DE LA « SPHERE DE SECURITE » AU « BOUCLIER DE PROTECTION » : ASPECTS CHOISIS DU *EU–US PRIVACY SHIELD*

FROM THE SAFE HARBOR TO THE PRIVACY SHIELD: SELECTED ASPECTS OF THE EU–US PRIVACY SHIELD

Philipp FISCHER*

LT EU law; International co-operation; Ombudsmen; Personal data; Privacy shield; Switzerland; Transborder data flows; United States

INTRODUCTION

Un transfert de données personnelles vers un Etat autre que l'Etat de résidence de la personne concernée accroît le risque pour cette dernière de perdre le contrôle sur ses données personnelles, respectivement de ne plus être en mesure d'exercer les droits que lui confère la législation en matière de protection des données de son Etat de résidence.

Pour ce motif, les flux transfrontaliers de données personnelles font l'objet d'une réglementation spécifique sous l'empire de la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données personnelles et à la libre circulation de ces données (la « Directive 95/46/CE »).[1] Ces règles sont en substance reprises dans le Règlement général sur la protection des données (Règlement no. 2016/679, le « RGPD ») qui sera directement applicable dans tous les Etats membres de l'UE à compter du 25 mai 2018.

TRANSFERT DE DONNEES PERSONNELLES VERS UN PAYS TIERS SOUS L'EMPIRE DU RGPD

A teneur de l'art.45(1) RGPD, un transfert de données personnelles vers un pays tiers (hors UE et Espace économique européen) est possible « sans autorisation

* Philipp Fischer, LL.M. (Harvard), partner at OBERSON ABELS SA in Geneva

INTRODUCTION

A transfer of personal data to a State other than the State of residence of the data subject increases his or her risk of losing control over the personal data, as well as the risk of no longer being able to exercise the rights conferred by the data protection legislation of his or her State of residence.

Accordingly, the cross-border flows of personal data are subject to specific regulatory requirements under the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the ''Directive 95/46/EC''). These rules are in essence also encapsulated in the General Data Protection Regulation (Regulation 2016/679, the ''GDPR''), which will be directly applicable in all EU Member States as of 25 May 2018.

TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY UNDER THE GDPR

According to art.45(1) GDPR, a personal data transfer to a third country (outside the EU and the European Economic Area) is possible without ''specific

authorization'' provided that the third country ensures an adequate level of data protection. The recognition of the adequate level is formalised by an ''adequacy decision'' issued by the European Commission (art.45(3) GDPR). Even though, as indicated, the transfer of personal data to such a State is not subject to a specific authorisation requirement, such transfer must still comply with the general data protection principles, particularly those set forth in art.5 GDPR.

spécifique » pour autant que ce pays tiers assure un niveau de protection adéquat. La reconnaissance du niveau adéquat est formalisée par une « décision d'adéquation » rendue par la Commission européenne (art.45(3) RGPD). Même si, comme indiqué, le transfert de données personnelles vers un tel Etat n'est pas soumis à une autorisation spécifique, il n'en demeure pas moins qu'un tel transfert doit s'effectuer dans le respect des principes généraux en matière de protection des données, notamment ceux visés à l'art.5 RGPD.[2]

A transfer of personal data to a State with data protection regulations which have not been subject to an adequacy decision is not prohibited, but is subject to additional requirements. The main additional requirements fall into the following two categories: (i) the ''appropriate safeguards'' (art.46 GDPR); and (ii) the ''derogations for special situations'' (art.49 GDPR):

Un transfert de données personnelles vers un Etat dont la réglementation en matière de protection des données n'a pas fait l'objet d'une décision d'adéquation n'est pas interdit, mais est soumis à des exigences additionnelles, qui peuvent, pour l'essentiel, être regroupées en deux catégories : (i) les « garanties appropriées » (art.46 RGPD) ; et (ii) les « dérogations pour des situations particulières » (art.49 RGPD) :

- Transfers subject to appropriate safeguards include situations in which the data controller/processor and the recipient of the personal data in the third country agree upon a contractual data protection framework, which meets the standards set forth by the European Commission and/or a national data protection authority (''standard data protection clauses'' within the meaning of art.46(2) GDPR).

- Les transferts moyennant des garanties appropriées comprennent notamment les situations dans lesquelles le responsable du traitement (ou le sous-traitant) convient avec le récipiendaire des données personnelles dans l'Etat tiers de garanties contractuelles en matière de protection des données, qui répondent à des standards minimaux approuvés par la Commission européenne et/ou une autorité de contrôle nationale (« clauses types de protection des données » au sens de l'art.46(2) RGPD).

- Derogations include situations in which: (i) the data subject has explicitly consented to the transfer (art.49(1)(a) GDPR); (ii) the transfer is necessary for the performance of a contract between the data subject and the controller (art.49(1)(b) GDPR) or the conclusion or performance of a contract concluded in the interest of the data subject (art.49(1)(c) GDPR); (iii) the transfer is necessary for important reasons of public interest (art.49(1)(d) GDPR); or (iv) the transfer is necessary in order to protect the vital interests of the data subject when the data subject is physically or legally incapable of giving consent (art.49(1)(f) GDPR).

