



Tags :

[vie privée](#), [données personnelles](#), [Europe](#), [RGPD](#), [CEPD](#), [Microsoft](#), [GAFAM](#)

Le Contrôleur européen de la protection des données (CEPD) recale les accords de licence avec Microsoft

[Retour à l'accueil de la catégorie...](#)

Le 2 juillet 2020, soit quelques jours à peine avant que [la Cour de Justice de l'Union Européenne \(CJUE\) n'invalide le « Privacy Shield »](#), le CEPD (Contrôleur européen de la protection des données¹⁾) a publié un *Public Paper* intitulé « **Résultats de l'enquête d'initiative sur l'utilisation des produits et services Microsoft par les institutions européennes** »²⁾. Et le moins que l'on puisse dire est que ce rapport soulève de très (trop ?) nombreux problèmes !

Concernant le contrôle de la localisation des données, si les institutions de l'UE souhaitent maintenir les protections accordées par ses règlements contre la divulgation non autorisée, elles devraient sérieusement envisager :

- premièrement, de **veiller à ce que les données traitées en leur nom soient situées dans l'UE/EEE**, et
- deuxièmement, **n'utiliser que des prestataires de services qui ne sont pas soumis à des lois de pays tiers contradictoires à portée extraterritoriale** !



Le CEPD conseille aux organisations de ne pas envisager d'engager un sous-traitant qui n'est pas disposé à fournir des garanties suffisantes ! Pour se conformer au principe de la protection des données [...], les organisations devraient vérifier [...] si aucune autre solution logicielle alternative ne permet des garanties de confidentialité plus élevées.

De l'avis du CEPD, les organisations qui externalisent la fourniture ou l'exploitation de services numériques auprès d'autres fournisseurs de services que Microsoft – chez Google par exemple – sont également



susceptibles de rencontrer des problèmes similaires.

Dans son rapport d'enquête, après avoir étudié la compatibilité des accords de licence entre Microsoft et l'UE avec la réglementation (EU) 2018/1725³⁾, le CEPD en est arrivé aux conclusions suivantes :

1. L'accord de licence entre Microsoft et les institutions européennes a permis à Microsoft de définir et de modifier les paramètres de ses activités de traitement effectuées pour le compte des institutions européennes et de ses obligations contractuelles en matière de protection des données. Le pouvoir discrétionnaire dont disposait Microsoft équivalait à un droit étendu pour Microsoft d'agir en tant qu'organe de contrôle. Compte tenu du rôle des institutions de l'UE en tant qu'institutions de service public, le CEPD a estimé que cela n'était pas approprié. Le CEPD a recommandé aux institutions de l'UE d'agir de manière à maintenir leur fonction de contrôleur.
2. Les institutions de l'UE doivent mettre en place un accord complet et réglementaire entre contrôleur et exécutant et se doter d'instructions claires envers leurs contractants. Leur manque de contrôle sur les sous-contractants de Microsoft et l'absence de droits d'audit significatifs posent d'importants problèmes. Le CEPD a fait des recommandations sur la manière d'améliorer la convention entre le responsable du traitement et le sous-traitant et de mettre en place des contrôles d'audit solides.
3. Les institutions européennes ont été confrontées à un certain nombre de problèmes liés concernant la localisation des données, les transferts internationaux et le risque de divulgation illicite de données. Elles n'ont pas été en mesure de contrôler la localisation d'une grande partie des données traitées par Microsoft. Elles n'ont pas non plus contrôlé correctement ce qui était transféré hors de l'UE/EEE et comment. Il y avait également un manque de garanties appropriées pour protéger les données qui quittaient l'UE/EEE. Les institutions de l'UE disposaient également de peu de garanties pour défendre leurs droits et protections, de façon à s'assurer que Microsoft ne divulguerait des données personnelles que dans la mesure où la législation européenne le permettait. Le CEPD a fait des recommandations pour aider les institutions de l'UE à traiter ces questions.
4. Le CEPD a examiné les mesures techniques que la Commission avait mises en place pour endiguer le flux de données personnelles générées par les produits et services Microsoft et envoyées à Microsoft. Le CEPD a recommandé que toutes les institutions européennes effectuent des tests en utilisant une approche rémanée et exhaustive, partagent entre elles les connaissances et les solutions techniques qu'elles ont développées pour empêcher les flux de données non autorisés vers Microsoft et s'informent mutuellement de tout problème de protection des données qu'elles identifient avec les produits ou services.
5. Les institutions de l'UE n'ont pas été suffisamment claires quant à la nature, à la portée et aux finalités du traitement des données et aux risques encourus par les personnes concernées pour pouvoir remplir leurs obligations de transparence à l'égard de ces dernières. Le CEPD a recommandé que les institutions de l'UE recherchent la clarté et les garanties leur permettant de tenir les personnes concernées correctement informées.

