

Confidentialité des données dès la phase de conception : Loi californienne sur la protection des consommateurs

Statistiques clés

- 69 % des consommateurs internationaux sont prêts à boycotter toute entreprise qu'ils estiment ne pas respecter les lois en matière de protection des données
- 62 % d'entre eux tiennent pour responsable l'entreprise plutôt que le pirate informatique en cas d'atteinte à la sécurité des données
- 83 % des consommateurs américains cesseront de dépenser pendant plusieurs mois après une atteinte ou un incident grave
- 21 % des consommateurs américains ne s'adresseront plus jamais à une marque ayant subi une atteinte à la sécurité des données¹

Encourager la préparation à la conformité pour renforcer la confiance des clients et réduire les risques de l'entreprise

Les résidents californiens obtiennent le contrôle de leurs informations personnelles et définissent les attentes en matière de confidentialité

La loi californienne sur la protection des consommateurs (California Consumer Protection Act, CCPA) s'inscrit dans le mouvement grandissant de la législation à l'échelle mondiale relativement à la confidentialité, visant à fournir des droits à la confidentialité aux individus et à leur accorder un meilleur contrôle sur l'utilisation de leurs informations personnelles.

La CCPA confère aux consommateurs des droits sur leurs données personnelles et empêche les entreprises de faire preuve de discrimination à leur encontre pour avoir exercé ces droits. Les consommateurs peuvent notamment poser des questions sur les catégories et les informations personnelles précises qu'une entreprise a recueillies à leur sujet, ainsi que sur les fins auxquelles l'entreprise utilise ces informations. Les clients peuvent demander à l'entreprise de supprimer les informations personnelles qu'elle a collectées à leur propos ou demander à ce que leurs données personnelles ne soient pas vendues à des tiers. La CCPA oblige également les entreprises à mettre en œuvre et à maintenir des procédures et des politiques raisonnables de sécurité des données adaptées à la nature des informations. Elle crée par ailleurs un droit d'action de nature privée (avec une responsabilité potentiellement élevée pour les entreprises) en cas de violation de cette obligation qui entraîne un accès non autorisé aux informations personnelles couvertes par la loi californienne de notification de violation.

Principales considérations relatives à la confidentialité des données

Les responsables de la confidentialité et les équipes de sécurité ont besoin d'outils automatisés pour gérer efficacement la confidentialité des données. Malheureusement, les responsables de la confidentialité sont souvent gênés par leur incapacité à identifier, localiser et évaluer les informations personnelles, à faciliter la coopération et la collaboration entre l'entreprise, les équipes chargées de la confidentialité et le service informatique, et à protéger et surveiller efficacement les informations personnelles.

Les solutions de confidentialité des données Informatica® sont conçues pour fournir une base qui prend en compte les réglementations en matière de confidentialité des données et la confiance des consommateurs. En gérant de manière proactive les exigences de conformité, les entreprises peuvent s'assurer que les risques liés aux données (utilisation abusive ou perte) sont résolus et surveillés, et que les parties prenantes peuvent collaborer efficacement à des fins de confidentialité, d'audits et de création de rapports.

¹ <https://www.infosecurity-technologine.com/news/fifth-consumers-never-return>

Les solutions de confidentialité des données Informatica fournissent aux entreprises la possibilité de (1) gérer les politiques de gouvernance des données (2) découvrir et gérer les données personnelles et sensibles (3) mapper les identités individuelles à leurs données personnelles (4) analyser et suivre les risques liés aux données (5) prendre des mesures pour protéger les informations personnelles et gérer les demandes de sujet des données et de consentement, et (6) suivre l'évolution de la confidentialité, et communiquer les actions et les états de confidentialité.

Pour relever les défis posés par la CCPA, les entreprises doivent disposer d'une meilleure intelligence et d'une meilleure sécurité des données personnelles afin de fournir aux résidents de la Californie le contrôle et la protection requis par la CCPA. Le tableau ci-dessous présente les principales problématiques liées à l'intelligence de données et à la sécurité à résoudre pour aider à assurer la conformité CCPA :

