CONSULTATION DU COMITE EUROPEEN POUR LA PROTECTION DES DONNEES (« CEPD ») SUR SA RECOMMENDATION 01/2020 SUR DES MESURES COMPLEMENTAIRES PERMETTANT D'ASSURER LA CONFORMITE DES OUTILS DE TRANSFERT VERS DES PAYS TIERS AVEC LE RGPD

Commentaires de l'Afep (Association française des entreprises privées)

Le Comité européen de la protection des données (« CEDP ») soumet à consultation jusqu'au 21 décembre sa Recommandation 01/2020 sur des mesures complémentaires permettant d'assurer la conformité des outils de transfert vers des pays tiers avec le RGPD.

Cette Recommandation apparaît comme une nécessaire mise à niveau à la suite du récent arrêt C-311/18 de la CJUE (« Schrems II »). Celui-ci en substance invalide le Privacy Shield (la décision d'adéquation avec les Etats-Unis) et confirme la validité -sous certaines conditions- des clauses contractuelles types qui permettent des transferts vers des pays pour lesquels un accord d'adéquation n'existe pas (ci-après « pays tiers »).

- Si les entreprises apprécient l'effort du CEPD de fournir un schéma procédural clair pour une application cohérente par les autorités de contrôle et les acteurs économiques européens, elles émettent cependant de fortes inquiétudes sur deux points issus des conditions posées par l'arrêt de la CJUE qui complexifient la mise en œuvre effective de ces clauses.
- Dans ce cadre, elles préconisent la suspension de l'application de cette Recommandation pour entamer un échange approfondi entre les autorités et les acteurs économiques européens afin de résoudre ces difficultés au mieux.

---

1 Fortes inquiétudes sur deux points majeurs

i) L'analyse des lois locales et les éventuelles mesures supplémentaires : une charge inadaptée pour les acteurs privés

Les acteurs économiques exportant (« data exporters ») des données dans des pays tiers devraient évaluer si le cadre juridique et les pratiques des pays tiers portent atteinte à une protection efficace des outils de transfert des données:

- La Recommandation exige (étape 3) que les exportateurs de données garantissent (« you must assess ») l'adéquation du cadre juridique général du pays tiers aux règles européennes au vu des circonstances spécifiques du transfert ; dans ce cadre juridique, l'accès aux données requis par certaines autorités ou gouvernements de pays tiers est expressément mentionné ;
- Si des inadéquations sont constatées, le CEPD requiert (étape 4) de l'exportateur de données qu'il prenne des mesures supplémentaires permettant de combler ces atteintes locales à la mise en œuvre effective du cadre européen; parmi ces mesures, figure le chiffrement ou la pseudonymisation des données (§ 49) ;
- Si l'adoption de telles mesures est impossible, alors le transfert de données doit être évité, suspendu ou arrêté.

L'Afep ne peut accepter cette procédure qui remet en cause le cadre posé par le RGPD qui charge la Commission Européenne ou une autorité de contrôle d'adopter des clauses types de protection des données (article 46-c et d). Cette « liste blanche » adoptée par la Commission crée un cadre juridique commun et stable. La recommandation du CEPD inverse cette logique en proposant que les entreprises remplacent la Commission, développent leurs propres « listes noires privées » de pays non conformes au RGPD et les réactualisent si ce cadre juridique évolue.

En outre, cette approche est juridiquement non pertinente et technologiquement irréaliste :

- Juridiquement, il n'est pas raisonnable d'envisager que des clauses contractuelles et des mesures supplémentaires puissent avoir une valeur juridique supérieure à des lois locales,
- Technologiquement, aucun opérateur européen ne peut proposer à ce stade aux entreprises européennes une offre technologique comparable aussi performante que celle déployée par les acteurs américains (maintenance, vitesse de flux, …). En outre, les rares acteurs européens tels que l'opérateur allemand SAP ne peuvent empêcher l'accès à distance à partir de pays tiers, qui cristallise une partie des préoccupations du juge européen.

Le CEPD alourdit donc la charge pesant sur les exportateurs européens de données.

- *En termes d'efficience :* les exportateurs privés de données (« data exporter ») souhaitant transférer -ou transférant depuis de nombreuses années- leurs données dans des pays tiers devront désormais analyser la compatibilité des lois nationales concernées. Il s'agit d'une charge lourde pour une seule entreprise. A l'évidence, il serait beaucoup plus efficace que l'essentiel de l'évaluation soit fait collectivement par les autorités susceptibles de contrôler les entreprises européennes.

