Conformité RGPD
La Gestion des Identités & des Accès au coeur de vos processus

EVIDEN

25 est.1999 Years of Evidian IAM products

Rappel

Préparer la mise en conformité avec le Règlement Général sur la Protection des Données (RGPD) est un défi dans sa mise en oeuvre et concerne toute les entreprises. Il s'agit d'une tâche longue et coûteuse synonyme de nombreux changements, parfois radicaux, au sein de votre organisation et de vos processus. De la désignation d'un Délégué à la Protection des Données (DPD) à l'intégration de technologies de chiffrement, le RGPD impactera votre entreprise à tous les niveaux.

Quand ?

Le RGPD entre en vigueur le 25 mai 2018.

Pourquoi ?

Pour protéger les citoyens européens de la perte, la destruction, la falsification et l'utilisation abusive de leurs données personnelles. La pénalité pour nonconformité peut aller jusqu'à 4 % du chiffre d'affaire ou 20 millions d'euros.

Qui ?

Toute organisation impliquée dans le contrôle ou le traitement des données à caractère personnel des citoyens de l'Union Européenne.

Quoi ?

Toutes les données à caractère personnel, c'est-à- dire les attributs pouvant être utilisés pour identifier un individu, comme le nom, le numéro d'identification, l'adresse électronique, les opinions politiques ou les données médicales.

Comment ?

Grâce à des audits (DPIA), des processus de gouvernance améliorés et des mesures de protection des données.

Le RGPD dans votre organisation

En plus d'une pénalité pour non-respect de la règlementation (Art. 83) et la désignation d'un Délégué à la Protection des Données (DPD, Art. 37), le RGPD introduit le concept de « confidentialité par la conception » comme un de ses principaux piliers. La gouvernance des processus est placée au coeur de la mise en conformité et implique des changements opérationnels, organisationnels et technologiques.

Donnez le droit

Le RGPD porte avant tout sur le renforcement des droits des citoyens. Les entreprises ne deviennent uniquement que gardiennes des données à caractère personnel des citoyens. Le consentement explicite de la personne concernée est désormais requis pour toute modification ou décision relative au traitement des données (Article 7). L'utilisateur dispose d'un droit illimité d'accès, de rectification ou de suppression de ses données (Article 16). Les fichiers de données doivent être portables (Article 19, Article 20) et le droit à l'effacement (« droit à l'oubli ») est accordé à la personne concernée (Article 17).

État des lieux

Le premier pas vers la conformité consiste à analyser votre politique actuelle et à exécuter une évaluation des risques et une analyse d'impact sur la protection des données (DPIA) pour procéder à l'inventaire des flux de données à caractère personnel et évaluer les risques ainsi que les impacts d'une violation au sein de votre organisation (Article 35).

Faites vos preuves

Le régulateur a défini de nouveaux outils de suivi et de certification pour l'application des codes de conduite. Il vise à encourager et à démontrer la bonne application du règlement (Article 40, Article 42).

(Re) pensez votre systèmer

Les concepts de « Protection dès la conception » et « conception par défaut » est l'un des trois piliers du RGPD et se concentre sur l'aspect technologique. Le principe est simple : renforcer la sécurité des données personnelles au moment du choix des moyens de traitement (Article 25) et du traitement lui-même : chiffrement des données, intégrité des données, procédures d'audit et mesures de résilience (Article 32).

Informez

Les entreprises sont tenues d'informer l'autorité de contrôle de toute violation de données personnelles dans les 72 heures. Il est également obligatoire de notifier la violation à la personne concernée (Article 33, Article 34).

Protégez vos données

La responsabilité de la sécurité du traitement est étendue au processeur de données (sous-traitant) et requiert la mise en oeuvre de mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité suffisant (Article 32).

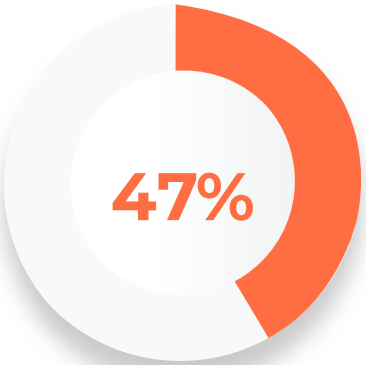
Conformité : plusieurs freins

Avec une entrée en vigueur prévue le 25 mai 2018 le RGPD vient remplacer l'ancienne directive européenne de 1995, moins stricte, et s'ajoute à la liste des règlements ayant un impact direct sur les processus opérationnels des entreprises. Pour près de la moitié de plus des 800 entreprises identifiées par McAfee dans son rapport 2017 Beyond the GDPR*, les nouvelles directives sont l'un des principaux motifs de migration de données. Cependant, même si les entreprises ont une bonne opinion du RGPD et si 74 % d'entre elles considèrent la protection des données comme un avantage concurrentiel, la mise en conformité reste une tâche coûteuse et fastidieuse que de nombreuses entreprises hésitent à initier.

