Powering GDPR
Identity & Access Management in your compliance journey

25 est.1999

Years of
Evidian
IAM products

Getting up to speed

Being compliant with the General Data Protection Regulation (GDPR) is a huge challenge to undertake for any organization. This is a long and costly task that will imply numerous, and sometimes deep, changes in your business and processes. From the designation of a Data Protection Officer (DPO) to the implementation of encryption technologies to protect personal data, the GDPR will impact your organization at all levels.

When?

GDPR takes effect May 25, 2018.

Why?

To protect EU's Citizens against the loss, destruction, falsification and abusive use of their Information. The penalty for non- compliance can reach up to 4% of revenue or €20M.

Who?

Any organization involved in controlling or processing EU Citizens' personal data.

What?

All Personally Identifiable Information meaning any attribute that can be used now or in the future to identify someone, such as name, ID number, email address, political opinions or medical data.

How?

With audits (DPIA), improved governance processes and data protection measures.

The GDPR in your business

Other than a penalty for non-compliance up to 4% of revenue or €20M (Art. 83) and the designation of a Data Protection Officer (DPO) with expert knowledge of data protection law and practices (Art. 37); the GDPR introduces the concept of "Privacy by Design" as its main pillar. Governance in processes is set at the core of compliance and involves operational, organizational and also technological changes.

Give the rights

The GDPR focuses on the reinforcement of Citizen's rights. Organizations become only acting as custodians for citizens' personal data. The explicit consent of the data subject is now required for any modification or decision related to data processing (Art. 7). The user has an unlimited right to access, rectify or delete his/her personal data (Art.16). Data files must be portable (Art. 19, Art 20), and right of erasure ("right to be forgotten") is granted to the data subject (Art. 17).

State of play

The first step to compliance is to analyze your current policy and run both Risk assessment and DPIA (Data Protection Impact Assessment) to carry out personal data flows inventory and assess the risks and impacts of a breach within your organization (Art. 35).

Prove yourself

The Regulator establishes new Monitoring and Certification plans/tools to implement Codes of conduct and intended to contribute and demonstrate the proper application of the regulation (Art. 40, Art. 42).

(Re)Think your system

"Protection by Design/by Default" is one of the 3 pillars of the GDPR and focuses on technology. The principle states to reinforce the security of personal data at the time of determination of the means for processing (art. 25) and at the time of processing itself: data encryption, Data Integrity, Audit procedures and resilience, (art. 32).

Let them know

Organizations are required to notify of personal data breach to the supervisory authority not later than 72 hours after discovering it. It is also mandatory to communicate a breach to the data subject (Art. 33, Art. 34).

Data matters

The security of Processing is extended to the data processor and requires the implementation of appropriate technical and organizational measures to ensure a sufficient level of security (Art.32).

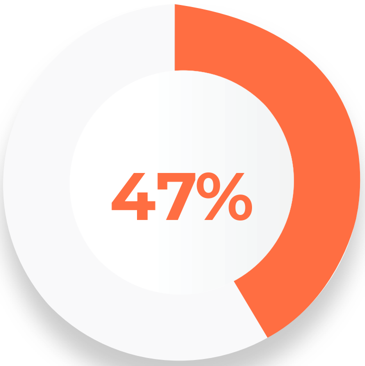
Compliance hurdles

With a start date in May 25th 2018, the GDPR replaces the former 1995's EU directive and makes it stricter, becoming one more regulation with a direct impact on organizations operational processes. For about half of the 800+.organizations identified by McAfee in their 2017 report Beyond the GDPR*, the new guidelines addressing data protection are one of the main reasons for migrating data. However, even though organizations have a good opinion of GDPR and 74% of them are seeing data protection as a competitive advantage*, getting "GDPR-Ready" stays a costly and tedious task that many organizations are reluctant to initiate and slow to execute.

