

Décision d'adéquation par l'Union européenne du niveau suisse de protection des données et Privacy Shield avec les Etats-Unis

Association la Suisse en Europe

Philippe G. Nell¹, 29 juillet 2020

Table des matières

Introduction.....	2
1. Base juridique de l'UE : Règlement général sur la protection des données.....	2
2. Décision d'adéquation : Règlement général sur la protection des données, art. 45	2
3. Suspension temporaire des processus d'adéquation	3
4. Implications pour la Suisse.....	4
4.1 Révision de la loi sur la protection des données	4
4.2 Liens avec les relations bilatérales Suisse-UE	5
4.3 Adéquation avec les Etats-Unis : Privacy Shield.....	5
4.4 Décision de la CJUE au sujet du EU-US Privacy Shield, 16.07.20.....	5
4.5 Suite des opérations pour le transfert des données personnelles vers les Etats-Unis....	7
a) Etats-Unis	7
b) Union Européenne.....	7
c) Suisse.....	8
4.6 Conséquences pour la Suisse : scénario de décision d'adéquation négative de l'UE ...	9
Conclusion.....	9
Annexe 1. Questions referred by M. Schrems, Case C-311/18.....	11
Annexe 2 : Eléments clés de la révision de la loi sur la protection des données	14

¹ Chef de la délégation suisse pour la négociation du Swiss-US Privacy Shield (2015-2017) et pour les deux premiers examens de l'arrangement (2018, 2019), Chef du groupe de travail interdépartemental Privacy Shield (2015-19) dans le cadre de ses fonctions de Ministre, Chef du secteur Amériques, SECO (2004-19). Membre du Comité de l'Association La Suisse En Europe. Les vues présentées dans ce document n'engagent que leur auteur.

Introduction

Lors de la réunion du Comité directeur de l'Association La Suisse en Europe du 18 juin 2020, son Président, le professeur Thomas Cottier, a demandé des renseignements au sujet de l'état du dossier concernant la **décision d'adéquation** de l'UE pour la Suisse en matière de protection des données personnelles.

Ce bref document présente les éléments clefs concernant cette décision qui se base sur un **examen comparatif** de la législation de l'UE et de celle de la Suisse dans le domaine de la protection des données à caractère personnel.

Les relations avec les **Etats-Unis** dans le domaine de la protection des données personnelles sont également traitées par le biais du **EU-US Privacy Shield** - déclaré pas valable par l'arrêt C-311/18 de la Cour de Justice de l'UE (CJUE) le 16 juillet 2020 - et des conséquences de cet arrêt pour le **Swiss-US Privacy Shield** et pour la décision d'adéquation de l'UE envers la Suisse.

1. Base juridique de l'UE : Règlement général sur la protection des données

Le **Règlement n° 2016/679**, dit **Règlement général sur la protection des données (RGPD)**, ou encore **GDPR**, de l'anglais *General Data Protection Regulation*), est un règlement de l'UE qui constitue le texte de référence en matière de protection des données à caractère personnel². Il renforce et unifie la protection des données pour les individus au sein de l'UE.

Après quatre années de négociations législatives, ce règlement a été définitivement adopté par le Parlement européen le 27 avril 2016. Ses dispositions sont **directement applicables** depuis le 25 mai 2018 dans l'ensemble des 27 Etats membres de l'UE.

Ce règlement remplace la directive sur la protection des données personnelles (95/46/CE) adoptée en 1995 (article 94 du Règlement) ; contrairement aux directives, les règlements n'impliquent pas que les Etats membres adoptent une loi de transposition pour être applicables.

Les principaux **objectifs** du RGPD sont d'accroître à la fois **la protection des personnes** concernées par un traitement de leurs données à caractère personnel et la responsabilisation des acteurs de ce traitement. Ces principes pourront être appliqués grâce à l'augmentation du pouvoir des **autorités de contrôle**.

2. Décision d'adéquation : Règlement général sur la protection des données, art. 45

L'article 45 du RGPD fait référence aux décisions d'adéquation. Une décision d'adéquation est une décision par laquelle la Commission européenne constate que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou une organisation internationale assure **un niveau de protection adéquat** (équivalent à celui de l'UE) aux données personnelles transmises de l'UE vers ce pays tiers.

Les éléments pris en compte par la Commission pour évaluer le caractère adéquat du niveau de protection sont précisés dans l'article 45. Parmi eux figurent notamment: a) l'état de droit; b) le respect des droits de l'homme et des libertés fondamentales; c) l'existence et le

² Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, disponible en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=EN>, consulté le 29/07/20.

fonctionnement effectif d'une ou de plusieurs **autorités de contrôle indépendantes**, chargées d'assurer le respect des règles en matière de **protection des données** et de les faire appliquer; d) les engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de **conventions** ou **d'instruments juridiquement contraignants**; e) la participation du pays tiers ou de l'organisation internationale en question à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel.

