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

Focus sur l'audit de données personnelles en Chine – Principales questions fréquemment posées

CHINE

Le régulateur chinois, a adopté des mesures relatives à l'audit de conformité en matière de protection des données personnelles (les « **Mesures** »), qui entreront en vigueur le 1er mai 2025. Les Mesures décrivent ce que les entreprises doivent vérifier pour se conformer à la législation chinoise sur la protection des données. En effet, conformément à la Loi chinoise sur la protection des données personnelles (« **Personal Information Protection Law**», ou « **PIPL** »), tous les responsables du traitement de données personnelles (les « **Données personnelles** ») doivent procéder régulièrement à un audit de leurs activités de traitement, afin de s'assurer que ces données sont traitées de manière légale et sécurisée.

Contrairement à la PIPL, les Mesures (dans les Lignes directrices qui y sont jointes) donnent une liste relativement claire des points clés à auditer.

Vous trouverez ci-dessous une liste des questions fréquemment posées en pratique.

Q1 : Qui doit se conformer aux règles sur l'audit ?
R : Les Mesures s'appliquent à tous les responsables du traitement de Données personnelles qui entrent dans le champ de la PIPL. Les entreprises à capitaux étrangers (les « FIE ») et les multinationales ayant des activités en Chine sont directement soumises à ces règles. Les autorités d'Etat et les organismes d'affaires publiques ne sont PAS soumis aux Mesures.

Q2 : Quand les audits de conformité sont-ils requis ?
R : Les Mesures font la distinction entre les audits « autonomes » et ceux demandés par le régulateur, avec des fréquences spécifiques basées sur le volume des personnes concernées par le traitement de Données personnelles.

- **Audits autonomes obligatoires** : Les responsables de traitement qui traitent les Données personnelles de +10 millions d'individus doivent effectuer un audit au moins une fois tous les deux ans. Dans ce cas, le rapport d'audit n'est PAS obligatoirement soumis à une quelconque autorité.

  Qu'en est-il des responsables de traitement qui n'atteignent pas le seuil des 10 millions de personnes concernées ? Ils ont l'obligation également de conduire des audits, tout en pouvant décider de leur fréquence.

  En outre, les responsables du traitement doivent également examiner s'il existe une autre réglementation impérative exigeant une fréquence plus stricte de l'audit autonome. Par exemple, les responsables de traitement de Données personnelles de mineurs doivent effectuer un audit chaque année, quel que soit le nombre de personnes concernées par le traitement de Données personnelles.

- **Audits déclenchés** : Les autorités peuvent exiger un audit par un auditeur externe si l'un des scénarios suivants se produit :
  - Des risques graves pour les droits des personnes sont identifiés (par exemple, des mesures de sécurité inadéquates).
  - L'activité de traitement des Données personnelles peut avoir un impact négatif sur un grand nombre d'individus/personnes concernées des Données personnelles.
  - La violation des Données personnelles non sensibles a une incidence sur +1 million de personnes ; ou, la violation des Données personnelles sensibles a une incidence sur +100,000 personnes.

Dans ce cas, l'audit doit être achevé dans les délais requis par l'autorité, et le rapport d'audit doit obligatoirement être soumis à l'autorité compétente. Après la rectification, le responsable du traitement doit également soumettre le rapport de remédiation à l'autorité dans les 15 jours ouvrables suivant l'achèvement des actions de remédiation. .

Q3 : Quelles sont les points clefs en pratique des Mesures et des Lignes directrices ?

R : Les Mesures reflètent les principes établis par la PIPL ainsi que les règlementations récentes, à savoir le Règlement sur la gestion de la sécurité des données en réseau (promulgué le 24 septembre 2024 et entré en vigueur le 1er janvier 2025). En outre, les Mesures prévoient des règles détaillées qui portent l'efficacité des efforts de mise en conformité à un niveau supérieur. Il ne s'agit plus de savoir « si vous l'avez ou non ; ou, si vous avez fait cela », mais plutôt de vérifier « comment vous l'avez fait et comment vous pouvez prouver ce que vous avez fait et comment vous l'avez fait ».

En particulier, les responsables de traitement doivent garder à l'esprit certains points essentiels sur lesquels les Mesures insistent et auxquels ils doivent se conformer, le cas échéant :

- Les responsables du traitement de Données personnelles de +1 million de personnes doivent nommer un délégué à la protection des Données personnelles chargé des audits de conformité. Lorsque le responsable de traitement fournit d'importants services via une plateforme Internet, qu'il dispose d'une large base d'utilisateurs et exerce un type d'activité complexe, il doit également mettre en place un organisme indépendant, composé principalement de membres externes, chargé de superviser les audits de conformité.

- Les compétences professionnelles du délégué à la protection Données personnelles et le fonctionnement de son travail feront également l'objet d'un audit. Il ne suffit plus d'avoir un délégué à la protection des Données personnelles nommément désigné. Ce délégué doit posséder à la fois une expérience et une expertise professionnelles, ainsi que les ressources et l'autorité nécessaires pour gérer efficacement les activités de traitement des Données personnelles et ordonner les rectifications nécessaires.

