DS NEWSLETTER savoir faire
NEWSLETTER – INFORMATIONS JURIDIQUES PROPOSÉES PAR LE CABINET DS AVOCATS

Quelles nouveautés concernant le transfert transfrontalier de données depuis la Chine en 2022 ?

CHINE

CONTEXTE

Depuis la mise en œuvre de la *Loi sur la Cybersécurité de la RPC* en 2017, les entreprises à investissement étranger se sont inquiétées des exigences de localisation des données, et se sont interrogées sur la manière dont l'évaluation de sécurité du transfert transfrontalier des données sera effectuée. L'année dernière, la *Loi sur la Sécurité des Données et* la *Loi sur la Protection des Informations Personnelles* (« PIPL ») *de la RPC* ont été promulguées et sont entrées en vigueur, mais elles restent vagues sur ce sujet.

Pour résoudre ce problème, l'Administration du Cyberespace Chinoise (« CAC »), autorité compétente en matière de transfert transfrontalier de données, a publié des *Mesures pour l'évaluation de sécurité des transferts transfrontaliers de données* (les « *Mesures* ») le 7 juillet 2022, qui sont entrées en vigueur le 1er septembre 2022.

Les *Mesures* précisent les scénarios et les conditions dans lesquels le transfert transfrontalier de données (y compris les données à caractère personnel, « DP ») est soumis à une évaluation de sécurité de la part de la CAC, de quelle manière demander l'évaluation de sécurité, les documents à soumettre, le calendrier et les conséquences d'un échec de l'évaluation de sécurité. En pratique, afin de faciliter cette nouvelle formalité pour les demandeurs, la CAC fournit déjà un guide détaillé (en chinois, http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm) et quelques modèles officiels pour la demande d'évaluation de la sécurité. Certains bureaux municipaux et provinciaux (Pékin, Tianjin, Shanghai, province du Zhejiang, province du Jiangsu et province du Hebei) de la CAC offrent également des lignes d'assistance téléphonique pour des consultations.

De toute évidence, le cadre réglementaire chinois en matière de transfert transfrontalier de données se développe rapidement. Compte tenu de ce contexte, les questions-réponses ci-après reprennent les points importants de ces mesures.

***

1. Question : quels types d'activités sont considérés comme des transferts transfrontaliers de données ?

   (1) Sont concernées les données collectées et/ou générées par les responsables du traitement au cours d'opérations en Chine et qui sont transmises et/ou sauvegardées à l'étranger par les responsables du traitement ;

   (2) Sont concernées les données collectées et/ou générées par les responsables du traitement qui sont sauvegardées en Chine par les responsables du traitement, mais qui peuvent également être consultées, interrogées, extraites, téléchargées et/ou exportées par des institutions, des organisations et/ou des personnes de l'étranger ;

   (3) Autres activités de transfert transfrontalier de données, conformément aux dispositions de la CAC.

2. Question : l'évaluation de sécurité de la CAC est-elle applicable à tous les transferts transfrontaliers de données ?

En réalité, l'évaluation de sécurité de la CAC n'est pas obligatoire pour tous les transferts transfrontaliers de données. Elle ne l'est que pour ceux qui présentent au moins une des conditions fixées par les *Mesures* (voir la question n° 3 pour plus de détails).

Le transfert transfrontalier de données doit, aussi, être conforme aux autres lois applicables (par exemple, la PIPL et d'autres lois et réglementations sectorielles, etc. Voir la question n°8 pour des informations sur les activités de transfert transfrontalier de DP qui ne déclenchent pas d'évaluation de sécurité CAC).

3. Question : qui doit faire une demande d'évaluation de sécurité auprès de la CAC ?

Les responsables du traitement des données qui fournissent à l'étranger des données et/ou des DP importantes collectées et/ou générées en Chine doivent, s'ils remplissent l'une des conditions suivantes, demander une évaluation de sécurité à la CAC :

(1) Les responsables du traitement des données fournissent des données importantes à l'étranger ;

(2) Les opérateurs d'infrastructures d'information critiques (« CIIO(s) ») ou les responsables du traitement qui traitent les DP de plus d'un million de personnes et fournissent des DP à l'étranger (cette notion est axée sur le volume total des DP traitées par les CIIO/les Responsables du traitement et non sur le volume des DP à transférer à l'étranger) ;

(3) Depuis le 1er janvier 2021, les responsables du traitement des DP qui ont fourni cumulativement les DP de plus de 100 000 personnes ou les DP sensibles de plus de 10 000 personnes à l'étranger, et fournissent des DP à l'étranger (cette notion est axée sur le volume cumulé des DP traitées par les responsables du traitement des DP *au cours d'une période déterminée* et non sur le volume des DP à transférer à l'étranger) ;

(4) Autres situations nécessitant la déclaration de l'évaluation de sécurité des transferts transfrontaliers de données, comme le stipule la CAC.

4. Questions : qu'en est-il des activités de transfert transfrontalier de données qui ont débuté avant la date d'entrée en vigueur des *Mesures* (1er septembre 2022) ?

La CAC accorde une période de transition si les données répondent à l'un des scénarios et/ou conditions susmentionnés à la question n° 3, les responsables du traitement des données concernés doivent achever l'évaluation de sécurité avant le 1er mars 2023.