Les motifs probables d'une transformation lente ou de la non-conformité comprennent :

Une mauvaise évaluation des risques

Selon McAfee, seulement 47 % des entreprises sont sûres de l'endroit où leurs données sont stockées, ce qui signifie qu'une claire appréciation des risques n'est pas possible pour la majorité des organisations. En s'appuyant sur le principe qu'«il est impossible de protéger ce qui ne se voit pas», la plupart des entreprises seront confrontées à de sérieux problèmes en matière de protection des données. Une mauvaise évaluation des risques peut conduire à sous-estimer la nécessité d'engager le processus de mise en conformité.



La peur de la stigmatisation

Même chiffre que ci-dessus: soucieuses de l'effet négatif qu'une perte de données aurait sur leur business, 47 % des entreprises « préféreraient prendre le risque d'avoir une amende plutôt que de reconnaître la perte en raison de l'impact négatif que l'annonce aurait sur la marque ».*

Un manque de connaissance

Seulement 44 % des entreprises ont une connaissance approfondie du RGPD et 15 % ont une connaissance basique ou aucune connaissance du réglement.*

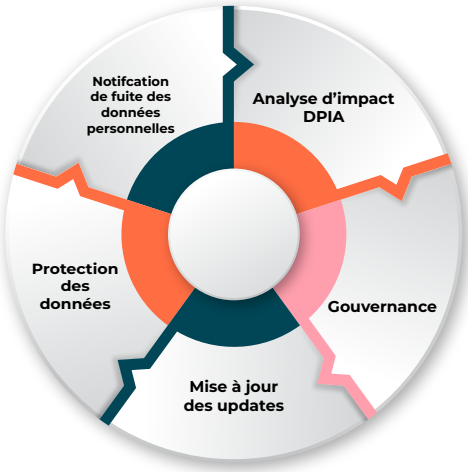
Ces problèmes sont liés à la difficulté pour les entreprises de pouvoir identifier des partenaires ayant les connaissances et les compétences requises pour les assister dans la mise en conformité RGPD.

*McAfee: Beyond the General Data Protection Regulation (GDPR): Enquête menée par McAfee auprès de plus de 800 cadres issus des secteurs 'activité dans le monde entier

L’approche d’Atos

Afin de relever les défis réglementaires liés au RGPD, Atos a mis au point une démarche d’amélioration continue. Le groupe propose à la fois des services de conseil RGPD et des solutions pour répondre aux questions techniques amenées par le règlement. À l’aide d’outils et de rapports dédiées, le cycle de conformité facilite la mise à niveau, depuis l’analyse d’impact (DPIA) vers un service de sécurité géré en continu garantissant une conformité RGPD de bout en bout.

Atos utilise son cycle d’amélioration continue* pour gérer les incidences multiples du RGPD :



Analyse d’Impact (DPIA)

Le RGPD spécifie qu’une analyse d’impact en cas de perte de données personnelles (DPIA) doit être menée pour analyser l’impact potentiel que pourrait avoir le mode de traitement sur la confidentialité de ces données.

Governance

Atos aide à définir les outils de contrôle organisationnels, met à jour les engagements contractuels si nécessaire et crée des matrices de responsabilité interorganisationnelles. Ces mises à niveau doivent également garantir l’auditabilité et la traçabilité des données, tant en interne qu’en externe. Le RGPD introduit également une nouvelle fonction : le Délégué à la Protection des Données (DPD).

Amélioration des processus

Le RGPD influencera aussi grandement de nombreux processus opérationnels. Le règlement réécrit les politiques et législations précédemment établies, et introduit de nouvelles normes sur la protection : Le « droit à l’oubli », pour lequel les responsables du traitement des données devront mettre en oeuvre des politiques, des processus et des technologies.

Le concept de onsentement pourrait évoluer et ne plus avoir la même signification que par le passé pour les responsables du traitement et les contrôleurs de données.

