LE CIAM, AU-DELÀ DES EXIGENCES DU RGPD

Ping Identity

RGPD
DOSSIER

L'imminence du règlement général sur la protection des données (RGPD) offre de grandes opportunités, mais pose aussi des défis importants pour les entreprises qui travaillent dans l'Union européenne. Les entreprises doivent évaluer et combler les manquements en termes de conformité pour les applications et les référentiels de données qui hébergent des données personnelles concernant des résidents de l'UE. C'est une tâche qui peut s'avérer considérable.

Mais les entreprises qui vont au-delà de la simple conformité ont une opportunité en or de se distinguer en tant que leaders de la prochaine ère numérique.

Ces entreprises, qui cherchent les moyens les plus efficaces et les plus sûrs de satisfaire les exigences techniques du RGPD, se tournent de plus en plus vers la gestion des accès et des identités clients (CIAM). Les solutions CIAM aident à garantir la conformité en termes de sécurité, de gouvernance et de transparence dans la collecte et l'exploitation de données personnelles. La mise en place d'une solution CIAM ne signifie pas automatiquement que votre entreprise est conforme au RGPD, mais elle peut vous aider à atteindre les nombreux objectifs du règlement tout en favorisant la fidélité et l'engagement client par le biais d'une expérience client exceptionnelle.

Voici quelques exigences techniques clés du RGPD et certaines des stratégies CIAM permettant de résoudre ces difficultés.

EXIGENCE DU RGPD : LE CONSENTEMENT

Le responsable (l'entité qui définit les finalités et les moyens du traitement des données personnelles) doit demander et enregistrer le consentement de la personne concernée (une personne physique identifiée et identifiable) pour la collecte, le stockage et l'exploitation des données personnelles. (articles 7, 8 et 13)

Dans l'idéal, un système CIAM complet est conçu pour enregistrer le consentement de l'utilisateur. Il vous permet d'enregistrer en continu le consentement du client quel que soit le canal, saisir le consentement pour des attributs de données spécifiques et appliquer les choix en fonction de règles centralisées telles que les réglementations locales et les règles de l'entreprise. Certaines solutions rationalisent le consentement par des notifications en push vers un appareil autorisé et intègrent même le consentement dans les applications mobiles existantes grâce à TouchID qui offre sécurité et confort.

EXIGENCE DU RGPD : L'ACCÈS AUX DONNÉES ET LA RECTIFICATION

La personne concernée peut accéder aux données personnelles collectées et procéder à des corrections et des mises à jour. (articles 15 et 16)

La possibilité pour les clients de gérer eux-mêmes leurs profils est une autre fonctionnalité clé d'une solution CIAM solide. Les utilisateurs peuvent visualiser et modifier leurs données personnelles, notamment les données de profil, les préférences personnelles et le consentement. Ces préférences sont appliquées systématiquement sur tous les canaux.

