Consultation de l'EDPB sur les mesures complémentaires d'ordre technique, contractuel et organisationnel pour assurer un niveau de protection adéquat des données personnelles en cas de transferts hors UE

Contribution de l'AFNUM, Syntec Numérique et TECH IN France

L'AFNUM, Syntec Numérique et TECH IN France ont bien noté le projet de recommandations publié par le Comité européen de Protection des données (EDPB) dans le cadre des mesures complémentaires pour la protection des données. Nos trois organisations souhaitent, par la présente, exprimer leur vive inquiétude suite à la publication de ce projet de recommandations.

De la nécessité d'un cadre juridique stable et cohérent

- La décision du 16 juillet 2020 de la Cour de Justice de l'Union Européenne (CJUE) concernant le « Privacy Shield » a rappelé la nécessité d'un haut niveau d'exigence en matière de protection des données des citoyens et des acteurs économiques, impliquant un réexamen des régimes de la donnée vis-à-vis des pays tiers. L'invalidation du mécanisme d'auto-certification « Privacy Shield » a entrainé une grande insécurité juridique, bien au-delà des seuls transferts des données vers les Etats-Unis. Cette décision a également pour conséquence de reporter sur les entreprises exportatrices, la responsabilité d'évaluer le niveau d'adéquation du pays tiers ne bénéficiant pas de décision d'adéquation valide.

- Ce manque de visibilité et de cadre juridique protecteur stable est d'autant plus préoccupant qu'il s'ajoute au contexte actuel éprouvant pour les entreprises, qui tentent de se remettre des répercussions économiques de la première vague de la pandémie de COVID-19, sont confrontées aujourd'hui à la deuxième, et se prépare probablement à en affronter une troisième. Nous l'avons exprimé publiquement[1] depuis plusieurs mois, il est aujourd'hui plus que nécessaire d'aller vite, tout en prenant le temps de consulter les parties prenantes concernées.

Nos recommandations

*Les recommandations de l'EDPB renforcent l'idée que la question des règles d'accès aux données européennes par les juridictions étrangères est d'ordre politique. Ces conflits ne peuvent être résolus par les entreprises qui sont désormais confrontées à une forte instabilité juridique****. S'il est plus que jamais important que l'Union européenne et les États-Unis poursuivent leurs négociations en vue d'une réforme du « Privacy Shield », le débat doit aller au-delà du politique, ce qui implique de prendre le temps de réfléchir à des mesures pérennes.***

Observations générales sur la mise en œuvre des recommandations

- Il est fait mention dans la consultation d'une application immédiate des recommandations après leur publication. En raison de la pertinence de ce sujet et de ses conséquences sur l'ensemble des secteurs de

[1] Pour consulter le communiqué de presse conjoint Asic-Syntec Numérique- TECH IN France (25 septembre 2020) et la tribune publiée dans Les Echos (30 novembre 2020)

l'économie, l'EDPB devrait **réexaminer les effets immédiats de ces recommandations et envisager des mesures appropriées pour examiner les contributions qu'elle recevra pendant la période de consultation publique**. Nous considérons nécessaire de donner aux responsables du traitement le temps nécessaire pour mettre en œuvre les recommandations.

- L'utilisation du terme « recommandations » à la place du terme « lignes directrices » tend à nous interroger sur le caractère prescriptif des mesures qui y sont proposées et sur les potentielles conséquences en cas de manquement à ces recommandations.

- Les recommandations s'appuient principalement sur le principe de responsabilité de l'article 5 (2) du RGPD, sans expliquer en détail en quoi ce principe est pertinent pour l'objet des transferts internationaux de données. **De manière générale, les recommandations appliquent le principe de responsabilité de manière très souple**, alors que le libellé de l'article 5 (2), limite très clairement ce principe au respect de l'article par le responsable du traitement.

- Dans le même temps, la Commission européenne a soumis à consultation ses clauses contractuelles types actualisées. **Si nous saluons les clarifications apportées par la Commission, nous restons convaincus qu'un accord type sera nécessaire.** Toute entreprise qui intègre dans ses services des méthodes avancées d'analyse des données et d'apprentissage automatique ou qui possède des employés dans plusieurs pays, voit son activité reposer sur les transferts de données. Il en est de même pour toutes les entreprises qui utilisent des services de cloud, des solutions Saas, des outils de communications et services de messageries.

- Au regard des recommandations de l'EDPB, il sera à notre sens difficile pour les entreprises de s'appuyer sur les clauses contractuelles types (CCT). **En l'état actuel, ces propositions entrent en conflit avec le projet d'actualisation des CCT de la Commission européenne et l'arrêt Schrems II lui-même.**

Pour une approche fondée sur le risque

- En complément de ses recommandations, l'EDPB a publié une liste d'exemples de mesures complémentaires assorties de certaines des conditions exigées, notamment les mesures techniques. Ceci peut obliger l'entreprise à combiner plusieurs mesures complémentaires. Dans les cas où aucune mesure complémentaire ne convient, l'EDPB conseille d'éviter, de suspendre voire de mettre fin au transfert pour éviter de compromettre le niveau de protection des données à caractère personnel.

