virtru

Qui détient les clés de vos données ?

Comment utiliser votre fournisseur de cloud préféré tout en préservant la confidentialité et la souveraineté des données

Le dilemme du numérique

Les entreprises sont confrontées à un dilemme : elles veulent bénéficier des gains de productivité et de sécurité offerts par les plateformes de cloud computing mondiales, mais craignent de devoir faire face à des obligations légales contradictoires qui mettent en danger la vie privée des clients.

Par exemple, une entreprise basée en Europe peut se retrouver dans une situation où elle est obligée de transmettre les données de ses clients au gouvernement américain.

Pourquoi ? Parce que : (a) les principaux fournisseurs de cloud sont majoritairement basés aux États-Unis et soumis à diverses lois exigeant une coopération avec les entités gouvernementales locales et fédérales américaines, et (b) il n'existe actuellement aucun cadre multilatéral de protection de la vie privée.

L'absence d'un cadre mondial de protection de la vie privée a amené les gouvernements à adopter des approches juridiques et politiques très différentes en matière de données. Par exemple, l'Union européenne a adopté des mesures de protection de la vie privée très strictes pour ses citoyens, tandis que les États-Unis délèguent certaines questions relatives à la vie privée au niveau des États (par exemple, la loi californienne sur les droits à la vie privée, CPRA) tout en prenant certaines mesures au niveau fédéral, comme la loi américaine Clarifying Lawful Overseas Use of Data (CLOUD) en 2018. En 2021, le Conseil européen de la protection des données a publié un ensemble de nouvelles recommandations pour les transferts internationaux de données, y compris quels types de protections sont suffisants pour protéger les données privées.

La protection de la vie privée est devenue une question polarisante pour ces alliés occidentaux. Le système de droit national et régional continue d'évoluer, et les entreprises ont besoin d'outils flexibles pour naviguer dans ce paysage changeant. La technologie qui place l'entreprise au centre du contrôle peut, et doit, être un élément central de la solution. Comme le soulignent les dernières recommandations de l'UE, "la protection accordée aux données personnelles dans l'Espace économique européen doit voyager avec les données, où qu'elles aillent."

Pour comprendre comment aborder cette question complexe, nous devons comprendre les principaux éléments en jeu : La loi américaine CLOUD, Schrems II, et le Règlement Général sur la Protection des Données (RGPD).

©Virtru Corporation. Tous droits réservés.

Loi américaine CLOUD (Clarifying Lawful Overseas Use of Data) (2018)

Entrée en vigueur : 23 mars 2018

De quoi s'agit-il ?
La loi américaine CLOUD donne au gouvernement américain la possibilité d'obliger un fournisseur de cloud américain à remettre des données, quel que soit l'endroit où ces données sont stockées, dans n'importe quel lieu géographique mondial (par exemple, les données stockées sur un serveur Google en Belgique seraient soumises à cette loi).

Pourquoi est-ce une préoccupation ?
Outre les vastes problèmes de protection des données et de respect de la vie privée que pose la transmission des données au gouvernement américain, cela cause également d'importants maux de tête opérationnels aux organisations qui doivent ou veulent faire des affaires sur le marché mondial. Alors que les États-Unis abritent la grande majorité des fournisseurs de services en cloud (Amazon, Microsoft et Google détiennent 66 % des parts du marché européen des services en cloud), on ne sait pas comment l'industrie technologique américaine équilibrera les demandes géopolitiques concurrentes en l'absence d'un accord politique multilatéral officiellement adopté pour remplacer le Privacy Shield.

Certains pourraient choisir d'éviter complètement la question et de ne pas adopter les technologies basées sur le cloud, ce qui pourrait élargir la fracture numérique. D'autres pourraient choisir de ne faire affaire qu'avec des fournisseurs de services en cloud de l'UE ou d'autres pays, alimentant ainsi la tendance inquiétante à l'isolationnisme et aux jardins clos qui se sont développés dans le monde entier.

©Virtru Corporation. Tous droits réservés.

Schrems II et le Règlement Général sur la Protection des Données (RGPD)

Établi : Schrems II a été jugé le 16 juillet 2020 et le RGPD est entré en vigueur le 25 mai 2018.

De quoi s'agit-il ?
Schrems II est connu comme l'arrêt de la Cour de justice de l'Union européenne (CJUE) qui a invalidé le cadre du bouclier de protection (Privacy Shield) de la vie privée entre l'UE et les États-Unis en raison de préoccupations concernant les pratiques de surveillance américaines. Juste ou injuste, la réalité est que les révélations d'Edward Snowden en 2013 continuent de jeter une longue ombre sur lesdites pratiques.