- Les cas de dérogation visent notamment les situations dans lesquelles : (i) la personne concernée a donné son consentement explicite au transfert (art.49(1)(a) RGPD) ; (ii) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement (art.49(1)(b) RGPD) ou à la conclusion ou l'exécution d'un contrat conclu dans l'intérêt de la personne concernée (art.49(1)(c) RGPD) ; (iii) le transfert est nécessaire pour des motifs importants d'intérêt public (art.49(1)(d) RGPD) ; ou (iv) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement (art.49(1)(f) RGPD).

FROM THE SAFE HARBOR TO THE PRIVACY SHIELD

DE LA « SPHERE DE SECURITE » (*SAFE HARBOR*) AU « BOUCLIER DE PROTECTION » (*PRIVACY SHIELD*)

The US data protection regulatory regime has not been the subject of an adequacy decision under the Directive 95/46/EC and it is unlikely that this situation will be

Les Etats-Unis n'ont pas fait l'objet d'une décision d'adéquation dans le cadre de la Directive 95/46/CE et il est peu vraisemblable que cette situation soit modifiée sous

l'empire du RGPD. Les transferts de données personnelles vers les Etats-Unis sont donc en principe soumis aux exigences additionnelles évoquées ci-dessus. Cela étant dit, la Commission européenne et les Etats-Unis avaient conclu un accord intitulé la « sphère de sécurité » (*EU–US Safe Harbor*) qui permettait aux entreprises américaines de prendre, sur une base volontaire, un certain nombre d'engagements en matière de protection des données. Les transferts de données personnelles vers les entreprises qui avaient adhéré au *EU–US Safe Harbor* étaient alors réputés intervenir vers un Etat au bénéfice d'une décision d'adéquation.[3]

modified under the GDPR. Transfers of personal data to the US are therefore, as a matter of principle, subject to the additional requirements referred to above. That being said, the European Commission and the US had reached an agreement called the EU–US Safe Harbor, which allowed US data controllers/processors to take, on a voluntary basis, a number of data protection commitments. Transfers of personal data to US data controllers/processors that had decided to take part in the EU–US Safe Harbor were deemed to be made to a State with the benefit of an adequacy decision.

Le *EU–US Safe Harbor* a été examiné en détail par la Cour de justice de l'UE dans le cadre de l'affaire *Schrems*.[4] Cette affaire a été déclenchée par un utilisateur du réseau social Facebook, Maximillian Schrems, qui se plaignait que les données personnelles qu'il fournissait à Facebook étaient transférées depuis la filiale irlandaise du Groupe Facebook (Facebook Ireland) vers des serveurs appartenant à Facebook, Inc. situés aux Etats-Unis. M. Schrems considérait que les règles en matière de protection des données en vigueur aux Etats-Unis n'offraient pas une protection suffisante. M. Schrems se référait notamment aux révélations faites par M. Edward Snowden au sujet des activités de la National Security Agency. L'autorité irlandaise de première instance rejeta la demande au motif que la Commission européenne avait considéré, dans le cadre de sa Décision 2000/520,[5] que les Etats-Unis offraient un niveau de protection adéquat dans le cadre de transfert de données personnelles vers des entreprises américaines ayant adhéré au *EU–US Safe Harbor*.

The EU–US Safe Harbor has been examined in detail by the Court of Justice of the EU in the context of the *Schrems* case. The proceedings were launched by a user of the social network Facebook, Maximillian Schrems, who complained that the personal data he provided to Facebook was being transferred from the Irish subsidiary of the Facebook Group (Facebook Ireland) to servers owned by Facebook, Inc. and located in the US. Mr Schrems considered that the data protection rules in force in the US did not offer a sufficient level of protection. Mr Schrems referred in particular to the revelations made by Mr Edward Snowden in respect of the activities of the National Security Agency. The Irish first instance authority rejected the claim on the ground that the European Commission had considered, in its decision 2000/520, that the US provided an adequate level of protection for the transfer of personal data to US data controllers/processors that have adhered to the EU–US Safe Harbor.

Saisie d'une question préjudicielle par l'autorité irlandaise de seconde instance, la Cour de justice de l'UE a, par jugement du 6 octobre 2015, invalidé la Décision 2000/520 au motif que les engagements souscrits dans le cadre du *EU–US Safe Harbor* étaient insuffisants pour retenir que les Etats-Unis assuraient effectivement un niveau de protection adéquat en matière de protection des données.[6]

On a preliminary ruling requested by the Irish second instance authority, the Court of Justice of the EU, in a 6 October 2015 judgment, invalidated the decision 2000/520 on the grounds that the commitments entered into under the EU–US Safe Harbor were insufficient to hold that the US provide an adequate level of data protection.

