elastic

Utiliser Elastic pour assurer la conformité aux lois mondiales sur la protection de la vie privée

Présentation

Afin de réussir dans le monde numérique moderne, les organisations mettent l'accent sur les données, notamment sur leur rôle au sein de l'IA.
Pour répondre à ces enjeux, une prolifération de réglementations sur la confidentialité est en train de remodeler le paysage commercial à l'échelle mondiale. S'adapter à ces évolutions réglementaires n'est pas qu'une question de gestion des risques ; c'est un levier de différenciation stratégique sur le marché, où la mise en conformité avec des règles de confidentialité en pleine mutation favorise la confiance des clients, soutient la croissance financière et renforce la résilience opérationnelle.

Ce livre blanc présente les concepts clés de la législation sur la protection des données et montre comment utiliser la plateforme d'Elastic pour respecter les obligations sur les données personnelles et les opérationnaliser avec rapidité, efficacité et confiance. Nous allons exposer les six principes de base de la confidentialité des données communs aux réglementations internationales et les mapper aux solutions d'Elastic, permettant ainsi aux organisations de convertir leurs obligations de conformité en un véritable atout sur le marché.

Attention : ce livre blanc est communiqué à titre d'information seulement et ne remplace en aucun cas un conseil juridique formel. Veuillez consulter votre service juridique pour obtenir un avis spécialisé.

Contexte et aperçu des lois mondiales sur la protection de la vie privée

L'évolution des lois mondiales sur la confidentialité multiplie les défis pour les organisations amenées à collecter des données personnelles. Puisque les données personnelles sont considérées comme l'une des ressources les plus prisées au monde, la mise en conformité avec les lois sur la vie privée représente un atout stratégique pour les entreprises, et tout manquement peut ralentir fortement leur progression.

Face à l'augmentation des données personnelles collectées, la mise en œuvre d'une solution capable de monter en charge pour protéger ces données est indispensable pour prouver votre engagement et devenir un fournisseur privilégié dans un environnement où la protection de la vie privée est primordiale.

Malgré les spécificités de chaque loi sur la vie privée, on retrouve souvent des principes généraux identiques au sein des différents cadres réglementaires.

Voici les principales lois sur la protection de la vie privée :

- Le Règlement général sur la protection des données de l'UE (« RGPD ») et son équivalent au Royaume-Uni
- Les législations d'États américains sur la confidentialité, comme le California Consumer Privacy Act (« CCPA »)
- La Loi générale brésilienne sur la protection des données (« LGPD »)
- La Loi canadienne sur la protection des renseignements personnels et les documents électroniques (« LPRPDE »)
- Loi japonaise sur la protection des renseignements personnels (« APPI »)

La plateforme d'Elastic offre une flexibilité et une échelle qui permettent aux organisations de naviguer parmi ces exigences juridiques complexes et de gérer leur mise en conformité en toute simplicité.

Données à caractère personnel

Finie l'époque où la définition des « données personnelles » se restreignait aux identifiants explicites comme les noms et prénoms, les adresses e-mail, les identifiants nationaux ou les numéros de téléphone. Aujourd'hui, les législations mondiales sur la confidentialité adoptent une définition étendue des données personnelles pour inclure toute donnée susceptible d'être reliée à un appareil particulier ou à une personne physique.

Un bon principe de précaution est d'admettre que les réglementations sur la vie privée s'appliquent si l'information peut être associée à l'identifiant unique d'une personne physique. Dans un monde où les smartphones et l'IoT sont partout, la quantité de données personnelles recueillies par les organisations a atteint des sommets, rendant indispensable l'usage de produits et de services qui garantissent un traitement des données à la fois sûr et efficace.

Contrôleurs et processeurs

Les réglementations internationales en matière de vie privée prévoient des responsabilités distinctes, mais parfois convergentes, pour les entités, selon qu'elles interviennent comme « responsable du traitement » ou comme « sous-traitant » de données personnelles.

- Les **responsables du traitement** (ou « entreprises » selon le CCPA) ont la maîtrise des objectifs et des méthodes de traitement des données. Il s'agit des organisations qui décident, de manière autonome, quelles données personnelles recueillir et comment les utiliser.
- En tant que **sous-traitants** (ou « prestataires de services » selon le CCPA), ces entités interviennent pour le compte d'un responsable du traitement (ou d'un autre sous-traitant) ; elles n'ont le droit de traiter les données personnelles que conformément aux directives précises du donneur d'ordre, dans l'unique but de remplir leur mission de service.

La conformité, qu'on soit responsable du traitement ou sous-traitant, nécessite une compréhension claire des catégories de données personnelles traitées ainsi qu'une aptitude à les retrouver de façon ciblée et efficace, à l'échelle de l'organisation.

