

Consultation publique sur la feuille de route en vue d'un rapport sur l'application du RGPD

REPONSE DE L'AFEP (ASSOCIATION FRANCAISE DES ENTREPRISES PRIVEES)

La Commission européenne a lancé une [consultation publique](#) jusqu'au 29 avril sur sa [feuille de route](#) en vue de l'établissement du **rapport sur l'application du règlement général sur la protection des données** (RGPD) qui sera rendu public d'ici le 25 mai 2020.

Ce rapport entend identifier les problèmes potentiels dans l'application du RGPD en se focalisant principalement sur la question du **transfert international de données à caractère personnel vers des pays tiers et les décisions d'adéquation existantes (chapitre V)** ainsi que sur le mécanisme de **coopération et de cohérence entre les autorités nationales de protection des données (chapitre VII)**.

En substance, les entreprises souhaitent :

- Une **évolution de l'approche en matière de transfert de données vers un principe de libéralisation accrue** du fait de la convergence croissante des régimes de protection des données personnelles,
- En tout état de cause, avoir la possibilité de **s'appuyer davantage sur les décisions d'adéquation** plutôt que de recourir par défaut aux instruments alternatifs (règles d'entreprises contraignantes et surtout clauses types de protection des données) et donc une **augmentation du nombre de décisions d'adéquation** et une **accélération des procédures d'adoption de celles-ci**,
- Pour ce faire, une **clarification des critères** sur lesquels la Commission européenne prend les décisions d'adéquation avec, notamment une priorité donnée aux pays avec lesquels sont négociés des accords de libre-échange et les pays dont l'architecture juridique est la plus proche,
- Un **renforcement de la réciprocité dans les échanges de données**, notamment par le levier des accords de libre-échange en l'incluant comme **critère explicite et obligatoire pour l'adoption des décisions d'adéquation**,
- Une **meilleure coordination des autorités nationales** pour la mise en œuvre de ce règlement,
- Une **harmonisation renforcée des pratiques et interprétations**,
- Une **mise à jour de certaines dispositions**.

1. Sur le chapitre V

Les grandes entreprises effectuent de nombreux transferts de données personnelles vers des pays tiers sur la base du chapitre V du RGPD dont elles apprécient le principe d'extra-territorialité. Pour autant, la réalité de ces échanges hors UE les conduit à souligner la nécessité pour la CE de corriger lors de l'élaboration de son futur rapport divers travers ou imprécisions relatifs aux **décisions d'adéquation (art 45) et aux clauses contractuelles types (« CCT » - art 46)**, outils majeurs dans la vie des entreprises pour la circulation pratique de ces flux de données que pour la responsabilité juridique y afférant (« accountability »).

- **Limites actuelles dans le maniement des outils de transfert de données vers les pays tiers**

Les entreprises ont appris à utiliser les outils de transferts de données vers les pays que sont les solutions donnant lieu à décisions d'adéquation comme le « Privacy Shield » ou les instruments prévus aux articles 46

et 47 du RGPD (notamment les règles d'entreprise contraignantes ou les clauses types de protection des données).

Elles estiment toutefois que, compte tenu de l'accroissement des volumes de transferts liés au développement du numérique et des applications industrielles (Internet des Objets), elles devraient pouvoir disposer de solutions plus globales, et en tout état de cause, plus efficaces et mieux articulées entre elles

- **Révision de l'architecture globale du mécanisme des transferts de données personnelles à la lumière de la convergence des systèmes juridiques de protection de données**

L'approche de l'UE en matière de protection des données a fait largement école et un nombre croissant de pays tiers tendent à se doter de régimes de protection des données personnelles dont les principes convergent avec ceux de l'UE, y compris avec les Etats-Unis (cf. législation adoptée par l'Etat de Californie)

Cette dynamique devrait conduire à 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 transatlantique 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 de données.

- **Des décisions d'adéquation plus nombreuses et prioritaires**

En tout état de cause, les entreprises souhaiteraient davantage se reposer sur des décisions d'adéquation que sur les règles d'entreprise contraignantes ou les clauses types de protection des données, même si elles reconnaissent qu'il faut parfois combiner le régime d'adéquation avec ceux-ci (notamment pour le cas du Privacy Shield).

