

Microsoft :

- [REDACTED]
- [REDACTED]
- [REDACTED]

CNIL

- [REDACTED]
- [REDACTED]
- [REDACTED]

Résumé :

Informations générales :

- Suite à l'invalidation du Privacy Shield, Microsoft a basculé sur le système des CCTs en septembre 2020.
- Récemment, entreprise de simplification et de modification du Microsoft Products and Services Data Protection Addendum.
- Mesures additionnelles
 - Techniques :
 - Haut degré de chiffrement dans les data centers et en transit. Les clients détiennent les clés pour les SaaS.
 - Pseudonymisation et anonymisation
 - Contractuelles : « Defending your data » = engagement contractuel à systématiquement contester les demandes d'accès dans les pays où il existe une base légale pour le faire. Système de compensation pour les consommateurs en cas d'accès des autorités malgré cet engagement. Ils essaient de « nudge » les autorités à demander l'accès aux données directement aux clients à la place de leur demander à eux.
 - MS indique avoir contesté le gouvernement US sur la base de la liberté d'expression devant des Cours et qu'ils poussent aussi dans cette direction dans le cadre de leurs échanges avec le gouvernement.
- Trans-Atlantic Data Privacy Framework : Ils ont pris acte de l'annonce de mars et se projettent dans sa mise en œuvre. Ils ont en effet souligné « leur engagement à se conformer au nouveau cadre annoncé le 25 mars et à remplir ou à aller plus loin que les conditions que ce cadre énonce pour les entreprises ». Ils souhaitent notamment :
 - Renforcer leur engagement « Defending your data », et
 - Investir des ressources dans la participation active au mécanisme de recours qui sera établi.

Le Projet EU Data Boundary s'inscrit dans leur engagement pour la priorité de la Commission européenne « a EU fit for Digital Age ». C'est une réponse à la demande des consommateurs et aux problèmes engendrés par l'arrêt Schrems II.

- Projet en cours, objectif de le mettre en œuvre d'ici la fin 2022
- Diffère du Projet Bleu dans lequel partenariat avec acteur européen. Ici construction d'infrastructures et investissement en ressources humaines en Europe. *N'ont pas souhaité donner plus d'informations sur le calendrier de mise en œuvre du Projet Bleu et ont renvoyé vers les partenaires européens. Projet Bleu n'a pas de réel équivalent dans d'autres pays.*

- Les données seront traitées et stockées en Europe avec 2 exceptions (cf. ci-dessous). Ils investissent dans la construction de nouveaux data centers en Europe, et l'augmentation des capacités de ceux préexistants.
- Les sous-traitants de Microsoft devront opérer dans le cadre des frontières du projet, sous les mêmes conditions que Microsoft. Ils limiteront également le nombre de sous-traitants ayant accès aux données des clients européens.
- Différences de modalité d'application du Projet aux clients en fonction des technologies Microsoft :
 - MS 365 : résidents EU/EEA inclus par défaut
 - Azure : résidents EU/EEA doivent « opt-in »

Par ailleurs, si un résident EU/EEA accède aux données hors des frontières définies, elles seront traitées en dehors de ces frontières.

- **Exceptions** :

Sécurité : Importance pour Microsoft d'avoir une base de données agrégées en matière de problèmes de sécurité afin de permettre aux utilisateurs de l'EU/EEA et du reste du monde de bénéficier des solutions trouvées dans les espaces respectifs.

Exemples de données concernées : métadonnées de dossiers, données du journal d'audit des services, processus et lignes de commande exécutés sur des dispositifs individuels

Dans ce cadre, mettent en avant 3 principes phares :

- Limitation des finalités
- Isolement des données
- Transparence : Les utilisateurs recevront de la documentation liée à la question et pourront choisir de continuer à utiliser ou non certains services de sécurité.

Maintenance : Même s'ils recrutent pour le service client en Europe, il y aura encore besoin d'accès par des développeurs situés hors UE, et notamment aux US.

- L'accès à distance aux données se fera de manière sécurisée, sans possibilité de télécharger les données, avec des technologies comme les infrastructures de bureau virtuelles (*virtual desktop infrastructure* ou VDI).