Partout dans le monde, les réglementations sur la vie privée accordent aux citoyens le pouvoir d'exercer divers droits concernant leurs données personnelles, comme l'accès à celles-ci, leur effacement ou encore leur modification. Grâce à la rapidité d'exécution d'Elastic pour analyser de vastes volumes de données (qu'elles soient structurées ou non), les organisations peuvent respecter des délais de réponse serrés, optimisant ainsi leur processus de conformité et prévenant les risques de sanctions ou de contentieux civils.

Principes fondamentaux de protection de la vie privée

Les lois mondiales sur la protection de la vie privée reposent souvent sur des principes fondamentaux en la matière. En règle générale, ce sont :

1

Avis

Les lois sur la protection de la vie privée exigent que les organisations fournissent une information exacte et actualisée sur leurs pratiques en matière de confidentialité.

2

La protection de la vie privée dès la conception

Les lois sur la protection de la vie privée exigent que les organisations mènent une réflexion approfondie sur l'impact de leurs pratiques sur les droits et les intérêts des individus, et qu'elles conçoivent leurs produits de manière à respecter ces législations.

3

Droits

Les lois sur la protection de la vie privée accordent aux individus certains droits sur leurs données personnelles, qui peuvent inclure les droits d'accès, de suppression et de rectification.

4

Minimisation des données

Les réglementations en matière de vie privée imposent aux entités de limiter la collecte de données au strict nécessaire (principe de minimisation) et d'appliquer des seuils de rétention et des protocoles de suppression afin de ne pas conserver de données superflues.

5

Sécurité

Les réglementations en matière de vie privée prescrivent des normes de sécurité obligatoires pour assurer la confidentialité et l'intégrité des données personnelles.

6

Notification de violation

Les réglementations en matière de confidentialité et de sécurité prescrivent de nombreuses responsabilités aux entités victimes d'un incident de sécurité ou d'une fuite de données à caractère personnel.

Le coût de la non-conformité

Le non-respect des lois sur la protection de la vie privée peut entraîner de lourdes amendes, des frais de justice et une atteinte à la réputation de l’entreprise. Le cadre répressif du RGPD et du CCPA prévoit des amendes substantielles susceptibles d'altérer l'équilibre financier d'une organisation, sans compter les risques de contentieux civils et de recours collectifs intentés par les victimes de violations de données personnelles.

Selon un rapport d'IBM Security et du Ponemon Institute, le coût moyen d'une violation de données en 2024 était de 4,88 millions de dollars, soit une augmentation de 10 % par rapport à l'année précédente. Le rapport sur les risques cybernétiques d'AON a révélé que 56 cyberévénements très médiatisés ont entraîné en moyenne une perte de 27 % du cours des actions des organisations touchées en 2024. De toute évidence, ce type de dommages à la réputation peut également avoir un impact irréversible sur l'avantage concurrentiel d'une organisation. Dans ce contexte, la conformité n'est pas seulement une dépense, c'est un investissement stratégique.

Utiliser Elastic pour vos besoins de conformité en matière de protection des données

Elastic accompagne les entreprises dans la recherche de réponses pertinentes et stratégiques à une vitesse record, en s'appuyant sur des solutions logicielles flexibles et open source. Le respect des réglementations mondiales en matière de confidentialité nécessite une vision claire de l'ensemble de votre écosystème de données : il s'agit de savoir où résident les données personnelles, comment elles se déplacent et de quelle manière elles sont exploitées. La plateforme Elasticsearch excelle dans ce domaine, en permettant de simplifier et d'automatiser ces étapes afin d'assurer une conformité sans faille. Dans la section suivante, nous soulignons l'apport d'Elastic par rapport aux six principes essentiels de protection de la vie privée qui ont été présentés ci-dessus.

Avis

Les capacités de mapping de données d'Elastic offrent aux organisations une vision claire du volume et de la nature des données personnelles traitées, que ce soit au sein de leurs serveurs ou dans des environnements délocalisés.

L'obligation d'information constitue l'un des piliers des législations sur la vie privée. Toute personne est en droit de connaître les catégories de données personnelles recueillies par une entité, les objectifs de ce recueil ainsi que les modalités de partage de ses informations avec des parties tierces. Ces réglementations imposent fréquemment la publication de politiques de confidentialité exhaustives ; c'est le cas pour Elastic, dont la Déclaration de confidentialité et le Trust Center détaillent précisément ces engagements.

Afin de se conformer à cette obligation d'information, il est essentiel pour une organisation de comprendre le périmètre exact des données personnelles qu'elle recueille. Cette démarche impose un exercice de mapping des données robuste, consistant en un processus méthodique d'identification et de documentation de tous les flux de renseignements personnels circulant dans l'entreprise.