Dans l’ensemble, le consentement vu par le RGPD est plus granulaire ; un consentement plus clair et moins ambigu que celui proposé habituellement par les entreprises est requis.

Protection continue des données

Les entreprises s’engagent à chiffrer toutes les données à caractère personnel, quelle que soit leur provenance. Auparavant, les entreprises utilisaient peu le chiffrement en raison des complexités et des coûts liés à gestion des clés mais, avec le RGPD, ces technologies deviennent légalement incontournables.

Notification

En cas de fuite de données, le contrôleur est tenu d’informer l’autorité de contrôle de la violation dans les 72 heures. Selon ce modèle, Atos fournit les outils de détection rapide, d’escalade, de correction et de notification si et lorsque des violations sont constatées. L’enjeu consiste à aligner les individus, les processus et les informations à l’aide de solutions intelligentes capables de notifier l’utilisateur en cas d’évènement lié àses données.

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

Bien qu'aucune technologie ne soit à elle-seule une réponse au RGPD, les solutions de Gestion des Identités et des Accès sont explicitement et implicitement requises dans le processus de conformité.

La Gestion des Identités et des Accès dans votre processus de conformité

Les solutions de Gestion des Identités et des Accès (IAM - Identity & Access Management) regroupent plusieurs outils de cybersécurité conçus pour définir et mettre en oeuvre des politiques de gouvernance au sein de votre entreprise. Intégré au portefeuille technologique d'Atos, Evidian est un éditeur de solutions IAM et leader européen bénéficiant d'une présence mondiale. La suite Evidian IAM se décompose comme ce suit :

Les technologies IAM peuvent être mises en place à chaque étape du cycle d'amélioration continue Atos

Gouvernance

La suite IAM permet la gestion, l'auditabilité et la traçabilité des droits, des accès et des flux de données des utilisateurs. Des fonctionnalités analytiques supplémentaires permettent aux entreprises et aux organisations de fournir les preuves de leur conformité et des renseignements d'identité, le cas échéant, au DPD et/ou aux autorités de contrôle.

Amélioration des processus

Les solutions IAM jouent un rôle dans l'amélioration des processus opérationnels en fournissant des outils en libre-service pour modifier l'accès aux données ou exiger une modification ou l'effacement de celles-ci.

Protection continue

Les solutions IAM visent la protection des données « dès la conception » avec leurs fonctionnalités de gestion et de certification des accès et permettent la mise en oeuvre de mesures de sécurité telles que le chiffrement et la pseudonymisation des données personnelles et d'audit.

Notification

Les solutions IAM peuvent être utilisées pour avertir les utilisateurs en cas d'évènement ou de modification dans le mode de traitement de leurs données. Elles peuvent constituer des outils clés pour la gestion du consentement, dans le cadre de l'alignement des individus, des processus et des informations.

IAM et GDPR

Le RGPD ne compte pas moins de 99 articles abordant de multiples sujets notamment ceux des droits des individus, du cadre du traitement et des technologies utilisées.

Les solutions IAM permettent aux entreprises de répondre à plusieurs exigences du RGPD en comblant le vide technologique amené par le règlement en matière d'Accès des Utilisateurs et de Sécurité du Traitement (Articles 5 à 32) :

Le droit à l'information pour l'utilisateur et le Consentement (Art. 5, 7, 13, 14)

- Notification lors de la collecte de données, le type de données et le motif du traitement.
- Demande de consentement explicite par objet de traitement.
- Possibilité d'accéder à l'historique d'authentification

Le droit d'accès des utilisateurs et la gestion des données personnelles (Art. 15, 16, 17)

- Possibilité d'accéder, modifier et effacer ses données personnelles.
- Droit de supprimer des données (directement dans l'annuaire): « droit à l'oubli ».

Le droit d'être informé des changements et portabilité des données (Art. 19, 20)

- Mail de confirmation/SMS avec OTP (One Time Password)* pour chaque modification de données.
- Dossier d'historique pour chaque changement avec calendrier consultable.
- Possibilité de transférer des fichiers de données d'un responsable à un autre.

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.

La Suite Evidian IAM – votre parcours vers la conformité

Les solutions IAM sont utilisées dans le monde entier pour aider les entreprises dans la gestion, le contrôle et la vérification de l'accès aux données et aux comptes. La tâche n'est pas facilitée par les pratiques d'accès multicanal actuelles : web, appareils partagés, intranet mobile et application web. Les employés, partenaires et même les consommateurs ont besoin d'un accès permanent depuis n'importe quel appareil. Ces accès doivent être suffisamment sécurisés pour protéger les données personnelles et garantir la conformité au RGPD.

