

ManageEngine 

E - B O O K

Les réglementations sur la confidentialité des données et leur impact : Une vue d'ensemble

Table des matières

1. Des préoccupations croissantes en matière de protection de la vie privée dans le monde entier	02
2. Besoin urgent de réglementations sur la confidentialité des données	03
3. Réglementation de la confidentialité des données	05
i. Règlement général sur la protection des données (RGPD)	05
ii. Loi californienne sur la protection de la vie privée des consommateurs (CCPA)	06
iii. Loi californienne sur la protection de la vie privée (CPRA)	06
4. L'impact de la réglementation sur la confidentialité des données sur les entreprises	07
5. La relation entre les réglementations sur la confidentialité des données et l'IAM	08
i. Rester en conformité avec les réglementations sur la confidentialité des données grâce à l'IAM	08
ii. L'impact des réglementations relatives à la confidentialité des données sur l'évolution des solutions d solutions IAM	09
iii. Ce qu'une solution IAM doit avoir pour rester conforme.....	09
6. Gestion des changements induits par la réglementation sur la confidentialité des données	10



Les données sont la clé d'une transformation numérique réussie, et il a souvent été observé que les entreprises qui traitent et manipulent efficacement les données se démarquent des autres. Avec une approche axée sur les données, les entreprises gagnent la capacité de faire face aux défis de manière plus subjective et informée. Une analyse précise des données peut également faire passer les stratégies commerciales d'une simple réactivité à une prédiction. Plus de 2,5 quintillions d'octets de données sont générés chaque jour, et on estime que 90% des données mondiales ont été collectées au cours des deux dernières années seulement.

Selon le McKinsey Global Institute, les organisations guidées par les données ont 23 fois plus de chances d'acquérir des clients, 600% plus de chances de les conserver et 19 fois plus de chances d'être rentables. L'exploitation efficace des données permet aux organisations de prendre des décisions éclairées et d'améliorer l'expérience client. En fin de compte, cela se traduit par des clients satisfaits qui reviennent toujours.



01 Des préoccupations croissantes en matière de protection de la vie privée dans le monde entier

Depuis longtemps, les entreprises collectent les données de leurs clients à leur insu et sans leur consentement. Comme le véritable objectif de cette collecte de données est caché aux consommateurs et dissimulé dans les conditions générales, de nombreux consommateurs cliquent sur la case "accepter les conditions générales" sans en comprendre l'impact. Ils ont cédé une grande partie de leurs informations à des entreprises sans même s'en rendre compte.

Les données des utilisateurs ont une valeur marchande énorme, ce qui amène les entreprises à mettre en commun et à vendre les données personnelles des individus à grande échelle. Les sites web du monde entier collectent et stockent ces données sous plusieurs formes

- **Données personnelles**, notamment le nom, le sexe, l'adresse IP et la localisation d'une personne.
- **Données d'engagement**, comme les messages texte, les courriels, les applications mobiles et les pages de médias sociaux.
- **Données comportementales**, telles que l'historique des achats et les informations sur l'utilisation des produits.
- **Les métriques des données comportementales**, telles que la satisfaction des consommateurs, les critères d'achat et la désirabilité des produits.

On a constaté que les géants mondiaux de la technologie conservent plus d'informations sur les utilisateurs que ce dont ils ont besoin, et ils prétendent souvent utiliser ces données pour personnaliser le contenu et améliorer l'expérience des utilisateurs. Mais le fait est que ces entreprises vendent ces données aux annonceurs, aux éditeurs et à d'autres tiers.

Par exemple, les performances des publicités concernant un utilisateur particulier sont partagées avec les annonceurs, qui personnalisent ensuite leurs publicités en fonction du comportement de l'utilisateur afin de l'hypercibler pour le convertir. Les informations de localisation des utilisateurs sont également couramment partagées et utilisées pour afficher des publicités locales personnalisées. En réaction, **86% des Américains** ont tenté d'effacer leurs empreintes numériques et de sécuriser leurs informations personnelles disponibles en ligne en raison de préoccupations liées à la protection de la confidentialité.

Les données désignent toute information susceptible d'identifier personnellement une personne. La confidentialité des données fait référence à la protection des données en termes de collecte, d'utilisation et de distribution.

L'objectif est de sécuriser plusieurs types de données, comme les données de première partie (informations que les marques et les créateurs collectent directement auprès de leurs consommateurs), les données de seconde partie (informations acquises auprès de l'entreprise qui les a collectées) et les données de tiers (informations achetées auprès d'autres sources, comprenant idéalement des données de différentes sources regroupées en un seul endroit).