Cette décision de la Cour de justice de l'UE a eu un impact considérable, dans la mesure où elle supprimait le fondement juridique de nombreux transferts de données personnelles de l'UE vers les Etats-Unis. Le 6 février 2016,[7] quelques mois seulement après la publication du jugement, la Commission européenne a annoncé avoir conclu un nouvel accord avec les Etats-Unis. Le *EU–US Safe Harbor* devait être remplacé par un « bouclier vie privée UE-Etats-Unis » (*EU–US Privacy Shield*), un nouveau dispositif visant à tenir compte des critiques formulées par la Cour de justice de l'UE à l'égard du *EU–US Safe Harbor*.

This decision of the Court of Justice of the EU had a significant impact, as it removed the legal basis of numerous transfers of personal data from the EU to the US. On 6 February 2016, just a few months after the publication of the decision, the European Commission announced that it had reached a new agreement with the US. The EU–US Safe Harbor was to be replaced by the EU–US Privacy Shield, a new mechanism designed to take into account the criticisms of the Court of Justice of the EU in respect of the EU–US Safe Harbor.

La Commission européenne a publié le 12 juillet 2016 la décision d'adéquation qui formalise la reconnaissance du

On 12 July 2016, the European Commission published the ''adequacy decision'' which formalises the

recognition of the EU–US Privacy Shield as an adequate protection mechanism in the context of the EU data protection regulatory framework. The EU–US

EU–US Privacy Shield comme un dispositif de protection adéquat dans le contexte du droit communautaire de la protection des données.[8] Le *EU–US Privacy Shield* est opérationnel depuis le 1er août 2016.

Every US data controller/processor intending to take part in the EU–US Privacy Shield must apply for a registration on the Privacy Shield list (which is publicly available) and self-certify that it meets the data protection standards provided in this mechanism. This application must be renewed on an annual basis. More than 2,400 US companies have joined the EU–US Privacy Shield. The US Department of Commerce is in charge of ensuring compliance by the participating companies, in addition to the range of instruments at the disposal of data subjects to assert their rights.

Chaque entreprise américaine qui souhaite adhérer au *EU–US Privacy Shield* doit demander son inscription sur la liste d'adhésion (qui est publiquement disponible[9]) et s'autocertifier comme répondant aux normes en matière de protection des données prévues dans ce dispositif. Cette inscription doit être renouvelée sur une base annuelle.[10] Plus de 2.400 entreprises américaines ont adhéré au *EU–US Privacy Shield*.[11] Le *US Department of Commerce* est en charge d'assurer le contrôle du respect des obligations souscrites par les entreprises participantes, en sus de l'éventail de mesures à disposition des personnes concernées pour faire valoir leurs droits.

EU–US PRIVACY SHIELD

EU–US PRIVACY SHIELD

Obligations for participating companies

Obligations à charge des entreprises participantes

The main obligations of companies which take part in the EU–US Privacy Shield can be summarised as follows.

Les principales obligations à charge des entreprises qui participent au *EU–US Privacy Shield* peuvent être résumées comme suit.

Right to information

Devoir d'information

The right to information towards the data subject covers in particular the following elements:

Le devoir d'information à l'égard des personnes concernées[12] porte notamment sur les éléments suivants :

- the types of personal data that are processed;
- les types de données personnelles qui sont traitées ;
- the purposes for which the personal data are processed;
- les finalités pour lesquelles les données personnelles sont traitées ;
- the intention to transfer the personal data to a third party and the reasons for this transfer;
- l'intention de transférer les données personnelles à un tiers et les motifs de ce transfert ;
- the right of the data subject to formulate a request for access to personal data;
- le droit de la personne concernée de formuler une requête d'accès aux données personnelles ;
- the right, for the data subject, to authorise the participating company: (i) to process the personal data for another purpose than the one for which the data collection took place; or (ii) to communicate the personal data to a third party;
- le droit, pour la personne concernée, d'autoriser l'entreprise participante : (i) à traiter les données personnelles pour une autre finalité que celle pour laquelle ces données ont été collectées ; ou (ii) à les communiquer à un tiers[13] ;
- the different legal avenues available to the data subject to assert his or her rights; and
- les différents instruments à disposition de la personne concernée pour faire valoir ses droits ; et
- the possibility that the participating company may be required to respond to legitimate requests from the US authorities to disclose information about the data subject.
- la possibilité que l'entreprise participante puisse être amenée à répondre à des demandes licites des autorités américaines de divulguer des informations au sujet de la personne concernée.

The participating company must publish a privacy notice on its website. The participating company is also to provide a link to the Privacy Shield list (*i.e.*, the

L'entreprise participante doit publier sur son site Internet sa politique de confidentialité (*privacy notice*). L'entreprise participante doit également fournir un lien vers la liste des

entreprises participantes[14] afin de permettre de vérifier facilement le statut de l'entreprise au regard du *EU–US Privacy Shield*.

list of participating companies) to allow a verification of the company's status under the EU–US Privacy Shield.

