Cigref (a non-profit association of digital user companies) had the opportunity 10 months ago to work with lawyers from its member companies on the Privacy Shield and produced a position paper on the proposed EDPB recommendations published in June 2021. This text (in French) can be found at the end of this document. Regarding the EDPB document published in June 2022, we will work again on this subject, but it seems to us that the questions and recommendations and the problems that companies encounter, expressed 10 months ago, are still relevant. We are therefore providing you with the full text as our contribution

Position paper – Privacy Shield

version 9.0 (novembre 2021)

Rappel du contexte

Entre 2000 et 2015, les transferts de données personnelles vers les USA étaient réglementés par le *Safe Harbor* qui permettait d'offrir des garanties équivalentes à celles qui existaient au sein de l'UE quant à leur protection. Mais la possibilité d'ingérence des autorités américaines sur les données personnelles des citoyens européens a été révélée avec l'affaire SNOWDEN, qui a montré que les services de renseignements américains pouvaient avoir accès à ces données, brisant ainsi le principe de confidentialité et de transparence.

En 2015, Max SCHREMS, considérant que les transferts de données personnelles avec les USA n'étaient pas légaux, obtient de la Cour de justice de l'Union européenne (CJUE) l'annulation du *Safe Harbor* au motif que les conditions de confidentialité n'étaient pas respectées et qu'il n'y avait pas de recours effectif pour les personnes physiques concernées.

En 2016, l'UE promulgue une décision d'adéquation du *Privacy Shield*, négocié entre USA et l'UE et qui propose, comme le *Safe Harbor,* des garanties équivalentes à celles de l'UE mais complétées par des conditions supplémentaires censées éviter la surveillance massive des autorités américaines sur les données personnelles des Européens (avec la création d'une autorité indépendante, un médiateur…).

En 2018, avec le RGPD, l'UE institue le principe d'une protection (accordée par l'Union européenne) qui voyage avec la donnée, où qu'elle aille dans le monde.

En 2020 , Max SCHREMS, suite au dépôt d'une nouvelle requête auprès de la CJUE pour les mêmes raisons qu'en 2015, obtient de la CJUE l'invalidation du *Privacy Shield*. La CJUE motive sa décision ainsi : « *le droit américain ne permet pas d'assurer un niveau de protection essentiellement équivalent* » à celui prévu par le RGPD « *en ce que les programmes de surveillance ne sont pas limités au strict nécessaire* » et que « *les ingérences par les autorités américaines ne confèrent pas d'accès à un tribunal impartial* ». La surveillance des données personnelles des européens est donc toujours possible par les autorités américaines, sans possibilité de recours efficace.

Conséquences immédiates

Les USA, pays inadéquat

Dans ses attendus, le juge de la CJUE s'est prononcé sur les garanties et particulièrement sur le régime juridique américain pour savoir si les clauses pouvaient être respectées. Notamment vis à vis de

l'exploitation des données personnelles des ressortissants non américains (« *non-US persons* »), des lois américaines FISA et de l'*Executive Order* 12333 (directive présidentielle autorisant les agences de renseignement à opérer au-delà des frontières, hors des cadres habituels). Pour ces dernières, il a considéré que les garanties n'étaient justement pas suffisantes, rendant *de facto* illégaux les transferts entre l'Europe et les USA, ces derniers pouvant être considérés alors comme un pays inadéquat. Enfin, si les transferts ont été interdits, les accès des autorités américaines aux données personnelles par le biais d'une société américaine qui aurait une filiale ou une antenne européenne, ont également été interdits puisque ces sociétés qui avaient adhéré au RGPD en Europe ont aussi dû adhérer en parallèle aux lois américaines.

Suite à cette invalidation du *Privacy Shield,* les entreprises échangeant des données avec les USA s'exposent désormais à un risque de non-conformité au RGPD, pouvant entraîner une atteinte à la sécurité et à la confidentialité des données traitées, avec des sanctions en termes financier, pénal et d'image. En conséquence, tous les traitements et transferts non conformes se devaient d'être interrompus, suspendus ou régularisés au plus tôt. Pour les contrats d'avant le 27 juin 2021 et qui comportaient déjà des de Clause Contractuelles Types (CCT), un délai courant a néanmoins été accordé jusqu'à la fin 2022.

Le 11 novembre 2020, deux nouvelles lignes directrices (*guidances*) du Comité européen de protection des données (CEPD) sont venues compléter l'invalidation du *Privacy Shield* : ces recommandations mettent en exergue des mesures supplémentaires pour l'ensemble des pays inadéquats (pas uniquement les USA). Pour chaque pays inadéquat, les entreprises devront alors passer un nombre d'étapes importantes et contraignantes pour savoir si le pays tiers vers lequel les données sont transférées à une autorité indépendante, une loi renforcée, des possibilités de recours...