À mesure que les consommateurs seront mieux informés de leurs droits en matière de données et de la manière dont celles-ci sont utilisées, ils exigeront que celles-ci soient sécurisées.

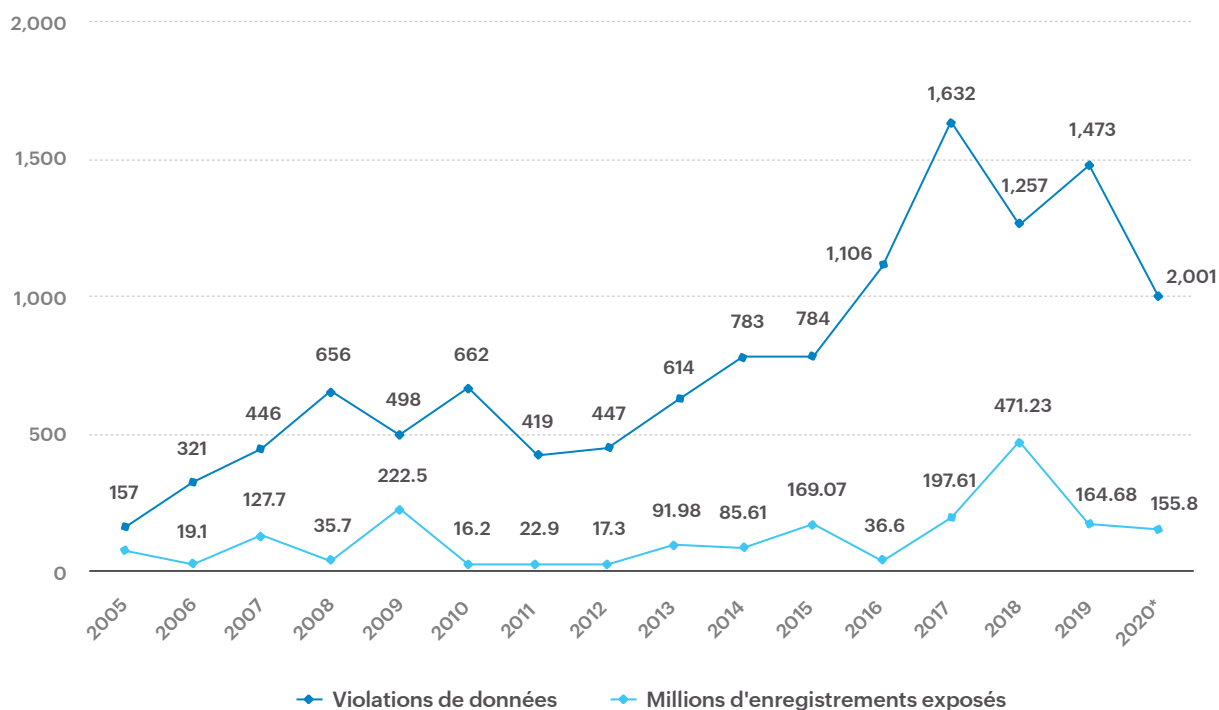
Soixante-dix-neuf pour cent des Américains ont exprimé des inquiétudes quant à la manière dont leurs informations personnelles sont utilisées par les entreprises. Face à l'inquiétude croissante de la population quant à l'utilisation abusive des données, il est nécessaire de mettre en place une réglementation mondiale des données axée sur le renforcement de la vie privée des consommateurs et de la protection des données.

02 **Besoin urgent de réglementations sur la confidentialité des données**

Au cours des dernières années, l'utilisation abusive des données s'est étendue bien au-delà des publicités effrayantes qui ciblent des clients individuels. L'attention accrue portée aux préoccupations en matière de vie privée est motivée par les nombreuses attaques de cybersécurité qui ont conduit à des violations massives de données personnelles. Les violations de données coûtent du temps et de l'argent aux organisations. Elles se traduisent par une perte de données, qui peut être compensée dans une certaine mesure, et par une atteinte irréversible à leur réputation, qui se traduit finalement par la perte de clients. La fidélité des clients est presque impossible à regagner.

