

Un moyen rapide pour connaître la nouvelle loi sur la sécurité des données en Chine ? Consultez nos FAQ !



ASIE

Face à un climat économique et politique international de plus en plus complexe et aux problèmes nationaux liés aux données (fuites de données, etc.), la loi sur la sécurité des données (*Data Security Law* « DSL ») était très attendue. En tant que première loi fondamentale sur les données en Chine, il a fallu près de trois ans pour l'élaborer. Elle a été approuvée le 10 juin 2021 et entrera en vigueur le 1er septembre 2021. La DSL affectera presque toutes les industries, qui n'ont que quelques mois pour se préparer. La DSL étant à la fois concise, vague et technique dans une certaine mesure, vous trouverez ci-après les questions fréquemment posées (FAQ) et leurs réponses.

■ QUELLE EST LA RELATION ENTRE LA LOI SUR LA CYBERSÉCURITÉ (« CSL »), LA DSL ET LE PROJET DE LOI SUR LA PROTECTION DES INFORMATIONS PERSONNELLES (« PIPL » (PROJET))

La CSL a été publiée en 2016 et est entrée en vigueur le 1er juin 2017. Elle s'applique à la construction, l'exploitation, la maintenance et l'utilisation du réseau ainsi qu'à la supervision et l'administration de la cybersécurité en Chine. La CSL exige des opérateurs de réseaux qu'ils remplissent plusieurs obligations basiques sur les « cyber-données » (qui se réfèrent à toutes sortes de données électroniques collectées, enregistrées, transmises, traitées et générées par le réseau). Toutefois, la CSL ne définit pas le terme « données » de manière générale et n'établit pas de régime juridique détaillé concernant les données.

La PIPL (projet) s'applique aux activités de traitement des données personnelles des personnes physiques à l'intérieur et à l'extérieur (dans certaines circonstances) de Chine. Par conséquent, les informations personnelles font partie des données qui doivent être spécialement réglementées par la future PIPL.

Le champ d'application de la DSL est plus général que celui de la PIPL (projet). À l'exception des données concernant les secrets d'État (régies par la loi chinoise sur la protection des secrets d'État – *National Security Law*) et des données militaires (régies par des mesures formulées par le gouvernement central), les données générales sont régies par la DSL. Quant aux informations personnelles, la DSL et la PIPL (projet) seront applicables en même temps, et la PIPL en tant que loi spéciale s'appliquera en priorité.

■ QUEL EST LE CHAMP D'APPLICATION TERRITORIALE DE LA DSL?

La DSL vise à réglementer les activités de traitement des données effectuées sur le territoire de la République Populaire de Chine et à y garantir la sécurité des données.

Elle mentionne également que la responsabilité juridique peut être engagée lorsque les activités de traitement des données effectuées en dehors du territoire chinois portent atteinte à la sécurité nationale, aux intérêts publics ou aux droits et intérêts légitimes des citoyens ou des organisations de la Chine. La DSL est la première loi d'application extra-territoriale sur les activités de traitement de données. Il est possible que les mesures discriminatoires compensatoires soient utilisées comme sanction dans ce scénario.

■ QUELLES SONT LES DONNÉES RÉGIES PAR LA DSL ?

Selon la DSL, les « données » désignent tout enregistrement d'informations sous forme électronique ou autre. En d'autres termes, les données désignent ici non seulement le contenu enregistré sous des dispositifs électroniques, mais aussi le contenu présenté de manière traditionnelle (c'est-à-dire par écrit). Cela est nécessaire car il est plus facile aujourd'hui de changer de support qu'auparavant. Par exemple, l'application mobile Wechat a déjà la fonction d'extraire des informations de documents papier, sans parler d'autres applications professionnelles permettant de transférer des fichiers dans différents formats.

■ QUELS SONT LES GRANDS PRINCIPES DE LA DSL?

La DSL prévoit les principes suivants :

- **Système de protection de la classification des données**

Les données doivent être gérées et évaluées en fonction de leur importance et des dommages qu'elles peuvent causer.

- ✂ **Système de protection des données importantes**

Les industries et les autorités doivent formuler un catalogue des données importantes et soumettre ces données importantes à une réglementation stricte.

- ✂ **Système national de protection des données essentielles**

Pour les données relatives à la sécurité nationale, à l'économie nationale, aux intérêts publics, etc., elles seront considérées comme des données nationales essentielles et soumises à une réglementation plus stricte.

- **Mécanisme d'alerte préventive et de réaction d'urgence en cas de risque pour la sécurité des données**

Les autorités partageront les informations sur la sécurité des données, analyseront conjointement les risques, décideront des mesures à prendre et émettront des alertes. Outre les exigences existantes pour les entreprises dans le cadre de la CSL, la DSL définit la manière dont les autorités géreront les incidents sur les données.

- **Mécanisme d'examen de la sécurité nationale des données**

Les autorités ont le droit de procéder à une évaluation de la sécurité des activités de traitement des données qui affectent ou peuvent affecter la sécurité nationale.

- **Système de contrôle de l'exportation des données**

Les autorités formuleront d'autres règles pour réglementer l'exportation de données importantes traitées par des non-CIIOs (*voir à ce sujet le paragraphe 7 ci-dessous*).

- **Lutte contre les mesures discriminatoires**

Pour toute mesure discriminatoire prise par un pays ou une région à l'encontre de la Chine en termes d'investissement et/ou de commerce de données et/ou d'utilisation de données, les autorités chinoises peuvent adopter des mesures équivalentes à l'encontre de ce pays ou de cette région.