Des Clauses Contractuelles Types (CCT) à renforcer

Pour faciliter la mise en œuvre des transferts de données personnelles vers des pays importateurs, le RGPD propose plusieurs outils juridiques au-delà du *Privacy Shield*, notamment la mise en place de CCT contractualisant les règles de transferts de données hors de l'Union européenne entre exportateurs et importateurs de données (responsables de traitements vis-à-vis de sous-traitants ou de responsables de traitement distincts ou conjoints).

Dans son arrêté, le juge a considéré que les garanties contenues dans ces clauses ne posaient pas de difficulté et donc que les CCT n'avaient pas besoin d'être invalidées et sont utilisables tout en devant être renforcées. La réalité montre que si les CCT restent utilisables, la capacité des entreprises à démontrer qu'elle répondent à l'attendu de la décision n'est pas, ou très difficilement, atteignable.

Pour beaucoup d'entreprises, les CCT semblent néanmoins protectrices. Pourtant le responsable de traitement / exportateur doit s'assurer de la protection fournie par l'outil juridique utilisé et dans le cas des USA, cette protection n'est pas assurée, ce qui fait tomber le *Privacy Shield* mais aussi les CCT sauf à mettre en œuvre des mesures supplémentaires mais inatteignables.

Dans sa décision (arrêt C-311/18 - SCHREMS II) , la CJUE précise effectivement que les responsables de traitement ou les sous-traitants, agissant en tant qu'exportateurs de données, sont chargés de vérifier, au cas par cas et, le cas échéant, en collaboration avec l'importateur dans le pays tiers, si la législation ou la pratique du pays tiers empiète sur l'efficacité des garanties appropriées contenues dans les outils de transfert de l'article 46 GDPR.

En effet, le lien entre les clauses et les garanties du pays importateur (destinataire) des données peut poser problème : si jamais la loi du pays ne permet pas à l'importateur de respecter son engagement

contractuel, il n'y a plus de protection. La question est donc de savoir si les éléments mis dans ces clauses contractuelles seront respectés dans le pays de destination. Tout en étant conscient que les clauses contractuelles ne prévalent pas sur la loi et la réglementation locale.

Du reste, le juge rappelle dans son arrêt qu'une vérification doit être faite par l'exportateur des données (l'entreprise européenne) en collaboration avec l'importateur avant la transmission. S'il y a un problème il doit alors mettre en place des mesures supplémentaires et si ce n'est pas le cas, les données ne peuvent pas être transmises. Cette décision est transposable pour l'ensemble des pays : le juge de la CJUE s'est basé sur les *European Essential Guarantees for surveillance measures* (qui ont été mises à jour suite à SHREMS II), pour considérer, ou pas, si le régime juridique américain offrait une protection suffisante et l'a répliqué pour les autres pays.

Le 13 novembre 2020 la Commission européenne a fait évoluer son cadre de transfert de données en revoyant les CCT et en les adaptant au RGPD. Deux *templates* de clauses qui n'existaient pas ont été ajoutés : aux *templates* existants de transfert « de responsable de traitement à responsable de traitement » et de « responsable de traitement à sous-traitant », la Commission a ajouté un jeu de clauses « de sous-traitant à sous-traitant » et « de sous-traitant à responsable de traitement ».

Regard sur les recommandations de l'EDPB

Au regard de l'arrêt SCHREMS II de la CJUE, l'EDPB (*European Data Protection Board*) a publié le 14 juin 2022 un ensemble de recommandations censées aider les entreprises exportatrices de données dans les transferts vers des pays tiers. Elle préconise notamment un ensemble d'étapes à suivre pour s'assurer de la conformité des transferts et décider de résilier ou non les contrats avec les importateurs de données des pays tiers.

Connaître ses transferts

L'EDPB rappelle que les entreprises exportatrices de données doivent posséder une cartographie de tous les transferts de données personnelles vers des pays tiers. Au regard de l'application du RGPD par les entreprises françaises, cette cartographie nous apparaît comme évidemment acquise ou en cours d'acquisition et mise à jour régulièrement par les experts idoines que sont notamment les DPO. Il faut néanmoins reconnaitre la difficulté pour ces experts d'avoir une connaissance parfaite de ces transferts vers des pays « inadéquats » en cas de sous-traitance « en cascade ». De plus, bien que l'EDPB écrit qu'il faut aller jusqu'au bout de la chaîne de sous-traitance, le niveau demandé de granularité de cette cartographie n'est pas clair et jugé irréaliste.

