_swissprivacy.law

Mesures techniques, contractuelles et organisationnelles à observer suite à l'arrêt Schrems II

Philipp Fischer et Kastriot Lubishtani, le 7 décembre 2020

Le 10 novembre 2020, le Comité européen de la protection des données (CEPD) a publié ses Recommandations 01/2020 sur les mesures supplémentaires quant aux outils de transfert de données personnelles en dehors de l'Union européenne. Elles font suite à l'arrêt Schrems II et offrent un aperçu des diverses mesures techniques, contractuelles et organisationnelles permettant de pallier les lacunes de protection des pays de destination.

Comité européen de la protection des données (CEPD), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10 novembre 2020 (disponibles uniquement en anglais à ce jour)

I. Introduction

L'arrêt Schrems II de la Cour de justice de l'Union européenne (CJUE) promettait de faire couler beaucoup d'encre et il n'a pas déçu. En substance, cet arrêt d'ores et déjà commenté sur swissprivacy valide dans leur principe les clauses contractuelles types ou « *Standard Contractual Clauses* » (SCC) publiées par la Commission européenne (décision 2010/87/UE). Néanmoins, un transfert de données hors de l'Union européenne et reposant uniquement sur ces clauses ne peut *ipso facto* être qualifié comme offrant un niveau de protection équivalent à la réglementation européenne au sens de l'art. 46 par. 2 let. c RGPD. En effet, ces clauses ne sont que de nature contractuelle et ne peuvent, partant, faire obstacle à des mesures prises par les autorités de l'État destinataire. La nouvelle version des SCC, qui a été publiée dans l'intervalle, ne change rien à cette faiblesse inhérente à un système contractuel.

Ainsi, les exportateurs de données doivent au préalable de tout transfert procéder à une évaluation des risques au cas par cas et, au besoin, accompagner les SCC de « garanties supplémentaires ». Circonspects, plusieurs commentateurs se sont toutefois demandé quelles pouvaient bien être ces mesures supplémentaires (cf. notamment David Vasella sur datenrecht.ch et Emilie Jacot-Guillarmod sur LawInside). Une ordonnance du 13 octobre 2020 du Conseil d'État français relative au *Health Data Hub* offre certaines pistes de réflexion préliminaires.

II. Recommandations 01/2020

C'est dans ce contexte que, le 10 novembre 2020, le CEPD a publié ses Recommandations 01/2020 pour venir en aide aux exportateurs de données, qu'il s'agisse de responsables de traitement ou de sous-traitants privés comme publics. De deux ordres, ces Recommandations portent, d'une part, sur l'évaluation du niveau de protection de l'État destinataire et des risques (A) et, d'autre part, sur l'identification des mesures supplémentaires envisageables en vue de pallier l'insuffisance des SCC (B).

A) Procédure d'évaluation du niveau de protection de l'État destinataire

Pour procéder à l'évaluation du niveau de protection de l'État destinataire, le CEPD propose une feuille de route (« *roadmap* ») constituée de six étapes :

1. Premièrement, tout exportateur doit connaître et identifier quelles sont les données transférées (« *know your transfers* ») et, à cet égard, le registre des activités de traitement (art. 30 RGPD) peut être particulièrement utile ;

2. Ensuite, il est nécessaire d'identifier le fondement juridique sur lequel repose le transfert et de distinguer selon qu'il s'agit (i) d'une décision d'adéquation (art. 45 RGPD) ou (ii) de garanties appropriées au sens de l'art. 46 RGPD, parmi lesquelles les SCC, mais aussi les règles d'entreprise contraignantes (« *binding corporate rules* » ou BCR), les clauses *ad hoc* ou encore les codes de conduite. Dans la première hypothèse, l'examen s'arrête tant et aussi longtemps que la décision d'adéquation demeure valide, alors qu'il se poursuit dans la seconde ;

3. Dans un troisième temps, le droit de l'État destinataire doit être examiné, afin de déterminer si les garanties précitées sont *in concreto* appropriées et suffisantes, en ce qu'elles assurent bel et bien un niveau de protection adéquat. Pour ce faire, le CEPD renvoie aux Garanties essentielles européennes (« EDPB European Essential Guarantees Recommendations »), en indiquant que l'examen doit être conduit avec soin (« *carefully examined* ») lorsque le droit en question permettant l'accès aux données par des autorités de poursuite ou de sécurité nationale est ambigu ou n'est pas public. Si la législation est lacunaire, l'examen doit reposer sur des critères objectifs et non subjectifs, à l'instar de la vraisemblance d'un accès aux données ne s'alignant pas sur les standards européens ;

4. Si l'évaluation qui précède révèle une insuffisance en termes de protection découlant soit du droit de l'État de destination, soit de sa pratique interne, qui empêcherait l'importateur de remplir ses obligations en vertu des SCC, des mesures supplémentaires doivent être prises qui, par définition, vont au-delà des garanties envisagées par l'art. 46 RGPD ;