Identity Governance & Administration

Les menaces internes sont au centre des débats en matière de cybersécurité et demeurent un défi considérable pour les entreprises. Selon une étude de Verizon Enterprises, 25 % des fuites avait comme sources des acteurs internes en 2017*. Ce problème place la gestion des droits d'accès et des identités des utilisateurs au coeur de toute politique de sécurité.

Le RGPD et son principe de « protection dès la conception » est explicite sur l'utilisation d'une approche basée sur les risques pour l'amélioration de la gouvernance des processus. La solution Evidian Identity Governance & Administration (IGA) est spécialisée dans l'attribution de droits et la gestion des identités et propose des outils de contrôle à un niveau granulaire.

Ces solutions permettent aux DPD et aux RSSI de gérer le cycle de vie complet de l'identité des utilisateurs. Elles contiennent un moteur de politique de sécurité permettant de définir une matrice des droits d'accès des utilisateurs. La gestion des rôles et des autorisations sont basées sur un modèle RBAC étendu (Role Based Access Control). Le modèle attribue des droits aux rôles et crée la matrice des droits d'accès des utilisateurs. Un portail permet aux utilisateurs de gérer le cycle de vie de leurs identités et les droits associés. Celuici comprend un ensemble de workflows d'identité et de droits d'accès prêt à l'emploi ainsi qu'un ensemble de connecteurs de provisionnement pour les applications.

Les campagnes de recertification des droits d'accès basées sur le niveau de risque constituent l'un des principaux outils dans la protection des données. Les tâches de recertification sont organisées au sein de campagnes redéfinissant les utilisateurs et les droits qui leurs sont attribués. Les droits à recertifier, pour une population donnée, peuvent être limités à une certaine catégorie de risques.

Les campagnes de recertificationsont divisées en deux étapes :

- L'étape de révision durant laquelle les décisions sur la légitimité des droits des utilisateurs sont recueillies et enregistrées mais où aucune action n'est effectuée ;

- L'étape de correction durant laquelle les décisions de révocation sont examinées, appliquées ou modérées.

Les entreprises sont de plus en plusdépendantes de leurs applications web et mobiles pour fournir des services à leurs utilisateurs. Elles sont donc amenées à relever des défis de performances et de sécurité liés à l'infrastructure de leur annuaire.

Intégré à Evidian IGA, le module IDSynchronization crée un référentiel d'identités unique et fiable en synchronisant intelligemment les sources de données d'identités distribuées dans votre entreprise.

Cette solution logicielle utilise les données stockées dans les répertoires, les bases de données et également les fichiers plats. Elle crée ainsi une base de données fiable et cohérente de tous les utilisateurs et vous permet de fonder votre politique d'accès sur des données fiables. ID Synchronization garantit la cohérence et la mise à jour de toutes les bases de données utilisateur.

Les RSSI peuvent utiliser ces règles de synchronisation pour créer un référentiel unique, centralisé et modifiable sur lequel fonder leur politique de gestion des accès et des identités afin d'être en conformité avec le RGPD.

En accord avec le « droit à l'oubli »(Article 17), ID Synchronization permet aussi de supprimer des données dans différents répertoires.

Analytics & Intelligence

Le RGPD tient le DPD pour responsable du niveau de protection des données traitées dans système. Selon ce rôle, le DPD doit mettre en place des technologies et des processus de sécurité pour se conformer mais aussi pour apporter des preuves de conformité à la demande des auditeurs et des régulateurs.

Evidian Analytics & Intelligence donne au DPD des capacités de reporting sur la gouvernance des identités et des accès au sein de son entreprise. Ce module autonome complète la suite Evidian IAM avec un ensemble de rapports et de tableaux de bord prêts à l'emploi tout en prenant en charge des requêtes ad hoc pour les besoins médico-légaux.

Les rapports varient selon le niveaud'informations commerciales et techniques fournies afin de répondre aux besoins des différents types d'utilisateurs. L'outil d'analyse met en évidence les tendances d'évolutiondes accès et des droits.

Cette vue globale permet de détecter les événements suspects et d'adopter une approche de l'IAM basée sur les risques.

