

# Nouveau Règlement sur les Données : un air de déjà-vu mais qui reste important



CHINE

Le 24 septembre 2024, le Règlement sur la Gestion de la Sécurité des Données en Réseau («Règlement sur les Données», en chinois 网络安全管理条例) a été promulgué et entrera en vigueur le 1er janvier 2025. Étant donné que ce Règlement sur les Données est relativement nouveau et étroitement lié à la Loi sur la Cybersécurité, la Loi sur la Sécurité des Données et la Loi sur la Protection des Informations Personnelles («PIPL»), nous avons compilé les questions suivantes pour fournir une brève introduction et répondre aux questions fréquemment posées sur le sujet.

## 1. Quelles sont les principales modifications et/ou impacts apportés par le Règlement sur les Données ?

Le Règlement sur les Données n'introduit pas de changements vraiment nouveaux dans le cadre réglementaire actuel sur les données. Il fournit plutôt des règles d'application basées sur les principes existants énoncés dans les lois et règlements en matière de cybersécurité et de traitement des données. De plus, il met l'accent sur des principes clés de protection des données en établissant des sanctions spécifiques pour les violations, affectant à la fois l'entité légale/le contrevenant et la personne responsable.

En d'autres termes, le Règlement sur les Données transforme des obligations légales vagues en obligations détaillées, spécifiques et réalisables. Ce faisant, il rend plus compréhensibles les obligations de conformité des données pour les responsables de traitement et les sous-traitants. Par conséquent, une approche attentiste ne sera plus tenable après l'entrée en vigueur du Règlement sur les Données.

À titre d'exemple, pour le traitement des données personnelles par un tiers, la PIPL exige que les responsables de traitement définissent les objectifs de traitement, la durée, les méthodes et d'autres détails avec les sous-traitants de données ; cependant, la PIPL n'est pas claire sur la manière de «définir» ces termes. Le Règlement sur les Données précise que ces termes doivent être établis «en concluant un contrat ou par d'autres moyens.» Une violation de cette disposition peut entraîner une amende pouvant atteindre 1 million de RMB pour l'entreprise, et dans les cas les plus graves, jusqu'à 100 000 RMB pour le responsable.

Des règles détaillées similaires sont fournies dans le Règlement sur les Données pour divers aspects, notamment :

- Gestion des Données Importantes : Désignation obligatoire d'un Responsable de la Protection des Données (DPO) et d'un organe de gestion ; exigences de qualification plus strictes pour le DPO et clarification des obligations de l'organe de gestion des données.
- Plan d'urgence et Réponse aux Incidents Cybersécurité : obligation de signaler les incidents dans un délai de 24 heures s'ils concernent la sécurité nationale et/ou l'intérêt public.
- Politique de Traitement des Données Personnelles : l'accent est mis sur les bonnes pratiques et interdictions pour le traitement des données personnelles basé sur le consentement, et la fourniture d'un guide succinct sur la façon de répondre aux droits des tiers sur leurs données personnelles.
- des obligations spécifiques pour les grands opérateurs de plateformes en ligne.

Ces règles détaillées assurent aux organisations des directives claires et réalisables à suivre, améliorant ainsi la conformité et la sécurité globales des données. Par conséquent, les responsables de traitement (entreprises, plateformes) doivent répondre aux règlements sur les données en mettant en œuvre des mesures de protection des données adaptées. De la même façon, les sous-traitants de données personnelles devraient prendre des actions adéquates pour répondre aux exigences légales et/ou aux clauses contractuelles stipulées par leurs clients/responsables de traitement.

## 2. Qu'est ce qui est important pour le traitement des données personnelles ?

En plus des exemples mentionnés précédemment, les responsables de traitement doivent faire preuve d'une plus grande prudence lors de la rédaction de politiques de confidentialité ou d'autres documents liés aux traitements de données, qu'ils soient basés sur le consentement ou non. Ces documents doivent clairement informer les individus sur la manière dont leurs données sont traitées et inclure des procédures réalisables pour qu'ils puissent exercer leurs droits sur leurs données personnelles. L'absence d'information adéquate pour les individus dans le cadre du traitement basé sur le consentement peut entraîner des pénalités pour l'entité légale et, dans les cas graves, pour l'individu responsable. Pour les responsables de traitement B2C, la bonne nouvelle est qu'au niveau de la réglementation, il est confirmé que les entreprises peuvent facturer des frais raisonnables pour répondre aux demandes de portabilité des données personnelles soumises par les individus.

