Septembre 2020

Newsletter n° 145

Le Swiss-US Privacy Shield n’assure pas un niveau adéquat de protection des données selon le PFPDT:

Le PFPDT suit donc - sans surprise - les considérations de la CJUE sur le EU-US Privacy Shield dans l'arrêt « Schrems II ». Même les clauses contractuelles types ne constituent pas, dans bien des cas, une base suffisante pour des transferts de données vers des pays tiers. Les entreprises suisses doivent dès lors examiner comment elles pourront, dans le respect des règles sur la protection des données, transférer des données personnelles vers des pays tiers qui ne présentent pas de niveau de protection des données adéquat.

walderwyss avocats

Dans un communiqué du 8 septembre 2020, le PFPDT a retiré les Etats-Unis de sa liste des Etats qui offrent un niveau de protection des données adéquat. Les transferts de données de la Suisse vers les États-Unis fondés uniquement sur le Privacy Shield ne devraient en principe plus être effectués. Les entreprises suisses ne peuvent également pas s'appuyer sans examen préalable sur des clauses contractuelles types. Il en résulte un besoin d'action pour les entreprises en Suisse.

De Jürg Schneider
Dr. iur., avocat
Associé
Téléphone direct:+41 58 658 55 71
juerg.schneider@walderwyss.com

et David Vasella
Dr. iur., avocat
Associé
Téléphone direct: +41 58 658 52 87
david.vasella@walderwyss.com

et Lena Götzinger
Avocate (Chambre des avocats de Frankfurt am Main)
Associate
Téléphone direct: +41 58 658 56 63
lena.goetzinger@walderwyss.com

Un résultat sans surprise

La prise de position du Préposé fédéral à la protection des données et à la transparence (PFPDT) selon laquelle il n'existe plus un niveau de protection adéquat pour les données transférées aux Etats-Unis dans le cadre du Swiss-US Privacy Shield n'est pas surprenante après l'arrêt "Schrems II" de la Cour de justice de l'Union européenne (CJUE). Avec cet arrêt, la CJUE avait invalidé le EU-US Privacy Shield avec effet immédiat et a fixé des exigences supplémentaires sur l'utilisation des clauses contractuelles types dans le cadre de transferts de données.

Le PFPDT justifie sa position (en suivant celle de la CJUE) principalement par les vastes possibilités d'accès des services de renseignement américains aux données transmises et par l'absence de protection juridique suffisante des personnes concernées. Par conséquent, le PFPDT a retiré les Etats-Unis de la liste des Etats garantissant un niveau de protection des données adéquat. Néanmoins, l'existence juridique du Swiss-US Privacy Shield perdure. La liste des États établit simplement une présomption réfragable quant à savoir si (et cas échéant dans quelles conditions) un niveau adéquat de protection des données existe dans le pays de destination. En pratique, cependant, un transfert de données vers les États-Unis basé sur le Swiss-US Privacy Shield n'est plus recommandé.

Au lieu de cela, les transferts de données vers les États-Unis devront être sécurisés différemment. L'accent sera mis, en particulier pour les volumes importants de données et pour les transmissions régulières, sur les garanties mentionnées à l'art. 6 al. 2 let. a LPD, notamment les clauses contractuelles types de l'UE. Le PFPDT estime toutefois que même les clauses contractuelles types n'offrent, "dans bien des cas", pas un niveau de protection des données adéquat, car elles ne sont pas en mesure d'empêcher l'accès des autorités étrangères à des données personnelles. Dès lors, ces clauses contractuelles ne représentent plus un véritable "standard", mais doivent être complétées en fonction des circonstances (bien que le PFPDT laisse la manière de le faire ouverte).

Une nécessité d'agir pour les entreprises suisses

Les clauses contractuelles types – et cas échéant les « règles d'entreprise contraignantes» (REC) – sont à analyser au cas par cas pour voir si elles offrent une protection adéquate pour le transfert de données vers le pays de destination. Cela s'applique aux clauses contractuelles types déjà conclues ainsi qu'aux nouvelles qui vont être utilisées. Toutefois, ces considérations ne sont pas réservées aux transferts de données vers les États-Unis. Les évaluations du PFPDT concernant les garanties contractuelles sont en effet pertinentes pour tous les Etats qui figurent dans la liste des pays ne disposant pas d'un niveau de protection des données adéquat.

L'exportateur de données doit, si les transferts reposent sur des garanties contractuelles, examiner au cas par cas (au moyen d'une évaluation des risques),

conformément à l'avis du PFPDT, si des mesures supplémentaires sont nécessaires pour assurer une protection adéquate des données personnelles exportées. Selon le PFPDT, il convient d'examiner tout particulièrement si l'importateur de données est soumis à une législation qui permet aux autorités étrangères d'accéder aux données qui lui sont transférées. L'élément décisif est uniquement de savoir si le destinataire est soumis à une telle législation. Une différenciation aurait été souhaitable à cet égard. Ce n'est pas seulement le risque théorique d'accès aux données par des autorités étrangères qui devrait déterminer si une transmission est conforme aux réglementations sur la protection des données. En réalité, certains fournisseurs, selon leur modèle commercial, seront plus susceptibles que d'autres de faire l'objet d'un accès des autorités, et ce bien qu'ils soient soumis à la même législation ; les exportateurs de données peuvent et doivent tenir compte de la probabilité effective d'un tel accès.