The possible reasons for slow shifting or non-compliance include:

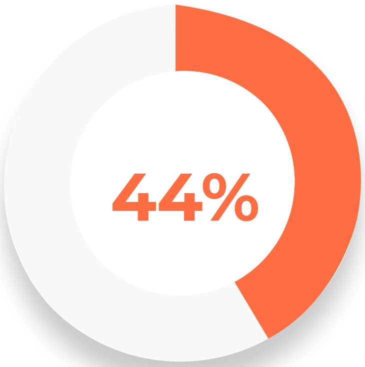
Wrong risk assessment

According to McAfee, only 47% of companies are confident about where their data are stored at all time, leaving a majority of organizations without a clear estimate of their level of risk. Based on the principle that "you cannot protect what you cannot see", most organizations will face issue when it comes to protect their data. A wrong risk assessment can lead to underestimate the need to initiate the compliance process.



Fear of stigma due to the negative effect of breaches

Same figure as above: 47% of the organizations "would rather risk a fine than admit a breach because of the negative impact a declaration of a breach would have on the brand."*



Lack of knowledge

Only 44% of companies have a complete understanding of GDPR and 15% have minimal or no understanding at all of the regulation.*

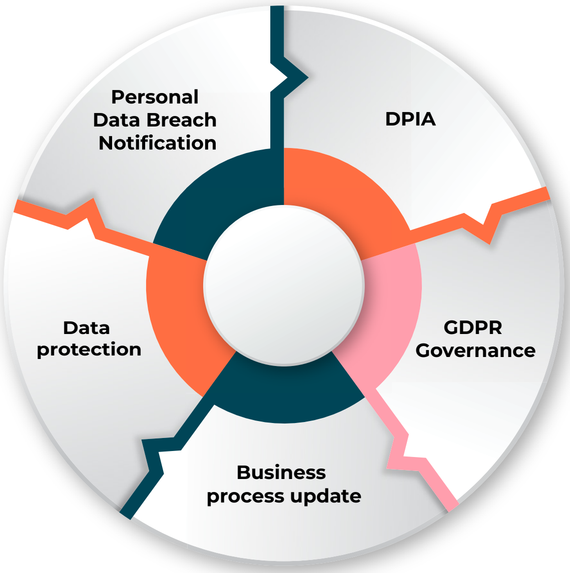
In these problems lies the difficulty for organizations to identify partners with the knowledge and skills to support GDPR readiness.

*McAfee: Beyond the General Data Protection Regulation (GDPR): Data residency insights from around the world, October 2017 Survey conducted by McAfee on 800+ senior executives from industries around the world.

Atos approach

To meet the regulatory challenges of GDPR, Atos implements a structured and continuous improvement approach.* The Group offers both GDPR consulting and solutions to answer technical questions of the regulation. Using formal tools and reports, the compliance cycle makes it easier to upgrade from the initial Risk Assessment and DPIA to an ongoing managed security service ensuring end-to-end GDPR compliance.

Atos uses its Continuous Improvement Cycle* to deal with the wide-ranging impacts of GDPR:



DPIA

GDPR specifies that a Data Protection Impact Assessment (DPIA) must be performed to analyze how the planned data processing could potentially impact the privacy of that data.

Governance

Atos helps define organizational controls, update contractual commitments where necessary and create cross-organizational responsibility matrices. Upgrades must also ensure auditability and traceability of data, both inside and outside the organization. GDPR also introduces a new role: the DPO (Data Protection Officer).

Business Process Upgrade

GDPR will also have a very arge impact on a variety f business processes. DPR rewrites previously established policies and rights, and introduces new protections standards:

The 'right to be forgotten', or which dataprocessors ill need to implement policies and processes and technologies).

The concept of consent ay be different for data processors and controllers than it has been in the past. Consent is generally more granular in GDPR, and is typically required to be clearer and less ambiguous than organizations may be used to providing.

On going Data Protection

Companies should be encrypting all personal data, no matter where it may be found. Historically, companies have shield away from encryption because of the complexities and costs of key management, but with GDPR, encryption and key management are essentially non-optional.

Notification

Atos helps define organizational controls, update contractual commitments where necessary and create cross-organizational responsibility matrices. Upgrades must also ensure auditability and traceability of data, both inside and outside the organization. GDPR also introduces a new role: the DPO (Data Protection Officer).

*Atos: Successfully meeting the challenges of GDPR; Brochure, June 2017.

While no single technology will by itself 'solve' GDPR, Identity and Access Management is explicitly or implicitly required at every stage of the compliance process.