Dès lors le CEPD conseille aux organisations de ne pas envisager d'engager un sous-traitant

(ou sous-contractants) qui n'est pas disposé à fournir des garanties suffisantes pour mettre en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement satisfasse aux exigences des règles de l'UE en matière de protection des données et assure la protection des droits des personnes concernées. Pour se conformer au principe de la protection des données dès la conception et par défaut, les organisations devraient vérifier à la fois lors de la planification du traitement et pendant le traitement, si aucune autre solution logicielle alternative ne permet des garanties de confidentialité plus élevées.

Concernant le contrôle de la localisation des données, les transferts internationaux et les divulgations de données, à moyen terme, si les institutions de l'UE souhaitent maintenir les protections accordées par le règlement (UE) 2018/1725 contre la divulgation non autorisée, elles devraient sérieusement envisager :

- premièrement, de veiller à ce que les données traitées en leur nom soient situées dans l'UE/EEE, et
- deuxièmement, n'utiliser que des prestataires de services qui ne sont pas soumis à des lois de pays tiers contradictoires à portée extraterritoriale.

Le CEPD reconnaît que la ligne de conduite recommandée aux institutions de l'UE peut sembler un défi de taille pour de nombreux clients, sinon pour la plupart, de licences en volume de Microsoft.

Le CEPD estime aussi que ces conclusions et recommandations sont susceptibles de présenter un intérêt plus large que celui des seules institutions de l'UE : elles peuvent présenter un intérêt particulier pour toutes les autorités publiques des États membres de l'UE/EEE. Elles sont également susceptibles d'être pertinentes au-delà de la conclusion et de la mise en œuvre d'accords de licence en volume pour les produits et services Microsoft. De l'avis du CEPD, les organisations qui externalisent la fourniture ou l'exploitation de services numériques auprès d'autres fournisseurs de services sont susceptibles de rencontrer des problèmes similaires.

Source

- [Consulter le rapport du CEPD](#) - Publié le 02/07/2020 [*Document en anglais*]



Il est à noter que quelques jours à peine après la publication du rapport du CEPD, la Cour de justice de l'Union européenne (CJUE) a invalidé le « Privacy Shield ». Ce qui corrobore et renforce notablement les arguments développés par le Contrôleur européen 🚨

Information complémentaire concernant la localisation des

données stockées par Microsoft

Concernant la localisation des données dans les différents *data centers* de Microsoft, la « [Déclaration de confidentialité Microsoft](#) » est assez explicite et annonce clairement que les données des utilisateurs sont susceptibles d'être stockées et dupliquées dans différentes régions du monde :

Les données personnelles recueillies par Microsoft peuvent être stockées et traitées dans votre région, aux États-Unis et dans tout autre pays dans lequel Microsoft, ses filiales ou fournisseurs de services sont implantés. [...] En règle générale, le lieu de stockage principal des données se situe dans la région du client ou aux États-Unis, une sauvegarde étant par ailleurs souvent stockée dans un centre de données situé dans une autre région. Les emplacements de stockage sont choisis de manière à assurer un fonctionnement efficace, à optimiser les performances et à créer des redondances afin de protéger les données en cas de panne ou de problème autre. [...]

Nous transférons des données personnelles issues de l'Espace économique européen, du Royaume-Uni et de Suisse vers d'autres pays, dont certains n'ont pas encore été reconnus par la Commission européenne comme offrant un niveau de protection adéquat des données. Par exemple, leurs lois peuvent ne pas vous garantir les mêmes droits, ou il est possible qu'il n'y ait pas d'autorité de contrôle en matière de protection des données personnelles capable de traiter vos plaintes.

[Déclaration de confidentialité Microsoft](#) - Section "Pays de stockage et de traitement des données personnelles" - Dernière mise à jour : Juillet 2021

Pages dans la catégorie :

- [Alternatives européennes aux services des gafam](#)
- [L'autorité française de protection des données déclare qu'elle ne peut pas confier des données personnelles européennes à de grandes entreprises américaines du secteur de l'internet, même si elles les conservent dans l'UE](#)
- [La Cour de justice de l'Union européenne \(CJUE\) invalide le « Privacy Shield » !](#)
- [Le Contrôleur européen de la protection des données \(CEPD\) recale les accords de licence avec Microsoft](#)
- [Les prochaines grandes batailles de la vie privée : les flux de données transfrontaliers et la localisation des données](#)
- [politique-des-cookies-de-badoo_com-20201227](#)

1) [Contrôleur européen de la protection des données](#) - Voir aussi [W l'article consacré au CEPD sur Wikipédia](#)

2) Le titre original en anglais est « Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services ».

3)

Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE. Ce règlement est également la base légale sur laquelle s'appuie le CEPD pour établir ses recommandations. – Voir le texte intégral : “[Règlement \(EU\) 2018/1725](#)”

From:

<https://wiki.educode.be/> - **Accompagner l'école face aux défis du numérique**

Permanent link:

https://wiki.educode.be/doku.php/vie_privee/le_cedp_recale_les_accords_de_licence_avec_microsoftLast update: **2021/09/08 11:32**