L'augmentation mondiale des attaques par ransomware est une source d'inquiétude majeure pour les entreprises. Selon l'AICPA, près de la moitié des Américains s'attendent à être victimes d'une fraude au cours de l'année prochaine. Statista estime que le coût moyen mondial d'une violation de données en 2021 était de 4,24 millions de dollars, soit une forte hausse de 10 % par rapport à 2020. Avec l'économie la plus puissante du monde, les États-Unis sont la principale cible des cyberattaques et ils présentent le coût total moyen le plus élevé d'une violation de données : 9,05 millions de dollars en 2021.

Nombre annuel de violations de données et d'enregistrements exposés aux États-Unis (en millions)



Le graphique ci-dessus indique le nombre de violations de données et d'enregistrements exposés aux États-Unis entre 2005 et 2020. Ces attaques rappellent de manière urgente la nécessité d'une réglementation mondiale en matière de confidentialité des données. Ces violations de données à grande échelle, qui entraînent la perte d'informations sensibles, d'argent et parfois de vies humaines, ont eu un impact sur les pays du monde entier.

Ainsi, les gouvernements commencent à réglementer la collecte et la gestion des données par les entreprises. La confidentialité étant déclarée comme un droit fondamental par la déclaration universelle des droits de l'homme des Nations unies, il existe une obligation immédiate de préserver le droit à la confidentialité.

03 Réglementation de la confidentialité des données

Afin de renforcer les mesures de confidentialité et de sécurité des données, les gouvernements du monde entier ont commencé à adopter des lois pour contrôler les types de données qui peuvent être collectées sur les utilisateurs, la manière dont elles peuvent être utilisées, et la manière dont elles doivent être stockées et protégées. Ces réglementations sont conçues pour permettre aux consommateurs de contrôler leurs données.

Un mandat important consiste à demander le consentement des consommateurs chaque fois que leurs données sont collectées. Les conditions générales doivent également être facilement compréhensibles pour les consommateurs. Ces lois exigent des entreprises qu'elles donnent à leurs utilisateurs le droit d'accéder à leurs données, de les emporter et de les utiliser ailleurs, et de demander aux entreprises d'effacer complètement leurs données personnelles de leurs dossiers.

Plus de 137 pays ont mis en œuvre des lois sur la confidentialité des données afin d'empêcher l'utilisation abusive des données personnelles. Voici quelques-unes des principales réglementations sur la confidentialité des données à travers le monde :



RGPD

i. Règlement général sur la protection des données (RGPD)

Considéré comme l'un des règlements les plus importants en matière de confidentialité, le RGPD a été adopté en 2018. Il a un impact sur toutes les organisations qui traitent des données personnelles et qui opèrent au sein de l'UE, ou qui vendent des biens à cette dernière. Tel que défini par le RGPD, le traitement des données couvre également les types d'utilisation possibles et les processus impliqués, comme la collecte, le stockage, l'extraction, la modification et la destruction des données.

Le RGPD exige également des analyses d'impact sur la protection des données pour tout traitement susceptible de mettre en danger les droits de la personne concernée. Afin de limiter la collecte à la source même, le RGPD insiste sur la minimisation des données, la limitation de la finalité et la limitation du stockage. La violation de ces directives peut entraîner des amendes allant jusqu'à 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaires mondial total de l'entreprise de l'exercice précédent, le montant le plus élevé étant retenu.



CCPA

ii. Loi californienne sur la protection de la vie privée des consommateurs (CCPA)

La CCPA couvre les résidents de Californie et s'applique aux entreprises dont le revenu annuel brut est supérieur à 25 millions de dollars, à celles qui achètent, reçoivent ou vendent les informations personnelles de 50 000 résidents, ménages ou appareils ou plus, et à celles qui tirent 50 % ou plus de leur revenu annuel de la vente d'informations personnelles de résidents.

La CCPA exige que les entreprises diffusent un message de "notification lors de la collecte" pour informer les consommateurs de la collecte de leurs informations personnelles et de son objectif. Elle comporte également une section entière consacrée à la réglementation du fonctionnement des courtiers en données. La violation de la réglementation peut entraîner des amendes allant de 2 500 dollars pour une violation non intentionnelle à 7 500 dollars pour une violation intentionnelle.



CPRA

iii. Loi californienne sur la protection de la vie privée (CPRA)

Introduite en 2020 comme une version plus complète de la CCPA, la CPRA vise à accroître les droits des consommateurs en termes de confidentialité et de sécurité des données. Avec une nouvelle catégorie appelée "informations personnelles sensibles" (SPI), la CPRA exige que les entreprises fournissent une protection supplémentaire en fonction de la sensibilité des informations personnelles. Elle prévoit des exigences actualisées en matière de divulgation, de limitation de la finalité et d'inclusion et d'exclusion.