Identity & Access Management in your compliance process

Identity and Access Management are cybersecurity tools designed to implement and sustain efficient and risk-based governance policies within your organization. As part of Atos technologies, Evidian is an Identity and Access Management (IAM) software publisher, European leader with a worldwide presence. Evidian IAM Suite is detailed as follow:

Identity Governance & Administration
Govern, manage, control user identities, mass updates, self-registration, auto activation resources provisioning risk based access rights reconciliation and access certification

Authentication Management
MFA Windows & Thin Client, Business Oriented, Kiosk & Cluster of PCs, Self-Service Password Reset

Enterprise SSO
Secure access to web and non-web applications from PC Win and Mac, tablets, mobiles Android and iOS

Web Access Management
Identity Federation, IdP & SP, SAML v2 –OIDC, Web SSO, Web Multifactor authentication

Analytics et Intelligence
Sustainable compliance, risk analysis, advanced analytics for Identity & Access

Directory Server
High-end Directory Server for enterprise and e-Business environments

High Availability
High availability with load balancing, synchronous replication and failover

Identity and Access Management

Multi-Factor Authentication

Identity Federation web authentication

ATAWAD Any time anywhere any device

Universal SSO Single Sign-On

Business Continuity software based

IAM technologies can be implemented at every stage of the GDPR Continuous Improvement Approach designed by Atos

Governance

IAM allows management, auditability and traceability of users' rights, access, and data flows. Additional analytical features help enterprises and organizations to supply proofs of compliance and provide identity intelligence when needed to the DPO and/or to supervisory authorities.

Ongoing Data Protection

IAM solutions aim to data protection "by design" with their access management & certification functionalities and implement security measures such as encryption/ pseudonymization of personal and audit data

Notification

IAM solutions can be used to notify users in case of changes in data processing and can act as key tools for consent management part of people, process & information alignment.

Business Process Upgrade

IAM solutions can be used to notify IAM plays a role in business process update in providing self-service tools for data access changes, modification and erasure requests.

IAM and GDPR

The GDPR includes no less than 99 articles, addressing multiple topics including people, processing and technology. IAM solutions are powering compliance within a defined scope, more particularly in filling the technological gap arising from the requirements for User Access and Security of Processing (GDPR articles 5 to 32).

User's Rights to be informed & Consent (Art. 5, 7, 13, 14)

- Inform when data is collected, what type of data and the reason of processing.
- Be able to consult authentication history.
- Notification for explicit consent.

User's Right to access and manage personal Data (Art. 15, 16, 17)

- Ability to access, modifiy and erase personal data.
- Possibility to delete data (from directory): « Right to be forgotten ».

Right to be informed of changes and Data portability - (Art. 19, 20)

- Confirmation mail/ SMS OTP(One Time Password) for every data modification.
- Record file for changes with consultable timeline.
- Possibility to transfer data file from a responsible to another.

Security of processing, encryption & pseudonymization - (Art. 6, 25, 32)

- Pseudonymization of audit events and data encryption requirements for «security of processing».
- Implementation of technical and organizational measures to ensure a level of security appropriate to the risk.

*Atos: Successfully meeting the challenges of GDPR, Brochure, June 2017.

Evidian IAM Suite – your path towards compliance

IAM solutions are used all over the globe to help companies manage, control and audit access to personal data and administer accounts. The task is not made easier by today's multichannel access-web, shared devices, mobile Intranet and internet application. Access from any device any time must remain in place for employees and partners while also being secure enough to protect personal data and ensure compliance with GDPR regulations.

Identity Governance

Insider threat is one of the most discussed topics in cybersecurity and remains a huge challenge for organizations. According to Verizon Enterprises, 25% of the breaches involved internal actors in 2017** This issue sets users' identity and access rights at the hearth of any security policy. The GDPR with the "protection by design" principle is explicit on using a risk-based approach to improve process governance. Evidian Identity Governance & Administration (IGA) is specialized in Identity and access rights governance and management and offers the tools to control access at a granular level. Such solutions allow DPOs and CISOs to manage the full lifecycle of users' identities and access rights. It contains a security policy engine to define the user access rights matrix. Role management and authorization are based on an extended RBAC model (Role-Based Access Control). The model assigns rights to roles and creates the user access rights matrix. An end-user portal lets users manage the identity and right lifecycle including a set of ready-to-use identity and access rights workflow processes and a set of provisioning connectors to address applications. One of the major data protection features is the Risk-driven Access Certification campaigns. Access certification work is organized inside campaigns that define the scope of users and rights. The rights to be certified, for a given population, can be reduced by limiting the rights to a chosen risk range.