5. Question : que faut-il soumettre à la CAC pour l'évaluation de sécurité ?

(1) Copie du code unifié du Crédit social de l'institution/entreprise ;

(2) Copie de la pièce d'identité du représentant légal ;

(3) Copie de la pièce d'identité de l'agent chargé de la formalité pour le demandeur ;

(4) Pouvoir d'autorisation à l'agent (modèle officiel de la CAC) ;

(5) Lettre de demande d'évaluation de sécurité des transferts transfrontaliers de données (modèle officiel de la CAC) ;

(6) Copie du ou des contrats et/ou autres documents juridiques conclus entre l'exportateur de données et l'importateur de données ;

(7) Le rapport d'auto-évaluation des risques liés au transfert transfrontalier de données (modèle officiel de la CAC) et l'auto-évaluation doivent être complété trois mois avant la demande d'évaluation de sécurité de la CAC ;

(8) Autres documents requis pour l'évaluation de sécurité par la CAC.

6. Question : combien de temps prend l'évaluation de sécurité ?

Après avoir reçu le dossier complet, le bureau compétent de la CAC informera les demandeurs par écrit de l'acceptation de leur demande dans un délai de 7 jours ouvrables. Au cours de cette période, il peut être demandé aux demandeurs de compléter ou de corriger leur dossier. Si les documents soumis ne répondent pas aux exigences, le bureau de la CAC peut mettre fin à l'évaluation. Dans les cas normaux, l'évaluation sera achevée dans les 45 jours ouvrables suivant l'acceptation. Dans les cas complexes, cette période peut être prolongée.

7. Question : combien de temps le résultat de l'évaluation de sécurité sera-t-il valable ?

Le résultat de l'évaluation sera valable pendant 2 ans. En cas de changement majeur de l'activité de transfert transfrontalier de données, le responsable du traitement doit refaire une demande d'évaluation de la sécurité.

8. Question : qu'en est-il des activités de transfert transfrontalier de DP qui ne déclenchent pas d'évaluation de sécurité CAC ?

Selon la *PIPL*, avant tout transfert transfrontalier, les responsables du traitement doivent :

(1) s'assurer qu'ils disposent de la base juridique pour le traitement des DP concernées (par exemple, le traitement des informations personnels dans le domaine RH ou d'une personne signataire d'un contrat à titre personnel d'un contrat avec une société ou un individuel…).

(2) réaliser une étude d'impact sur la protection des DP et obtenir le consentement séparé des personnes concernées si nécessaire.

Après les tâches susmentionnées, en théorie, si un transfert transfrontalier de données personnelles ne déclenche pas d'évaluation de sécurité CAC obligatoire, le responsable du traitement/l'exportateur de DP peut choisir de légitimer le transfert en concluant des « Clauses contractuelles types » chinoises (« CCT chinoises ») avec l'importateur de DP ou tout autre moyen à sa disposition.

En pratique, il semble que les CCT chinoises soient actuellement la voie la plus praticable. Un récent projet de règlement indique que la CAC pourrait mettre en œuvre les CCT chinoises en tant que contrat standard pour le transfert transfrontalier de DP établi par la *PIPL*. Le projet de CCT chinoises a déjà été publié par la CAC. À l'avenir, les exportateurs de DP seront tenus de conclure les CCT avec les importateurs de DP et de les déposer auprès de la CAC.

9. Question : quel est le contenu des CCT chinoises ?

Les CCT chinoises (qui ne sont encore qu'un projet pour le moment) présentent les exigences de conformité pour les responsables du traitement en tant qu'exportateurs de DP et les obligations pour les importateurs de DP, et elles fonctionneraient d'une manière similaire aux CCT du RGPD.

Pour être plus précis, les CCT chinoises comprennent les informations de base, les droits et les obligations des exportateurs et des importateurs de DP, les détails du traitement des DP à transférer (par exemple, la finalité, la portée et les catégories de DP, la sensibilité et la quantité de DP, la méthode de traitement, etc.), l'impact des lois et règlements du pays/de la région des importateurs de DP, et la protection des droits des personnes concernées. Selon le projet actuel de CCT chinoises, les exportateurs et les importateurs de DP peuvent convenir d'autres aspects en plus des points susmentionnés.

***

En pratique, jusqu'à présent, il semble qu'il n'y ait pas eu beaucoup de cas de sanctions administratives appliquées par la CAC concernant le transfert transfrontalier de données, mais la situation devrait bientôt évoluer. Ainsi, le 8 septembre 2022, la CAC a publié des *Dispositions sur les procédures d'application des lois administratives des départements d'administration du cyberespace (projet pour commentaires)*. Ces Dispositions constitueront la base juridique permettant à la CAC de superviser et d'appliquer les lois relatives au cyber contenu, à la cyber sécurité, à la sécurité des données et à la protection de la vie privée.

En outre, étant donné que les *Mesures* sont effectives et que les CCT chinoises sont presque en place, nous recommandons aux entreprises, en ce qui concerne les activités de traitement des données, de donner la priorité à la tâche de mise en conformité du transfert transfrontalier des données et de désigner des professionnels dédiés en interne et/ou en externe pour estimer leur situation dans les meilleurs délais.

Pour toute information complémentaire, merci de contacter :

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com