Par ailleurs, les grandes plateformes en ligne traitant les données personnelles de 10 millions d'individus ou plus devraient désigner leur propre Responsable de la Protection des Données (DPO) et établir un organe interne dédié à la gestion des données. Ces plateformes doivent assumer des responsabilités similaires à celles requises pour le traitement des données importantes.

*Pour des informations plus détaillées sur la protection des données personnelles, veuillez cliquer sur les newsletters suivantes, qui sont en anglais :*

[\*"Comment va votre politique de confidentialité \(2024\) ?"\*](#)

[\*"Mises à jour légales sur la protection des IP en 2023"\*](#)

[\*"Introduction du RGPD chinois - PIPL \(2021\)"\*](#)

## 3. Quelle est l'importance des « données importantes » ?

En confiant le traitement des données importantes à un tiers sous-traitant, le responsable de traitement doit effectuer une évaluation des risques et s'assurer que des garanties contractuelles sont en place, précisant les obligations de sécurité. Le sous-traitant doit répondre aux normes de sécurité des données, et si les données sont transférées à l'étranger, une évaluation de sécurité de l'Administration du cyberspace de Chine (CAC) est requise. Une surveillance continue et des audits sont essentiels, et les responsables de traitement ainsi que les sous-traitants restent légalement responsables de la conformité.

Des règles plus détaillées sont fournies pour la gestion des données importantes. Par exemple, au-delà de la désignation d'un DPO et de l'établissement d'un organe interne de gestion des données, le Règlement sur les Données précise les qualifications requises pour les DPO. Le DPO doit être membre de l'équipe de direction et posséder une expertise et une expérience suffisantes en matière de conformité des données. Il exige également que les responsables de traitement de données importantes effectuent une évaluation annuelle complète des risques et soumettent un rapport du résultat aux autorités compétentes.

*Pour des informations plus détaillées sur la conformité générale aux données, veuillez cliquer sur les newsletters suivantes, qui sont en anglais :*

[\*"Introduction à la Loi chinoise sur la Sécurité des Données \(2021\)"\*](#)

[\*"Données : les gérer ou en risquer les conséquences ? \(2022\)"\*](#)

## 4. Qu'en est-il des transferts transfrontaliers de données ?

L'accent est principalement mis sur les règles importantes déjà établies par les lois existantes et les Dispositions sur la Facilitation et la Régulation des Flux de Données Transfrontaliers publiées en mars 2024. Il n'y a pas de changements substantiels ou de nouveaux développements concernant les transferts transfrontaliers de données.

Pour des informations plus détaillées sur les transferts transfrontaliers, veuillez cliquer sur les newsletters suivantes (en anglais) :

["Ce qu'il faut savoir sur les Clauses Contractuelles Standard Chinoises pour le Transfert Transfrontalier des Données Personnelles \(2023\)"](#)

["Quoi de neuf concernant les transferts transfrontaliers de données depuis la Chine en 2022 \(à propos de l'évaluation de sécurité\)?"](#)

["Comment se passe la certification de protection des IP en Chine \(2022\)?"](#)

## 5. Quelles sont les éventuelles pénalités en cas de violation ?

La violation du Règlement sur les Données pourrait entraîner des sanctions allant jusqu'à 10 millions de RMB pour l'entité légale et jusqu'à 1 million de RMB pour la personne responsable. Cela est conforme à la "responsabilité juridique" prévue dans la Loi sur la Sécurité des Données et la PIPL.



Pour toute information complémentaire, merci de contacter :

Isabelle DOYON  
Senior Associate- Shanghai Office  
[donyon@dsavocats.com](mailto:donyon@dsavocats.com)

ZHANG Beibei  
Senior Associate - Shanghai Office  
[beibeizhang@dsavocats.com](mailto:beibeizhang@dsavocats.com)

Enzo TRUPIANO  
Intern- Shanghai Office  
[Enzotrupiano@dsavocats.com](mailto:Enzotrupiano@dsavocats.com)

12 Novembre 2024