    - Il est essentiel de conserver la hiérarchie prévue par le RGPD dans les mécanismes permettant le transfert. Pour un même pays, des interprétations divergentes par les différentes entreprises ne permettront pas une bonne application des CCT et, de manière générale, des mesures protectrices des données ; une telle divergence de vues est contraire aux objectifs de cohérence recherchés par cet outil et source de forte insécurité juridique pour les acteurs économiques.
    - Les évaluations d'adéquation devraient donc être menées par la Commission ou le CEPD qui devraient maintenir une base de données des évaluations au niveau européen, base pouvant évoluer à mesure que les lois et les pratiques changent, et qui serait librement accessible aux organisations.
    - Sans cette cohérence générale, l'utilité des CCT est remise en question, dès lors qu'elles impliquent des diligences complémentaires au cas par cas, alors qu'elles visaient à fournir un cadre juridique global aux acteurs opérant des transferts.
    - Les mesures supplémentaires -telles que le chiffrement des données- alourdissent un peu plus la charge des entreprises dont le développement à l'international s'en trouvera considérablement freiné. Dès lors que des données -de toute nature- seraient localisées ou accessibles depuis un pays tiers non conforme au RGPD, elles devraient être chiffrées. Imagine-t-on la complexité d'échanges chiffrés au sein d'un groupe avec ses filiales réparties dans ces pays pour finaliser un contrat commercial ou la gestion d'une carrière ?

- *En termes de process* : l'ensemble de la procédure envisagée est lourde, coûteuse et longue ; cette multiplication de charges administratives ne semble pas conforme à l'esprit du RGPD qui préconise en particulier une approche par les risques : ici, les mêmes contraintes sont requises quel que soit le type de données transférées (données sensibles ou pas, biométriques, financières et « critiques », B2B, B2C, etc.) alors que :

    - Certains pays tels que l'Australie ou l'Inde opèrent cette distinction qui allège de facto la charge pesant sur les acteurs économiques ;
    - Les textes américains encadrant l'accès gouvernemental aux données ("FISA 702", en particulier) opèrent également une différentiation dans les données visées : par ex, les données RH ne sont pas concernées ;

- Le risque d'être réellement soumis à une demande de données varie selon le modèle commercial de l'exportateur et de l'importateur (transferts de données à des fins commerciales ou réseaux sociaux), et selon la catégorie de données (données commerciales ou données personnelles).

- *En termes de responsabilité :* selon la Recommandation, les « data exporters » seraient responsables d'une telle analyse et des mesures supplémentaires à prendre, le cas échéant. Pour les raisons évoquées supra, ce n'est pas envisageable. Cette évaluation doit revenir en premier chef à la Commission européenne ou aux Autorités de protection des données, conformément aux dispositions prévues par le RGPD. A défaut c'est au « data importer » que doit revenir cette tâche. Il aurait en effet une meilleure connaissance de la réglementation de son propre pays et son évaluation garantirait la qualité de cette analyse.

ii) La date d'entrée en vigueur de cette décision : à reporter

L'ensemble des mesures de cette Recommandation est d'application immédiate.

Mettre en place de telles mesures est un défi pour de nombreuses entreprises, de toute taille. Si la conformité au RGPD n'est pas assurée, il est requis de suspendre le transfert de données et de mettre fin au contrat. Mais quelle est la conséquence pour les données dont le traitement serait suspendu ? Comment remplacer les importateurs de données habituels ?

Cette contrainte calendaire induit en outre pour les entreprises européennes de forts risques de sanctions (jusqu'à 4% de leur CA monde) ou réputationnels peu souhaitables dans cette période économique complexe.

<u>L'Afep recommande donc les modalités suivantes :</u>

i) Développer les décisions d'adéquation

Les entreprises souhaiteraient davantage se reposer sur des décisions d'adéquation que sur les clauses types de protection des données ou les règles d'entreprise contraignantes. Il est donc important d'accroître le nombre de décisions d'adéquation, et, pour se faire, d'établir des priorités sans pour autant renoncer à l'impératif d'un niveau équivalent de protection.

En premier lieu, les entreprises soulignent l'intérêt d'adopter rapidement des décisions d'adéquation pour les pays tiers avec lesquels les volumes d'échanges matériels et numériques sont importants (Australie, Brésil, Grande-Bretagne, Inde). Elles saluent l'approche suivie avec le Japon qui a consisté à jumeler les négociations de l'accord de partenariat économique avec le processus d'adoption de décisions jumelles d'adéquation.

A titre secondaire, une solution pourrait être d'accélérer et/ou de simplifier l'adoption de décision d'adéquation avec les pays qui présentent non seulement un niveau de protection équivalent mais aussi des architectures juridiques assez proches avec notamment un rôle décisif accordés aux autorités indépendantes de protection des données.

A minima, il est indispensable que les autorités européennes examinent l'adéquation des dispositifs nationaux des pays tiers et spécifient les difficultés que ceux-ci présentent vis-à-vis du RGPD

ii) A terme, adopter une approche plus flexible du transfert des données en cas de convergence juridique

Compte tenu du fait qu'un nombre croissant de pays adoptent des régimes de protection des données inspirés par le RGPD, il serait souhaitable que l'UE opte pour une nouvelle approche du transfert des données vers les pays tiers, avec comme principe de base, le libre transfert des données personnelles vers les pays tiers lorsque leur système juridique garantit un niveau équivalent de protection des données et sous réserve d'exception d'ordre public. Cette nouvelle approche ne signifie pas nécessairement la remise en cause des décisions d'adéquation mais

pourrait aboutir à ce qu'elles soient plus faciles à adopter et que l'UE se dote au contraire d'une logique de listes noires des pays vers lesquels les transferts seraient prohibés et restreints.