EXIGENCE DU RGPD : LA SUPPRESSION

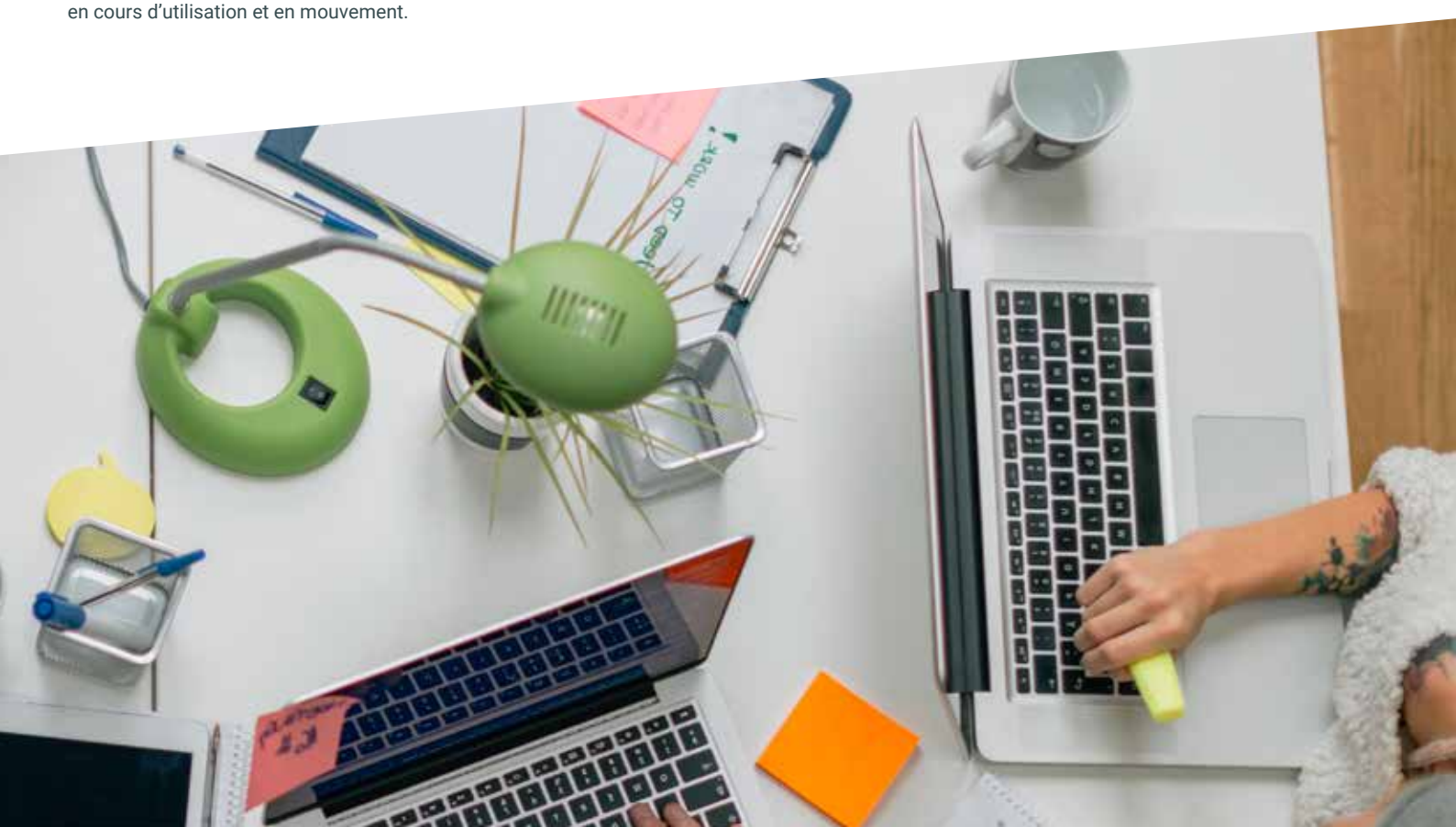
Une personne a le droit de demander au responsable d'« oublier » ou de supprimer toutes les données personnelles qui la concernent. (Article 17)

Pour avoir pleinement confiance en la suppression de toutes les données sur tous les référentiels de données et les sauvegardes, il faut d'abord avoir la garantie qu'un profil client unifié existe dans un référentiel de données d'identités de hautes performances capable de gérer les données structurées et non structurées. Les référentiels d'identité client offrent cette possibilité et bien plus encore, notamment l'évolution vers des centaines de millions d'utilisateurs et la prise en charge de l'accès aux applications par des API REST sécurisées.

EXIGENCE DU RGPD : LA PROTECTION DES DONNÉES DÈS LA CONCEPTION ET LA SÉCURITÉ

Le responsable doit concevoir des systèmes pour protéger et sécuriser les données personnelles en se basant sur les risques. (articles 25 et 32)

La gouvernance de l'accès des données est essentielle quand il est question de protection des données. Une solution CIAM transparente et sécurisée aide à satisfaire les exigences de sécurité dès la conception du RGPD. La gestion des accès en fonction du contexte offre une approche basée sur les risques et s'adapte à l'utilisateur, à l'appareil et aux données d'application, dont la localisation, le réseau et le statut de l'appareil. Enfin, le chiffrement de bout en bout garantit la sécurité des données au repos, en cours d'utilisation et en mouvement.