3. Suspension temporaire des processus d'adéquation

Le **24 juin 2020** la Commission européenne a publié son rapport sur les deux premières années du RGPD³.

Selon le rapport, les décisions d'adéquation des pays tiers seront prises après **l'arrêt Schrems II** du 16 juillet 2020 en fonction de la mise en œuvre des **standards européens** dans la législation nationale des pays tiers et de clarifications éventuelles liées à l'arrêt Schrems II.

Extrait de la page 11 du rapport :

“As part of the first evaluation of the GDPR, the Commission is also required to review the adequacy decisions that were adopted under the former rules. The Commission services have engaged in an intense dialogue with each of the 11 concerned third countries and territories to assess how their data protection systems have evolved since the adoption of the adequacy decision and whether they meet the standard set by the GDPR.

The need to ensure the continuity of such decisions, as a key tool for trade and international cooperation, is one of the factors that has prompted several of these countries and territories to modernize and strengthen their privacy laws. Additional safeguards are being discussed with some of these countries and territories to address relevant differences in protection.

However, given that the Court of Justice in a judgment to be delivered on 16 July may provide clarifications that could be relevant for certain elements of the adequacy standard, the Commission will report separately on the evaluation of the existing adequacy decisions after the Court of Justice has handed down its judgment in that case.”

Dans l'arrêt Schrems II du 16 juillet 2020, la CJUE n'a pas remis en question les **clauses contractuelles standards** mais a déclaré pas valable le **EU-US Privacy Shield** (Annexe 1 : questions posées par M. Schrems à la CJUE ; les questions 9 et 10 concernent le EU-US Privacy Shield⁴).

³ *Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU approach to the digital transition – two years of application of the General Data Protection Regulation*, COM(2020) 264, Brussels, 24/06/20, disponible en ligne:

https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v6_1.pdf , consulté le 29/07/20.

⁴ La décision d'adéquation de l'UE envers les USA est basée sur le EU-US Privacy Shield (bouclier de protection des données). Il s'agit d'un arrangement par lequel les organisations/firmes US bénéficiaires se soumettent à un ensemble de règles équivalentes à celles du RGPD et acceptent que des personnes concernées par les transferts de données déposent des plaintes auprès d'un « independent recourse mechanism » ou d'un organe arbitral. Des demandes d'information peuvent aussi être effectuées auprès d'une Ombudsperson au Département d'Etat (US State Department) concernant l'accès et l'utilisation de données personnelles par les services d'intelligence US. Le Swiss-US Privacy Shield règle les relations entre la Suisse et les USA ; son contenu est identique au EU-US Privacy Shield. Pour l'arrangement Swiss-US Privacy Shield et les derniers développements voir en ligne :

<https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland/transmission-des-donnees-aux-etats-unis.html>, consulté le 29/07/20.

4. Implications pour la Suisse

4.1 Révision de la loi sur la protection des données

Le projet de révision de la loi sur la protection des données (voir annexe 2 pour les éléments clés) devrait, selon la planification actuelle, être adopté à la **session d'automne** du Parlement.

Selon la Commission européenne, le droit suisse actuel est tout à fait insuffisant. La décision d'adéquation dépendra de la révision en cours, perçue comme largement meilleure.

Le projet de la loi suisse étant avancé, il n'est pas impossible que l'adéquation avec la Suisse soit assortie d'une « review clause » avec un délai permettant de voir si le projet de loi a été approuvé entretemps et si aucun obstacle ne contrevient à son **entrée en vigueur**.

Actuellement, les deux chambres rencontrent des difficultés à s'accorder sur une des dernières divergences concernant le **profilage**⁵, ce qui pourrait faire échouer le projet.

Si le Parlement adopte le projet de loi, la Suisse peut être relativement confiante concernant l'adéquation d'autant que le Parlement a approuvé récemment la ratification du *Protocole d'amendement à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108)*⁶, élément important pour la Commission européenne.

Malgré l'insistance de la Commission Européenne, la Suisse n'a **signé** ce Protocole d'amendement que le 30 octobre 2019⁷ car l'acceptation de ses dispositions dépendait de la révision de la loi sur la protection des données par le Parlement qui était largement en cours en octobre 2019.

Les objectifs de la modernisation de la Convention 108 sont d'une part, répondre aux défis nés de l'usage des nouvelles technologies de l'information et de la communication et, d'autre part, renforcer une mise en œuvre effective de la Convention.

