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

Données : les gérer ou les mettre en péril ?

ASIE

Les questions relatives aux données sont probablement, depuis l'année dernière, à l'ordre du jour de nombreuses entreprises présentes en Chine notamment les entreprises à capitaux étrangers ("**FIEs**"). Depuis la promulgation des principales lois chinoises sur les données à savoir la Loi sur la Sécurité des Données ("**DSL**") et la Loi sur la Protection des Informations Personnelles ("**PIPL**"), des mesures et recommandations additionnelles ont été publiées, donnant une idée plus précise de ce qui est attendu de la part des entreprises.

Ainsi, ces derniers mois, plusieurs guides relatifs à la conformité des données ont été publiés au niveau national et au niveau régional en Chine. Malgré quelques différences, ces guides ont tous le même objectif. Ils peuvent être utilisés comme guide pratique de la mise en conformité, car si la DSL ou la PIPL sont claires sur les obligations principales, elles restent vagues sur la mise en pratique de ces obligations.

A titre d'exemple, les autorités du district de Shanghai Yangpu ont publié fin janvier 2022 un guide sur la conformité des données des entreprises (le "**Guide de Shanghai**"). Le district de Yangpu dispose de solides ressources éducatives et technologiques, ainsi que de nombreuses FIE figurant dans le classement Fortune 500. Le Guide de Shanghai se concentre principalement sur la méthodologie et les grands principes de mise en conformité des données au sein d'une entreprise.

Ainsi, pour les entreprises, il est clair que la protection des informations personnelles ("**PI**") n'est pas le seul objectif : elles doivent adopter et mettre en place un mode de gestion complet de la conformité des données.

Cet article se concentrera sur les principales exigences en matière de conformité des données sans entrer dans les détails sur la manière d'aborder la protection des informations personnelles. Sur ce dernier sujet veuillez-vous reporter à notre précédente newsletter "Le GDPR chinois vous affectera-t-il? Préparez-vous à la loi sur la protection des informations personnelles en RPC".

- **QU'EST-CE QUE LA CONFORMITÉ DES DONNÉES ?**

Le Guide de Shanghai définit la conformité des données comme le fait pour une entreprise et ses employés, de répondre aux exigences des lois et règlements sur la protection des informations personnelles, la cybersécurité et la sécurité des données. Il est vrai que la notion de conformité des données intègre le sujet de la protection des PI et repose sur la conformité en matière de cybersécurité, cette dernière étant plus fréquemment contrôlée par les autorités compétentes qui vérifient que les entreprises respectent le système de protection à plusieurs niveaux ("**MLPS**") conformément à la loi sur la cybersécurité de la RPC ("**CSL**"). En d'autres termes, la conformité des données exige que les entreprises se conforment à la DSL et à la PIPL, ainsi qu'à la CSL.

Il est donc suggéré aux entreprises de savoir d'où elles partent en réalisant un audit effectué par des professionnels, et de formuler une feuille de route sur mesure.

- **QUI EST CONCERNÉ ?**

Chaque personne est concernée au sein de l'entreprise : de la direction générale à chaque employé. Les dirigeants de l'entreprise (tel que le directeur général) sont responsables de la conformité des données et doivent donc allouer les ressources nécessaires et adéquates (autorisation/droits/pouvoir, soutien RH et financier) pour élaborer et mettre en œuvre la stratégie de conformité des données. En outre, pour s'assurer du respect par tous de la conformité des

données, il convient de mettre en place un mécanisme de responsabilisation approprié et de lier l'évaluation des performances du personnel interne concerné à des tâches spécifiques de conformité des données.

- **QUEL DÉPARTEMENT DOIT ÊTRE EN CHARGE DE LA CONFORMITÉ DES DONNÉES ?**

Le Guide de Shanghai encourage les entreprises à mettre en place un département dédié à la conformité des données, directement dirigé par le conseil d'administration sur le long terme, mais ne suggère pas que le département juridique interne prenne en charge ce sujet. Le département dédié formulera une stratégie globale de conformité des données, des mesures organisationnelles et techniques internes, gérera les relations avec les partenaires/clients externes sur la question des données, organisera des formations régulières et fournira des conseils à la direction et aux employés en interne. En outre, ce département doit être compétent en matière de communication transversale au sein de l'entreprise et gérer intelligemment les relations publiques avec les autorités de contrôle.

Le Guide de Shanghai souligne qu'il est indispensable et crucial d'impliquer des professionnels externes et d'établir avec eux une relation de coopération à long terme en matière de conformité des données.

- **CATÉGORISATION DES DONNÉES**

Fin 2021, une norme nationale chinoise encadrant la catégorisation et le classement des données de réseau a été publiée ("Guide National"). Le Guide National a pour but d'aider les entreprises à remplir l'obligation fondamentale, mais vague, de catégorisation et de classement des données exigée par la CSL et la DSL. En termes simples, pour gérer les données comme un actif, la première étape consiste à connaître leur catégorie et le niveau de risque lié à chaque catégorie.

1. Le Guide National se concentre principalement sur la manière de classer les données générales dans la pratique.

   Pour la catégorisation, les critères peuvent varier en fonction de la situation réelle des entreprises (type d'entreprise, industrie, échelle, etc.). Cependant, le Guide National donne également quelques critères universels applicables à la plupart des scénarios, tels que les données personnelles/ non personnelles, les données publiques/sociales, les données diffusées (non)/publiques. Il est intéressant de noter qu'un ensemble de données peut appartenir à différentes catégories selon différents critères/dimensions (par exemple, les PI des employés peuvent appartenir à la catégorie des données personnelles ainsi qu'à celle des données des utilisateurs internes d'un système ERP).

2. Pour le classement, le Guide National classe les données de réseau en trois catégories, plus la catégorie est élevée, plus l'impact d'une fuite de données est risqué: données essentielles (catégorie la plus élevée), données importantes et données générales.

   Les entreprises doivent d'abord vérifier si elles possèdent des données essentielles et des données importantes. Si c'est le cas, ces données doivent être gérées avec soin sous la supervision d'un professionnel, car le responsable de traitement est soumis à des obligations légales strictes.

   En ce qui concerne les données générales, la plupart des entreprises en possèdent un certain volume, et elles peuvent être classées en quatre catégories. Là encore, plus le niveau est élevé, plus l'impact des données est risqué. Le Guide national donne quelques références pour classer les PI.

- Les PI sensibles doivent être classées au moins au niveau 4 des données générales ;
- Les PI ordinaires (y compris celles des salariés) doivent être classées au moins au niveau 2 des données générales ;
- Les données publiques dont le partage avec des tiers est interdit doivent être classées au moins au niveau 4 des données générales ;
- Les données publiques dont le partage avec des tiers sous certaines conditions doivent être classées au moins au niveau 2 des données générales.

En résumé, la catégorisation et le classement des données doivent être basés sur les directives officielles applicables (c'est-à-dire le catalogue des données essentielles et des données importantes publié par les autorités et les associations industrielles, le cas échéant), sinon les entreprises doivent faire en fonction de leur propre situation.

Il est évident que la mise en conformité des données demande de la patience. Plus le projet est bien planifié, plus l'équipe interne est efficace, moins le coût sera important. Ce qui rend cette tâche plus urgente, c'est que les bonnes ressources disponibles sur le marché sont limitées. Alors, n'attendez plus pour vous mettre en ordre de marche.

Pour toute information complémentaire, merci de contacter :

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

Isabelle DOYON
Lawyer- Shanghai Office
DOYON@dsavocats.com