En plus d'étendre les lois de la CCPA, la CPRA introduit quatre nouveaux droits pour les consommateurs : le droit de corriger des informations personnelles inexactes, le droit de limiter l'utilisation et la divulgation de SPI, le droit d'accéder à des informations sur la prise de décision automatisée, et le droit de refuser la technologie de prise de décision automatisée. Ces nouveaux droits protègent les clients contre l'utilisation abusive des données par les technologies axées sur l'IA.

Outre ces trois règlements, il existe plusieurs autres lois concernant le droit à la vie privée des clients et la collecte de données. Le Health Insurance Portability and Accountability Act (HIPAA) régit le secteur de la santé et empêche la collecte et le partage illégaux des informations de santé des patients sans leur consentement préalable. La loi Gramm Leach-Bliley (GLBA) s'applique aux institutions financières pour garantir la sécurité et la confidentialité des informations financières des clients concernant leurs prêts, leurs statuts financiers, leurs transactions, etc.

La norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) garantit la sécurité et la légalité des transactions par carte de crédit. Le Fair Credit Reporting Act (FCRA) réglemente la collecte et l'utilisation des informations de crédit des particuliers. Pour garantir la sécurité des enfants, la loi sur la protection de la vie privée en ligne des enfants (COPPA) régit la collecte d'informations sur les mineurs.

04 L'impact de la réglementation sur la confidentialité des données sur les entreprises

Les réglementations sur la confidentialité des données permettent aux entreprises d'optimiser leurs pratiques de traitement des données et de faciliter les transactions numériques transfrontalières. Mais elles obligent les entreprises à renforcer leurs technologies de gestion des données afin de se doter de solides capacités numériques. L'idée centrale est de créer des modèles commerciaux conformes et efficaces qui protègent la confidentialité des données des clients.

Les entreprises peuvent s'attendre à deux changements majeurs à la suite de la réglementation sur la confidentialité des données. Premièrement, la confidentialité deviendra une attente fondamentale des clients. Deuxièmement, la transparence des politiques de confidentialité ne sera plus facultative. Les consommateurs étant de plus en plus conscients des politiques en matière de données et les gouvernements imposant des exigences en matière de protection de la vie privée, les entreprises apprennent que la mise en œuvre de politiques de protection de la vie privée peut créer un avantage commercial en leur permettant de garder une longueur d'avance.

D'un autre côté, d'un point de vue commercial, le coût de la mise en conformité va grimper en flèche, car les organisations devront peut-être affecter du personnel et des ressources financières distincts uniquement pour se conformer à ces réglementations. Avec des pénalités élevées pour non-conformité et le risque potentiel de perdre la valeur de leur marque, les organisations seront obligées de payer pour se mettre en conformité. L'autre impact sur les entreprises est la surréglementation des politiques. Les clients deviennent accablés par des formulaires de consentement interminables pour chaque traitement de données, ce qui enlève la facilité d'utilisation des plateformes en ligne.

Avec la mise en œuvre généralisée des réglementations à travers le monde, les entreprises risquent de ne pas se conformer et de voir leurs investissements augmenter. De nombreux cadres sont en cours d'élaboration pour aider les entreprises à trouver la bonne combinaison entre un investissement optimal et la conformité aux réglementations. Le [cadre de gouvernance de la sécurité des données de Gartner](#) décrit comment les entreprises peuvent satisfaire aux exigences légales tout en traitant les données des consommateurs.

Le cadre suggère les étapes suivantes

- Identifier et se concentrer sur les données qui sont impactées par les réglementations de conformité en matière de confidentialité des données.
- Développez des évaluations d'impact pour la protection des données et administrez-les périodiquement tout en gardant toutes les parties prenantes de l'entreprise impliquées.
- Configurer les contrôles technologiques pour ramener le risque à un niveau acceptable.
- Revoir les politiques de sécurité systématiquement et chaque fois que les risques commerciaux changent.

