge amounts of time that otherwise would be spent manually pulling data and reports from disparate systems, with Omada's centralized dashboard.

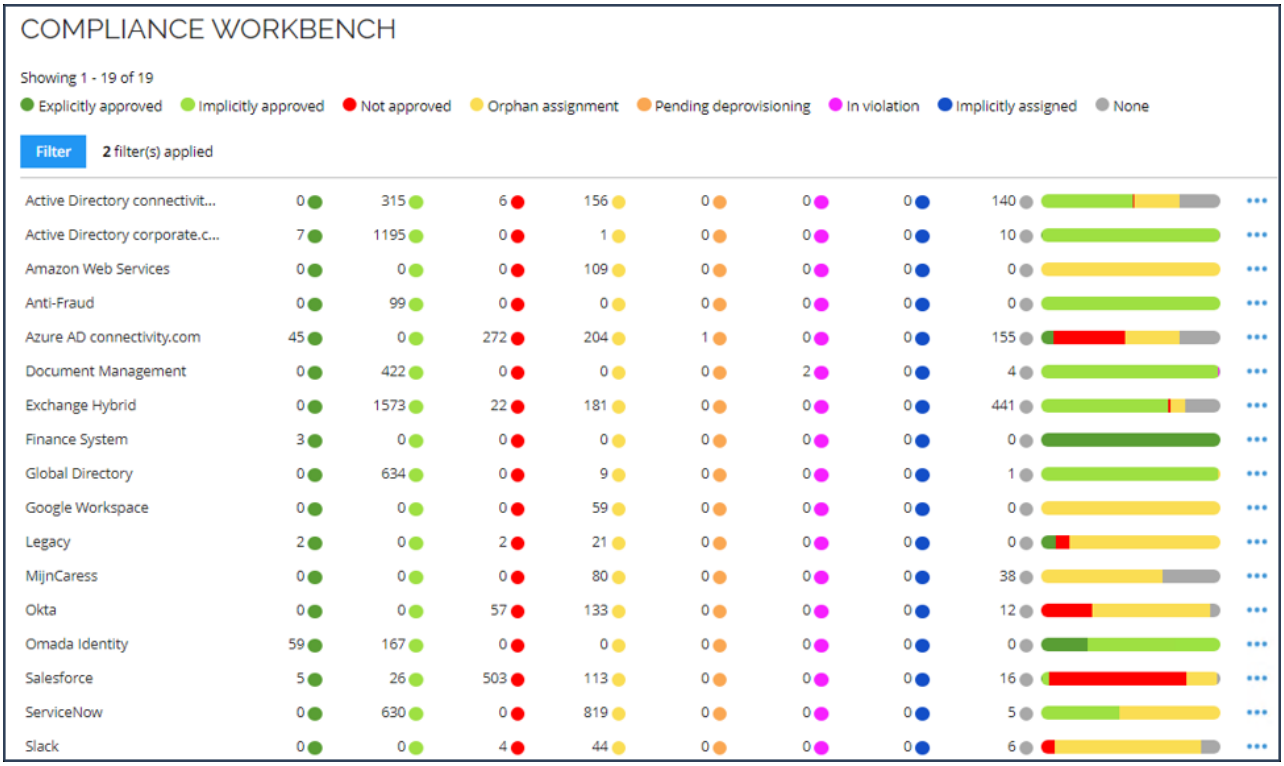

Figure 1

A Solution Delivering a Step-by-Step Approach to Access Compliance

The Omada solution provides a well-proven step-by-step approach to get you in control of the data that your enterprise collects:

Initial Preparation

The essential first step is to identify where privacy data is stored, and locate all internal and external repositories and data stores containing relevant data. These systems are then tagged as containing GDPR sensitive data for continuous monitoring.

Data import and Data Matching

An organization's HR system tends to contain critical identity data across the business. The Omada solution imports this data, making it visible in our user-friendly Compliance Dashboard, providing a fast overview of the actual state of identities and their access across the business, immediately highlighting access risks and providing reports for auditing and stakeholder purposes. This identity data is automatically matched with access data from multiple systems such as ERP software, directory services like Azure Active Directory, and more. Account ownership is also established and determined in this step, as well as surfacing orphaned, or unowned accounts to be assigned or deleted.

Initial Compliance Overview

Access risks and toxic combinations of access rights are highlighted in the Compliance Dashboard, as the data is automatically compared with built-in best practice access rules and policies and any company policies added. When the policies are applied to the data, inconsistencies and critical observation points are automatically highlighted. Non-compliant access is identified and removed. Rich reporting capabilities support both audit and business requirements, and processes are established to minimize time spent proving compliance.

Validation of Account Ownership

Orphaned or unowned accounts identified in step two are automatically sent to the assumed owners for confirmation. Accounts that cannot be confirmed are seamlessly deprovisioned or deleted, all while continuously monitored from the Compliance Dashboard.

Access Review and Certification

Certification of access verifies that users only have the access they need and when they are entitled to the access. This eliminates non-compliant and excess access, and enhances the overall security of the organization. In this step, managers review and attest to employee access rights across GDPR sensitive applications, and then follow this with automated or manual removal of excess and non-compliant access.

Validation

The compliance status are validated and can be monitored in the Compliance Dashboard. Data is continually imported into the Omada solution to validate that all required actions such as de-provisioning of non-compliant access have been taken, and companies can drill directly into the details from this dashboard to understand compliance in depth.

Continuous Compliance, Governance and Overview

The Compliance Dashboard provides continuous overview, insights into access rights for all identities, including third-party contractors, and auditable access control, allowing enterprises to confirm and certify GDPR compliance. The solution provides full-featured identity management and access governance functionalities to provide 360-degree access visibility across your hybrid IT environments for all identities.

Omada

Omada, a global market leader in Identity Governance and Administration (IGA), offers a full-featured, enterprise-grade, cloud native IGA solution that enables organizations to achieve compliance, reduce risk, and maximize efficiency. Founded in 2000, Omada delivers innovative identity management to complex hybrid environments based on our proven best practice process framework and deployment approach.

080722