Le principal **risque** pour la décision d'adéquation de l'UE envers la Suisse est le **rejet du projet de révision** de la loi sur la protection des données par le Parlement au vote final ou un **référendum**, si aucune solution ne devait être possible pour le **profilage**.

Les prochaines étapes concernant la décision d'adéquation sont les suivantes :

- Avis du Comité Européen de la Protection des Données (EDPB⁸).
- Consultation d'un comité composé de représentants des Etats membres (procédure de comitologie).
- Information de la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen.

⁵ Le profilage est un ensemble d'outils et de méthodes d'analyse et de prédictions comportementales. Selon les objectifs et les cibles choisis, un profilage peut être appliqué dans divers domaines, comme dans la criminologie, dans la politique et dans le domaine social. À partir des données personnelles, le profilage fournit des renseignements sur le déplacement, les habitudes, la localisation et les relations internationales. Le RGPD définit le terme « profilage » dans l'article 4.4.

⁶ Pour les nouveautés de la Convention 108 modernisée, voir : Conseil de l'Europe, *La Convention 108 modernisée : aperçu des nouveautés*, disponible en ligne : <https://rm.coe.int/la-convention-108-modernisee-apperçu-des-nouveautés-fr/16808b07e8>, consulté le 29/07/20.

⁷ Conseil fédéral, *Le Conseil fédéral signe la nouvelle Convention du Conseil de l'Europe sur la protection des données*, communiqué de presse, 30/10/19, disponible en ligne :

<https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-76861.html>, consulté le 29/07/20.

⁸ Acronyme anglais pour European Data Protection Board.

- Adoption de la décision d'adéquation par le collège des commissaires.

4.2 Liens avec les relations bilatérales Suisse-UE

S'agissant des relations bilatérales entre la Suisse et l'UE, le dossier de la protection des données se caractérise par un **intérêt de l'UE** pour une protection rigoureuse en Suisse, et, entre la Suisse et ses autres partenaires. Il en résulte qu'il s'agit d'une situation **win-win** qui ne devrait pas être affectée par les négociations concernant l'accord-cadre entre la Suisse et l'UE.

Ceci ressort également d'un interview au cours duquel Didier Reynders, Commissaire européen en charge de la protection des données, a présenté le 24 juin les récents développements dans l'UE avec COVID-19 et les décisions d'adéquation notamment celle la Suisse.

Didier Reynders a relevé qu'il « espère que le Parlement suisse va pouvoir adopter prochainement la nouvelle loi qui est en discussion au Parlement. Cela nous aiderait, évidemment, à montrer que cette nouvelle loi est en adéquation avec le règlement général.

Et puis, nous avons dans le courant du mois de juillet une décision importante qui doit être prise à la CJUE sur un recours concernant l'ensemble de ses relations avec les pays tiers qui aura aussi un impact.

*Je crois que si le Parlement suisse peut avancer sur cette nouvelle loi, nous aurons l'occasion de **négoier rapidement** une **façon de confirmer l'adéquation** qui existe aujourd'hui mais qui doit être mise à jour⁹. »*

4.3 Adéquation avec les Etats-Unis : Privacy Shield

L'UE a octroyé l'adéquation aux Etats-Unis en 2000 sur la base d'un premier arrangement (Safe Harbor). Celui-ci a été déclaré **pas valable** par la CJUE en **2015** suite à l'arrêt Schrems I. Le EU-US Safe Harbor a été remplacé en 2016 par le EU-US Privacy Shield afin de renforcer la protection des données transférées aux Etats-Unis et de répondre aux insuffisances mises en évidence par la CJUE.

La Suisse a également conclu un arrangement **Safe Harbor** avec les Etats-Unis qui est entré en vigueur en 2009. Elle l'a ensuite remplacé en 2017 avec le Swiss-US Privacy Shield.

La grande similarité entre les régimes de protection des données suisses et de l'UE, et la coopération conjointe dans le cadre de Schengen, ont permis à la Suisse de convaincre les Etats-Unis que la Suisse devait obtenir exactement le même Privacy Shield que l'UE inclus la possibilité pour des personnes de disposer de l'accès au «**binding arbitration mechanism** » pour des plaintes pas résolues et à l'**Ombudsperson** du Département d'Etat pour les questions liées à l'accès et à l'usage de données personnelles par des organes d'intelligence du gouvernement des Etats-Unis.

