

Où en est-on de la certification relative à la protection des informations personnelles en Chine ?



CHINE

Depuis la promulgation de la loi sur la Protection des Informations Personnelles («PIPL»), les entreprises anticipent que cette nouvelle loi pourrait fournir une solution pour légitimer le transfert transfrontalier d'informations personnelles («PI»). Il est vrai que l'article 38 de la PIPL prévoit certaines conditions pour le transfert transfrontalier de données. Le responsable de traitement doit remplir une de ces conditions avant de procéder au transfert transfrontalier de PI.

Selon le point 2 de l'article 38 du PIPL, lorsqu'un responsable de traitement a besoin de transférer des PI en dehors de Chine, il peut choisir d'obtenir une certification de protection des PI délivrée par une institution professionnelle conformément aux exigences pertinentes fixées par l'Administration du Cyberspace de Chine («CAC»). Cependant, de nombreuses entreprises ne savent pas comment remplir cette condition en raison du manque de directives dans la pratique.

De nombreuses multinationales soucieuses de leur conformité à la réglementation sur les données attendent avec impatience une solution pour légitimer définitivement le transfert transfrontalier des PI. La PIPL encourage également les institutions qualifiées à fournir des services de certification et d'évaluation sur la protection des PI. Il semble ainsi que la certification de la protection des PI puisse être une bonne option. Ainsi, de nombreuses multinationales ont déjà fait des efforts pour améliorer leur conformité en matière de données par l'obtention d'une certification en matière de données/de protection de la vie privée auprès de prestataires de services existants sur le marché.

Alors, qui sont les prestataires de services concernés en Chine ? Si oui, sont-ils qualifiés pour répondre à l'article 38 de la PIPL en tant que prestataires de services de certification de la protection des données personnelles ?

Dans le domaine de la protection des données, certaines certifications sont largement et mondialement connues, comme les certifications ISO (par exemple, ISO/IEC 27001, ISO/IEC 27701 et ISO/IEC 29151). En Chine continentale, par exemple, le CCRC (China Cybersecurity Review Technology and Certification Center) dispose également d'une certification sur l'aspect sécurité des applications mobiles. Cependant, à l'heure actuelle, ni la PIPL ni les autres circulaires émises par le CAC n'ont confirmé la possibilité d'utiliser ces certifications comme base juridique pour légitimer le transfert transfrontalier de PI. Jusqu'à présent, certaines multinationales qui ont déjà obtenu des certifications sur la protection des données et/ou de la vie privée, se demandent encore ce qui est ou pourrait être exigé en Chine pour le transfert transfrontalier des PI.

Un projet de norme nationale publié fin avril 2022 fournit un indice.

En effet, le comité technique national de normalisation de la sécurité de l'information a publié un projet de norme nationale sur les spécifications techniques des activités de traitement transfrontalier des informations personnelles («Projet de norme»). Bien qu'il ne s'agisse encore que d'un projet, il est toujours utile pour les entreprises de savoir quels seraient les aspects clés ou les conditions préalables à évaluer pour obtenir la certification pour les transferts de PI.

CE PROJET DE NORME INTRODUIT LA CERTIFICATION DE LA PROTECTION DES IP DANS LES ASPECTS SUIVANTS.

I. SCÉNARIOS APPLICABLES, MÉTHODES ET PRINCIPES DE CERTIFICATION

Le projet de norme prévoit que, dans le cadre des activités de traitement transfrontalier des PI, c'est normalement la partie qui se trouve en Chine continentale qui doit demander la certification de la protection des PI. Ce peut être le responsable de traitement qui agit en tant qu'exportateur de données ou l'institution chinoise qui agit en tant que représentant d'un responsable de traitement établi à l'étranger. Le projet de norme n'exclut pas clairement le fait que les entités

étrangères puissent être des demandeurs potentiels. Ainsi, il faudra attendre la version finale de ce projet de norme et la pratique pour savoir si une entreprise étrangère peut demander une certification de protection des données personnelles.