Exigences de confidentialité des données	Résultats
1. Déterminer comment notre entreprise traite les données personnelles de la Californie (politiques de gouvernance de données)	<ul style="list-style-type: none"> • Créer des définitions qui englobent les données personnelles des résidents de Californie • Définir les données collectées et la manière dont elles seront utilisées
2. Où se trouvent les données personnelles californiennes ? (Découvrir et classer les données personnelles)	<ul style="list-style-type: none"> • Localiser et mapper précisément où les données personnelles des résidents californiens sont conservées, notamment en ce qui concerne les données soumises à une notification de violation en vertu de la loi californienne
3. Créer un registre d'identité (liaison des identités californiennes à leurs données personnelles)	<ul style="list-style-type: none"> • Prendre en charge d'une réponse rapide aux demandes de droits des résidents californiens • Référencer rapidement de l'emplacement de distribution des données dans une entreprise
4. Déterminer comment les données personnelles californiennes sont protégées (analyser le risque de sécurité des données des résidents californiens)	<ul style="list-style-type: none"> • Comprendre où les données des résidents californiens sont exposées à un risque d'utilisation abusive ou d'accès non autorisé, hiérarchiser et planifier la remise en état, en particulier en ce qui concerne les données soumises à une notification de violation en vertu de la loi californienne • Identifier les mesures de sécurité nécessaires pour les différents types de données des résidents californiens
5. Protéger les données personnelles californiennes et répondre aux demandes de droits de demandes (sécurité des données, traitement des droits)	<ul style="list-style-type: none"> • Prendre en charge des demandes de suppression et de vente des données • Protéger les données des résidents californiens dans les opérations, le développement, les tests et les analyses
6. Suivre la progression et comprendre l'état actuel de la préparation à la confidentialité en vertu de la CCPA (mesure, communication, collaboration)	<ul style="list-style-type: none"> • Répondre aux demandes d'état • Suivre la progression du programme CCPA

À propos d'Informatica

La transformation digitale fait évoluer les attentes : service amélioré, livraisons plus rapides, à moindre coût. Les données sont la clé de la réussite des entreprises, ces dernières doivent évoluer pour rester compétitives.

En tant que leader mondial dans la gestion des données Cloud d'entreprise, nous sommes prêts à vous guider de manière intelligente – quel que soit le secteur, la catégorie ou la niche. Informatica vous permet de prendre une longueur d'avance pour gagner en agilité, concrétiser de nouvelles opportunités de croissance ou même innover. Nous nous concentrons sur les données afin de vous offrir la polyvalence nécessaire pour réussir.

Découvrez nos solutions et libérez tout le potentiel de vos données en vue de la prochaine révolution intelligente.

Alimentée par l'IA et la plate-forme de données intelligente leader du secteur, la solution Informatica Data Privacy fournit des fonctionnalités permettant de prendre en charge les principes centrés sur les données de la CCPA :

1. Définir et gérer les politiques de gouvernance

La gouvernance des données définit, documente et mesure les politiques, responsabilités, processus et termes de données d'un point de vue commercial et technologique. Grâce au cadre de gestion des tâches de gouvernance et aux flux de travail visuels d'Axon™, les entreprises peuvent identifier les utilisateurs professionnels participants critiques et les aligner sur les données et les processus qu'elles possèdent.

2. Découvrir, classer, et comprendre les données personnelles et sensibles

Exploitez l'IA pour fournir une vue et une analyse d'entreprise des ressources en matière d'informations personnelles et des métadonnées afin que les entreprises puissent rapidement localiser, classer et comprendre tous leurs environnements de données : multi-cloud, Hadoop, systèmes de stockage relationnel et de fichiers, ainsi que les données structurées et non structurées.

3. Mapping des identités

Le registre des sujets de données relie les identités aux données personnelles afin que les entreprises puissent rapidement déterminer quelles données personnelles appartiennent à quelle personne (client, salarié, etc.). Cela assure une prise en charge des droits d'accès des sujets de données et s'intègre aux systèmes de gestion des consentements.

4. Analyser les risques liés aux données, établir des plans de protection

Analyser les risques liés aux informations personnelles (probabilité d'utilisation abusive ou de perte) et fournir des modèles d'impact des risques personnalisables, afin que les entreprises puissent hiérarchiser les mesures correctives et déployer efficacement les ressources et les investissements. Le risque est mesuré et enregistré en continu afin de fournir des indicateurs de risque clés pour les programmes de confidentialité et de protection.

5. Protéger les données, gérer les droits et le consentement de la personne

Rendre anonymes et utiliser un pseudonyme pour les informations personnelles afin de s'assurer que les entreprises contrôlent l'accès et l'affichage des informations personnelles des clients et des salariés. Créer un affichage à 360 degrés des sujets de données et des consentements en capturant et en documentant la traçabilité, l'historique et les périodes de conservation des données, tout en prenant en charge les droits des sujets de données par le biais de flux de travail et d'actions.

6. Mesurer, communiquer, préparer l'audit

Des visualisations riches fournissent des renseignements à l'échelle mondiale pour aider les décideurs, des vues détaillées à destination des spécialistes et des détails immédiats sur les informations personnelles, afin de prendre en charge les exigences d'audit pour gérer et suivre les programmes de protection et de confidentialité.



Siège mondial Tour CB 21, 16 Place de l'Iris, 92040 Paris La Défense Cedex Tél : +33 01 42 04 89 00 Numéro gratuit aux États-Unis : 1.800.653.3871

IN08_0419_03601