4.4 Décision de la CJUE au sujet du EU-US Privacy Shield, 16.07.20

Le 16.07.20, la CJUE a **invalidé** la décision 2016/1250 relative à l'adéquation de la protection assurée par le EU-US Privacy Shield (PS). Les principales raisons sont liées aux conditions

⁹ La Matinale, *Publier des règles sur l'usage des données permet de créer la confiance*, 24/06/20, disponible en ligne : <https://www.rts.ch/info/monde/11424605-publier-des-regles-sur-lusage-des-donnees-permet-de-creer-la-confiance.html>, consulté le 29/07/20.

d'obtention et à l'utilisation de données personnelles par les services de renseignement des Etats-Unis et à l'impossibilité pour des ressortissants de l'UE de défendre leurs droits auprès de tribunaux aux Etats-Unis. La Cour résume sa position dans les termes suivants¹⁰ :

« La Cour procède, enfin, à l'examen de la validité de la décision 2016/1250 au regard des **exigences** découlant du RGPD, lu à la lumière des dispositions de la **Charte** garantissant le respect de la vie privée et familiale, la protection des données à caractère personnel et le droit à une protection juridictionnelle effective....

Selon la Cour, les **limitations de la protection des données** à caractère personnel qui découlent de la réglementation interne des Etats-Unis portant sur l'accès et l'utilisation, par les autorités publiques américaines, de telles données transférées depuis l'Union vers ce pays tiers, et que la Commission a évaluées dans la décision 2016/1250, ne sont **pas encadrées** d'une manière à répondre à des exigences substantiellement équivalentes à celles requises, **en droit de l'Union**, par le principe de proportionnalité, en ce que les **programmes de surveillance** fondés sur cette réglementation ne sont **pas limités au strict nécessaire**.

En se fondant sur les constatations figurant dans cette décision, la Cour relève que, pour certains programmes de surveillance¹¹, ladite réglementation ne fait ressortir d'aucune manière l'existence de **limitations à l'habilitation** qu'elle comporte pour la mise en oeuvre de ces programmes, pas plus que l'existence de garanties pour des **personnes non américaines** potentiellement visées.

La Cour ajoute que, si la même réglementation prévoit des exigences que les autorités américaines doivent respecter, lors de la mise en oeuvre des programmes de surveillance concernés, elle ne confère pas aux personnes concernées des **droits opposables** aux autorités américaines devant les **tribunaux**.

Quant à l'exigence de protection juridictionnelle, la Cour juge que, contrairement à ce que la Commission a considéré dans la décision 2016/1250, le mécanisme de médiation visé par cette décision ne fournit pas à ces personnes **une voie de recours** devant un organe offrant des garanties substantiellement équivalentes à celles requises en droit de l'Union, de nature à assurer tant **l'indépendance du médiateur** prévu par ce mécanisme que l'existence de normes habilitant ledit médiateur à adopter des **décisions contraignantes à l'égard des services de renseignement américains**. Pour toutes ces raisons, la Cour déclare la décision 1250/2016 pas valable. »

*Le Comité Européen de la Protection des Données*¹² a pris position le 17 juillet 2020 et relevé sa disponibilité pour coopérer avec les Etats-Unis et la Commission européenne afin de parvenir à un Privacy Shield conforme au droit européen¹³.

¹⁰ Cour de Justice de l'Union Européenne, *La Cour invalide la décision 2016/1250 relative l'adéquation de la protection assurée par le bouclier de protection des données UE-Etats-Unis*, Arrêt dans l'Affaire C-311/18, Data Protection Commissioner/Maximilian Schrems et Facebook Ireland, Communiqué de presse no 91/20, 16/07/20, disponible en ligne : <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091fr.pdf>, consulté le 29/07/20.

¹¹ Il s'agit notamment de : Section 702 FISA [Foreign Intelligence Surveillance Act] et EO [Executive Order] 12333.

¹² Le Comité Européen de la Protection des Données (European Data Protection Board) se compose de représentants des autorités nationales chargées de la protection des données et du Contrôleur européen de la protection des données (CEPD). S'ajoutent les autorités de contrôle des Etats de l'AELE-EEE en ce qui concerne les questions liées au RGPD, mais sans droit de vote et sans possibilité de se présenter aux élections pour la présidence ou vice-présidence.

¹³ Comité Européen de la Protection des Données, *Statement on the Court of Justice of the European Union Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*, disponible en ligne : <https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protect>, consulté le 29/07/20.