En ce qui concerne les principes, ce projet de norme insiste également sur le fait que le transfert transfrontalier des PI doit toujours se conformer aux exigences obligatoires de base tout au long des activités de traitement des PI (notamment traitement fondé sur une base légale, respect des principes de minimisation des données, qualité des données, *accountability*).

II. EXIGENCES DE BASE (SUR LES RÈGLES DE TRAITEMENT TRANSFRONTALIER DES PI ET ETUDE D'IMPACT «PIA»)

Le présent projet de norme confirme que l'exportateur et l'importateur de données devraient conclure des documents juridiquement contraignants pour garantir la protection des droits sur les PI des personnes concernées, et énumère le contenu devant être inclus dans ces documents, tels que :

1. Les parties impliquées dans les activités de traitement transfrontalier des PI ;
2. Les catégories et la portée des PI impliquées dans les activités de traitement transfrontalier des PI ;
3. Les mesures mises en œuvre pour la protection des PI des personnes concernées ;
4. Les parties s'engagent à respecter les principes de traitement des PI et à garantir que les PI concernées seront protégées à un niveau équivalent à celui requis par les lois et règlements de la Chine ;
5. Les parties s'engagent à être supervisées par l'institution ou les institutions de certification qualifiée(s) et par les lois et réglementations applicables en Chine ; et,
6. l'institution située en Chine qui sera légalement responsable des activités de traitement des IP doit être précisée.

Outre les exigences légales en matière de documentation, l'exportateur et l'importateur de données doivent procéder à l'évaluation de l'impact du transfert sur les PI, désigner leur propre responsable de la protection des PI (DPO) et/ou leur service chargé de la protection des PI, et définir clairement leurs droits et obligations en matière de gestion des PI après le transfert.

III. PROTECTION DES DROITS DES PERSONNES CONCERNÉES.

À cet égard, outre l'énumération des droits des personnes concernées et des droits/obligations des parties, le projet de norme mentionne que la personne concernée a le droit d'intenter une action en justice auprès du tribunal populaire de son lieu de résidence habituelle contre les parties impliquées dans le transfert transfrontalier de données personnelles, et/ou de déposer un rapport auprès de l'autorité de contrôle compétente.

La facilité offerte aux personnes concernées pour la protection de leurs droits pourrait être un cauchemar pour les responsables du traitement, en particulier lorsque les personnes concernées se trouvent dans des endroits différents. Toutefois, il n'est pas nécessaire de s'inquiéter outre mesure de cette disposition au stade actuel, car ce projet de norme doit encore être ajusté avant son approbation et sa publication officielles. Ce qui est pertinent et doit être pris en compte dès maintenant est le maintien de la cohérence des clauses de résolution des litiges dans les politiques de confidentialité concernées.

La protection des données personnelles n'est pas un sujet purement juridique/technique, mais une question complexe qui varie largement en fonction des secteurs d'activité, du volume de données et des objectifs du traitement, etc. Comme la PIPL promeut officiellement l'outil de transfert de la certification de la protection des PI, les prestataires de services concernés arriveront tôt ou tard sur le marché. Il est également possible que certains d'entre eux soient

désignés par les autorités compétentes, car ils peuvent dans une certaine mesure alléger la supervision par les autorités. Par conséquent, le mécanisme de certification de la protection des PI a le potentiel d'être un outil important pour légitimer le transfert transfrontalier des PI. Actuellement, si le flux de données transfrontalier se poursuit, nous suggérons de se conformer aux exigences obligatoires existantes (par exemple, les contrats de transfert de données, PIA, etc) établies par la PIPL.

Nous suivrons de près l'évolution de ce projet de norme et des autres règles et principes relatifs au flux de données transfrontalier.

**Veuillez noter que cette nouvelle norme nationale sur le transfert transfrontalier de données personnelles reste un projet au stade actuel.*



Pour toute information complémentaire,
merci de contacter :

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

Isabelle DOYON
Lawyer - Shanghai Office
DOYON@dsavocats.com