

Nous notons particulièrement :

1. "The Guidelines specify three cumulative criteria that qualify a processing as a transfer: (1) the data exporter (a controller or processor) is subject to the GDPR for the given processing; (2) the data exporter transmits or makes available the personal data to the data importer (another controller, joint controller or processor); (3) the data importer is in a third country or is an international organisation."

2. "the EDPB considers that collection of data directly from data subjects in the EU at their own initiative does not constitute a transfer."

Si nous faisons une analyse d'impacts de ce document en prenant quelques cas d'école pour illustrer, sauf erreur de notre part :

1. Cas Microsoft/Health Data Hub : la relation entre Microsoft NL et le Ministère de la Santé Français pour le Health Data Hub, n'a pas en réalité de difficulté de transfert de données hors UE tel qu'envisagé par le Conseil d'État, du fait que le RGPD s'applique directement à Microsoft NL du fait de sa localisation sur le sol de l'UE et son traitement de données de personnes de l'UE. Ainsi l'enjeu se pose sur le choix par le Ministère d'un sous-traitant sur la base de l'article 28 du RGPD "qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée." ... Ainsi cela ne peut alors pas être possible avec un prestataire de services soumis au droit US. Donc ce n'est pas une question de transfert de données, mais de gestion de la sous-traitance... Alors, l'ordonnance du Conseil d'Etat qui autorise le choix de Microsoft pour le Health Data Hub en considérant possible le transfert de données vers les USA sur la base de l'article 49 du RGPD (dérogation), est bancal sur la base de cette interprétation du CEPD. L'enjeu n'est pas ici de permettre un transfert de manière dérogatoire, mais de déroger aux règles de sélection d'un sous-traitant.

2. Cas Amazon Europe/US : prenons maintenant le cas d'un transfert entre Amazon Europe et Amazon US (comme indiqué dans la politique de confidentialité d'Amazon), il s'agit bien là d'un transfert de données dont l'illicéité ne fait plus de doute depuis l'arrêt Schrems II, les USA ne permettant pas de garantir un niveau de droit adéquat, et le droit étant supérieur à tout contrat/CCT dans la hiérarchie des normes, nous sommes bien là sur un défaut lié à un transfert de données.

3. Facebook US: Cet exemple est théorique, car aujourd'hui FB fonctionne comme Amazon avec FB Ireland qui transfère des données à FB US... mais le cas théorique est intéressant à envisager : en admettant que ce soit Facebook US qui collecte directement les données de résidents de l'UE, l'enjeu n'est donc plus un transfert de données mais le respect du RGPD dans ses principes de base (par l'entrée dans l'article 3 du texte), et en particulier la notion de licéité... et comme le dit l'art.6.1.c) "le traitement est

nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis" cela permet à FB US de dire "le traitement qui consiste à communiquer des données aux agences d'espionnage US est permis par la loi US à laquelle nous sommes soumis, c'est donc licite". Cela pourrait amener FB US à vouloir se déclarer à nouveau comme RT à la place de FB Irlande, ce qui résoudrait le pb des transferts illégaux pour incompatibilité du droit US.

Bref, ça simplifie en partie le débat technique, mais ouvre une nouvelle porte de débat politique, qui devrait être soumis au Parlement UE.

Sur la partie collecte directe de données depuis l'extérieur de l'UE et les libertés fondamentales pour les personnes, cette approche constitue un recul manifeste pour les droits des personnes (perte de capacité de recours juridique effectif, par exemple pour le droit US). Alors les droits fondamentaux des personnes physiques résidant dans l'UE, dans ce cas d'espèce encore théorique, pourraient ne plus être garantis en permettant des traitements qui vont à l'encontre de la charte des droits fondamentaux de l'UE. C'est donc une manière de trouver un accord transatlantique sans négociation avec les USA et en rognant sur les fondements de l'UE. C'est astucieux. Nous constatons donc et sauf erreur qu'en Europe on arrive à adopter des textes (RGPD) à portée extra-territoriale permettant l'application de lois non-UE contraires à l'esprit des nôtres. C'est un bien beau rapport de force avec des pays aux lois non-adéquates avec notre Charte des Droits fondamentaux, qu'il serait bon d'exposer au Parlement Européen.

Cordialement,

Association OD
www.0d.network