Si, après analyse des risques, les clauses contractuelles types devaient s'avérer insuffisantes, elles devraient être complétées par d'autres clauses. Toutefois, le PFPDT ne précise pas de quelles clauses il pourrait s'agir. Si les garanties contractuelles complémentaires s'avèrent également inadaptées pour réduire suffisamment le risque identifié par l'exportateur, la prise de position du PFPDT indique que des mesures techniques doivent être prises pour empêcher ou entraver l'accès des autorités.

A cet effet, selon le PFPDT, un cryptage des données à transmettre est envisageable – en suivant les principes BYOK (bring your own key) et BYŒ (bring your own encryption) – si les données sont uniquement stockées par le destinataire. De ce fait, aucune « donnée claire » n'est disponible dans le pays de destination. Cependant, le PFPDT estime que, dans le cas d'une prestation allant au-delà du simple stockage des données dans le pays de destination, l'application de ces mesures techniques s'avère plus « complexe », ce qui n'est certainement pas un euphémisme. Si l'accès des autorités étrangères ne peut être empêché par des mesures techniques, le PFPDT recommande de renoncer au transfert de données personnelles vers le pays non listé sur la base de garanties contractuelles.

Recommandations

Nous recommandons premièrement aux entreprises suisses de créer une liste de tous les transferts de données tombant sous leur responsabilité, si une telle liste devait ne pas encore exister (par exemple en tant que partie d'un registre des activités de traitement ou dans le cadre de la gestion par un fournisseur ou un tiers.). Ainsi, il est possible de déterminer si les données sont transférées à son propre partenaire contractuel dans des pays tiers sans niveau de protection adéquat ou si elles sont transmises à des sous-traitants du partenaire contractuel opérant dans ces pays. Si tel est le cas, les entreprises suisses devraient alors envisager de prendre contact avec les partenaires contractuels concernés à l'étranger, les informer de la prise de position du PFPDT et des conséquences qui en découlent et – dans le cas des grands fournisseurs – s'enquérir des mesures correctives du fournisseur.

Sur la base de cette liste, une analyse des risques pourra ensuite être effectuée. Le prestataire de services ou le partenaire contractuel pourra apporter son soutien à ce sujet si nécessaire – par exemple, en clarifiant les pratiques administratives des autorités du pays de destination ou les possibilités de protection juridique pour les parties concernées. Si des données sont transférées non seulement depuis la Suisse, mais également depuis l'Espace économique européen vers des pays ne disposant pas d'un niveau de protection des données adéquat, il convient d'examiner en même temps si les exigences de la CJUE et des autorités compétentes en matière de protection des données exigent que des adaptations soient apportées à la pratique existante en matière de transfert.

Les mesures à prendre dépendent des risques. Si un complément aux clauses contractuelles types peut suffisamment atténuer les risques, les entreprises suisses devraient convenir avec le destinataire des données d'une modification des dispositions de ces clauses. Le guide d'orientation (en allemand) publié par le Préposé à la protection des données et à la liberté d'information du Land de Bade-Wurtemberg peut fournir des informations à ce sujet.

Si les ajustements contractuels s'avèrent insuffisants, des mesures techniques peuvent, dans certaines circonstances, contribuer à réduire les risques. Cependant, pour de nombreux services – en particulier les services SaaS et PaaS – le cryptage est pratiquement impossible. Les alternatives peuvent être l'anonymisation ou la pseudonymisation des données transmises.

Dans le cas où ni les modifications contractuelles ni les mesures techniques ne peuvent contrer les risques de manière suffisante, il reste à examiner s'il existe un fournisseur de services dans un pays apportant un niveau de protection des données adéquat. Il s'agira en particulier des pays de l'Espace économique européen (auquel cas il faut examiner si et dans quelles circonstances l'accès aux données à partir d'un autre lieu est possible et quels risques résultent de cette possibilité).

La CJUE et les autorités ont transmis un problème politique aux entreprises. Toutefois, il est évident que ce problème – qui repose sur une compréhension différente de la protection des données et de son importance – ne peut être résolu en adaptant les pratiques commerciales. Les autorités de protection des données auront donc à fonder leurs actions sur le

principe de proportionnalité, si l'on veut que la protection des données des entreprises reste crédible. Mais, à tout le moins, l'UE et les États-Unis sont en pourparlers. A l'heure actuelle, on peut donc espérer un "Privacy Shield Plus" et des clauses contractuelles types déjà annoncées et adaptées à "Schrems II". En outre, le PFPDT a annoncé qu'il fournira en temps utile des informations complémentaires sur l'exportation de données personnelles vers les Etats-Unis et d'autres pays tiers non répertoriés, qui permettront d'assurer la protection des données. Nous espérons que ces informations seront bientôt disponibles et que leur contenu sera pertinent.