En l'absence d'une solution scalable, les organisations se retrouvent souvent à dépendre d'un amalgame de fichiers Excel désuets, de sondages d'inventaire et d'interviews disparates auprès des directions métiers pour essayer de cartographier les données personnelles et leur parcours au sein de l'organisation et au-delà.

Dans le meilleur des cas, les relevés ne sont fidèles que de manière ponctuelle, car ils pâtissent rapidement de l'intensité des activités de collecte et de traitement au sein d'une économie centrée sur la donnée.

Grâce à Elastic, les entreprises bénéficient d'une visibilité stratégique permettant d'optimiser leurs méthodes de mapping des données. À défaut de savoir quelles catégories de données personnelles sont recueillies, où elles résident et à qui elles sont transmises, une organisation ne peut garantir le respect des réglementations en matière de confidentialité. L'intégration des métadonnées de vos flux dans Elastic permet, via ses fonctions de recherche avancées, de repérer instantanément toute application, table ou requête traitant des données personnelles.

Le recours à Elastic pour simplifier le mapping des données permet aux entreprises de mieux se conformer à leurs engagements contractuels : les flux de données ainsi identifiés servent à désigner les tiers avec lesquels il est nécessaire d'établir un avenant de protection des données, des protocoles de transfert ou tout autre contrat encadrant la sécurité des données à caractère personnel. De même, les chaînes logistiques modernes peuvent impliquer des centaines ou des milliers de prestataires et de sous-traitants. La capacité d'indexer et d'effectuer instantanément des recherches plein texte parmi des milliers de contrats peut également faciliter la production de rapports d'état sur les fournisseurs et, plus important encore, permettre la mise en œuvre de programmes de gestion proactive des prestataires.

La protection de la vie privée dès la conception

Les organisations peuvent utiliser Elastic pour renforcer la protection de la vie privée dès la conception, notamment en y intégrant les principes de minimisation des données.

Pour les organisations prévoyant de stocker des données personnelles dans Elastic, l'utilisation d'Elastic Cloud Enterprise (« ECE ») — la solution d'orchestration centrale d'Elastic — garantit un démarrage optimal en intégrant nativement les exigences de protection des données. Adopter la protection des données dès la conception, c'est gérer les informations personnelles comme des actifs stratégiques. Cette approche repose sur la limitation des accès, le maintien de la qualité des données, l'instauration de contrôles de sécurité et la définition de périodes de rétention strictes.

Contrairement aux structures classiques où un stockage centralisé unique impose une gestion complexe des droits d'accès pour isoler les données, Elastic offre la possibilité de créer des clusters Elasticsearch distincts par projet. Ainsi, chaque environnement ne contient que les informations strictement nécessaires à sa finalité.

Cette structure répartie favorise la minimisation des données à caractère personnel, s'inscrivant ainsi dans l'un des principes clés de la protection de la vie privée. En utilisant Elastic pour segmenter les données selon des niveaux de stockage, les organisations s'appuient sur les journaux d'accès pour détecter les informations dormantes, facilitant ainsi l'application rigoureuse des durées de conservation réglementaires.

L'utilisation d'Elastic aide les organisations à évaluer l'opportunité et les modalités d'exécution des analyses d'impact relatives à la protection des données (« AIPD »), une étape cruciale pour les traitements à haut risque. Selon le RGPD et d'autres cadres réglementaires équivalents, l'AIPD constitue une évaluation, dont le caractère peut être obligatoire, visant à s'assurer d'un traitement responsable des données à caractère personnel et à limiter les risques d'atteinte à la vie privée des personnes concernées. Une visibilité claire sur l'hébergement, le traitement et le parcours des données facilite la finalisation des AIPD. Sans cela, ces analyses imposent souvent un effort de coordination complexe entre différentes directions pour identifier précisément l'exploitation faite des données privées. En retour, les AIPD apportent la preuve d'une mise en conformité structurelle et offrent aux organisations les moyens de cantonner le traitement des données privées au strict cadre défini par les réglementations mondiales.

Droits des personnes concernées

L'utilisation d'Elastic permet aux organisations de localiser précisément les informations privées, d'analyser la recevabilité des demandes et de garantir le respect des droits des personnes concernées.

À travers le monde, les réglementations sur la vie privée garantissent aux citoyens des droits de regard et de décision sur l'usage qui est fait de leurs données à caractère personnel. De manière générale, cela englobe les droits d'accès, de suppression et de rectification, tout comme le droit d'opposition à certaines formes d'exploitation des données privées. Grâce à ses fonctions de « data mapping », Elastic offre le socle indispensable sur lequel les entreprises peuvent s'appuyer pour répondre aux requêtes des individus concernant leurs données personnelles.