Selon Thomas Boué, Directeur-Général pour l'Europe, le Moyen Orient et l'Afrique du Business Software Alliance, qui représente des entreprises comprenant Microsoft, Oracle et IBM : « Today's Privacy Shield decision just removed from the table one of the few, and most trusted, ways to transfer data across the Atlantic.¹⁴ »

4.5 Suite des opérations pour le transfert des données personnelles vers les Etats-Unis

A ce jour, **5300 organisations et firmes américaines** sont certifiées par le DoC sous le EU-US PS ; le 65% d'entre elles sont des petites et moyennes entreprises. Elles obtiennent des données personnelles de firmes de l'UE en s'engageant à respecter les principes du EU-US PS qui étaient considérés équivalents au RGPD par la Commission européenne jusqu'à l'arrêt Schrems II du 16.07.20.

De nombreuses firmes de l'UE n'utilisaient cependant pas ou peu le EU-US PS mais procédaient par le biais de clauses contractuelles standards ou de « binding corporate rules »¹⁵.

a) Etats-Unis

Wilbur Ross, Secrétaire du commerce, s'est montré **très déçu** au sujet de l'arrêt Schrems II de la CJUE. Le Département du commerce (DoC) étudie l'arrêt de la CJUE afin d'en comprendre toutes les implications pratiques. Il entretient des contacts étroits avec la Commission européenne et le Comité Européen de la Protection des Données et espère pouvoir limiter les **conséquences négatives**.

Le DoC a communiqué la décision de la CJUE sur son site internet et indiqué qu'il continuerait à certifier et à recertifier des organisations et des firmes des Etats-Unis dans le EU-US PS et qu'elles **maintenaient** toutes leurs **obligations**¹⁶.

b) Union Européenne

Le EU-US PS **ne peut plus être utilisé** pour le transfert de données personnelles à des fins commerciales vers les Etats-Unis depuis le 16 juillet 2020.

Le Comité Européen de la Protection des Données a adopté le 23 juillet 2020 des « Frequently Asked Questions ¹⁷ » concernant les implications de l'arrêt de la CJUE portant sur le EU-US PS et mis en évidence les points suivants :

- 1) La décision 2016/1250 concernant l'adéquation de la protection du EU-US PS est **invalidée** avec effet immédiat sans aucune période de grâce. Tout transfert électronique de données personnelles sous le EU-US PS est désormais **illégal**.

¹⁴ Financial Times, *US-EU data sharing deal Privacy Shield struck down by European court. ECJ Rules main mechanism for transferring information fails to protect EU citizens' privacy*, July 17, 2020, disponible en ligne: <https://www.ft.com/content/b7a713e0-fe7e-4893-927c-7e90a1dd56d9>, consulté le 29/07/20.

¹⁵ Les « binding corporate rules » sont des règles appliquées au sein d'un groupe d'entreprises pour le transfert de données personnelles hors de l'UE.

¹⁶ Département du commerce, *Privacy Shield Framework*, Washington, disponible en ligne: <https://www.privacyshield.gov/Program-Overview>, consulté le 29/07/20.

¹⁷ Comité Européen de la Protection des Données, *Frequently asked questions on the Judgment of the Court of Justice of the European Union in Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* 23/07/20, disponible en ligne : https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faoncjec31118_en.pdf, consulté le 29/07/20.

- 2) Les entreprises peuvent utiliser des **clauses contractuelles standardisées** (« standard contractual clauses ») avec les destinataires américains de données personnelles à transmettre électroniquement. Ces clauses devront cependant être assorties d'une **évaluation** (« assessment ») basée sur les **circonstances** du transfert de données personnelles et de **mesures supplémentaires** afin de garantir que le droit des Etats-Unis ne porte pas atteinte à la protection que ces mesures garantissent. Ces entreprises devront **consulter** leur autorité de surveillance (autorité de protection des données) et leur soumettre les clauses contractuelles standardisées avant de transmettre les données personnelles par voie électronique aux Etats-Unis.

- 3) Le *Comité Européen de la Protection des Données* examine les **mesures supplémentaires** envisageables et fournira davantage d'orientations.

c) Suisse

Plus de **3200 organisations** et **firmes** des Etats-Unis sont certifiées sous le Swiss-US PS. Quasiment toutes sont également certifiées sous le EU-US PS.

L'arrangement du Swiss-US PS a fait l'objet d'une lettre adressée le 09.01.17 par Penny Pritzker, Secrétaire du commerce, à Johann N. Schneider-Ammann, Conseiller fédéral, chef du Département de l'économie, de la formation et de la recherche avec les textes du Swiss-US PS en annexe.

Le Conseiller fédéral Johann N. Schneider-Ammann a répondu le 12.01.17 à la lettre de Penny Pritzker en indiquant que la Suisse octroyait l'**adéquation** aux Etats-Unis sur la base du Swiss-US PS. La compétence pour l'octroi de l'adéquation relève cependant **du Préposé fédéral à la protection des données et à la transparence (PFPDT)** qui établit et publie une **liste** de pays sur la base de critères spécifiques.

