

Les données à caractère personnel peuvent-elles de nouveau être transmises librement aux États-Unis ?

Flash spécial. Saviez-vous que la Commission européenne a publié une nouvelle décision d'adéquation pour un « EU-US Data Privacy Framework » le 10 juillet 2023 ? Une telle décision d'adéquation signifie en principe que l'UE considère que le niveau de protection des données est suffisamment élevé et qu'elle autorise le transfert de données à caractère personnel de l'UE vers certaines entreprises aux États-Unis. Quelles en sont toutefois les implications pour votre entreprise ? Et combien de temps cette décision tiendra-t-elle, sachant que les deux précédentes décisions d'adéquation pour les États-Unis ont, à chaque fois, été invalidées ?

L'EU-US Data Privacy Framework

Selon le Règlement général sur la protection des données (RGPD ou GDPR), il est en principe interdit de transmettre des données à caractère personnel collectées dans l'UE à des organisations ou des entreprises établies dans des pays situés en dehors de l'UE. Un tel transfert n'est possible que s'il est démontré que l'organisation ou l'entreprise en question assure un niveau de protection adéquat (sur la base de la législation nationale ou de sa propre politique). Pour plusieurs pays tiers et organisations internationales, la Commission européenne a adopté une décision d'adéquation reconnaissant que le pays ou l'organisation en question assure un niveau de protection adéquat. Les données à caractère personnel peuvent alors être transférées au départ de l'UE sans autre formalité. Pour les États-Unis, il n'y avait jusqu'à récemment (plus) aucune décision d'adéquation et les entreprises devaient donc s'appuyer sur des règles d'entreprise contraignantes ou des clauses contractuelles types (CCT) approuvées par la Commission. La décision d'adéquation du 10 juillet 2023 a de nouveau changé la donne.

Cette décision d'adéquation s'est traduite par le « EU-US Privacy Framework ». Les organisations et entreprises américaines qui adhèrent à ce cadre ou « Framework » sont réputées garantir une protection adéquate des données à caractère personnel. La décision ne va donc pas jusqu'à déclarer l'ensemble des États-Unis comme adéquats. Prudence donc : vous ne pouvez transférer librement des données à caractère personnel qu'à des entreprises américaines inscrites dans ce « Framework ». Vérifiez [ici](#) si tel est bien le cas de l'entreprise avec laquelle vous collaborez

Les organisations et entreprises participantes s'engagent à respecter un ensemble de principes en matière de protection des données, élaborés par la Commission en collaboration avec le « Department of Commerce » américain. Ces organisations et entreprises procèdent ensuite à une auto-analyse de leur politique en matière de protection de la vie privée (appelée « Self-certification »), qu'elles soumettent au « Department of Commerce ». Si l'analyse est complète, le « Department of Commerce » inscrit l'entreprise sur la liste du « Framework ». Cette autocertification doit être renouvelée chaque année.

La grande nouveauté du « Framework » réside dans l'introduction de garanties contraignantes destinées à limiter l'accès des agences de renseignement américaines aux données à caractère personnel provenant de l'Union européenne à ce qui est « nécessaire et proportionné ». Il a également créé une autorité distincte et indépendante auprès de laquelle les Européens peuvent déposer une plainte concernant l'accès et l'utilisation de leurs données par les agences de renseignement américaines.

Véritable innovation ou du neuf avec du vieux ?

Ce système n'est pas sans rappeler les deux précédentes décisions d'adéquation de la Commission européenne concernant les États-Unis : le « US-EU Safe Harbor agreement » (2000-2015) et le « EU-US Privacy Shield » (2016-2020). Ces deux accords entre l'UE et les États-Unis ont été contestés par Maximilian Schrems devant la Cour de justice de l'Union européenne. Dans les deux affaires, la Cour a estimé que les décisions d'adéquation fondées sur ces accords violaient le RGPD et étaient donc non valides.

Ces deux systèmes prévoyaient eux aussi un engagement volontaire d'organisations et d'entreprises américaines de respecter les principes prescrits en matière de protection de la vie privée et une autocertification. Ce système d'autocertification n'était pas nécessairement problématique selon la Cour. Ce qui posait problème, c'était l'accès quasi illimité des agences de renseignement

américaines à toutes les données à caractère personnel. Cet accès devrait être limité à ce qui est strictement nécessaire et proportionné à la protection de la sécurité nationale. En outre, les citoyens européens n'avaient pas non plus de voie d'action devant un tribunal indépendant en cas de violation de leur vie privée par le gouvernement américain.

Dans son communiqué de presse sur le nouveau Data Privacy Framework, la Commission européenne assure qu'elle a maintenant vraiment répondu aux préoccupations de la Cour de justice de l'Union européenne et qu'elle a introduit des garanties suffisantes pour limiter l'accès des services de renseignement américains. Le scepticisme et les critiques restent toutefois très vifs dans les milieux professionnels.

L'ordre exécutif qui devrait intégrer ces garanties dans le système juridique américain n'est en réalité qu'une simple directive interne du président et non une loi. Ce texte semble en outre avoir été rédigé principalement pour brosser l'UE dans le sens du poil. Il contient des références aux principes de stricte nécessité et de proportionnalité, mais il subsiste de sérieux doutes quant à la mise en œuvre de ces principes dans la pratique. En effet, l'interprétation américaine de la notion de nécessité en matière de sécurité nationale est bien plus large que l'interprétation européenne. La nouvelle autorité fait également l'objet de critiques. Elle se présenterait de manière bien plus indépendante et transparente dans son travail qu'elle le serait en réalité. C'est pourquoi Maximilian Schrems a d'ores et déjà annoncé son intention de saisir la Cour de justice pour contester le Data Privacy Framework. Affaire à suivre...

Conséquences concrètes pour les entreprises européennes

Les entreprises belges et européennes peuvent en principe de nouveau partager librement des données à caractère personnel avec des entreprises américaines depuis le 10 juillet 2023, pour autant qu'elles soient reprises dans le « Framework ».

Attendez toutefois avant de déchirer vos clauses contractuelles types existantes ! Compte tenu de l'ampleur de la controverse, la plus grande prudence semble de mise. Si votre entreprise a déjà trouvé des bases alternatives pour les transferts de données vers les États-Unis, continuez de les privilégier. Si ces bases alternatives n'existent pas, ce n'est plus un problème pour l'instant, mais les choses pourraient de nouveau changer dans un avenir plus ou moins proche.

Pour l'instant, il suffit donc de vérifier si l'entreprise avec laquelle vous souhaitez collaborer est reprise dans le « Framework » (vérifiez [ici](#)). Si votre entreprise recherche une sécurité à long terme, nous vous suggérons toutefois d'envisager dès à présent des solutions alternatives. N'hésitez pas à contacter notre équipe pour analyser ensemble la meilleure solution pour votre entreprise.

Mechelsesteenweg 127A, b1 - 2018 Anvers

t. +32 3 260 98 60 | +32 2 790 44 44

Rue de la Régence 58 boîte 8 - 1000 Bruxelles

info@schoups.be

www.schoups.com