La fonction d'analyse multidimensionnelle permet également aux professionnels de la sécurité d'approfondir les analyses et de se focaliser sur un indicateur spécifique. Cette recherche peut être

étendue aux événements d'audit associés à cet indicateur. Le responsable peut également personnaliser les tableaux de bord afin de mieux répondre à ses besoins organisationnels.

La fonction d'analyse des évènements d'audit examine directement les événements liés au cycle de vie des utilisateurs via des fonctionnalités de filtrage avancées.

L'outil fournit une vue orientée métier des événements générés par votre système IAM afin de détecter la cause racine d'une anomalie.

Le responsable a la possibilité de filtrer en fonction des dates de début et de fin d'un événement, de sa catégorie, de son type et d'autres critères. Il est possible de filtrer par groupes d'événements d'audit corrélés et/ ou d'obtenir des informations détaillées sur les utilisateurs concernés ou les personnes soumises à la politique.

Evidian Enterprise SSO

Les applications sont de plus en pluscruciales pour les entreprises. Les partenaires, les employés et à présent les clients ont besoin d'un accès direct aux applications à tout moment et n'importe où. Le défi est de trouver l'équilibre entre facilité d'accès et sécurité des systèmes.

Evidian Enterprise SSO Authentification unique: Single Sign-On) fait partie de la suite IAM d'Evidian. Ce produit peut être intégré aux solutions IGA pour automatiser la gestion des mots de passe ou fournir des données d'accès réelles permettant de contrôler et d'affiner la politique de sécurité.

Grâce à l'authentification unique (SSO), un utilisateur se connecte via une méthode d'authentification unique et sécurisée pour accéder à toutes ses applications. Conformément aux exigences du RGPD, Evidian Enterprise SSO gère l'authentification et garantit un accès aux bonnes données par les bonnes personnes.

Les méthodes d'authentification fortes du SSO renforcent la sécurité et répondent aux contraintes réglementaires.

La combinaison connexion/mot de passe est la méthode d'accès la plus courante, en particulier dans les environnements Microsoft. Cependant, ce sésame universel est souvent insuffisant pour protéger les ressources essentielles. En créant un point de passage obligatoire entre un utilisateur et ses applications, une entreprise est en mesure de contrôler les accès de manière efficace.

C'est pourquoi certains choisissent parfois de renforcer le SSO avec des méthodes d'authentification fortes. Ces méthodes peuvent être déployées sur l'ensemble ou un groupe de postes de travail; il s'agit d'une pratique courante pour protéger certains postes de travail et applications sensibles.

Le SSO est souvent le prélude à un projet IAM plus ambitieux. Avec Evidian SSO il est possible de définir rigoureusement une politique d'accès, de la valider selon un processus strict et de la passer en revue régulièrement. Les employés s'y conformeront naturellement par le biais du mécanisme SSO existant. Et ce n'est pas tout : puisque SSO fournit des informations sur l'utilisation réelle des applications, ilest possible de contrôler en continu la conformité à la politique de sécurité.

IAM et chiffrement

Selon le RGPD, les données personnelles chiffrées ne sont plusconsidérées comme des données personnelles, si bien qu'il n'est plusnécessaire d'en déclarer la perte ou le vol. Le RGPD stipule égalementqu'en cas de fuite les autorités peuvent réduire considérablement le montant de l'amende si des mesures appropriées, comme le chiffrement, sont mises en place.

Le chiffrement peut être exécuté à plusieurs niveaux (ou couches), enréponse à différentes menaces :

Couches	Le chiffrement prévient l'accès aux données pour :
Logiciel	Administrateur d'annuaires ou de base de données
Base d'annuaires	Administrateur des Systèmes opérationnels
Système de fichiers (Diques durs)	Voleurs de disques ne disposant pas des identifiants

Avec le RGPD, le chiffrement et la gestion des clés ne sont plus facultatifs. Les données personnelles existent à tous les niveaux dans les entreprises et peuvent être transmises à tout moment 24 heures sur 24, 7 jours sur 7 ; la nécessité de chiffrer ces données, où qu'elles se trouvent, n'a jamais été aussi évidente. Les solutions IAM d'Evidian sont entièrement compatibles avec les solutions de chiffrement telles que le HSM (Hardware Security Module) Bull Trustway* :

Les entreprises s'engagent à résent à chiffrer toutes les données personnelles où qu'elles se trouvent:

· les bases de données ;

· les serveurs - applications, fichiers, web ;

· le réseau - chiffrement de tout le trafic de données tout au long du cycle de transmission ;

· le stockage ;

· Les Machines Virtuelles (VM).