05 La relation entre les réglementations sur la confidentialité des données et l'IAM

Les réglementations sur la confidentialité des données ont fondamentalement changé la manière dont les entreprises traitent les informations personnelles des consommateurs. Toute information relative à un individu et pouvant être utilisée pour l'identifier doit être protégée. L'objectif ultime est d'éviter l'utilisation abusive des données personnelles en contrôlant la collecte des données et en prévenant les violations de données. Avec l'expansion constante des entreprises, il devient forcément difficile de garantir le respect de toutes les lois.

i. Rester en conformité avec les réglementations sur la confidentialité des données grâce à l'IAM

Les solutions IAM offrent aux entreprises des fonctions de sécurité très fiables pour les aider à respecter les exigences strictes de conformité des lois sur la confidentialité. Grâce à l'IAM, les entreprises peuvent facilement respecter les mandats stricts et empêcher les traitements illégaux lorsqu'elles traitent les données privées des clients. Une solution IAM centralisée fournit des mesures de sécurité telles que MFA, PAM et des politiques d'accès basées sur l'organisation. Grâce à ces mesures, les entreprises peuvent s'assurer que seuls les utilisateurs autorisés accèdent aux données sensibles.

En outre, des fonctionnalités telles que l'authentification basée sur les rôles et les méthodes de moindre privilège renforcent l'accès interne au sein de l'entreprise. Les fonctions

d'authentification fédérée facilitent l'octroi et la révocation de l'accès, une fonction très utile lors de l'intégration des nouveaux employés et des travailleurs temporaires. Les options de cryptage avancées et les mesures de protection contre les menaces fournies par les solutions IAM peuvent être déployées pour protéger les données stockées sur site et dans le cloud.

À l'heure où les lois sur la confidentialité des données sont renouvelées pour couvrir les opérations centrées sur le cloud, de telles fonctionnalités permettront aux entreprises de rester sur la bonne voie avec une perturbation minimale des opérations. Les solutions IAM sont également conçues pour lutter contre plusieurs types de cyberattaques, comme le phishing, les logiciels malveillants, les virus et les attaques DDoS. Ainsi, les entreprises qui déploient des solutions IAM pour gérer et exécuter leurs processus de sécurité seront en mesure de rester en conformité avec les lois sur la confidentialité des données.

ii. L'impact des réglementations relatives à la confidentialité des données sur l'évolution des solutions d solutions IAM

Avec l'introduction de réglementations strictes en matière de confidentialité des données, les solutions IAM doivent évoluer pour répondre à leurs exigences. L'une des raisons pour lesquelles les lois sur la confidentialité des données sont pertinentes pour le développement éthique des solutions IAM est que des facteurs tels que les informations d'identification des utilisateurs sont basés sur des informations personnelles des utilisateurs, comme les empreintes digitales, les emplacements géographiques et les caractéristiques des appareils personnels.

Si une organisation choisit d'adopter une solution IAM, il est absolument nécessaire qu'elle garantisse la conformité avec toutes les lois sur la confidentialité des données dès le stade du développement. Si des fonctionnalités telles que le MFA et le PAM assurent la sécurité au niveau de l'utilisateur, les protocoles qui les exécutent à partir de l'arrière-plan doivent également utiliser des algorithmes avancés et une technologie de pointe. doivent également utiliser des algorithmes et des techniques de cryptage avancés pour rester sécurisés. Tous les processus et applications doivent être maintenus à jour.

iii. Ce qu'une solution IAM doit avoir pour rester conforme

Au fur et à mesure que les solutions IAM sont développées et mises à jour, elles doivent rester conformes à la législation applicable en matière de confidentialité des données. Voici quelques points que les entreprises doivent prendre en compte pour créer des solutions IAM juridiquement durables :



Assurer la conformité en matière de confidentialité et de sécurité des données dès le début de la de développement et réévaluer tout au long de la durée de vie du produit.



En termes de collecte et de gestion des données personnelles des clients, ne collectez que ce qui est nécessaire et ne les conservez que le temps nécessaire. Le stockage sécurisé et l'élimination sécurisée des données sont tout aussi importants. Veillez à ce que les données sensibles ne soient accessibles qu'aux personnes qui en ont besoin.



Évitez autant que possible de stocker des données sensibles. Au lieu de cela, ne collectez ces données qu'en cas de besoin.



Gardez un œil attentif sur les solutions de sécurité et les outils d'exploration de données pilotés par le ML et l'IA. Empêchez les accès non autorisés en réduisant les permissions et en limitant l'accès aux ressources.