5. Lorsque les mesures supplémentaires consistent en une modification (et non seulement un complément) des SCC ou y contreviennent, alors le transfert est réputé ne plus reposer sur des SCC au sens de l'art. 46 RGPD (cf. CEPD, Avis 17/20), si bien que l'autorisation de l'autorité de contrôle compétente (art. 46 par. 3 RGPD) est nécessaire (en droit suisse, la LPD en vigueur prévoit une information au Préposé fédéral à l'art. 6 al. 2 let. a et al. 3) ;

6. Enfin, il sied de réévaluer de manière régulière les développements au sein de l'État de destination qui pourraient impacter la procédure d'évaluation.

B) Mesures supplémentaires

1. Mesures techniques

Les mesures techniques évoquées par le CEPD sont (i) le cryptage et (ii) la pseudonymisation, pour autant que ces mesures puissent garantir que l'importateur des données, situé par hypothèse dans un État réputé non adéquat, ne dispose pas d'un accès aux données en *clear text*. Dans une perspective pratique, seules ces mesures techniques apparaissent, à l'heure actuelle, capables d'empêcher l'accès des autorités publiques du pays de l'importateur aux données personnelles transférées.

Toutefois, si l'importateur a besoin d'un accès aux données pour rendre le service, les mesures techniques précitées ne pourront pas être mises en place et seules des mesures contractuelles (2) et organisationnelles (3) pourront être envisagées.

2. Mesures contractuelles

Le CEPD évoque également la possibilité de recourir à des mesures contractuelles, étant précisé toutefois que de telles mesures pourraient être mises en échec par le droit local applicable au récipiendaire, ce qui est précisément le point critiqué dans le cadre de Schrems II. Ces mesures contractuelles peuvent notamment consister en :

- l'obligation, à charge de l'importateur, d'informer l'exportateur sur le cadre légal applicable à l'importateur, notamment s'agissant des mesures d'enquête des autorités, cette information permettant à l'exportateur de mener à bien le « *risk assessment* » exigé par Schrems II (cf. ci-dessus) ;
- une garantie de l'importateur que la solution d'hébergement de données ne contienne pas de « *back doors* » ;
- des droits d'audit étendus en faveur de l'exportateur, de manière à permettre à ce dernier de s'assurer de l'absence de divulgation à des autorités ;

- une obligation, à charge de l'importateur, de confirmer à intervalles réguliers l'absence de requête d'accès d'une autorité (la non-transmission d'une telle confirmation signalant ainsi à l'exportateur qu'une telle requête a été reçue / un tel système est désigné par l'appellation « *warrant canary* » en référence aux mineurs qui apportaient des canaris dans les mines de charbon pour déceler des gaz toxiques) ;
- une obligation, à charge de l'importateur, de prendre toute mesure utile pour protéger les données, par exemple l'obligation de requérir des mesures provisionnelles pour suspendre l'ordre de divulgation, de contester cet ordre en justice et de limiter toute divulgation au strict minimum requis.

3. Mesures organisationnelles

Les mesures organisationnelles comprennent les politiques et processus de l'exportateur, dont l'importateur doit également garantir le respect, de manière à assurer la protection des données durant tout le cycle de traitement des données. Ces mesures organisationnelles peuvent notamment porter sur la mise en œuvre d'une structure de gouvernance relative aux transferts transfrontaliers de données, sur la documentation des requêtes d'accès émanant d'autorités étrangères et sur la fixation de principes en matière de minimisation de données.

III. Conclusion

En résumé, l'on retiendra que ces Recommandations reflètent les attentes très élevées du CEPD s'agissant des mesures à prendre suite à l'arrêt Schrems II. Les mesures contractuelles proposées dans les Recommandations constituent une palette intéressante de clauses qui pourraient, à l'avenir, faciliter les négociations avec les prestataires de services par l'émergence d'un certain « standard minimal » concernant les engagements contractuels. Un premier pas en ce sens a du reste déjà été franchi vu que, moins de 10 jours après la publication de ces Recommandations, Microsoft a annoncé (le 19 novembre 2020) une modification de ses conditions contractuelles, afin de refléter certains des points évoqués ci-dessus. En tout état de cause, on gardera à l'esprit que le CEPD considère que les mesures contractuelles et organisationnelles ne sont efficaces de manière autonome que lorsque la législation de l'État de destination est conforme aux Garanties essentielles européennes, donc quand l'accès aux données personnelles par les autorités publiques en vertu du droit national est suffisamment encadré et limité.

_swissprivacy.law

Proposition de citation : Philipp FISCHER / Kastriot LUBISHTANI, Mesures techniques, contractuelles et organisationnelles à observer suite à l'arrêt Schrems II, 7 décembre 2020 *in* www.swissprivacy.law/40