The access certification campaigns are divided in two distinct stages:

· The review stage, where decisions on legitimacy of users' rights are gathered and recorded, but where no action takes place.

· The remediation stage, where revocation decisions are examined, applied or tempered.

Organizations are becoming increasingly dependent on their online and mobile applications to provide critical services to their users. They are therefore facing performance and security challenges because of issues related to their underlying directory infrastructure.

Integrated to Evidian IGA, the ID Synchronization module creates a single trusted identity repository and intelligently synchronizes your identity data sources distributed in the company. This software-based solution uses the data stored in directories, databases and even flat files. It thus creates a reliable and consistent database of all users, helping you to base your access policy on reliable data and ensure the consistency and update of all your user databases.

CISOs can use synchronization rules to create a single, centralized and modifiable repository to base your access and identity management policy and be in compliance with GDPR.

In order to comply with the Right to erasure or "Right to be forgotten" (Art. 17), ID Synchronization also enables deleting data in different directories, .

Analytics & Intelligence

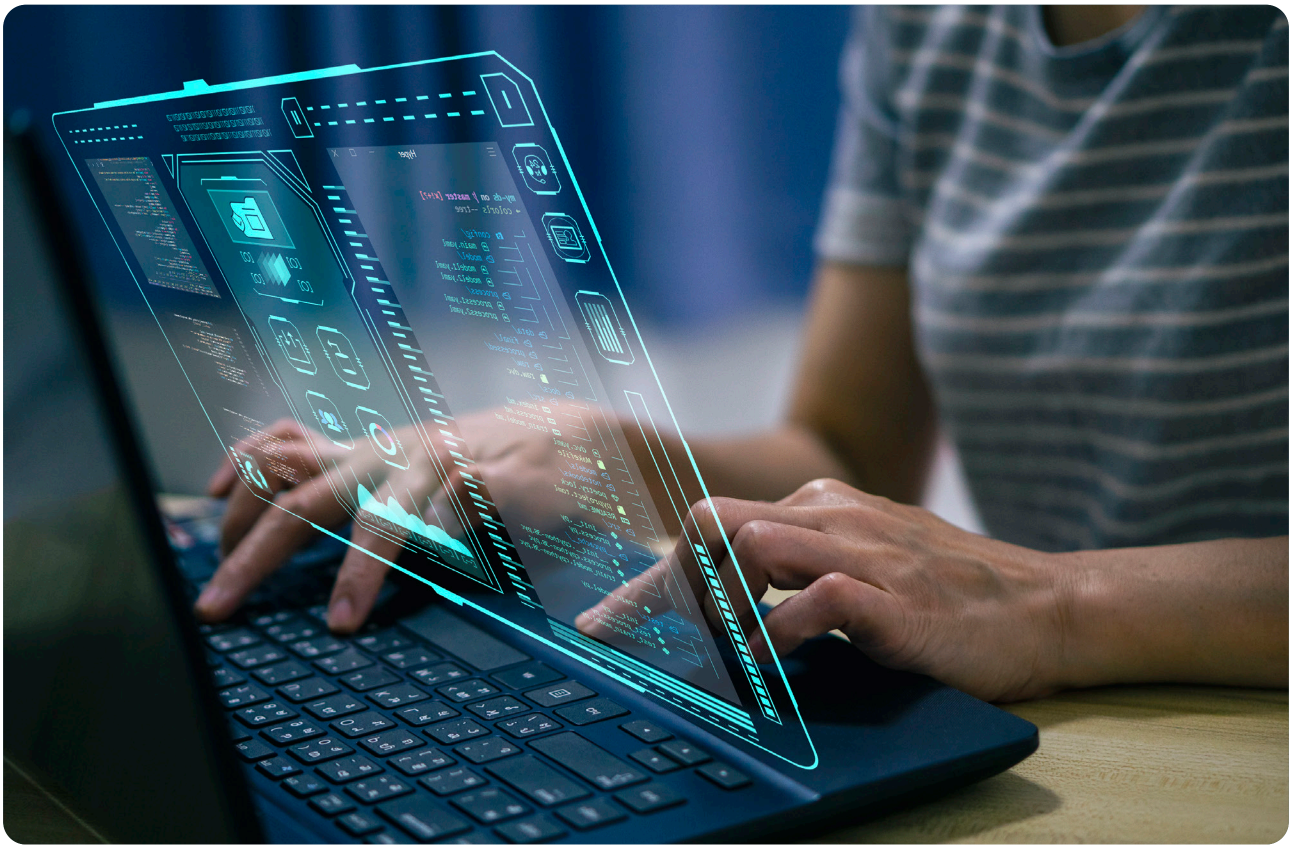
GDPR sets the DPO as responsible for the level of protection of the data processed by the system. In this role, the DPO must implement security technologies and processes to comply with GDPR but also to bring proofs of compliance when asked by auditors and regulators.