06 Gestion des changements induits par la réglementation sur la confidentialité des données

L'idée fausse la plus répandue concernant les réglementations sur la confidentialité des données est qu'elles n'ont d'impact que sur le service juridique. Mais ce que l'on oublie souvent, c'est que tous ceux qui travaillent avec des données dans une entreprise doivent être au courant de ces réglementations et s'y conformer. De nombreux experts étudiant ces réglementations proposent que cela a moins à voir avec la gestion des données qu'avec les processus de gestion du changement. Les entreprises doivent repenser et restructurer la manière dont elles traitent les données des clients. La meilleure façon de mettre en œuvre ces réglementations sur la confidentialité dans une entreprise est de mettre en place une gestion du changement.

Investir dans les technologies d'analyse et d'automatisation devrait être la première étape de toute entreprise vers la mise en place d'un système robuste et conforme qui garantit le respect de toutes les réglementations en matière de confidentialité. La plupart des lois sur la confidentialité des données mentionnent les droits d'accès des clients, ce qui signifie essentiellement qu'un client peut à tout moment demander une copie de toutes les données recueillies à son sujet, ou que ses données soient supprimées.

Les entreprises auront besoin de solutions numériques et automatisées pour répondre efficacement à ces demandes. Par exemple, des formulaires qui remplissent automatiquement les détails nécessaires, des outils de guidage sur le bureau ou des assistants virtuels rendront le processus plus rapide avec un minimum d'effort manuel. Les risques de mauvaise manipulation des données s'en trouveront réduits.

Voici quelques pratiques que les organisations devraient suivre pour gérer efficacement les changements apportés par la réglementation :

- Pour garantir la conformité avec toutes les lois applicables en matière de données, les organisations doivent en avoir une connaissance actualisée. Faire appel à un conseiller juridique à cette fin permettra de responsabiliser et de mettre en place un processus rigoureux.
- Il est essentiel d'auditer et d'évaluer en permanence les contrôles de l'entreprise pour mettre en place un système capable de résister aux changements complexes de la réglementation sur la protection de la confidentialité.
- Chaque organisation est unique, et il n'existe donc pas de solution unique pouvant être appliquée à toutes. Il est essentiel pour une entreprise de comprendre la nature des données qu'elle traite et ses fonctions avant de chercher une solution. Ce qui fonctionne pour une entreprise dans un secteur donné peut ne pas fonctionner pour une autre.
- Un autre facteur important à prendre en compte est la localisation des clients. Chaque pays ou juridiction possède des lois locales spécifiques, et il est obligatoire de s'y conformer également.
- Les entreprises doivent s'assurer que ces réglementations sur la vie privée sont ajoutées à leurs valeurs fondamentales. Avec un tel changement culturel établi, la confidentialité sera prise en compte dès le début de chaque nouveau projet et suivie jusqu'à la fin.
- Les entreprises doivent s'éloigner de l'approche traditionnelle de collecte de données, qui consiste à essayer de rassembler et de stocker autant de données clients que possible. Avec le durcissement des réglementations, les entreprises ne devraient recueillir, traiter et stocker que ce qui est nécessaire. L'idée d'une collecte de données minimaliste doit être employée. En outre, la suppression des données après leur expiration ou après leur utilisation est tout aussi importante pour se conformer aux réglementations en matière de protection de la confidentialité.
- Les organisations doivent faire preuve de transparence en ce qui concerne les données personnelles collectées auprès de leurs clients et gérer les demandes de suppression des données afin de garantir la conformité légale.

Les lois mondiales sur la confidentialité des données, en constante évolution, ne feront que devenir plus strictes avec le temps. L'idéal pour toute entreprise serait de se conformer volontairement à toutes les lois sur la protection de la confidentialité en vigueur dans les pays où elle exerce ses activités. En outre, les pays et les États affectés indirectement par leurs activités doivent également être pris en considération comme l'exigent des réglementations telles que le GDPR. Afin d'éviter des amendes coûteuses, des interruptions opérationnelles et la perte de clients, plus tôt les entreprises planifient et se conforment à ces lois, plus elles auront de succès.

À propos d'AD360

AD360 est une solution de gestion des identités et des accès (IAM) permettant de gérer les identités des utilisateurs, de régir l'accès aux ressources, de renforcer la sécurité et de garantir la conformité. AD360 fournit toutes ces fonctionnalités pour Windows Active Directory, Exchange Server et Office 365. Avec AD360, vous pouvez choisir les modules dont vous avez besoin et commencer à relever les défis de l'IAM dans les environnements sur site, en cloud et hybrides, le tout à partir d'une seule console.

Pour plus d'informations sur AD360, veuillez consulter <https://pgsoftware.fr/iam/ad360>

\$ Obtenir un devis

↓ Télécharger