Cette approche faciliterait également la conclusion des dispositions sur les données dans les accords de libre-échange puisque la plupart des pays tiers acceptent le standard adopté dans l'Accord de partenariat transpacifique qui reconnaît le principe de libre transfert des données non personnelles et personnelles, sous réserve de limites liées aux objectifs de politique publique dans la protection des données personnelles.

iii) Suspendre la mise en œuvre de ces dispositions

L'application immédiate de cette Recommandation est totalement irréaliste pour les agents économiques. Des expériences passées similaires ont démontré l'importance de donner du temps aux opérateurs économiques pour une mise en œuvre opérationnelle des nouvelles exigences (ex : les lignes directrices de l'Autorité Bancaire Européenne sur l'outsourcing publiées en février 2019 ont prévu une mise en conformité au plus tard en décembre 2021 pour les contrats en cours). Par analogie pragmatique, un délai de grâce de trois ans devrait être privilégié.

Ce délai permettrait notamment de :

- réfléchir à l'opportunité de distinguer le type de données (sensibles ou non, BtoB/ BtoC) visées par cette recommandation en conformité avec l'approche par les risques prônée par le RGPD ; il est à noter que le projet de CCT de la Commission européenne a une approche proportionnée en la matière ;
- en ce sens, établir une liste des données ne faisant pas l'objet de demandes au titre de la Section 702 du "Foreign Intelligence Surveillance Act" ("FISA 702") ; une telle liste permettrait d'alléger les contraintes des entreprises et de fonder une future décision d'adéquation sur des bases juridiques plus solides
- revoir certains exemples produits en annexe 2 : les cas 6 et 7 illustrant des exemples de mesures supplémentaires non appropriées sont trop larges dans leur application et conduisent à des situations de blocages pour des sociétés ayant des filiales dans de nombreux pays.

iv) Eviter toute rétroactivité en précisant le champ d'application de ce projet

Seuls les nouveaux projets de CCT devraient être concernés par ces contraintes, à l'exception des contrats en cours. De nombreux contrats étant valides au-delà de cette seule année, les CCT présentes dans les contrats en cours devraient demeurer valides jusqu'à l'expiration ou le renouvellement de ces contrats. Les CCT actuelles ayant offert un niveau de protection et de garanties adéquat pendant plusieurs décennies et les parties étant déjà tenues de vérifier si des mesures supplémentaires doivent être mises en place, la demande de mise à jour de tous les contrats semble peu utile et extrêmement lourde. Exiger des importateurs et exportateurs d'appliquer les CCT révisées aux seuls nouveaux contrats suffira à remplir les exigences en termes de sécurisation des transferts de données dans des pays tiers.

***

Les entreprises de l'Afep soutiennent les ambitions des autorités européennes de faire respecter les normes de protection des données personnelles en faveur des citoyens, consommateurs ou salariés de l'UE. Cela doit cependant aller de pair avec des flux de données fluides dans le monde entier et sans contraintes administratives et financières inutiles et disproportionnées pour les entreprises européennes.

A ce stade, cette Recommandation conduit les entreprises européennes dans une impasse juridique et technologique, les chargeant d'une responsabilité allant au-delà des dispositions du RGPD sans leur apporter de solutions pragmatiques.

Les difficultés, rencontrées depuis plusieurs années par les institutions gouvernementales, à conférer un cadre juridique stable et sécurisé aux transferts hors Union Européenne -après avoir encouragé les échanges entre

économies ouvertes et le développement des transferts d'informations- ne devraient pas conduire à faire peser tous les risques liés à ces transferts sur les seuls exportateurs de données.

Les entreprises sont disposées à travailler en collaboration étroite avec les autorités de contrôle et les principaux prestataires informatiques afin de parvenir à des solutions réalistes et proportionnées (mutualisation d'une partie des analyses, révision des mesures complémentaires, valorisation de l'approche par les risques) pour maintenir les opérations de transfert qui sont un élément clé de leur fonctionnement et de leur développement comme elles sont stratégiques pour la compétitivité mondiale de l'Europe.

***

AU SUJET DE L'AFEP

Depuis 1982, l'Afep regroupe de grandes entreprises présentes en France. L'association, basée à Paris et à Bruxelles, a pour objectif de favoriser un environnement favorable aux entreprises et de présenter la vision de ses membres aux pouvoirs publics français, aux institutions européennes et aux organisations internationales. Le rétablissement de la compétitivité des entreprises pour parvenir à la croissance et à l'emploi durable en Europe et relever les défis de la mondialisation est la priorité de l'Afep. L'Afep compte environ 113 membres. Plus de 8 millions de personnes sont employées par les entreprises de l'Afep et leur chiffre d'affaires annuel cumulé s'élève à 2 600 milliards d'euros.

CONTACTS

Emmanuelle Flament-Mascaret – Directrice Droit économique / concurrence@afep.com

Alix Fontaine – Chargée de mission Affaires européennes / a.fontaine@afep.com