Les solutions Bull Trustway génèrent et gèrent les clés de manière extrêmement sécurisée, au niveau physique et non logique. Ce système réduit la « propagation de clés » et donc les risques de perte de clé. Lorsque le chiffrement est effectué dans un logiciel, plusieurs copies de clés sont générées, ce qui crée des vulnérabilités.

Non seulement les HSM évitent la propagation des clés mais ils peuvent également être utilisés pour la pseudonymisation ou la segmentation des données à caractère personnel, les masquant et les rendant «non personnelles».

Outre les HSM, Atos propose des fonctionnalités de chiffrement avancées sous la forme de VPN certifiés conformes aux normes internationales les plus strictes en matière de sécurité et à la norme OTAN*.

Dans le cas de SSO par Evidian, les mots de passe sont stockés chiffrés dans le répertoire qui existe déjà dans la plupart des entreprises, assurant un niveau élevé de confidentialité grâce à un chiffrage irréversible de type AES256. Par exemple, le service Active

Directory où les utilisateurs sont déclarés et par lequel ils accèdent à Windows, ou les services Microsoft AD LDS où sont stockées les données d'application associées aux utilisateurs déclarés dans Active Directory.

Le RGPD stipule qu'en cas de fuite, les autorités peuvent réduire considérablement le montant de l'amende si des mesures de contrôle appropriées (comme le chiffrement) sont mises en place.

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

Web Access Manager

Face à l'importance croissante des applications au sein des entreprises, une solution Web Access Manager (WAM) constitue le seul point d'accès pour protéger toutes vos applications web. La solution garantit la sécurité de vos applications sans qu'un logiciel supplémentaire ne soit nécessaire, ni côté navigateur, ni côté serveur, et n'impose aucune configuration spécifique au navigateur. Elle fournit une architecture pour un contrôle d'accès Web flexible.

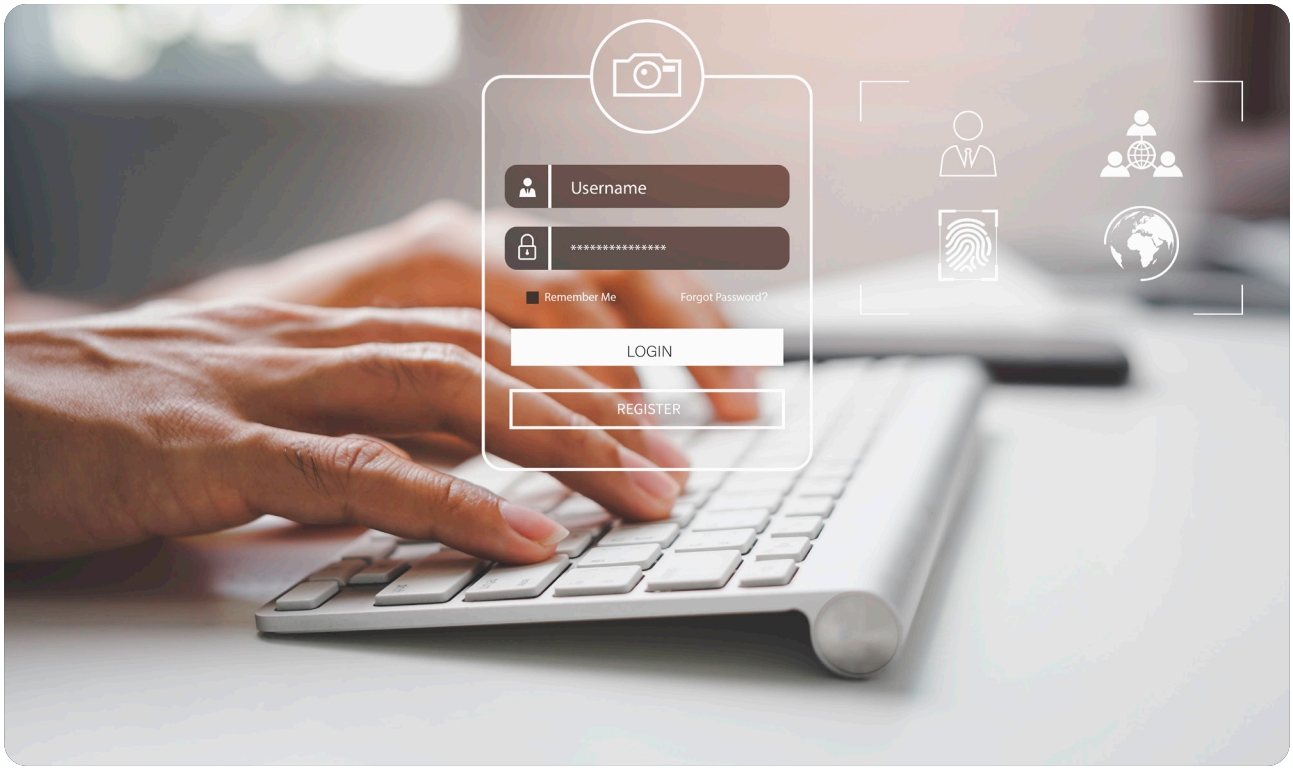
WAM favorise la conformité au RGPD à l'aide d'un ensemble de pages en libreservice permettant aux utilisateurs d'accéder à leurs données et de les gérer directement. Les protocoles de fédération sont aussi utilisés pour fournir un SSO aux applications Cloud ou pour utiliser des identités externes provenant de fournisseurs d'identité Cloud. Web Access Manager permet aux entreprises de bâtir une plateforme d'e-business sécurisée avec un seul point d'autorisation et de gestion des accès aux ressources Web (Web pur ou système hérité compatible Web), en filtrant l'accès des utilisateurs aux URL suivant leurs profils.