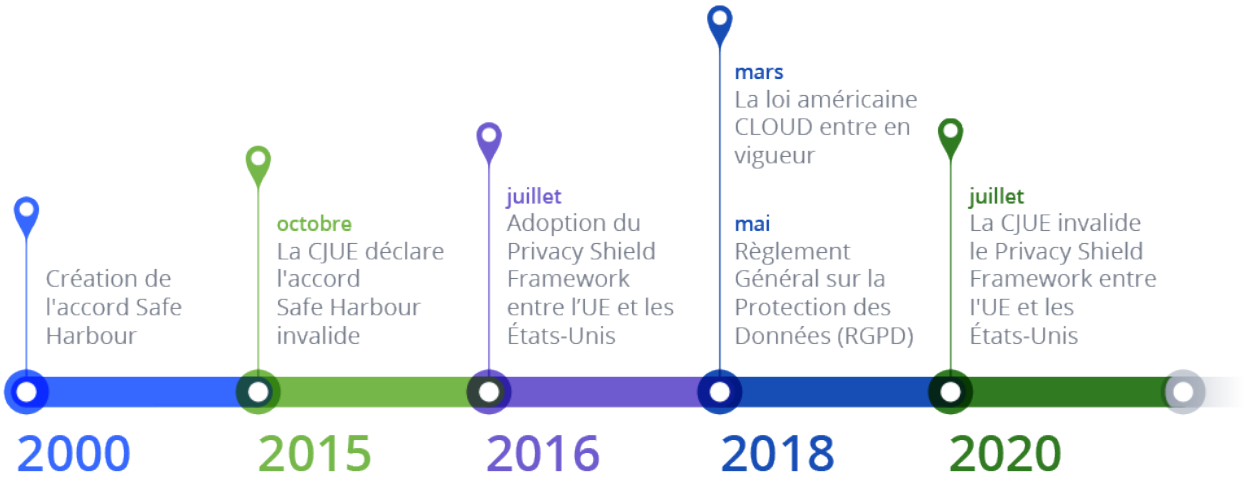
Le RGPD est un règlement européen qui régit les mécanismes selon lesquels le transfert de données personnelles en dehors de l'UE peut être légal. Son objectif principal est de donner aux individus (et aux entreprises pour les données de leurs employés et de leurs clients) le contrôle de leurs propres données, de la manière dont elles sont utilisées, dans quel délai et dans quel but.

Qu'est-ce que cela signifie ?
Schrems II s'est penché sur la validité du Privacy Shield et des Standard Contractual Clauses (SCCs, clauses contractuelles types). Alors que les transferts de données à caractère personnel sur la base du Privacy Shield sont désormais illégaux, au cas par cas et si des contrôles rigoureux supplémentaires sont observés, les SCCs restent un mécanisme valide et légal pour les transferts de données. Les responsables du traitement des données ou les sous-traitants (ici, pour nos besoins, les "fournisseurs de cloud") qui ont l'intention de transférer des données sur la base des SCCs, doivent désormais déployer un mécanisme de transfert pour s'assurer que la personne concernée bénéficie d'un niveau de protection équivalent à celui garanti par le RGPD.

©Virtru Corporation. Tous droits réservés.

Le paysage changeant de la réglementation des données entre l'UE et les États-Unis

Le paysage mondial de la confidentialité des données a connu une évolution considérable au cours des 20 dernières années, le partage des données étant devenu omniprésent. Voici quelques-unes des étapes clés de la réglementation qui ont façonné notre environnement actuel.



Création de l'accord Safe Harbour - 2000
Conçu pour garantir que les transferts de données entre l'UE et les États-Unis soient conformes à la directive européenne sur les données de 1995 (prédécesseur du Règlement Général sur la Protection des Données (RGPD)).

La CJUE déclare l'accord Safe Harbour invalide - 6 octobre 2015
Résultat d'un procès contre Facebook (Schrems I) intenté par Max Schrems, un défenseur autrichien de la vie privée, qui contestait le transfert de ses données (et des données des citoyens de l'UE en général) vers les États-Unis par Facebook, qui est constitué en société en Irlande.

Adoption du Privacy Shield Framework entre l'UE et les États-Unis - 12 juillet 2016.
Conçu par le ministère du Commerce des États-Unis et la Commission européenne et l'administration suisse pour fournir aux entreprises des deux côtés de l'Atlantique un mécanisme permettant de se conformer aux exigences en matière de protection des données lors du transfert de données personnelles de l'UE et de la Suisse vers les États-Unis à l'appui du commerce transatlantique.

La loi américaine CLOUD entre en vigueur - 23 mars 2018
Cela a permis aux autorités policières américaines de demander des données personnelles aux entreprises technologiques basées aux États-Unis, quelle que soit la localisation des données.

Le Règlement Général sur la Protection des Données (RGPD) entre en vigueur - 25 mai 2018
Conçu pour donner aux citoyens de l'UE plus de contrôle sur leurs données personnelles et pour simplifier les règles pour les organisations qui opèrent au sein des États membres de l'UE et celles qui font des affaires avec eux.

La CJUE invalide le Privacy Shield Framework entre l'UE et les États-Unis - 16 juillet 2020
Connue sous le nom de Schrems II, cette décision a rejeté le Framework en raison de préoccupations relatives aux pratiques de surveillance des États-Unis.

©Virtru Corporation. Tous droits réservés.