Respect du principe de finalité

Respect of the principle of purpose limitation

Une entreprise participante ne peut traiter les données personnelles que : (i) dans le cadre de la finalité pour laquelle la collection de données est intervenue ou ; (ii) une finalité autorisée ultérieurement par la personne concernée.[15]

A participating company may only process personal data: (i) for the purpose for which the data collection took place; or (ii) for a purpose subsequently authorised by the data subject.

Si la nouvelle finalité, tout en étant différente de la finalité initiale, est néanmoins liée à celle-ci, l'entreprise participante peut utiliser les données personnelles si la personne concernée ne s'y oppose pas (*opt-out*). L'utilisation pour une finalité incompatible avec la finalité initiale présuppose un consentement préalable spécifique (*opt-in*). Un tel consentement spécifique est également nécessaire pour tout changement de finalité dans le cadre du traitement de données sensibles.

If the new purpose, while different from the original purpose, is nevertheless linked to the original purpose, the participating company may use the personal data if the data subject does not object to it (opt-out). The use for a purpose incompatible with the original purpose presupposes a specific prior consent (opt-in). Such consent is also necessary for any change of purpose in the processing of sensitive data.

Ainsi, si un employeur a transféré des données personnelles vers les Etats-Unis à des fins de traitement, l'entreprise américaine (qui, par hypothèse, a adhéré au *EU–US Privacy Shield*) pourrait être autorisée à utiliser ces données pour proposer une police d'assurance ou un système de pension, tant que la personne concernée ne s'y oppose pas (*opt-out*). Par contre, sans un consentement spécifique (*opt-in*), l'entreprise américaine ne peut pas vendre ces données personnelles à une entité commerçante tierce afin que celle-ci propose des produits ou services qui n'ont pas de rapport avec l'emploi de la personne concernée.

Thus, if an employer has transferred personal data to the US for processing, the US data controller/processor (which takes part in the EU–US Privacy Shield) may be allowed to use that data to market an insurance policy or a pension system, as long as the data subject does not oppose to it (opt-out). On the other hand, without a specific consent (opt-in), the US data controller/processor cannot sell these personal data to a third-party commercial entity to allow the acquirer to offer products or services that are not related to the employment of the data subject.

Obligation de minimisation des données

Obligation of data minimisation

L'entreprise participante ne peut recevoir et traiter des données personnelles que si celles-ci sont pertinentes aux fins du traitement envisagé. Elle est autorisée à conserver les données personnelles uniquement pendant le temps nécessaire aux fins du traitement. Une conservation plus longue présuppose l'existence de certaines finalités déterminées, telles que l'archivage dans l'intérêt public ou la recherche scientifique.[16]

The participating company may receive and process personal data only if it is relevant for the purposes of the contemplated activities. It is authorised to keep personal data only for the time necessary for processing purposes. A longer storage presupposes the existence of specific purposes, such as archiving for public interest reasons or scientific research activities.

Obligation d'assurer la sécurité des données

Obligation to ensure data security

L'entreprise participante doit veiller à ce que les données personnelles soient conservées dans un environnement sûr et protégé contre la perte, l'abus, l'accès non autorisé, la divulgation, la modification ou la destruction, en tenant dûment compte de la nature des données et des risques liés au traitement.[17]

The participating company must ensure that personal data is kept in a secure environment and protected against loss, abuse, unauthorised access, disclosure, alteration or destruction, with due regard to the nature of the data and risks related to the processing.

Enforcement mechanisms

Legal avenues available to data subjects

The EU–US Privacy Shield contains a set of mechanisms available to the data subjects in order to assert their rights:

1. Contact with the participating US data controller/processor: Each participating controller/processor must indicate the contact details of a person who can be contacted directly for any question or complaint. A response must be provided within 45 days.

2. Mechanism of Alternative Dispute Resolution (''ADR''): Each participating company must offer the data subject an access to an ADR mechanism in order to settle disputes relating to the processing of personal data. Such ADR mechanism can take the following two forms:

   Firstly, the participating company may elect an independent ADR body. The ADR body must be able to impose corrective actions and effective sanctions (for example the publication of the decision) to ensure that the participating company fulfills its obligations to protect personal data. As a matter of principle, the procedure before the ADR body is free of charge for the data subject.

   Secondly, a participating company may also elect a national data protection authority (in the EU) as the ADR body. An obligation to choose such authority as an ADR body exists only in cases where the participating company processes personal data that has been collected in the context of an employment relationship. Hence, an employee always has the possibility to liaise with a national data protection authority (in the EU) in order to formulate complaints in connection with personal data that was collected in the employment relationship and then transferred to a participating company.

