15 minutes d'avance

Fiche conseil. 03

Est-ce que je peux utiliser des outils États-Uniens ?

Le marché américain a inondé nos environnements numériques d'outils devenus incontournables : *MS365, Azure WhatsApp, Google Analytics*.... Ces solutions font l'objet de nombreux débats concernant les garanties qu'elles offrent en termes de sécurité des données et donc de conformité au RGPD. L'actualité nous invite à faire le point et mettre à jour nos habitudes.

Risques

1. Aux Etats-Unis, la protection des données à caractère personnel fait l'objet d'un vide juridique. De surcroit, les services de renseignements pratiquent la surveillance de masse au nom de la sécurité nationale et la loi dite « Cloud Act » permet aux autorités judiciaires d'accéder aux données électroniques stockées à l'étranger par les entreprises américaines, dans le cadre de procédures pénales.

2. L'Union Européenne estime que la collecte et l'utilisation des données à caractère personnel est une ingérence dans les droits des personnes.

3. Utiliser des outils américains, c'est donc prendre le risque que les données transférées soient utilisées à d'autres fins que celles prévues initialement (voir : base légale, registre de traitement, AIPD).

4. Sans garanties appropriées, les DCP de vos bénéficiaires, de vos bénévoles ou de vos salariés ne sont donc pas protégées.

Que dit le RGPD ?

- Art. 3 relatif au champ d'application territorial
- Art. 45 relatif aux transferts fondés sur une décision d'adéquation
- Art. 46 relatif aux transferts moyennant des garanties appropriées

Les transferts de données peuvent être réalisés uniquement dans des pays justifiant de garanties suffisantes :

- Pays membres de l'Union Européenne ou de l'Espace Économique Européen.
- Pays dits « adéquats » : Andorre, Argentine, Iles Féroé, Jersey, Guernesey, Israël, Île de Man, Suisse, Nouvelle-Zélande, Uruguay, Japon.
- Pays non adéquats sous réserve de garanties supplémentaires (voir. CCT, BCR, TIA).

Bonnes pratiques

- Privilégier les **outils européens** qui présentent une conformité RGPD (voir : privacy by design, privacy by default).
- Sélectionner des outils américains dont les entreprises sont inscrites sur la plateforme Data Privacy Framework et sont validées par le Department of Commerce. Vérifier chaque année que la certification est à jour.
- Dans tous les cas, rédiger un **contrat** avec des **clauses contractuelles type.**
- Privilégier les **versions payantes** : elles permettent de paramétrer les fonctionnalités qui protègent les données et sont mises à jour plus régulièrement.
- Demander conseil à mon DSI ou mon DPO lorsque le fournisseur me propose un outil non conforme.
- Les accords UE-EU sont sujets à de nombreux débats ; Rester en veille et en cas de doute, consulter son DPO.

Pour aller plus loin

CNIL – guide de sensibilisation au RGPD pour les associations

FAQ de la CNIL (13/07/2023)

15 minutes d'avance

Fiche conseil. 03

Est-ce que je peux utiliser des outils États-Uniens ?

Actualités

Un peu d'histoire

2000 : accord d'adéquation **Safe Harbor**

2015 : invalidation du Safe Harbor par l'UE : arrêt Schrems I

2016 : accord d'adéquation **Privacy Shield**

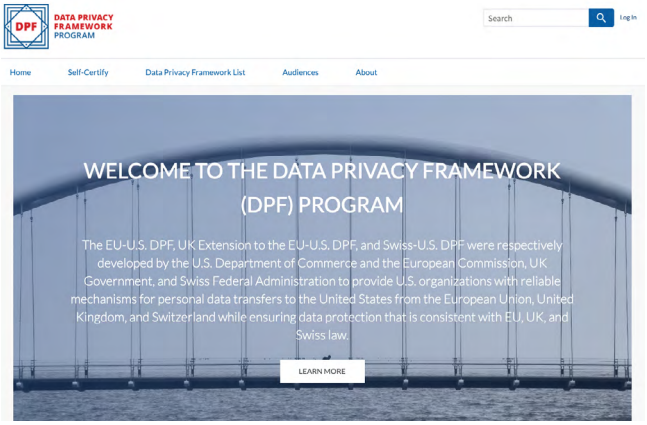
2020 : invalidation par CJUE : arrêt Schrems II

07/10/2022 : décret présidentiel J. Biden : **Executive Order***

13/12/2022 : soumission à CEPD

28/02/2023 : adoption par le CEPD avec « préoccupations »

10/07/2023 : accord d'adéquation **Data Privacy Framework**



Data Privacy Framework

- **Cadre de Protection** en FR
- Issu du décret présidentiel de Joe Biden (Executive Order n°14086 du 07/10/2022) relatif à la surveillance numérique de masse et qui vise à renforcer la protection des données sur 2 axes :
  1. **Principes de nécessité et de proportionnalité**
  2. **Mécanisme de recours indépendants et impartiaux**
- Mise en application **à compter du 10 juillet 2023**
- **Auto-certification** auprès du DPF Program mis en place par ITA.
- Engagement à respecter et **à renouveler chaque année**.
- Obligations & exigences **similaires à Privacy Shield** + mise à jour des notes d'information et politique de protection des données (cad : faire référence au RGPD et non plus à la Directive 95/46)
- **Périmètre** : US-UE; US-UK; US-Suisse
- **Autorités de contrôle** :
  1. DoC - Department of Commerce (Ministère du Commerce)
  2. FTC - Federal Trade Commission (agence indépendante pour la protection des consommateurs)

Quelles sont les entreprises certifiées ?

- Les entreprises déjà **inscrites dans le Privacy Shield** sous réserve de mettre à jour leurs notes d'information et leur politique de protection des données avant le 1er octobre 2023 (maj = réf. RGPD et non plus réf. à Directive 95/46), elles sont certifiées **automatiquement** DPF > les DCP peuvent circuler librement entre l'Espace Économique Européen et les États-Unis sans garantie supplémentaire.
- Les entreprises **nouvellement inscrites à la certification DPF** (auto-certification) doivent répondre aux attentes du nouveau cadre + **attendre la validation** d'adéquation par le DoC (Department of Commerce).
- Les entreprises **sans certification** restent non adéquates : besoin de **garanties appropriées** : CCT/BCR & TIA (voir. Art. 46).
- Les **sous-traitants** d'entreprises certifiées doivent utiliser des **garanties appropriées,** c'est-à-dire CCT + TIA (toujours requises).

Cela dit...

09/08/2023 - BNP Paribas et Société Générale paient très cher pour avoir utilisé WhatsApp