Vérifier l'outil de transfert sur lequel repose le transfert des données

Les entreprises qui transféraient déjà des données, avant l'invalidation du *Privacy Shield*, utilisaient les outils énumérés à l'article 46 du RGPD, et dans certains cas spécifiques s'appuyaient sur des dérogations prévues à l'article 49 du RGPD. Mais il apparait que ces outils ne sont plus applicables aujourd'hui dans le cadre des échanges avec les USA.

Évaluer les lois et réglementations des pays importateurs de données

La responsabilité de l'évaluation des lois et réglementations de pays tiers incomberait aux entreprises exportatrices de données. Or les grandes organisations ont souvent un volume important d'échanges de données avec un nombre conséquent de prestataires internationaux, en particulier américains du fait de leur présence globale et mondiale. De même, de nombreuses entreprises plus petites effectuent également des transferts de données vers l'international, et notamment les USA.

L'identification et l'évaluation des lois et réglementations de pays tiers nécessitent de se doter des bonnes ressources d'expertise. Cette expertise est essentiellement juridique, mais pas seulement : sont également impliquées toutes les ressources qui contribuent aux processus de traitement des données exportées. On y retrouve notamment les directions achats, les directions des systèmes d'information et dans une certaine mesure, les directions métiers.

Cette évaluation risque également de diverger d'une entreprise à l'autre sur la compréhension des lois locales. Une autorité qui validerait cette compréhension semble indispensable. De plus la Commission européenne a déjà identifié un ensemble de pays non conformes, ce qui indique qu'il y a eu déjà une analyse de faite, sur laquelle les entreprises pourraient s'appuyer, et donc qu'elle possède les critères qui permettent de qualifier un pays non conforme.

Identifier et adopter des mesures supplémentaires si nécessaire

Dans le cas où l'évaluation révèle que la législation et/ou les pratiques du pays tiers empiètent sur l'efficacité de l'outil de transfert de l'article 46 GDPR, des mesures complémentaires doivent être prises pour assurer un niveau de protection des données au niveau de la norme européenne. Mais l'EDPB définit un niveau d'exigence qui n'est ni atteignable ni démontrable à ce jour par les mesures techniques et ne permet pas d'évaluer le risque pris.

L'EDPB donne dans son avis un ensemble de recommandations mais précise que cette liste n'est pas exhaustive. Elle laisse surtout à l'entreprise exportatrice de données la responsabilité d'évaluer l'efficacité des mesures supplémentaires prises, alors qu'aucun critère d'évaluation n'est fourni. Or cette évaluation dépend de multiples facteurs : lois locales, typologies et sensibilité des données, acteurs dans la chaîne de traitement, etc.

Prendre les mesures procédurales formelles liées aux mesures complémentaires

Il s'agit ensuite de mettre en place les formalités procédurales liées aux mesures supplémentaires qui auront été décidées. L'EDPB conseille de s'appuyer sur les autorités de contrôle compétences pour cela, la CNIL pour la France. La question est de savoir si la CNIL saura répondre aux interrogations dans un temps suffisamment court pour ne pas nuire aux entreprises.

Réévaluer à intervalles réguliers le niveau de protection

La mise en place du RGPD implique déjà ce processus de révision régulière et était déjà prévu ou mis en place avant l'invalidation du *Privacy Shield*.

Problématiques posées aux entreprises

Profondeurs des audits

L'EDPB note (§112 premier alinéa) que « *Pour être pleinement efficace, la portée de l'audit doit couvrir, sur le plan juridique et technique, tout traitement par les sous-traitants ou sous-traitants secondaires de l'importateur des données à caractère personnel transmises dans le pays tiers* ».

Cela signifierait donc que l'entreprise exportatrice de données ait le pouvoir d'auditer les sous-traitants secondaires des pays tiers. Or le contrat qui comprend les CCT est passé entre l'entreprise importatrice de données et son sous-traitant direct. Si c'est effectivement le cas, on outrepasse les obligations du RGPD lui-même : les obligations doivent être contractualisées avec le sous-traitant (le responsable de traitement) de premier niveau mais pas avec toute la chaîne de sous-traitance. Il ne doit pas être possible d'aller au-delà de ce qui est déjà écrit (article 28-3 du RGPD).

Évaluation de la conformité des transferts

Comment évaluer de manière objective la conformité d'un transfert ? La question est importante car d'une entreprise à l'autre, l'expertise juridique peut différer pour le même contexte de transfert, vers un même pays. Il n'existe pas aujourd'hui de base harmonisée d'analyses qui définissent en fonction des pays, des typologies de données ou des acteurs ce qu'est un transfert légal.

De plus, de nombreuses entreprises ont mis en place des CCT mais que cela soit au niveau du contrat ou des mesures, les entreprises restent dans une situation d'incertitude juridique globale, quelles que soient les mesures mises en œuvre car les CCT sont difficiles à faire appliquer, notamment par les USA.