Evidian Analytics & Intelligence gives the DPO reporting capabilities on identity and access governance within his/her organization. This stand-alone completes Evidian IAM Suite with an extensive set of out-of-the-box reports and dashboards while supporting ad hoc queries for forensic requirements.

Reports vary in the level of business and technical information provided in order to address the needs of the different user types. The analysis tool highlights evolution trends for accesses and entitlements. This overall view enables the detection of suspicious events and takes a risk-driven approach to IAM.

The multidimensional analysis feature also allows security professionals to go deeper into detail and focus on a specific indicator. This search can be extended to the audit events involved with this indicator. The user can also customize the dashboards in order to better answer his/her organizational needs.

The Audit Analysis feature makes it easier to investigate by looking directly into audit events via a user-oriented layout and advanced filtering capabilities. The feature provides a business-oriented view of the audit events generated by your Identity and Access Management system, in order to find the root cause of an anomaly. The ability to filter according to the start and end dates of an event, its category, type, or other criteria is enhanced by the ability to filter also all the correlated audit events, and/or to obtain detailed information about the concerned users or objects of the policy.



Evidian Enterprise SSO

Applications become more and more criticalfor organizations. Partners, employees and now customers need a direct access to applications anywhere anytime. The choice lies between ease of access and security of data.

Evidian Enterprise SSO is part of Evidian's IAM suite. It can be connected to IGA to automate password management or provide actual access data to audit and refine the security policy. With Single Sign-On (SSO), a user only has to log in once using a secured and single authentication method to access all his applications.

With respect to GDPR requirements, Evidian Enterprise SSO manage authentication and makes sure the right data are accessed by the right people.

SSO's Strong Authentication methods reinforce security and satisfy regulatory constraints.

The login/password combination is the most common access method, especially in Microsoft environments. However, this universal "open sesame" is often not enough to protect critical resources. By creating a mandatory crossing point between a user and his applications, an organization can control the accesses efficiently.

This is why people sometimes choose to reinforce SSO with strong authentication methods. These can be deployed on all or part of the workstations; it is a common practice to protect some workstations and sensitive applications.

SSO is often a prelude to a more ambitious Identity and Access Management project. With Evidian SSO, an access policy can be idefined rigorously, validated according to a strict process and audited regularly. Employees will naturally comply with it through the existing SSO mechanism. And that is not the end of it: since SSO provides information on the actual use of applications, it is possible to continuously audit the compliance with the security policy.

IAM and Encryption

According to the GDPR, encrypted personal data is not considered as PII any longer—so if encrypted data is stolen or lost, it would not result in a violation of the regulation. Also, GDPR states that if a breach occurs, authorities may well reduce fines if appropriate controls, such as encryption, are in place.

Encryption can be performed at several levels (or layers), responding to different threats:

Companies should now be encrypting all personal data, no matter where it may be found, including*:

- Databases.
- Servers - application, file, web.
- Network - encrypting all data traffic throughout the transmission cycle.
- Storage.
- VM's.

Bull Trustway solutions generate and manage keys in an extremely secure way - in hardware, not software. This reduces 'key spread' and with it the risks of key loss. When encryption is done in software multiple copies of keys are produced, creating vulnerabilities.