Il en résulte que le PFPDT a informé le 16 juillet 2020 les milieux économiques par le biais de son site internet avoir pris connaissance de l'arrêt de la CJUE. Celui-ci n'est **pas directement applicable** à la Suisse ; le PFPDT l'examinera en détail et le commentera ultérieurement¹⁸.

Jusqu'ici, la Suisse a **systématiquement** repris la même liste de pays que l'**UE** pour l'octroi de l'adéquation. Comme en 2015, il faut s'attendre à ce que la Suisse **retire** les Etats-Unis de la liste des pays remplissant les conditions de l'adéquation. Ceci interviendra suite à une analyse approfondie des arguments de la CJUE par le PFPDT et les experts de la Confédération, et après des consultations avec le DoC ainsi que la Commission de l'UE.

Par ailleurs, la Suisse ne voudra en aucun lieu maintenir une situation avec les Etats-Unis qui pourrait causer des **difficultés** pour sa propre décision d'adéquation avec l'UE. L'UE pourrait difficilement accepter que, vu les liens commerciaux très étroits entre ses entreprises et celles de la Suisse, les données personnelles de ses ressortissants soient envoyées aux Etats-Unis via le Swiss-US Privacy Shield qui aurait été conservé.

De plus, le DoC a besoin de **ressources importantes** pour administrer le EU-US PS qui proviennent de versements annuels par les organisations et firmes américaines certifiées au

¹⁸ Préposé fédéral à la protection des données et à la transparence, *Arrêt de la Cour de Justice de l'Union européenne (CJUE) sur les clauses contractuelles types européennes et le bouclier de protection des données entre l'UE et les Etats-Unis (Privacy Shield)*, communiqué de presse, 16/07/20, disponible en ligne : https://www.edoeb.admin.ch/edoeb/fr/home/actualites/aktuell_news.html#979050109, consulté le 29/07/20.

PS. Le financement de l'organe arbitral est aussi assuré par les participants US du PS. Le Swiss-US PS pourrait difficilement justifier et financer les structures actuelles.

4.6 Conséquences pour la Suisse : scénario de décision d'adéquation négative de l'UE

Selon l'article 45 du règlement général sur la protection des données (RGPD), l'équivalence est une **décision unilatérale**.

Au cas où la Suisse n'obtenait pas une décision d'adéquation positive de l'UE, les art. 46 et 47 du RGPD s'appliqueraient. Ceci signifierait des procédures relativement **lourdes** pour les entreprises. Les échanges de données personnelles de l'UE vers la Suisse devraient s'effectuer avec notamment des **clauses contractuelles standards** ou des règles d'entreprises contraignantes (Corporate binding rules).

En acceptant ces clauses détaillées, les firmes suisses s'engageraient à appliquer les principes du RGPD en matière de protection des données à caractère personnel (**art. 5 RGPD**) avec notamment: la limitation de la finalité, la minimisation des données, la limitation des durées de conservation des données, la protection des données dès la conception et la protection des données par défaut, le traitement de catégories particulières de données à caractère personnel, les mesures visant à garantir la sécurité des données, ainsi que les exigences en matière de transferts ultérieurs à des organismes dans d'autres pays qui ne sont pas liés par les clauses contractuelles.

Les clauses contractuelles sont déjà utilisées aujourd'hui par les firmes de l'UE et suisses avec tous les pays ne bénéficiant pas d'une **décision d'adéquation** de l'UE ou de la Suisse.

S'agissant des relations économiques Suisse-UE, le volume d'échanges de marchandises (CHF 1 milliard/jour) et de services et si volumineux que l'adéquation est **indispensable**. Sans adéquation, il en résulterait des **coûts administratifs et juridiques** importants pour les firmes suisses et de l'UE, voire le déplacement d'activités dans l'UE.

Conclusion

La Suisse devrait obtenir au cours des prochains mois une décision d'adéquation de l'UE témoignant de l'équivalence de sa législation sur la protection des données personnelles avec celle de l'UE. Il est autant dans l'intérêt de l'UE que de celui de la Suisse de disposer d'un régime de protection des données élevé et le plus proche possible.

Avec les Etats-Unis, un rétablissement du EU-US Privacy Shield sera très difficile et le Swiss-US Privacy Shield devrait aussi être dénoncé étant donné la similarité des régimes suisse et de l'UE de protection des données personnelles et de leur approche en la matière.