■ QUELLES SONT LES PRINCIPALES OBLIGATIONS DES ENTREPRISES CONFORMÉMENT AU DSL?

- Obtenir les données de manière légale et appropriée ;

- Établir et améliorer l'ensemble du processus du système de gestion de la sécurité des données, organiser et réaliser la sensibilisation et la formation à la sécurité des données, et prendre les mesures techniques correspondantes et autres mesures nécessaires pour assurer la sécurité des données. Lors de l'utilisation d'Internet et d'autres réseaux d'information pour effectuer des activités de traitement des données, les obligations de protection de la sécurité

des données susmentionnées doivent être remplies sur la base du schéma de protection à plusieurs niveaux requis par CSL (« MLPS ») ;

- La surveillance des risques doit être renforcée pour les activités de traitement des données. Lorsque des risques tels que des défauts et des failles dans la sécurité des données sont détectés, des mesures correctives doivent être prises immédiatement. De la même façon, lorsque des incidents liés à la sécurité des données se produisent, des mesures correctives doivent être prises immédiatement, et les utilisateurs doivent être informés à temps conformément à la réglementation et ces incidents doivent être signalés aux services compétents concernés ; et,
- Pour les institutions qui fournissent des services d'intermédiation dans les transactions de données, les fournisseurs de données sont tenus d'expliquer la source des données, de vérifier l'identité des deux parties et de conserver des registres d'audit et de transaction.

■ QUELLE EST L'AUTORITÉ COMPÉTENTE EN MATIÈRE DE SÉCURITÉ DES DONNÉES EN CHINE ?

L'Administration chinoise de la cybersécurité (CAC) et ses antennes à tous les niveaux sont responsables de la coordination globale de la sécurité des données et de la supervision correspondante. Dans la pratique, d'autres autorités peuvent également participer aux activités de réglementation, telles que les bureaux de la sécurité publique, les autorités chargées de la sécurité nationale, les autorités compétentes de certaines industries.

■ QUELLES SONT LES NOUVEAUTÉS APPORTÉES PAR LA DSL DANS LES TRANSFERTS DE DONNÉES TRANSFRONTALIERS ?

La CSL énonce les exigences relatives au transfert transfrontalier de données pour les Opérateurs d'Infrastructures d'Information Critiques (« CIIOs »). Alors, qu'en est-il des exigences relatives au transfert transfrontalier de données pour les non-CIIOs ? En fait, la DSL ne répond pas directement à la question et indique seulement que les mesures pertinentes seront formulées par les autorités. Cette question doit donc être résolue par la loi et les règlements à venir, qui restent encore à l'état de projet.

■ QU'EN EST-IL DES DONNÉES UTILISÉES DANS UNE JURIDICTION OU PAR DES AUTORITÉS CHARGÉES DE L'APPLICATION DE LA LOI À L'ÉTRANGER ?

L'État traitera les demandes de données émanant d'autorités judiciaires ou répressives étrangères conformément aux traités et accords internationaux ou au principe d'égalité et de réciprocité. Sans l'approbation des autorités compétentes de la Chine, les organisations nationales (y compris les entreprises) et les particuliers ne doivent pas fournir de données stockées en Chine aux autorités judiciaires ou de police étrangères. La violation de cette exigence entraînera une amende pouvant aller jusqu'à 5 millions de RMB pour la personne morale et 500.000 RMB pour la personne responsable, ainsi que la révocation de la licence d'exploitation dans le pire des cas.

■ QUELS SONT LES CONSÉQUENCES DU NON-RESPECT DES DISPOSITIONS DE LA DSL ?

Exemple de situations (liste non-exhaustive)	Sanctions (liste non-exhaustive)
Violation de l'obligation de protection de la sécurité des données	• L'amende maximale pour une personne morale est de 2 millions de RMB, et il peut être ordonné à cette personne morale de suspendre les activités concernées, de suspendre les activités pour rectification, et de révoquer son agrément commercial ou sa licence d'exploitation. • L'amende maximale pour la personne en charge et les autres personnes directement responsables est de 200.000 RMB.

Violation du système national de gestion des données essentielles, qui met en danger la souveraineté nationale, la sécurité et les intérêts au développement.	• une amende d'au moins 2 millions RMB et d'au plus 10 millions RMB ; • ordonner la suspension des activités concernées ou l'arrêt des opérations pour rectification, ou faire l'objet d'une révocation des permis d'exploitation ou de la licence d'exploitation concernés ; • si un délit / crime est constitué, les personnes responsables seront tenues pénalement responsables conformément à la loi.
Fourniture de données importantes à des pays étrangers en violation des dispositions de la DSL	• une amende d'au moins 100.000 RMB et d'au plus 10 millions de RMB ; • ordonner la suspension des activités concernées ou l'arrêt des opérations pour rectification, ou faire l'objet d'une révocation des permis d'exploitation ou de la licence d'exploitation concernés ; • L'amende maximale pour la personne responsable et les autres personnes directement responsables est de 1 million RMB.

Les données sont un actif clé du monde digital et de plus en plus d'entreprises se lancent dans la course à la digitalisation. Dans ce contexte, la conformité sur la question des données n'est pas un sujet accessoire mais une condition obligatoire et fondamentale à laquelle les entreprises sont confrontées. Même si nous pensons que les autorités laisseront aux entreprises le temps de se préparer, il est conseillé de prendre sérieusement en compte la conformité des données et de mettre le sujet à l'ordre du jour dès que possible.



Pour toute information complémentaire, merci de contacter :

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

Isabelle DOYON
Lawyer - Shanghai Office
doyon@dsavocats.com