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.

Une décision d'adéquation avec le Royaume-Uni doit donc être la priorité principale : il s'agit à la fois d'un partenaire économique de premier plan et d'un pays dont le système juridique de protection des données, même après le retrait, est calqué sur celui du RGPD.

- **Une meilleure prise en compte de la réciprocité des transferts de données personnelles**

Les entreprises ont à cœur de garantir le niveau de protection assuré par le RGPD dans leurs transferts vers les pays tiers mais souhaitent également pouvoir transférer des données personnelles des pays tiers. Or cette libéralisation réciproque continue de se heurter à un certain protectionnisme de la donnée personnelle et non-personnelle.

Le processus engagé avec le Japon visant à obtenir des décisions jumelles d'adéquation constitue un progrès important vers cet objectif de réciprocité.

Deux éléments pourraient permettre de renforcer encore l'exigence de réciprocité :

- (1) D'une part, le **rapprochement de la position de l'UE avec celles de ses principaux partenaires commerciaux** sur les dispositions des accords de commerce sur les données personnelles, ce qui permettrait d'exiger en retour d'eux le même degré d'ouverture dans les transferts de données vers l'UE
 - (2) En tout état de cause, d'inscrire la **réciprocité comme un critère explicite et obligatoire** pour adopter une décision d'adéquation. Cette clarification constituerait en elle-même un effet de levier sur nos partenaires
- **Nécessité de rendre les décisions d'adéquation encore plus efficaces**

Les transferts de données vers des pays tiers requérant des niveaux de protection adéquats définis par la Commission européenne, les entreprises déplorent que des outils aussi essentiels que le « Privacy Shield » ne soient pas pleinement déployés et souhaitent, en conséquence, des précisions supplémentaires visant tant les décisions déjà existantes (futurs révisions) que celles à venir sur :

- Les modalités de fonctionnement des **autorités des pays tiers** : celles-ci sont en effet réputées faire appliquer le RGPD et les assurances en ce sens doivent être mieux prises en compte par la CE,
 - Les **obligations de réalisation d'audit** sur la sécurité informatique, en particulier, que les sous-traitants des responsables de traitement doivent faciliter pour assurer une protection des données personnelles en réelle adéquation avec le règlement européen (article 28),
 - Les **critères d'analyses** retenus pour envisager et conclure des décisions d'adéquation avec des pays tiers.
- **Mise à jour des dispositions relatives aux clauses contractuelles type (« CCT »)**
- La référence à la **directive de 1995 doit être supprimée et s'accompagner de la** confirmation que les CCT signées depuis l'entrée en vigueur du RGPD demeurent valables,
 - Les conditions de **gestion des données personnelles devant être remplies par le sous-traitant** d'un pays tiers devraient être précisées (lieu de transfert et type de données visées).

2. Sur le chapitre VII

Les entreprises soulignent et déplorent vivement le **défaut d'harmonisation entre autorités de contrôle** dans leur approche et leur mise en œuvre du règlement européen, instrument juridique retenu notamment pour conforter l'harmonisation nécessaire à la fluidité de la gestion des données personnelles au sein du marché unique comme dans les pays tiers.

La mise en œuvre hétérogène de ce texte par les autorités nationales complexifie la vie des entreprises (charges administratives, incertitudes juridiques...) alors même que leur responsabilité a été renforcée. Elle peut également être source de distorsions de concurrence au sein du marché unique, puisqu'elle suppose des obligations et charges différentes pour des entreprises basées sur le territoire européen, agissant sur le même marché mais dépendant d'autorités de référence différentes.

Des interprétations variées sont ainsi déplorées dans divers domaines tels que :

- Les ventes sur Internet, conditionnées par l'autorité française au recueillement du consentement préalable des personnes sur leurs données bancaires, tandis que celles-ci peuvent être recueillies sans consentement explicite par toutes les entreprises basées hors de France,
- La gestion des consentements aux cookies, qui font l'objet de recommandations d'application notoirement différentes entre les pays membres de l'UE,
- La durée de conservation des données, encadrée par des référentiels nationaux rendant la gestion de ce sujet complexe, risquée et chronophage dans le cadre des transferts internationaux.