   The national data protection authority shall issue its notice setting out its position within 60 days of receipt of the complaint. The data subject is informed of the notice, which is, as matter of principle, publicly available. The participating company then has 25 days to comply with the notice, otherwise the national authority may take the case to the US Federal Trade Commission for a decision on possible enforcement actions. It may also notify the US Department of Commerce of the company's refusal to comply with the notice, which may result in the company

Instruments de mise en œuvre

Eventail de mesures à disposition des personnes concernées

Le *EU–US Privacy Shield* contient une série de mécanismes à disposition des personnes concernées pour faire valoir leurs droits :

1. Contact avec l'entreprise participante : Chaque entreprise participante doit indiquer les coordonnées d'une personne qui peut être contactée directement pour toute question ou réclamation. Une réponse doit être fournie dans les 45 jours.

2. Mécanisme de règlement alternatif de litiges (*Alternative Dispute Resolution*, « ADR ») : Chaque entreprise participante doit offrir aux personnes concernées une voie d'ADR afin de trancher les litiges relatifs au traitement de données personnelles. Cette voie d'ADR peut prendre deux formes :

   En premier lieu, l'entreprise participante peut choisir un organisme d'ADR indépendant.[18] L'organisme d'ADR doit être en mesure d'imposer des actions correctrices et des sanctions efficaces (par exemple la publication de la décision) pour garantir que l'entreprise participante remplit ses obligations de protéger les données personnelles. La procédure devant l'organisme d'ADR est en principe gratuite.

   En second lieu, une entreprise participante peut également choisir une autorité nationale (de l'UE) en matière de protection des données en tant qu'organisme d'ADR.[19] Une obligation de choisir une telle autorité en tant qu'organisme d'ADR n'existe que dans les cas dans lesquels l'entreprise participante traite des données personnelles qui ont été collectées dans le cadre d'une relation de travail. Ainsi, un employé dispose toujours de la possibilité de s'adresser à l'autorité nationale (dans l'UE) en matière de protection des données pour formuler des griefs en lien avec des données personnelles recueillies dans le cadre d'une relation de travail et qui ont été transférées à une entreprise participante.

   L'autorité nationale donne son avis dans les 60 jours qui suivent la réception de la réclamation. La personne concernée est informée de l'avis, qui est en principe publié. L'entreprise participante dispose alors de 25 jours pour se conformer à l'avis, faute de quoi l'autorité nationale pourra porter l'affaire devant la *US Federal Trade Commission* en vue du prononcé d'éventuelles mesures coercitives. Elle peut également informer le *US Department of Commerce* du refus de l'entreprise de se conformer à l'avis, ce qui

peut entraîner son retrait de la liste des entreprises participantes.

Par ailleurs, si la réclamation montre que le transfert des données personnelles à l'entreprise participante viole la législation européenne (par exemple le RGPD à compter du 25 mai 2018), l'autorité nationale peut également prendre des mesures à l'encontre de la société de l'UE qui transmet les données, telles que l'ordre de suspendre le transfert de données.

3. *US Department of Commerce* ou *US Federal Trade Commission* : La personne concernée peut introduire une réclamation directement auprès de ces deux autorités, sans nécessairement contacter au préalable une autorité nationale (dans l'UE) en matière de protection des données.

being removed from the list of participating companies.

In addition, if the complaint shows that the transfer of personal data to the participating company is not in line with EU law (typically the GDPR as of 25 May 2018), the national data protection authority may also take actions against the EU company that transferred the personal data. For instance, the national data protection authority may order a suspension of the data transfer.

3. US Department of Commerce or US Federal Trade Commission: The data subject may file a claim directly with these two US authorities, without necessarily contacting beforehand a national data protection authority (in the EU).

Procédure arbitrale

Si la personne concernée estime que sa réclamation n'a pas été tranchée de manière satisfaisante par le biais des instruments évoqués ci-dessus, la personne concernée peut recourir à l'arbitrage. Ce mécanisme constitue donc un instrument de dernier ressort.[20]

Seule la personne concernée (personne physique) peut engager une procédure arbitrale contre un participant au *EU–US Privacy Shield*. La personne concernée doit notifier formellement à l'entreprise l'intention d'initier une procédure arbitrale. Cette notification doit comporter une description de la violation alléguée et un résumé des démarches déjà entreprises. Différentes mesures ont été mises en place pour assister la personne concernée dans le cadre de l'initiation et le déroulement de la procédure arbitrale :

- le droit de demander l'assistance de l'autorité nationale (dans l'UE) en matière de protection des données pour préparer la réclamation ;
- la possibilité de participer aux audiences par téléphone ou vidéoconférence ;
- la possibilité d'obtenir gratuitement la traduction des documents de l'anglais vers une autre langue ; et
- la prise en charge des frais d'arbitrage (sauf les honoraires d'avocat) par un fonds spécialement créé par le *US Department of Commerce* et financé par les contributions annuelles des sociétés adhérant au *EU–US Privacy Shield*.

Les arbitres (un ou trois en fonction de l'accord des parties) sont choisis au sein d'un groupe d'au moins 20 arbitres désignés par le *US Department of Commerce* et la Commission européenne. La procédure d'arbitrage doit être clôturée dans les 90 jours. Si le tribunal arbitral constate l'existence d'une violation des principes de

Arbitral proceedings

If the data subject is of the view that his or her claim has not been addressed in a satisfactory manner through the legal avenues mentioned above, the data subject may initiate arbitral proceedings. This mechanism is therefore an instrument of last resort.