HSMs not only avoid key spread but can also be used for pseudonymization or tokenization of personal data, thereby masking it and making it 'not personal'. In addition to HSMs, Atos offers advanced encryption capabilities in the form of VPNs which are certified to the highest international standards for security and are NATO compliant*.

In the case of Evidian SSO, passwords are stored encrypted in the directory that already exists in most companies, ensuring a high level of privacy with a non-reversible encryption of type AES256. For instance, the Active Directory where users are declared and throughwhich they access Windows, or Microsoft ADLDS in which is stored application data associated with the users declared in the Active Directory.

The GDPR states that if a breach occurs, authorities may well reduce fines if appropriate controls (such as encryption) are in place

Web Access Manager

With the growing role of applications within organizations, Evidian Web Access Manager (WAM) acts as single point of access to protect all your Web Applications. The solution provides security without requiring any additional software, neither on the browser side nor on the Web server side, and does not impose any specific configuration on the browser. It offers architecture for flexible Web access control.

WAM enables GDPR compliance using a set of self-service pages to allow users to access and manage directly their data. Federation protocols are also used to provide SSO in Cloud Apps, or to use external identities from Cloud Identity Providers. Web Access Manager allows enterprises to build a secure e-business platform, with a single point for enabling and managing secure access to their Web resources (pure Web or Web-enabled legacy), by filtering user access to the URLs according to user profiles.

Additionally to secure web access, Web Access Manager provides all the required features to handle authentications, authorizations, end-user interface, and a set of dedicated self-service modules for authentication activation and reactivation, lost-password in compliance with GDPR regulations.

For access to data, users will be able to access and manage their profile via selfservice pages. Changes in PIIs or in the processing will trigger notifications. The consent, core principle of the GDPR, is handled via pop-up pages. WAM allows to track audits events: logging and any user request, multi-directory administration and self-registration, multiple administration user roles, secondary accounts self-provisioning or sharing... The solution becomes a key enabler for compliance as its answers most of the technical challenges sets by the EU's GDPR;

Web Access Manager and IGA work together and offer a set of processes for identity and right governance, ready-to-use and also customizable to meet your business and GDPR requirements. IGA will drive the access policy of Web Access Manager, and it will provide a unique centralized audit and reporting integration for all your accesses.