Comment la confidentialité et la collaboration dans le cloud peuvent coexister avec le chiffrement de bout en bout

Compte tenu de la domination du marché par les fournisseurs américains de solutions logicielles et de services en cloud (c'est-à-dire les organisations qui relèvent du champ d'application du CLOUD Act américain), la plupart des entreprises concurrentes de l'UE qui exploitent les technologies en cloud et collectent les données des consommateurs (c'est-à-dire les organisations qui relèvent du champ d'application de la décision Schrems II) doivent faire face à la question des réglementations américaines et européennes dans leurs activités quotidiennes.

Heureusement, il existe une solution pour ces entreprises - une solution qui leur permet de participer pleinement à l'économie mondiale, de conserver les avantages du cloud public et d'assurer un contrôle total de l'accès aux données.

En novembre 2020, le European Data Protection Board (EDPB) a adopté des orientations clarifiant que le **chiffrement de bout en bout est une mesure efficace pour permettre à la fois l'adoption du cloud et les exigences de souveraineté des données de l'UE**, qui sont souvent considérées comme la norme d'or mondiale en matière de confidentialité.

Le chiffrement de bout en bout permet aux entreprises de :

- Adopter des services cloud mondiaux tout en répondant aux exigences de souveraineté des données.
- Protéger les droits à la vie privée des clients.
- Garder le contrôle total des données qui leur ont été confiées.
- S'assurer que les concurrents, les gouvernements étrangers et d'autres entités qui ne devraient pas y avoir accès ne peuvent pas accéder à leurs informations exclusives ou autrement sensibles.

En substance, les entreprises de l'UE peuvent associer les contrôles de sécurité rigoureux offerts par la technologie de chiffrement avec les SCCs, assurant ainsi la conformité avec la loi européenne post-Schrems II tout en offrant un chemin géré vers l'accès autorisé pour les agences gouvernementales américaines et autres entités. C'est là que Virtru peut vous aider.

©Virtru Corporation. Tous droits réservés.

Le chiffrement de bout en bout de Virtru permet le partage sécurisé et la souveraineté des données dans le cloud.

Virtru a adopté une approche de la sécurité des données qui donne la priorité à la confidentialité au contrôle qui sont entièrement gérés par leurs clients - également connu sous le nom de souveraineté des données. La plateforme Virtru fournit un chiffrement de bout en bout qui garantit que vos données - et celles de vos clients - restent chiffrées et illisibles (conformément aux directives de l'EDPB), même en cas d'activation de la loi américaine CLOUD.

Comment ?
La solution de Virtru est indépendante de l'infrastructure et du fournisseur de cloud, elle est crypto-agile et mise en œuvre de bout en bout par défaut. Les options de gestion des clés chiffrées garantissent qu'aucune entité - y compris les fournisseurs de cloud - ne peut accéder aux données sans le consentement du propriétaire des données, qui est le seul à pouvoir accorder l'accès par le biais du déchiffrage.

En un mot, Virtru soutient la collaboration mondiale par le biais de flux de données transfrontaliers conformes en garantissant :

et

Nous aidons déjà les organisations à garder le contrôle de leurs données :

Un grand retailer européen a besoin d'une sécurité supplémentaire pour garantir une véritable confidentialité des données sensibles provenant d'un fournisseur de services en cloud.

Lire l'étude de cas

1. **Les données peuvent être stockées sur n'importe quelle solution de cloud, y compris celles proposées par des fournisseurs** basés aux États-Unis, notamment les solutions commerciales prêtes à l'emploi de Google, Microsoft et Amazon.
2. **Les données sont enveloppées dans une couche de protection (chiffrement)** qui ne peut être déverrouillée que par le client ou le destinataire désigné. Bien que les données soient toujours accessibles, elles restent chiffrées et illisibles.
3. **Les clés qui déverrouillent cette couche protectrice sont gérées en dehors de la solution en cloud.** Virtru offre la possibilité de stocker les clés de chiffrement - le cœur du mécanisme de chiffrement - sur site ou dans un cloud privé qui est uniquement détenu et géré par le client, ce qui permet d'assurer la souveraineté des données.

©Virtru Corporation. Tous droits réservés.

Dans un paysage politique en constante évolution, Virtru reste concentré sur ce qui compte : **garantir la souveraineté des données, donner aux clients finaux un contrôle unique sur leurs données et favoriser une collaboration de confiance au-delà des frontières**.

Vous voulez savoir comment le chiffrement de bout en bout de Virtru peut protéger les données de votre entreprise, où qu'elles soient stockées et partagées ? Contactez-nous pour une démonstration dès aujourd'hui.

Chez Virtru, nous permettons aux entreprises de libérer la puissance des données tout en gardant le contrôle, partout où elles sont stockées et partagées. Notre portefeuille de solutions et d'outils de chiffrement, basé sur notre plateforme ouverte de protection des données, gère les données tout au long de leur cycle de vie. Plus de 6 000 clients font confiance à Virtru pour la sécurité des données et la protection de la vie privée. Pour plus d'informations, visitez virtru.com ou suivez-nous sur Twitter à @virtruprivacy.

©Virtru Corporation. Tous droits réservés.