- **Les recommandations ne réduisent pas le risque juridique pour les entreprises qui dépendent de fournisseurs de services non européens pour l'activité et le développement de leur entreprise**, car la majorité de ces services relèveront des cas d'utilisation 6 et 7 pour lesquels l'EDPB n'a pas présenté de mesures complémentaires efficaces. De plus, les entreprises européennes ayant des activités aux États-Unis et ailleurs auront des difficultés à maintenir leurs activités mondiales sur la base des recommandations pour les mêmes raisons. Par exemple, elles ne pourront pas transférer des données sur les ressources humaines en dehors de l'UE.

- Nous espérions que l'EDPB fournirait aux exportateurs de données une boîte à outils de mesures pratiques qui les aideraient à se conformer à la décision de la CJUE. **A l'inverse, les recommandations proposent une approche prescriptive, non fondée sur le risque, qui va bien au-delà des exigences de la décision Schrems II.** Plutôt que de suivre l'instruction de la CJUE de prendre en compte le contexte d'un transfert, l'EDPB a adopté une interprétation restrictive du droit européen, ce qui aura pour conséquence d'induire des obstacles considérables aux transferts de données personnelles en dehors de l'UE.

- De plus, les cas d'utilisation présentés par l'EDPB ne semblent pas adaptés aux besoins des entreprises pour se conformer à la décision de la CJUE. L'EPDB lui-même indique que, dans les cas où la législation ou les pratiques d'un pays tiers empiètent sur l'efficacité des garanties appropriées contenues dans les outils de transfert de l'article 46 du RGPD, **la CJUE laisse la possibilité pour les exportateurs d'introduire des mesures complémentaires qui comblent ces lacunes conformément au niveau de protection requis par le droit européen.** Aucun des cas d'utilisation présentés ne semble réellement combler ces lacunes.

- Enfin, il convient de rappeler que le *business model* des entreprises exportatrices de données repose pour partie sur cette approche fondée sur le risque. La prestation fournie a des coûts variables selon le type d'exportation, les lieux de transit et de stockage des données. Remettre en cause cette approche fondée sur le risque porterait atteinte à l'ensemble des acteurs économiques de cet écosystème.

Nos recommandations

Les recommandations de l'EDPB devraient adopter l'approche fondée sur le risque de la décision Schrems II de la CJUE et le principe fondamental correspondant inscrit dans le RGPD. L'exportateur (assisté par l'importateur) devrait pouvoir prendre en compte tous les critères subjectifs ou objectifs pertinents pour évaluer au cas par cas le risque d'un transfert vers un pays tiers. A ce jour, le guide de l'EDPB juge certains facteurs pertinents (finalité du traitement, différentes catégories de données, etc.) comme étant des facteurs « subjectifs ». Nous pensons au contraire que ces indicateurs sont légitimes pour l'évaluation au cas par cas requise par l'arrêt de la CJUE.

Cette évaluation devrait également inclure la probabilité d'accès, d'interférence ou de demande par un gouvernement étranger. La probabilité et les précédents fondés sur l'expérience ne peuvent être les seuls facteurs, mais l'exportateur et l'importateur doivent être en mesure de prévoir le risque réaliste de transferts spécifiques sur la base des demandes d'accès préalables des autorités publiques. La probabilité basée sur le nombre de demandes d'accès exécutées par les autorités publiques est un élément clé de l'évaluation des risques, car le risque réaliste d'être soumis à une telle demande varie considérablement en fonction du modèle commercial de l'exportateur et de l'importateur, et de la catégorie de données.

Il conviendrait d'ajouter aux recommandations que la probabilité de l'accès des autorités publiques dans le cas spécifique d'un scénario de transfert peut compléter les autres facteurs d'évaluation du risque de transfert (paragraphe 33).

Il conviendrait également de clarifier le paragraphe 42 en précisant que lorsque la législation d'un pays tiers peut faire défaut, la probabilité d'accès ne peut être utilisée comme seul critère pour déterminer le risque mais doit être prise en compte dans l'évaluation.

Des difficultés de mise en application pour les entreprises, notamment les PME

Toute organisation souhaitant transférer ses données dans un pays tiers ne faisant pas l'objet d'une décision d'adéquation devra entreprendre ses propres analyses des lois et pratiques du pays. Si les recommandations sont adoptées dans leur forme actuelle, toute organisation qui utilise des services en ligne pour traiter et transférer des données à caractère personnel pourrait se voir infliger des amendes, que les autorités publiques d'un pays tiers aient ou non accès aux données. **Les entreprises qui opèrent des transferts dans plusieurs pays tiers devront réaliser plusieurs analyses à la fois. Il sera par conséquent irréaliste, car très coûteux, pour une grande partie des PME de mener une telle démarche d'analyse des lois et pratiques d'un pays tiers ; ce qui nous apparaît être le rôle des autorités européennes.** Les effets négatifs potentiels sur la compétitivité, l'innovation et la société sont considérables.