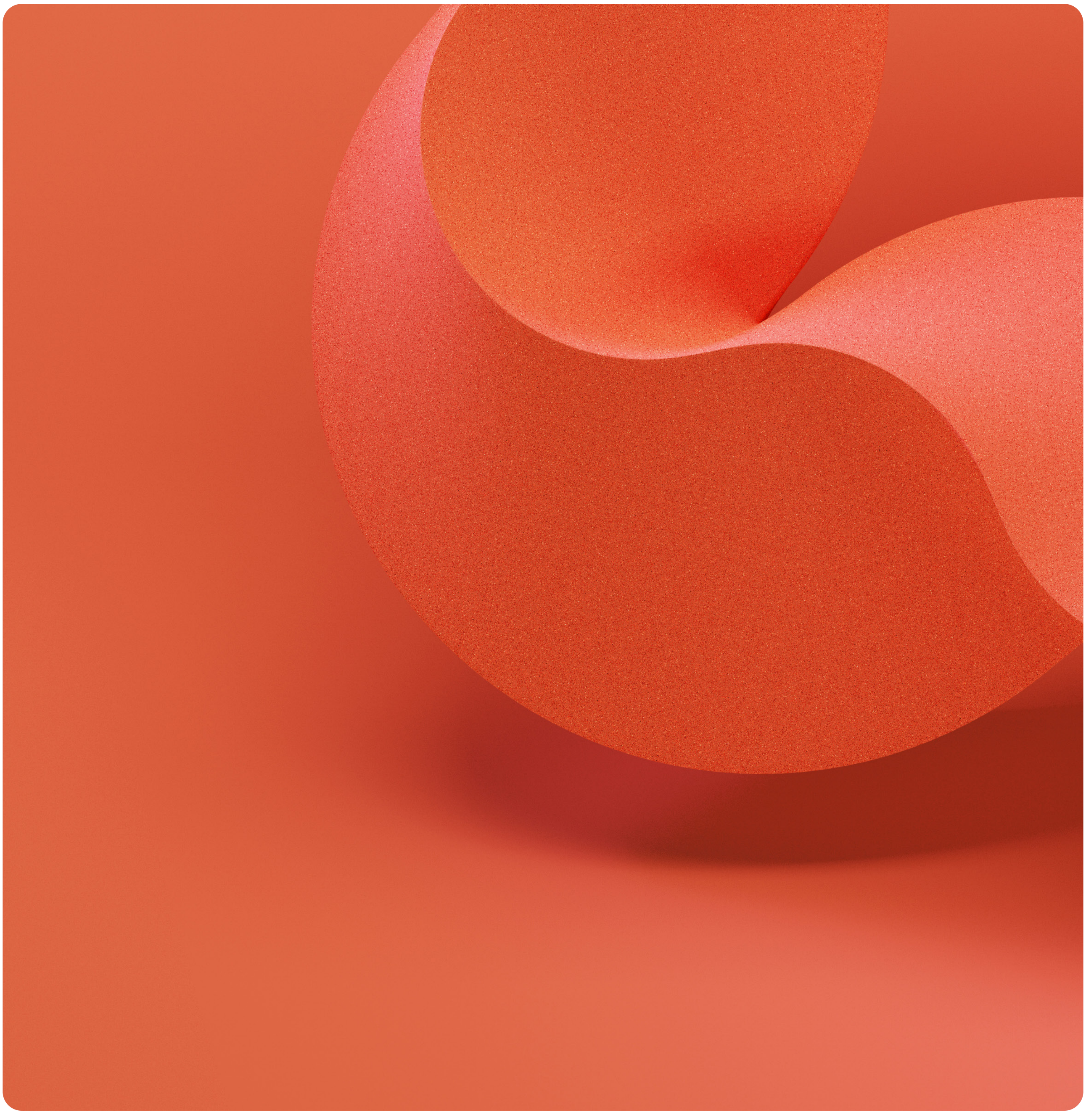
IAM compliance features

While it is clear that IAM products are essential in a context of reinforced data protection, they cannot be seen as all-inone solutions to 'solve' GDPR. IAM is one among many elements in the wide range of security, monitoring and process improvement tools such as: Microsoft Office, Privileged Access Management, Data Loss Prevention, GRC systems, Cloud Access Security Brokers, API security, etc.

We have seen how Evidian offers a suite of comprehensive IAM products to meet requirements related to User Access and Security of Processing (Art. 5 to Art. 32). To answer the growing needs of our customers for guidance and GDPR-ready software, we present our product features in the following compliance matrix:

	Evidian IAM Suite	
GDPR Requirements	Identity Governance	Access Management
Access to personal data	Access via self-service interface, Role based Access Control (RBAC) for PII and audit data	Access to data and changes records via self-service pages
Modification and Deletion	Self-service interface for modifications and deletion, automation pseudonymisation after retention period	Modifications and deletion via self-service interface Customizable modification and deletion features
Restriction of processing	Restriction request and suspension with the User Departure mode	Possibility to deactivate/ reactivate accounts Deactivation & reactivation feature
Notification & Consent	Automatic propagation with Provisioning & deprovisioning	Consent-management tool via Pop-Up
Data Portability	Data transfer via API	Export of data via Self-Service pages; possibility to receive SSO data via email, possibility to reveal passwords from SSO engine on desktop or from web portal
Security of Processing	Pseudonymization for audit events and report data; compatibility with Atos Trustway encryption systems, RBAC to audit data	Access via self-service interface, Role based Access Control (RBAC) for PII and audit data
Risk-based Governance	Risk-driven approach with Access certification campaigns	Access via self-service interface, Role based Access Control (RBAC) for PII and audit data
Audit & Monitoring	Access to audit events via the consol Reports & Dashboards to demonstrate compliance	Access via self-service interface, Role based Access Control (RBAC) for PII and audit data

With its enhanced capabilities to power GDPR, Evidian IAM Suite is a privileged partner in your compliance journey.



Connect with us

eviden.com

ECT-240711-SJ-WP-Powering GDPR: Identity & Access Management in your compliance journey