# Protection et sécurité des données pour les services financiers

Ce qu'il faut savoir

Les institutions financières opèrent une migration vers le Cloud. À leur tour, les régulateurs scrutent la capacité des entreprises à s'adapter et à se remettre des perturbations opérationnelles, en particulier celles qui impactent les données.

Les principales avancées réglementaires préoccupantes sont celles qui concernent la confidentialité des données et la cybersécurité, ainsi que le RGPD et Schrems II pour ceux qui gèrent leurs activités dans et avec des institutions financières européennes.

## Confidentialité des données

Les organismes de réglementation demandent aux entreprises spécialisées dans les services financiers d'identifier les actifs informationnels critiques et l'infrastructure dont ils dépendent. Les efforts en matière de cybersécurité doivent également être hiérarchisés en fonction de l'importance de ces actifs informationnels pour les opérations critiques de la banque.

**Considérations relatives à l'accès à distance, au déploiement rapide et à l'extension de la bande passante :**

**Atténuation des risques :** Calculer de manière préventive les risques potentiels associés à une interruption ou à une compromission de la technologie et/ou des applications.

**Gestion :** Définir, documenter et déployer des processus qui incluent l'utilisation d'actifs à distance, des utilisateurs privilégiés et le développement d'applications.

**Partenariat TIC :** Informer régulièrement les équipes TIC, y compris en matière de cybersécurité, pour permettre l'accès à distance à long terme de manière appropriée.

Vous devez élaborer des plans pour maintenir l'intégrité des informations critiques à la suite d'un cyberévénement et évaluer régulièrement le profil des menaces qui planent sur les actifs d'informations critiques. Il convient également de tester régulièrement vos vulnérabilités et de garantir votre résilience face aux risques liés aux TIC.

## Cybersécurité

Non seulement les cyberattaques sont de plus en plus sophistiquées, mais elles peuvent désormais perturber davantage les institutions ainsi que les marchés entiers en raison d'une numérisation, d'une interconnexion et d'une dépendance accrues à l'égard des tiers.

Maintenir et améliorer la résilience des entreprises constitue une nouvelle façon d'instaurer la confiance avec les clients et les régulateurs.

**Niveaux d'attente de la Banque centrale européenne concernant les infrastructures des marchés financiers :**

**Évolution :** Capacités essentielles établies, évoluées et maintenues pour identifier, gérer et atténuer les cyber-risques. Performances des pratiques suivies et gérées.

**Progression :** En plus du niveau précédent, implémenter des outils plus avancés, intégrés à tous les secteurs d'activité et améliorés au fil du temps pour gérer de manière proactive les cyber-risques.

**Innovation :** En plus des niveaux précédents, stimuler l'innovation des personnes, des processus et de la technologie pour le FMI et l'écosystème au sens large afin de gérer les cyber-risques et d'améliorer lacyber-résilience. Cela peut nécessiter le développement de nouveaux contrôles et outils ou la création d'un nouveau groupe de partage d'informations.

Les actifs technologiques doivent être tenus à jour et corrigés pour atténuer les cybermenaces nouvelles et existantes et le manque de support de certaines technologies. Il faudra peut-être mettre en place des changements pour faire face à tout retard technologique.



teradata.

## Schrems II

Cette décision porte principalement sur la souveraineté des données et le contrôle de l'emplacement des informations d'identification personnelle (PII). En ce qui concerne le transfert de données personnelles vers les États-Unis, un accord d'adéquation était en place et reconnaissait le cadre américain de protection de la confidentialité. Cet arrêt, rendu en juillet 2020 par la Cour européenne de justice, supprime effectivement le statut d'adéquation de la protection des données et apporte une incertitude aux transferts de données entre les États-Unis et l'Union européenne.

**Le Comité européen de la protection des données (European Data Protection Board - EDPB) fixe six étapes pour évaluer les transferts transfrontaliers et les pays tiers des importateurs :**

- Exportateurs, maîtrisez vos transferts
- Vérifiez l'outil de transfert sur lequel repose votre transfert
- Évaluez si une loi ou une pratique dans le pays tiers peut compromettre l'efficacité des mesures de sauvegarde pour votre transfert
- Identifiez et adoptez des mesures pour rendre les niveaux de protection des données conforme à la norme européenne d'équivalence essentielle pour le transfert de données
- Appliquez la procédure formelle pour l'adoption de ces mesures complémentaires
- Réévaluez et surveillez selon des intervalles appropriés tout développement susceptible d'affecter votre transfert de données

Bien que Schrems II ne semble pas avoir d'impact direct sur le Royaume-Uni, qui se trouve en dehors de l'UE, le Royaume-Uni a tendance à surenchérir en matière de réglementation avec l'UE. Il ne souhaite pas s'écarter des décisions de l'UE ni être perçu comme s'éloignant des pratiques européennes.

## RGPD

Cette loi européenne sur les données personnelles affecte les entreprises du monde entier depuis son entrée en vigueur en 2018. Le RGPD indique ce que les entreprises peuvent et ne peuvent pas faire avec les informations d'identification personnelle (PII).

**Exemples de PII :**

| | |
|---|---|
| Nom | sociaux |
| Numéro de téléphone | Ciblage géographique |
| Adresse | Dossiers de santé |
| Date de naissance | Nationalité |
| Compte bancaire | Croyances religieuses |
| Numéro de passeport | Affiliation politique |
| Utilisation des réseaux | |

Tout incident entraînant la perte, le vol, la destruction ou la modification de données personnelles est considéré comme une violation de données et peut entraîner une amende pouvant atteindre 20 millions d'euros (23 millions de dollars) ou 4 % du chiffre d'affaires mondial annuel.

## Quelle action devez-vous prendre ?

La protection et la sécurité des données sont des préoccupations majeures pour les institutions financières internationales de demain car le modèle de fonctionnement standard donnera la priorité au numérique. La flexibilité sera déterminante pour réussir, afin que toute nouvelle réglementation ayant un impact sur le traitement des données puisse être respectée avec un minimum de perturbations. Une nouvelle infrastructure hybride et multi-Cloud permettra de disposer d'une flexibilité optimale. Les données et les workloads pourront être déplacées entre plusieurs fournisseurs de Cloud, et même renvoyées sur site si nécessaire. Tout déplacement de données se fera rapidement avec un minimum d'interruptions.

## À propos de Teradata

Teradata est une société spécialisée dans les plateformes de données multicloud connectées. Notre analytique d'entreprise contribue à relever les défis commerciaux du début à la fin. Seule Teradata est capable de vous offrir la flexibilité nécessaire pour gérer dès aujourd'hui les charges de travail de données massives et mixtes de demain. Teradata Vantage est une architecture Cloud native, fournie as-a-service et construite sur un écosystème ouvert. De par sa conception, Vantage est la plateforme idéale pour optimiser les performances tarifaires dans un environnement multi-Cloud. Rendez-vous sur **Teradata.com.**

17095 Via Del Campo, San Diego, CA 92127 Teradata.com



teradata.