- Il sera très risqué pour les entreprises de l'UE de s'engager dans des échanges commerciaux hors UE. **Les recommandations ne réduisent pas le risque juridique pour les entreprises qui dépendent de fournisseurs de services non européens pour l'exploitation de leur entreprise.** Ainsi, les entreprises européennes ayant des activités aux États-Unis mais aussi ailleurs, auront des difficultés à maintenir leurs activités mondiales sur la base de ces recommandations. A noter que sans décision d'adéquation, il pourrait en être de même avec le Royaume-Uni, vers lequel un bon nombre d'entreprises européennes transfèrent des données. A titre d'exemple, les entreprises européennes ayant des bureaux ou du personnel hors UE ne pourront plus communiquer avec eux en ligne, transférer des données sur les ressources humaines voire même exécuter certaines tâches quotidiennes nécessaires. A noter que la majorité de ces services relèveront des cas d'utilisation 6 et 7 pour lesquels l'EDPB n'a pas pu identifier de mesures complémentaires efficaces.

- En se concentrant uniquement sur les juridictions non adéquates, **les recommandations menacent de créer un équilibre international inégal pour la protection des données**, où les exportateurs de données sont tenus d'appliquer des règles différentes aux différentes juridictions, même si des niveaux de protection des données similaires existent entre elles. Tous les pays tiers ayant obtenu une décision d'adéquation de la Commission européenne n'offrent pas forcément tous un niveau de protection des données « essentiellement équivalent » à celui prévu dans le RGPD et la Charte des droits fondamentaux de l'UE.

- Les recommandations de l'EDPB ne semblent pas prendre en considération **la question de savoir comment les entreprises pourront fournir un service international aux utilisateurs.** Si des données doivent être conservées dans l'UE, il est pertinent de se demander comment un utilisateur pourra partager un document avec un utilisateur basé dans un pays tiers. Si les dérogations à l'article 49 doivent être interprétées de manière aussi restreinte que le suggèrent les recommandations de l'EDPB, il ne semble pas que l'on puisse se prévaloir de dérogations dans ces cas. De plus, les start-ups et les PME qui dépendent de certains services largement utilisés pour maintenir ou développer leurs activités seront dans l'incapacité de remplacer leurs fournisseurs de services existants par des alternatives appropriées.

Nos recommandations

Les mesures organisationnelles telles que les certifications ISO sont des mécanismes certifiés dans le cadre du RGPD. Le caractère international de ces normes peut aider les entreprises à évaluer et à respecter les lois pertinentes en matière de protection de la vie privée, en particulier si la norme est mise à jour pour traiter de questions spécifiques telles que les lois locales de surveillance.

Afin d'obtenir une approche homogène du respect des transferts et de garantir une sécurité juridique, l'analyse des lois et pratiques des pays tiers doit rester du ressort des autorités européennes, comme cela est le cas pour les décisions d'adéquation de la Commission européenne. Les entreprises exportatrices de données ne peuvent endosser une telle responsabilité.

Mesures techniques : sécurité et chiffrement

- Si le chiffrement est nécessaire pour les données les plus sensibles, il ne doit pas être systématiquement imposé aux entreprises dans le transfert de données personnelles hors UE. **En application de l'approche par les risques, c'est à l'entreprise de déterminer les données et les circonstances nécessitant un chiffrement.** Dans certains cas, le chiffrement n'est pas adapté au traitement notamment lorsque les données doivent être transmises en clair. Les cas d'usage présentés par l'EDPB (cas d'usages 1 et 3)

imposent l'utilisation d'un chiffrage, décrit par le terme « flawless », autrement dit, parfait. D'un point de vue juridique et technique, il est impossible d'assurer un chiffrement infaillible à long terme.

- Dans la mesure où les recommandations ne soutiennent pas l'idée que les mesures organisationnelles et contractuelles peuvent être utilisées comme mesures complémentaires, les mesures techniques restent l'outil le plus important pour protéger les transferts de données. Les mesures techniques décrites dans les recommandations, en particulier le chiffrement de bout en bout, auraient pour conséquence **de réduire l'expérience de l'utilisateur de nombreux services, voire même d'en rendre certains inutilisables.**

- L'EDPB ne tient pas compte du fait que même dans le cas de services chiffrés de bout en bout, **au moins certaines métadonnées doivent être non cryptées afin de fournir un service.** Cela est notamment le cas pour les adresses IP, les informations de connexion, l'état de la session et les données de base de l'abonné. Nous regrettons que les recommandations ne tiennent pas compte de cet aspect.