L'arrêt Schrems I de la CJUE (2015) avait déjà mis en évidence les mêmes problèmes que l'arrêt Schrems II (2020) concernant le degré d'accès des services de renseignement des Etats-Unis aux données transmises outre-Atlantique et l'impossibilité pour les ressortissants de l'UE de faire valoir leurs droits devant des tribunaux aux Etats-Unis dans ce domaine. Ces deux questions, ainsi que celle de l'indépendance et des moyens d'action de l'Ombudsperson, avaient été longuement traitées lors de chaque examen annuel du Privacy Shield, notamment en raison de l'arrêt Schrems II.

Les Etats-Unis s'étaient efforcés de démontrer que l'accès des services de renseignement aux données personnelles était limité et sujet à des contrôles internes stricts. S'agissant de la

possibilité pour un ressortissant de l'UE de déposer une plainte auprès d'un tribunal concernant un service de renseignement, la demande de l'UE n'a pas pu être satisfaite et ne saurait l'être à l'avenir. L'Ombudsperson était la meilleure solution possible en disposant, selon les Etats-Unis, de toute l'indépendance requise pour exercer sa fonction.

Finalement, on ne saurait manquer de relever que, au cours des quatre ans du EU-US Privacy Shield, l'Ombudsperson n'a eu aucun cas à traiter. Dans ces circonstances, il est regrettable qu'un régime, qui, en fin de compte, avait simplifié les procédures et renforcé la protection des données aux Etats-Unis, soit invalidé. La Commission européenne avait très bien compris ce risque en défendant le EU-US Privacy Shield avec conviction et détermination.

Il est également difficile de concevoir comment des clauses contractuelles standards pourraient mieux protéger un ressortissant de l'UE que le défunt EU-US Privacy Shield face à des actions des services de renseignement des Etats-Unis ou lui octroyer davantage de moyens de clarifications et de corrections que l'Ombudsperson.

Avec un commerce transatlantique annuel de 7.1 trillions de dollars, les flux de données personnelles continueront à être effectués par des milliers d'entreprises, grandes, moyennes et petites, sans pour autant assurer davantage de sécurité aux ressortissants de l'UE. La révolution industrielle 4.0 et le nouveau réseau 5G ne pourront que contribuer à accélérer les transferts électroniques de données, inclus les données personnelles.

Annexe 1. Questions referred by M. Schrems, Case C-311/18

Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 — Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems

(Case C-311/18)

2018/C 249/21 Language of the case: English

Referring court

High Court (Ireland)

Parties to the main proceedings

Applicant: Data Protection Commissioner

Defendants: Facebook Ireland Limited, Maximillian Schrems

Questions referred

¹In circumstances in which personal data is transferred by a private company from a European Union (EU) member state to a private company in a third country for a commercial purpose pursuant to Decision 2010/87/EU ([1](#)) as amended by Commission Decision 2016/2297 ([2](#)) ('the SCC Decision') and may be further processed in the third country by its authorities for purposes of national security but also for purposes of law enforcement and the conduct of the foreign affairs of the third country, does EU law (including the Charter of Fundamental Rights of the European Union ('the Charter')) apply to the transfer of the data notwithstanding the provisions of Article 4(2) of TEU in relation to national security and the provisions of the first indent of Article 3(2) of Directive 95/46/EC ([3](#)) ('the Directive') in relation to public security, defence and State security?

²(1) In determining whether there is a violation of the rights of an individual through the transfer of data from the EU to a third country under the SCC Decision where it may be further processed for national security purposes, is the relevant comparator for the purposes of the Directive:

- a) The Charter, TEU, TFEU, the Directive, ECHR (or any other provision of EU law); or
- b) The national laws of one or more member states?

(2) If the relevant comparator is b), are the practices in the context of national security in one or more member states also to be included in the comparator?

3. When assessing whether a third country ensures the level of protection required by EU law to personal data transferred to that country for the purposes of Article 26 of the Directive, ought the level of protection in the third country be assessed by reference to:
- a) The applicable rules in the third country resulting from its domestic law or international commitments, and the practice designed to ensure compliance with those rules, to include the professional rules and security measures which are complied with in the third country;
or
 - b) The rules referred to in a) together with such administrative, regulatory and compliance practices and policy safeguards, procedures, protocols, oversight mechanisms and non judicial remedies as are in place in the third country?
4. Given the facts found by the High Court in relation to US law, if personal data is transferred from the EU to the US under the SCC Decision does this violate the rights of individuals under Articles 7 and/or 8 of the Charter?
5. Given the facts found by the High Court in relation to US law, if personal data is transferred from the EU to the US under the SCC Decision:
- a) Does the level of protection afforded by the US respect the essence of an individual's right to a judicial remedy for breach of his or her data privacy rights guaranteed by Article 47 of the Charter?