Finalement, les transferts vers les USA apparaissent aujourd'hui de facto illégaux. Sauf à organiser un système de sécurité qui nécessite un investissement important et qui n'est pas forcément possible en fonction du type de prestataire.

Lourdeur du processus

Celle réglementation ne s'applique pas qu'aux grandes organisations et nous avons vu précédemment que le processus proposé par l'EDPB pour la mettre en œuvre mobilise de nombreuses ressources et des compétences diverses.

Si au niveau juridique les tâches à mener sont clairement identifiées, sur les autres métiers ce n'est pas véritablement le cas :

- Les nombreuses étapes recommandées pénalisent par exemple les chefs de projets qui vivent un véritable « parcours du combattant » lorsqu'ils doivent transférer des données personnelles vers des pays tiers.
- L'innovation et la transformation numérique des organisations internationales risquent d'être freinées par une mise en attente de nombreux projets notamment Métiers alors qu'ils pourraient être déployés plus vite.
- La vérification et le façonnage des contrats par les acheteurs n'en deviennent que plus complexes. Le risque étant alors de privilégier les gros prestataires qui pourront répondre au détriment des petits qui n'en n'auront pas les moyens, les ressources ou le temps. Là encore, l'innovation qui vient pour beaucoup des petites structures (en Europe ou ailleurs) risque d'en pâtir.

Impact sur le citoyen

La complexité de la mise en œuvre de ces recommandations risque également de mettre en péril le consommateur final. Notamment parce que si les grosses organisations peuvent, tant que faire se peut, respecter au mieux la réglementation, les petites organisations qui n'en n'ont ni les moyens ni les compétences risquent de prendre des raccourcis pouvant mener à de graves problèmes pour le client, et au final le citoyen européen. Par exemple, si les entreprises françaises et européennes ne sont pas aidées efficacement pour être au clair avec la réglementation, de nombreux projets d'innovation se trouveront freinés et le citoyen risque de se tourner vers des services offerts par des opérateurs internationaux et notamment américains.

Recommandations

Les entreprises sont particulièrement attentives à respecter la réglementation européenne. La protection des données personnelles des citoyens européens dans le cas d'échanges avec des partenaires ou prestataires internationaux est l'une de leurs principales priorités.

Cela fait maintenant une année que le *Privacy Shield* a été invalidé. Les entreprises, bien que jusqu'à présent dans un *no man's land* juridique, sont constamment sur le qui-vive pour s'assurer que les données transférées et les traitements afférents ne nuisent pas à la sécurité des citoyens européens.

Or les autorités doivent assumer leur propre règlement et s'impliquer davantage pour la mise en œuvre rapide de solutions. Il ne s'agit plus de savoir quoi faire, mais de faire, or le temps est notre ennemi. La prolongation de cette situation et la difficulté d'implémentation des solutions proposées peuvent nuire à la compétitivité internationale des entreprises françaises et européennes.

Dans un esprit constructif, afin d'aider toutes les entreprises françaises et européennes, grandes comme petites, de l'écosystème numérique ou utilisatrices de solutions numériques, nous proposons trois chantiers qui nous paraissent indispensables pour avancer rapidement

1. Mettre en place un mécanisme d'analyse juridique harmonisé des lois locales des pays tiers.

   L'objectif est d'une part d'avoir une compréhension commune des législations et réglementations en vigueur concernant les données personnelles. D'autre part d'aider les entreprises à définir un cadre d'application des solutions à mettre en œuvre : en effet, si les GE ont des structures juridiques importantes, ce n'est pas le cas des PME. Enfin, cela permettrait aux entreprises de savoir ce qui est une mesure réglementaire acceptable ou pas.

2. Construire de manière consensuelle une *white / black list* de recommandations

   Cette liste devrait permettre d'apporter des réponses pratiques sur la légalité du transfert au regard de la loi de l'importateur et la validité des mécanismes de protection mis en place (CCT, BCR...). Elle pourrait être étendue aux mesures techniques supplémentaires. L'EDPB dans son avis du 18 juin 2021 en propose certaines, mais cette liste est trop imparfaite et limitée. De plus, elle ne tient pas suffisamment compte des contextes d'application (lois, types de données, niveaux d'acteurs…).

3. Définir une approche par les risques dans la mise en œuvre des solutions

   Cette approche serait basée sur les recommandations de la *white / black list* pour permettre d'agir en conséquence en fonction des types de données mais aussi de leur qualité ou de leur volumétrie. il serait par exemple très utile de savoir :

   - Quelles sont les mesures *a minima* pour les acteurs qui ont des données sensibles ?
   - Quelles sont les mesures *a minima* si les données ne sont pas sensibles mais les volumes conséquents ?
   - Quelles sont les mesures *a minima* si les données ne sont pas sensibles et les volumes de données peu conséquents ?