Les entreprises souhaitent donc de nombreuses améliorations dans cette coopération et ce mécanisme de cohérence traités dans le chapitre VII.

Ces améliorations devraient en particulier reposer sur le cadre rappelé par un [récent arrêt de la CJUE](#) à l'occasion d'un renvoi préjudiciel. La Cour mentionne que les États membres « *ne sauraient ni ajouter de nouveaux principes relatifs à la légitimation des traitements de données à caractère personnel audit article ni prévoir des exigences supplémentaires qui viendraient modifier la portée de l'un des six principes prévus à cet article* ».

La CJUE refuse qu'un État prédétermine le choix de la base légale ou ses conditions d'application. Le RGPD s'oppose à ce qu'un État membre exclue de façon catégorique et généralisée la possibilité pour certaines catégories de données à caractère personnel d'être traitées, sans permettre une pondération des droits et des intérêts opposés en cause dans un cas particulier.

Cette approche tendant vers une plus grande harmonisation au sein des États membres est bienvenue et devrait contribuer à simplifier les démarches des entreprises vis-à-vis de la Commission comme des autorités nationales.

Le renforcement de cette harmonisation doit s'accompagner de différentes dispositions touchant à la fois au CEPD et à la notion d'autorité chef de file.

- Renforcement des **compétences du CEPD**

- Les recommandations nationales prises pour l'interprétation du RGPD devraient être soumises plus systématiquement à l'avis du Comité notamment lorsque la recommandation d'une autorité porte sur la base légale d'un traitement et tend à en imposer le choix (conformément à l'article 63 du RGPD),
- Les recommandations assorties de sanctions concernant l'interprétation du RGPD ne devraient pouvoir être prises par les autorités nationales qu'après édicition des guidelines du Comité Européen proposant une interprétation harmonisée. Le cas échéant, un moratoire concernant l'application de la recommandation nationale et les sanctions devrait être pris par l'autorité locale,
- Le CEPD étant le garant de la cohérence de l'interprétation du RGPD, il devrait pouvoir être saisi directement par des sociétés ou des particuliers sur la cohérence de certains avis ou recommandations émis par des autorités locales sur la base de traitements locaux,
- Le CEPD devrait rendre plus transparents ses travaux et sujets à l'ordre du jour (à titre d'exemple, la CNIL indique depuis plus d'un an que le sujet de la conservation des données bancaires est à l'ordre du jour et que des travaux sont en cours sur l'élaboration d'une recommandation commune mais l'agenda du CEPD n'en fait pas mention).

- Précisions sur l'**autorité chef de file compétente** :

Présentée lors de l'élaboration du RGPD comme un outil essentiel de mise en cohérence des approches nationales, la mise en œuvre des compétences de l'autorité « chef de file » devrait être rendue plus efficiente en :

- Accroissant la transparence sur les relations entre autorité chef de file compétente et autorités nationales (par exemple, aucune information n'est donnée sur une éventuelle saisine de l'autorité de protection des données luxembourgeoise de plaintes concernant la conservation des données bancaires des clients français d'Amazon, ni si d'autres autorités nationales ont été saisies),
- Envisageant un dispositif qui permettrait une fois un certain nombre de plaintes de ressortissants nationaux déposées, que l'autorité chef de file compétente se dessaisisse du dossier au profit de l'autorité nationale concernée.

A PROPOS DE L'AFEP

Représentant 113 des plus grands groupes privés exerçant leurs activités en France, l'afep – Association française des entreprises privées – participe au débat public avec pour ambition d'apporter des réponses pragmatiques en faveur du développement d'une économie française et européenne compétitive.

Les entreprises membres de l'afep contribuent pour plus de 13 % au PIB français, emploient 2 millions de salariés directs et versent 19 % des prélèvements obligatoires pesant sur les entreprises.

Emmanuelle Flament-Mascaret - Directrice Affaires commerciales et Propriété intellectuelle
e.flament-mascaret@afep.com

Marc Poulain - Directeur des Négociations Commerciales Internationales
m.poulain@afep.com