Only the data subject (natural person) can initiate arbitral proceedings against a participant in the EU–US Privacy Shield. The data subject must formally notify the company of its intention to initiate arbitral proceedings. This notification must include a description of the alleged violation and a summary of the steps already taken. Various measures have been put in place to assist the data subject in initiating and taking part in the arbitral proceedings:

- the right to request assistance from the national data protection authority (in the EU) to prepare the claim;
- the possibility to participate to hearings through telephone or videoconference;
- the possibility to obtain free translation of documents from English to another language; and
- the coverage of arbitration fees (except for legal fees) by a special fund created by the US Department of Commerce and financed by the annual contributions of the companies joining the EU–US Privacy Shield.

The arbitrators (one or three depending upon the agreement of the parties) are chosen from a panel of at least 20 arbitrators appointed by the US Department of Commerce and the European Commission. The arbitral proceedings must be closed within 90 days. If the arbitral tribunal finds a violation of privacy protection principles, it may impose corrective action such as the

access to personal data, their correction, their deletion or their restitution. The arbitral tribunal cannot, however, grant financial indemnification.

protection de la vie privée, il peut imposer une action correctrice telle que l'accès aux données personnelles, leur correction, leur suppression ou leur restitution. Le tribunal arbitral ne peut, en revanche, pas accorder d'indemnisation financière.

Privacy Shield Ombudsperson (in the field of US national security)

Médiateur du EU–US Privacy Shield *(dans le domaine de la sécurité nationale)*

The EU–US Privacy Shield introduces a new independent organ intended to regulate the processing of personal data in the field of US national security: the Privacy Shield Ombudsperson.

Le *EU–US Privacy Shield* instaure un nouvel organe indépendant destiné à encadrer les traitements de données personnelles dans le domaine de la sécurité nationale des Etats-Unis : le Médiateur du *EU–US Privacy Shield*.[21]

A request regarding the processing of personal data in the US in the field of national security must, as a first step, be submitted to the national data protection authority (in the EU).

Une requête relative à un traitement de données personnelles intervenu aux Etats-Unis dans le domaine de la sécurité nationale doit, dans un premier temps, être introduite auprès de l'autorité nationale (dans l'UE) en charge de la protection des données.

Before being submitted to the Ombudsperson, the application is examined to verify: (i) the identity of the applicant; (ii) that the applicant is acting solely on his own behalf and not on behalf of a government or an intergovernmental organisation; (iii) that the application contains all the appropriate information; (iv) that it relates to personal data transferred to the US; and (v) that it is not unfounded, vexatious or made in bad faith.

Avant d'être soumise au Médiateur, la demande est examinée pour vérifier : (i) l'identité du demandeur ; (ii) que le demandeur agit uniquement pour son propre compte et non pour le compte d'un gouvernement ou d'une organisation intergouvernementale ; (iii) que la demande contient toutes les informations appropriées ; (iv) qu'elle porte sur des données personnelles transférées vers les Etats-Unis ; et (v) qu'elle n'est pas dénuée de fondement, vexatoire ou faite de mauvaise foi.

Once it has been determined that the application is complete, the Ombudsperson (a senior official from the US State Department) forwards it to the appropriate US agencies. The Ombudsperson may cooperate with one of the independent supervisory bodies that benefit from investigative powers. At the end of the procedure, the Ombudsperson will confirm that the application has been duly examined and that US laws have been complied with or, if not, that the violation has been remedied. The Ombudsperson's response will not specify, however, whether the data subject has been under the surveillance of the US National Intelligence Service.

Une fois qu'il a été constaté que la demande est complète, le Médiateur (un haut fonctionnaire du *US State Department*) la transmet aux organismes américains appropriés. Le Médiateur peut coopérer avec l'un des organes de contrôle indépendants dotés de pouvoirs d'enquête. A la fin de la procédure, le Médiateur confirmera que la demande a été dûment examinée et que le droit américain a été respecté ou, dans le cas contraire, que la violation a été réparée. La réponse du Médiateur ne précisera toutefois pas si la personne concernée a fait l'objet d'une surveillance de la part des services de renseignement nationaux des Etats-Unis.

RESULTS OF THE FIRST ANNUAL REVIEW (SEPTEMBER 2017)

RESULTAT DE LA PREMIERE REVUE ANNUELLE (SEPTEMBRE 2017)

The implementation of the EU–US Privacy Shield is being reviewed on an annual basis, for the first time in September 2017. The report in relation to this review was released by the European Commission on 18 October 2017.