POURQUOI PING ?

Avoir une solution CIAM complète ne signifie pas pour autant que votre entreprise est conforme au RGPD et vice-versa. La conformité au RGPD ne garantit pas non plus que vos clients fassent confiance à votre marque, bénéficient d'expériences fluides et restent fidèles.

Les vrais gagnants sont ceux qui vont au-delà de la simple conformité au RGPD et profitent de tous les bénéfices du CIAM. Vous fournissez des expériences clients pratiques et personnalisées, quels que soient les canaux et les appareils, tout en appliquant les directives de confidentialité et en satisfaisant les exigences rigoureuses de sécurité de bout en bout. Notre formule pour une solution CIAM continue et sécurisée :

ANNUAIRE

Sécurisez les données personnelles de bout en bout avec un profil client unifié entièrement chiffré dans un annuaire hautes performances capable de gérer des données structurées et non structurées, d'évoluer pour prendre en charge des centaines de milliers d'utilisateurs et de permettre l'accès aux applications par des API REST sécurisées.

GOUVERNANCE DES DONNÉES

Centralisez les règles de gouvernance d'accès aux données et permettez un contrôle précis des attributs d'identité client accessibles par les applications internes et externes. Réunissez et actualisez le consentement pour toutes les tâches de collecte et d'exploitation des données.

AUTHENTIFICATION MULTI-FACTEURS

Déclenchez un deuxième facteur d'authentification (par SMS ou biométrie sur un appareil mobile) basé sur l'évaluation des risques contextuels ou transactionnels. Intégrez la fonctionnalité d'authentification multi-facteurs directement à votre propre application mobile au contact de la clientèle.

AUTHENTIFICATION UNIQUE (SSO)

Donnez aux clients une expérience SSO cohérente et sécurisée avec un seul couple d'identifiant/mot de passe pour tous les services numériques ainsi que la possibilité de l'authentification sociale.

SÉCURITÉ DES ACCÈS

Fournissez un contrôle centralisé de l'accès aux services numériques en ligne fournis à vos clients. Offrez des règles pour contrôler l'accès aux applications entières, URL spécifiques et terminaux API.

La plateforme modulaire extensible de Ping Identity s'appuie sur des standards ouverts ainsi que des fonctionnalités IAM riches et modulaires. Elle peut se déployer dans des environnements on-Premise, Cloud ou hybrides. Votre entreprise peut ainsi offrir à ses clients une expérience transparente et sécurisée pour renforcer la confiance en votre marque et améliorer la fidélité client. Pour en savoir plus, rendez-vous sur: www.pingidentity.com/GDPR_FR

Ping Identity.

Ping Identity envisage un monde numérique basé sur l'identité. En tant qu'entreprise spécialisée dans la sécurisation des identités, nous simplifions la prévention des failles de sécurité pour les plus grandes entreprises du monde, améliorons la productivité des employés et des partenaires et fournissons des expériences clients personnalisées. Les entreprises choisissent Ping pour notre expertise en matière d'identités, notre leadership au niveau des normes ouvertes, notre partenariat avec des entreprises comme Microsoft, Amazon et Google ainsi que notre collaboration avec des clients comme Boeing, Cisco, Disney, GE, Kraft Foods, Walgreens et plus de la moitié des entreprises classées au Fortune 100. La plateforme Ping Identity permet aux entreprises et à leurs utilisateurs d'accéder aux applications Cloud, mobiles et sur site en toute sécurité tout en offrant la gestion adaptée des données d'identités et de profils. Les architectes et les développeurs disposent d'options flexibles pour améliorer et étendre leurs applications et environnements existants grâce aux fonctionnalités d'authentification multi-facteurs, d'authentification unique, de gestion des accès, d'annuaire et de gouvernance des données.

#3256 | 7.17 | v02