- **Accès :** Elasticsearch permet aux organisations d'effectuer des recherches au sein de leurs entrepôts de données pour identifier les informations personnelles à l'échelle de l'entreprise, notamment en repérant les tables, les requêtes, les rapports ou les applications qui reposent sur ces données. Les organisations peuvent également exploiter Elastic pour alimenter les fonctions de recherche destinées aux utilisateurs finaux, afin qu'ils puissent rechercher leurs propres données. Offrir aux utilisateurs des capacités de recherche puissantes réduit les sollicitations du support client, car les utilisateurs peuvent utiliser des outils en libre-service pour identifier et exporter leurs données. Lorsque ces outils en libre-service ne suffisent pas, Elastic permet aux organisations de fouiller rapidement leurs propres bases de données pour honorer les demandes d'accès des personnes concernées.

- **Suppression :** Après avoir utilisé Elastic pour identifier les données personnelles conservées sur un individu, une organisation peut ensuite utiliser Elastic pour transformer ces données. Cela inclut le marquage des données (tagging) pour leur conservation en cas d'exception à la suppression, l'effacement définitif, ainsi que l'utilisation d'autres techniques de suppression autorisées par les lois sur la vie privée, telles que l'anonymisation et certains types de pseudonymisation. L'utilisation d'Elastic pour transformer rapidement les données personnelles — sans nécessiter de développements techniques coûteux — aide les organisations à rester conformes, à éviter les contrôles réglementaires et à préserver l'utilité des données dans les limites fixées par les législations mondiales.
- **Rectification :** De la même manière, les lois sur la protection de la vie privée permettent souvent aux individus de demander la correction de leurs données personnelles. Elastic peut isoler les données personnelles conservées sur un individu afin que l'organisation puisse se concentrer sur le traitement de la demande — et non sur la recherche des données.
- **Restrictions :** Certaines lois sur la protection de la vie privée, comme le RGPD et son équivalent au Royaume-Uni, prévoient également un droit d'opposition ou un droit de demander la limitation du traitement des données personnelles. Les organisations peuvent utiliser les capacités de cartographie et de catégorisation des données d'Elastic pour déterminer rapidement comment répondre à de telles demandes et restreindre les autorisations d'accès et d'utilisation en conséquence. Cela permet de gagner un temps précieux et donne aux équipes de conformité les moyens de répondre dans les délais courts imposés par ces législations.

Minimisation des données

Comme évoqué dans la section sur la *Protection des données dès la conception*, Elastic soutient les capacités de minimisation des données pour les entreprises. Les principes de minimisation des données exigent que les organisations collectent, traitent et limitent la conservation des données personnelles aux seules informations nécessaires à la réalisation des finalités de traitement autorisées par l'organisation.

Par exemple, une façon de minimiser le traitement des données personnelles pour remplir cette obligation consiste à utiliser la **pseudonymisation** (c'est-à-dire le remplacement des identifiants personnels dans les données par des valeurs de substitution) ou l'**anonymisation** (c'est-à-dire la suppression complète des identifiants personnels afin qu'une personne ne puisse plus être identifiée). Découvrez comment une compagnie aérienne européenne de premier plan utilise le pipeline d'ingestion d'Elastic pour masquer les données sensibles avant leur stockage. De tels résultats peuvent être obtenus grâce à Logstash, une intégration disponible dans Elastic qui collecte des données provenant d'une multitude de sources pour en faciliter la transformation — y compris l'anonymisation et la pseudonymisation — favorisant ainsi les objectifs de minimisation des données et réduisant les risques liés à la sécurité informatique.

En s'appuyant sur Elastic pour cartographier et auditer leurs actifs, les entreprises peuvent examiner de près l'exploitation effective des données stockées, ce qui leur permet d'ajuster avec plus de pertinence leurs règles de rétention et leurs procédures internes.

Notification de sécurité et de violation

Pour en savoir plus sur la manière dont Elastic peut aider les organisations à sécuriser leurs données personnelles et à réagir rapidement en cas de violation de données, nous vous invitons à consulter notre Livre blanc sur la sécurité.

Conclusion

La protection des données n'est pas seulement une exigence réglementaire ; c'est un impératif commercial. Compte tenu des sanctions financières massives, des risques opérationnels et de l'enjeu majeur que représente la confiance des consommateurs, les entreprises doivent impérativement disposer d'une solution robuste et capable de monter en charge pour assurer la cartographie, la classification, la gestion, la transformation, l'analyse et l'effacement de leurs actifs informationnels. Elastic simplifie chaque étape de ce processus, en offrant la puissance évolutive dont votre organisation a besoin pour garantir sa conformité et renforcer la confiance de ses clients.