La mise en œuvre du *EU–US Privacy Shield* fait l'objet de revues sur une base annuelle, pour la première fois en septembre 2017. Le rapport relatif à cette revue a été publié par la Commission européenne le 18 octobre 2017.[22]

This report indicates that, according to the European Commission, the mechanism set forth in the EU–US Privacy Shield ensures an adequate level of data protection. The three main areas of improvement that have been highlighted are: (i) the need for enhanced

Ce rapport indique que le fonctionnement du *EU–US Privacy Shield* permet, de l'avis de la Commission européenne, d'assurer un niveau adéquat en matière de protection des données. Les trois principaux points d'amélioration qui ont

été mis en exergue sont : (i) la nécessité d'assurer une meilleure surveillance des entreprises participantes par le *US Department of Commerce* ; (ii) la nécessité de mieux informer les personnes concernées au sein de l'UE des droits conférés par le *EU–US Privacy Shield* ; et (iii) un renforcement de la coopération entre les autorités américaines et leurs homologues au sein de l'UE.

compliance checks to be made by the US Department of Commerce; (ii) the need to better inform the data subjects within the EU of the rights granted under the EU–US Privacy Shield; and (iii) the need to enhance the cooperation between the concerned US authorities and their counterparts in the EU.

SWISS–US PRIVACY SHIELD

SWISS–US PRIVACY SHIELD

Un mécanisme tout à fait similaire au *EU–US Privacy Shield* a été mis en place entre la Suisse et les Etats-Unis. La réglementation en matière de communication transfrontalière de données personnelles entre la Suisse et les Etats-Unis est basée sur des principes tout à fait similaires à la réglementation européenne, à savoir une subdivision entre : (i) des Etats (de destination) dont la législation est réputée adéquate (dans une perspective suisse) ; et (ii) d'autres Etats (de destination) dont la législation n'est pas jugée adéquate. Les Etats-Unis sont classés dans la seconde catégorie. Cela étant dit, des entreprises américaines pouvaient obtenir une certification dans le cadre du *Swiss–US Safe Harbor* (un mécanisme très largement inspiré du *EU–US Safe Harbor*). Le Préposé fédéral à la protection des données et à la transparence a estimé que l'arrêt de la Cour de justice de l'UE dans l'affaire *Schrems* avait de facto également une portée en Suisse : Suite à la publication de cet arrêt, l'autorité suisse a considéré que le *Swiss–US Safe Harbor* ne constituait plus une base juridique suffisante pour les transferts de données personnelles de la Suisse vers les Etats-Unis.[23]

A similar mechanism to the EU–US Privacy Shield has been put in place between Switzerland and the US. The rules on cross-border communication of personal data between Switzerland and the US are based on principles similar to those applicable at EU level, namely a subdivision between: (i) States (of destination) whose data protection legislation is deemed adequate (from a Swiss perspective); and (ii) other States (of destination) whose legislation is not considered adequate. The US has been allocated to the second category. That being said, US data controllers/processors could obtain certification under the Swiss–US Safe Harbor (a mechanism based on the EU–US Safe Harbor). The Federal Data Protection and Information Commissioner considered that the judgment of the Court of Justice of the EU in the *Schrems* case was also relevant in Switzerland. Following the publication of this judgment, the Swiss authority took the position that the Swiss–US Safe Harbor was no longer a sufficient legal basis for the transfer of personal data from Switzerland to the US.

Suite aux développements intervenus au niveau de l'UE, la Suisse a également négocié avec les autorités américaines la conclusion d'un « bouclier de protection » (*Swiss–US Privacy Shield*), dont les dispositions sont substantiellement équivalentes à celles du *EU–US Privacy Shield*. Le *Swiss–US Privacy Shield* est entré en vigueur le 12 avril 2017.[24]

Following the developments that occurred at the EU level, Switzerland negotiated with the US authorities the conclusion of a privacy shield (Swiss–US Privacy Shield), which is substantially equivalent to the EU–US Privacy Shield. The Swiss–US Privacy Shield came into force on 12 April 2017.

CONCLUSION

CONCLUSION

Le transfert de données personnelles sur une base transfrontalière vers les Etats-Unis revêt une importance considérable en pratique, notamment au sein de groupes de sociétés et en raison de l'implantation, aux Etats-Unis, d'entreprises dont le modèle d'affaires est principalement axé sur l'exploitation de données personnelles.

The transfer of personal data on a cross-border basis to the US is of significant importance in practice, particularly within groups of companies and because of the existence, in the US, of companies whose business model is mainly focused on the exploitation of personal data.

Les approches en matière de protection des données sont toutefois radicalement différentes entre l'Europe continentale et les Etats-Unis. La mise en place du *EU–US Privacy Shield* (et de son pendant suisse, le *Swiss–US Privacy Shield*) vise à permettre à certaines entreprises américaines de souscrire sur une base volontaire à un

That being said, the approach to data protection regulations is radically different between continental Europe and the US. The purpose of the EU–US Privacy Shield (and its Swiss counterpart, the Swiss–US Privacy Shield) is to allow US data controllers/processors to undertake, on a voluntary basis, certain data protection commitments so as to facilitate the cross-

border flows of personal data between the EU and the US, while ensuring the protection of the rights of the data subjects.