Outre un accès Web sécurisé, Web Access Manager fournit toutes les fonctionnalités nécessaires pour gérer les authentifications, les autorisations, et l'interface d'utilisateur final. La solution apporte un jeu de modules en libre-service dédiés à l'activation et la réactivation de l'authentification (conformément au RGPD) et à la perte de mot de passe.

Concernant l'accès aux données, principe de base du RGPD, les utilisateurs seront en mesure d'accéder à leur profil et de le modifier via les pages en libre-service. Les modifications apportées aux renseignements personnels ou au traitement déclencheront des notifications. Finalement, WAM fait office d'outil de gestion automatique du consentement via des pages pop-up.

Le WAM permet de suivre les événements d'audit : suivi et pistage de toutes les requêtes d'utilisateur, administration de plusieurs répertoires et auto-enregistrement, rôles d'utilisateur à administration multiple, auto-allocation ou partage des comptes secondaires...

La solution devient un élément clé de la conformité car elle répond à la plupart des défis techniques posés par le RGPD européen. Les services Web Access Manager et IGA travaillent ensemble et proposent des processus de gouvernance des droits et des identités prêts à l'emploi et personnalisables pour répondre aux besoins de votre entreprise et aux exigences réglementaires. IGA détermine la politique d'accès de Web Access Manager et fournira un audit unique centralisé et un reporting intégré de tous les accès.