- De plus, l'obligation de mettre en œuvre un cryptage de bout en bout rendra également plus difficile pour les forces de l'ordre la lutte contre les crimes en ligne. En effet, le **déchiffrement partiel de données est impératif à certaines opérations de sécurité, telles que l'inspection de paquets de données dans la lutte contre les attaques DDoS.** La conséquence d'un tel agissement serait un abaissement des standards en matière de cybersécurité, ce qui serait contraire au contexte d'une augmentation du nombre de cyberattaques connu par l'UE[2].

- L'obligation de mettre en œuvre un cryptage de bout en bout crée également **une barrière technique** entre les entreprises qui ont les capacités et les moyens de mettre en place ce type de solution et les petites entreprises qui n'ont pas les ressources nécessaires, les excluant de fait de réaliser des transferts de données.

Nos recommandations

Les recommandations de l'EDPB devraient tenir compte du fait que l'accès à des mesures de sécurité informatique conformes aux normes du secteur est essentiel pour toute entreprise qui traitent des données. *L'accès à des services de sécurité de pointe doit être pris en compte dans toute évaluation des risques liés au transfert de données vers un pays tiers. Les recommandations devraient préciser que pour tous les scénarios décrits dans les cas d'utilisation (en particulier les cas 6 et 7), de nombreux autres facteurs peuvent être pris en compte. A titre d'exemple, des mesures contractuelles et organisationnelles devraient être envisagées pour contribuer à garantir la protection des données à caractère personnel transférées.*

Minimisation des données

L'EDPB semble se référer au principe de minimisation des données et indique que les entreprises responsables du transfert des données devront vérifier que les données transférées soient « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont transférées et traitées dans le pays tiers ».

- L'application qui est faite de ce principe est toutefois erronée. Le principe de minimisation des données considère la quantité de données par rapport à une finalité de traitement, et non par rapport à chaque activité de traitement effectuée à cette fin. Si les données sont « adéquates, pertinentes et limitées » à ce

[2] https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic

qui est nécessaire au regard des finalités pour lesquelles elles sont traitées, le principe est respecté, y compris pour tous les traitements effectués à cette fin.

- Lorsqu'un transfert est réalisé dans le cadre d'un traitement entrepris pour une finalité spécifique, il n'y a pas de test distinct dans le cadre du principe de limitation de la finalité qui se concentre sur ce transfert séparément des autres activités de traitement. Or, le RGPD distingue la minimisation des données (Article 5) pour un traitement et le transfert de données (Article 44) souvent nécessaire pour l'exécution du traitement pour lequel les données ont été collectées.

[A propos de l'AFNUM]

L'Alliance Française des Industries Numériques (AFNUM), est l'association professionnelle qui représente en France les industriels des réseaux d'infrastructure télécom, de l'électronique grand public, de l'informatique, de l'impression, de la photographie et des objets connectés. Elle compte parmi ses adhérents à la fois des filiales de grands groupes internationaux et des PME françaises innovantes. Le poids économique des 55 entreprises adhérentes de l'AFNUM est de 90.000 emplois en France pour 26 Md € de chiffre d'affaires cumulé.

www.afnum.fr

[A propos de Syntec Numérique]

Syntec Numérique est le syndicat professionnel des entreprises de services du numérique (ESN), des éditeurs de logiciels et des sociétés de conseil en technologies. Il regroupe plus de 2 000 entreprises adhérentes qui réalisent 80% du chiffre d'affaires total du secteur (plus de 57 Md€ de chiffre d'affaires, 530 000 employés dans le secteur). Il compte 30 grands groupes, 120 ETI, 1 000 PME, 850 startups et TPE ; 11 Délégations régionales (Hauts de France, Grand Est, Auvergne Rhône-Alpes, Provence Alpes Côte d'Azur, Occitanie, Nouvelle Aquitaine, Pays de la Loire, Bretagne, Bourgogne Franche-Comté, Centre Val de Loire, Normandie) ; 20 membres collectifs (pôles de compétitivité, associations et clusters).

www.syntec-numerique.fr

[A propos de TECH IN France]

Créée en 2005, TECH IN France est une association professionnelle de loi 1901 qui a pour but de rassembler et de représenter les éditeurs de logiciels, de services internet et de plateformes en France. Porte-parole de l'industrie numérique, TECH IN France compte 400 entreprises adhérentes : de la startup à la multinationale en passant par la PME et les grands groupes français ; soit 8 milliards d'euros et 90 000 emplois. TECH IN France s'est donnée pour mission de mener une réflexion permanente sur l'évolution de l'industrie numérique et promouvoir l'attractivité du secteur.

www.techinfrance.fr