If the answer to a) is yes,
 - b) Are the limitations imposed by US law on an individual's right to a judicial remedy in the context of US national security proportionate within the meaning of Article 52 of the Charter and do not exceed what is necessary in a democratic society for national security purposes?
6. (1) What is the level of protection required to be afforded to personal data transferred to a third country pursuant to standard contractual clauses adopted in accordance with a decision of the Commission under Article 26(4) in light of the provisions of the Directive and in particular Articles 25 and 26 read in the light of the Charter?
- (2) What are the matters to be taken into account in assessing whether the level of protection afforded to data transferred to a third country under the SCC Decision satisfies the requirements of the Directive and the Charter?
7. Does the fact that the standard contractual clauses apply as between the data exporter and the data importer and do not bind the national authorities of a third country who may require the data importer to make available to its security services for further processing the personal data transferred pursuant to the clauses provided for in the SCC Decision preclude the clauses from adducing adequate safeguards as envisaged by Article 26(2) of the Directive?
8. If a third country data importer is subject to surveillance laws that in the view of a data protection authority conflict with the clauses of the Annex to the SCC Decision or Article 25 and 26 of the Directive and/or the Charter, is a data protection authority required to use its enforcement powers under Article 28(3) of the Directive to suspend data flows or is the exercise of those powers limited to exceptional cases only, in light of Recital 11 of the Directive, or can a data protection authority use its discretion not to suspend data flows?

- 9.(1) For the purposes of Article 25(6) of the Directive, does Decision (EU) 2016/1250 ([4](#)) ('the Privacy Shield Decision') constitute a finding of general application binding on data protection authorities and the courts of the member states to the effect that the US ensures an adequate level of protection within the meaning of Article 25(2) of the Directive by reason of its domestic law or of the international commitments it has entered into?
- (2) If it does not, what relevance, if any, does the Privacy Shield Decision have in the assessment conducted into the adequacy of the safeguards provided to data transferred to the United States which is transferred pursuant to the SCC Decision?
10. Given the findings of the High Court in relation to US law, does the provision of the Privacy Shield ombudsperson under Annex A to Annex III of the Privacy Shield Decision when taken in conjunction with the existing regime in the United States ensure that the US provides a remedy to data subjects whose personal data is transferred to the US under the SCC Decision that is compatible with Article 47 of the Charter?
11. Does the SCC Decision violate Articles 7, 8 and/or 47 of the Charter?

Annexe 2 : Éléments clés de la révision de la loi sur la protection des données

La révision **renonce** à la protection des données des **personnes morales**, en adéquation avec les règles européennes de protection des données et la majorité des législations étrangères. Cette mesure facilite notamment les échanges de données avec l'étranger.

La **transparence** des traitements est améliorée : le **devoir d'information** lors de la collecte est étendu à tous les traitements dans le secteur privé. Il est assorti d'exceptions et peut être rempli de manière standardisée. La révision introduit en outre un devoir spécifique d'information lors de **décisions individuelles automatisées** ainsi que le droit pour la personne concernée, à certaines conditions, de faire valoir son point de vue et de demander que la décision soit revue par une personne physique. Elle étend également les informations à fournir à la personne concernée lorsque celle-ci exerce son droit d'accès.

La révision encourage le développement de l'**autoréglementation**, par le biais de **codes de conduite** qui visent à faciliter les activités des responsables du traitement et à contribuer au respect de la législation. Ces codes sont élaborés par les branches et peuvent être soumis au préposé.

Le statut et l'**indépendance** du **préposé** sont renforcés. La révision prévoit que celui-ci peut prendre, à l'instar de ses homologues européens, des **décisions contraignantes** à l'égard des responsables du traitement et des sous-traitants, au terme d'une enquête ouverte d'office ou sur dénonciation.

Le **volet pénal** de la loi est renforcé à plusieurs égards, pour compenser notamment le fait que le préposé, contrairement à la quasi-totalité de ses homologues européens, n'a pas le pouvoir d'infliger des sanctions administratives.

En sus de la révision totale de la loi fédérale sur la protection des données, le projet comprend également une révision partielle d'autres lois fédérales, notamment afin de mettre en œuvre les exigences de la directive (UE) 2016/680. Il s'agit principalement du **code pénal, du code de procédure pénale, de la loi sur l'entraide pénale internationale et de la loi sur l'échange d'information Schengen**.

Source : Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales

<https://www.admin.ch/opc/fr/federal-gazette/2017/6565.pdf>