Fonctionnalités de conformité IAM

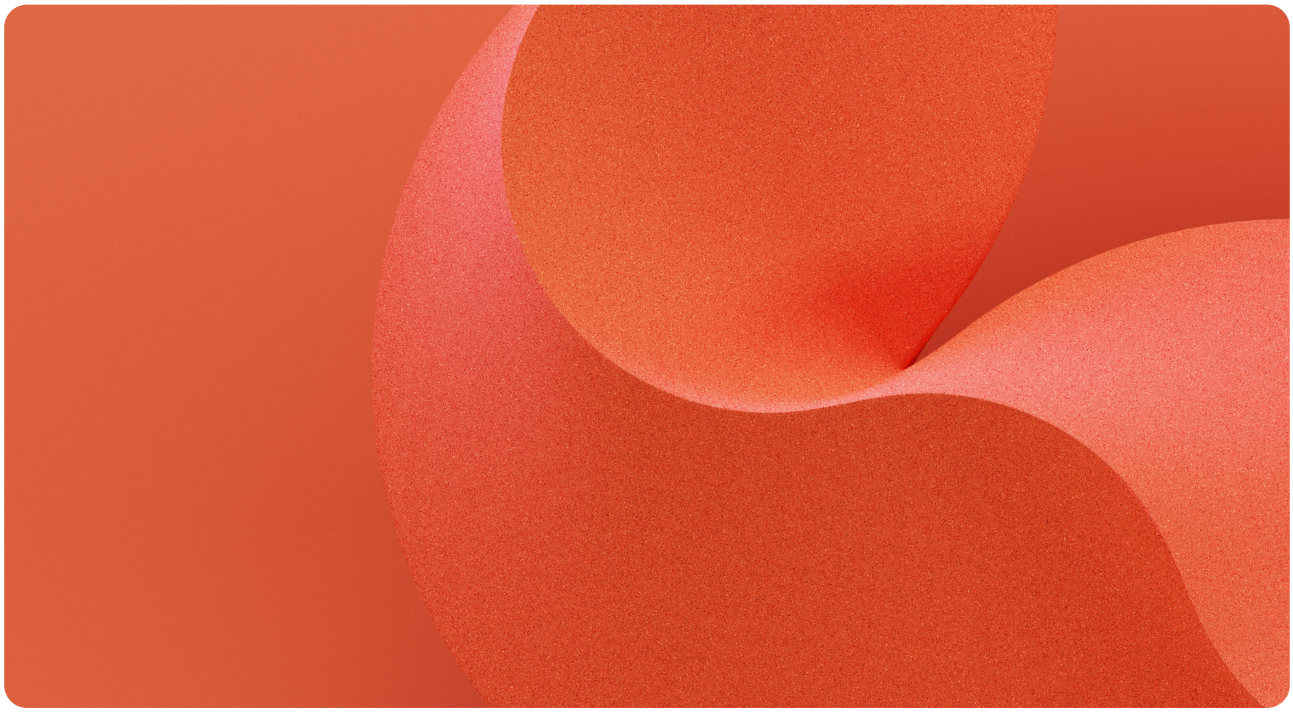
S'il est évident que les produits IAM sont essentiels dans un contexte de protection renforcée des données, ils ne peuvent pas être considérés comme des solutions tout-en-un pour «résoudre» le RGPD. L'IAM est l'un des nombreux éléments parmi la gamme d'outils de sécurité, de surveillance et d'amélioration des processus tels que : Microsoft Office, Gestion des Accès et Comptes à Privilèges (PAM/PIM), prévention des pertes de données (Data Loss Prevention), Gestion de risque et Conformité (GRC), Cloud Access Security Brokers, sécurité API, etc.

Nous avons montré comment Evidian propose une suite de produits IAM complets pour répondre aux exigences liées aux l'accès des utilisateurs et à la sécurité du traitement (Articles 5 à 32). Pour répondre aux besoins croissants de nos clients en matière d'expertise et de logiciels adaptés au RGPD, nous présentons les caractéristiques de nos produits dans une matrice de conformité :

	Suite Evidian IAM	
Exigences GDPR	**Gouvernance des Identités**	**Gestion des Accès**
Accès aux données personnelles	Accès via une interface libre-service, modèle RBAC (contrôle d'accès basé sur rôle) pour l'accès aux données personnelles et d'audit	Accès aux données personnelles et d'audit via des pages libre-service
Modification et suppression	Interface libre-service pour modifications et suppression, pseudonymisation automatique après une période de rétention	Modifications et suppression via une interface libre-service, fonctionnalités de modification et de suppression personnalisables
Restriction du traitement	Demande de restriction et suspension avec le mode 'Départ de l'utilisateur'	Fonctionnalités de désactivation et réactivation
Notification & consentement	Propagation automatique lors du provisionnement et déprovisionnement	Outil de gestion du consentement via pop-up
Portabilité des données	Transfert de données via API	Export de données via des pages libre-service ; possibilité de recevoir ses données SSO par e-mail, possibilité de révéler les mots de passe du moteur SSO sur le bureau ou depuis le portail Web
Sécurisation du traitement	PPseudonymisation pour les événements d'audit et les données de rapport ; compatibilité avec les systèmes de chiffrement Atos Trustway, modèle RBAC pour l'accès aux données	Pseudonymisation des événements d'audit, compatibilité avec les systèmes de chiffrement Atos Trustway
Gouvernance basée sur les risques	Approche appropriée au niveau de risque avec des campagnes de recertification des accès	Méthodes d'authentification fortes pour un accès à différents niveaux de risque

Audit & surveillance	Accès aux événements d'audit via la console Rapports et tableaux de bord pour prouver la conformité	Accès aux événements d'audit (jour/semaine/ mois) Rapports dédiés et tableaux de bord Accès au fichier d'enregistrement des événements d'audit

Avec ses fonctionnalités améliorées permettant la mise en action du RGPD, la suite Evidian IAM est un partenaire privilégié dans votre processus de conformité.



Connect with us

eviden.com