The first annual review of this new mechanism shows that there is room for improvement as regards the ''administrative'' enforcement of the commitments undertaken by companies that have adhered to the EU–US Privacy Shield. The EU–US Privacy Shield does provide for rather sophisticated mechanisms to allow data subjects to assert their rights. The individual enforcement of data protection rules by the data subjects is however often an illusion. This is true for the processing of personal data within the same State, but applies *a fortiori* to the cross-border communications of personal data.

faisceau d'obligations en matière de protection des données de manière à faciliter les flux transfrontaliers de données personnelles entre l'UE et les Etats-Unis, tout en assurant la protection des droits des personnes concernées.

Le premier rapport d'évaluation de ce nouveau mécanisme montre que la mise en œuvre (*enforcement*) « administrative » des obligations souscrites par les entreprises qui ont adhéré au *EU–US Privacy Shield* doit encore été améliorée. Le *EU–US Privacy Shield* prévoit certes des mécanismes relativement sophistiqués pour permettre aux personnes concernées de faire valoir leurs droits. En matière de protection des données, la mise en œuvre individuelle par les personnes concernées reste toutefois souvent une illusion. Ce constat vaut pour les traitements de données personnelles au sein d'un même Etat, mais s'applique a fortiori en cas de communication transfrontalière de données personnelles.

Notes

1. Cf. arts 25 et suivants de la Directive 95/46/CE.

2. L'article 5 RGPD liste les principes généraux suivants : licéité, loyauté, transparence / limitation des finalités / minimisation des données / exactitude / limitation de la conservation / intégrité et confidentialité.

3. Décision 2000/520/CE de la Commission du 26 juillet 2000 conformément à la Directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du Commerce des Etats-Unis d'Amérique.

4. CJUE, 6 octobre 2015, *Maximillian Schrems c/. Data Protection Commissioner,* aff. C-362/14.

5. Cf. note de bas de p.3.

6. CJUE, 6 octobre 2015, *Maximillian Schrems c/. Data Protection Commissioner,* aff. C-362/14, paras 97 ss. Sur ces questions, cf. également Clotilde Camus, David Chekroun, Patrick-Hubert Petit, Les entreprises au regard du Règlement Général sur la Protection des Données : quelles réformes à opérer ?, *Revue de Droit des Affaires Internationales*, 2018, p.125.

7. Communiqué de presse de la Commission européenne du 2 février 2016, disponible à l'adresse : *http://europa.eu/rapid/press-release_IP-16-216_fr.htm* [Consulté le 13 février 2018].

8. Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la Directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le *EU–US Privacy Shield* UE-Etats-Unis.

9. Cette liste est disponible à l'adresse suivante : *https://www.privacyshield.gov/welcome* [Consulté le 13 février 2018].

10. Les entreprises qui n'adhèrent plus au *EU–US Privacy Shield* sont radiées de la liste, mais doivent continuer à appliquer les principes du dispositif aux données personnelles obtenues lorsqu'elles en étaient membres.

11. Communiqué de presse de la Commission européenne du 18 octobre 2017, disponible à l'adresse suivante : *http://europa.eu/rapid/press-release_IP-17-3966_fr.htm* [Consulté le 13 février 2018].

12. Annexe II de la Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la Directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-Etats-Unis (« Annexe II de la Décision d'exécution (UE) 2016/1250 »), para.II.1.

13. Dans un tel cas de figure, la société qui reçoit les données doit contractuellement garantir le même niveau de protection des données personnelles que celui qui est garanti dans le cadre du *EU–US Privacy Shield* (Annexe II de la Décision d'exécution (UE) 2016/1250, para.II.3).

14. Cf. note de bas de p.9.

15. Annexe II de la Décision d'exécution (UE) 2016/1250, para.II.2.

16. Annexe II de la Décision d'exécution (UE) 2016/1250, para.II.5.

17. Annexe II de la Décision d'exécution (UE) 2016/1250, para.II.4.

18. Cf. par exemple l'organisme « TRUSTe » qui a été choisi par la société *Facebook, Inc.* (*https://www.privacyshield.gov/participant?id=a2zt0000000GnywAAC&status=Active*) [Consulté le 13 février 2018].

19. A titre d'exemple, cette alternative semble avoir été choisie par la société *Microsoft Corporation* (*https://www.privacyshield.gov/participant?id=a2zt0000000KzNaAAK&status=Active*) [Consulté le 13 février 2018].

20. Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la Directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-Etats-Unis, considérant 56.

21. Annexe III de la Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la Directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-Etats-Unis.

22. Ce rapport est disponible à l'adresse suivante : *https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_fr* [Consulté le 13 février 2018].

23. Communication figurant sur le site Internet du Préposé fédéral à la protection des données, supprimée depuis lors.

24. La liste des entreprises participant au *Swiss–US Privacy Shield* peut être consultée sur le même site Internet que la liste des entreprises participant au *EU–US Privacy Shield* : *https://www.privacyshield.gov/welcome* [Consulté le 13 février 2018].