- Les Mesures examinent spécifiquement l'installation d'équipements de capture d'images et d'identification personnelle dans les lieux publics, exigeant que les principes de légalité et de nécessité soient remplies (Par exemple, lorsque les Données personnelles sont utilisées à des fins autres que la sécurité publique, il convient de vérifier si un consentement distinct est obtenu après que la personne concernée des Données personnelles en a été dûment informée.)

- Le traitement des Données personnelles rendues publiques dans l'un des cas suivants serait considéré comme illégal :
  - Envoyer des informations commerciales sans rapport avec l'objectif de divulgation à des adresses électroniques, des numéros de téléphone portable et d'autres Données personnelles accessibles au public ;
  - Utiliser des Données personnelles divulguées publiquement à des fins telles que le harcèlement en ligne, la propagation de rumeurs ou la diffusion de fausses informations ;
  - Traiter des Données personnelles dont la personne concernée a explicitement refusé le traitement, même si elles ont été divulguées publiquement ;
  - Ne pas obtenir le consentement de la personne pour le traitement des Données personnelles qui a un impact significatif sur les droits et intérêts de cette personne ; ou
  - Recueillir, conserver ou traiter des Données personnelles divulguées publiquement au-delà d'une portée, d'une période ou d'un objectif raisonnable.

- Lorsqu'un organisme est choisi pour effectuer l'audit des Données personnelles, il ne doit pas sous-traiter l'audit à un autre organisme. Un même organisme et ses entités affiliées, ainsi qu'un même agent d'audit de conformité, ne peuvent pas effectuer plus de trois (3) audits consécutifs pour le même « audité ». Dans la pratique, il reste à clarifier si « l'audité » désigne le responsable du traitement/la personne morale indépendante, ou s'il peut également s'agir de projets/systèmes différents du même responsable du traitement.

Q4 : Quels sont les principaux domaines d'audit ?

R : Les FIE devront accorder une attention particulière au transfert transfrontalier de données et au consentement. Au niveau opérationnel, les audits doivent être conformes aux Lignes directrices jointes aux Mesures. Les points clés comprennent :

- Base légale du traitement (par exemple, consentement valide, exceptions pour le traitement non consensuel).
- Transparence et notification (divulgation claire des règles de traitement).
- Transfert transfrontalier des Données personnelles (conformité aux évaluations de sécurité/certifications).
- Prise de décision automatisée (équité, transparence, mécanismes de désactivation).
- Traitement des Données personnelles sensibles (par exemple, biométrie, Données personnelles de santé ; consentement distinct requis).
- Protection des mineurs (consentement du tuteur pour les moins de 14 ans).
- Plans d'intervention en cas d'incident (protocoles testés en cas de violation).

Q5 : Quel est l'impact des Mesures sur les flux transfrontaliers de Données personnelles ?

R : En plus des règles existantes sur le transfert transfrontalier des Données personnelles, une nouvelle disposition mérite notre attention. Les Données personnelles ne doivent pas être fournies à des organisations et/ou des individus situés en dehors de la Chine et figurant sur la liste noire ou dans le groupe de restriction. Il reste à préciser dans les futures communications gouvernementales comment les listes fonctionnent dans la gestion du transfert transfrontalier de Données personnelles.

A l'exception de ce qui précède, les Mesures ne modifient pas substantiellement les règles existantes qui s'appliquent au transfert des Données personnelles à l'étranger. Toutefois, les Mesures soulignent que les documents de conformité pour le traitement légal des Données personnelles doivent être correctement préparés et conservés, en cas de futurs audits et/ou inspections gouvernementales.

Q6 : Quelles sont les exigences spécifiques en matière de systèmes de gestion interne ?

R : Les Mesures exigent que les responsables de traitement mettent en place des cadres de gouvernance interne complets, notamment :

- Politiques et procédures : règles documentées alignées sur la PIPL, couvrant la classification des données, les périodes de conservation, les contrôles d'accès et la réponse aux incidents.
- Gouvernance : définir les responsabilités du délégué à la protection des Données personnelles, des équipes d'audit interne et de la direction.
- Classification des données : classer les données en fonction de leur sensibilité (par exemple, biométrie, données financières) et mettre en œuvre des mesures de sécurité à plusieurs niveaux.
- Etude d'impact : effectuer régulièrement des évaluations des risques pour les activités à risque élevé (par exemple, prise de décision automatisée, transfert transfrontalier).
- Formation : formation régulière pour tous les employés, en mettant l'accent sur la gestion du consentement, le signalement des violations et le traitement des demandes de droits des tiers.

Les responsables du traitement doivent conserver l'historique des travaux d'audit, de mises à jour des politiques et des dossiers de formation en cas d'inspection par les autorités.

Q7 : Quelles sont les obligations pour le traitement des demandes de droits individuels ?

R : Les responsables de traitement doivent mettre en place des canaux de communication facilement accessibles (par exemple, des portails en ligne, des lignes d'assistance téléphoniques) pour répondre aux demandes suivantes :

- Demande de droit d'accès/de correction : les demandes doivent être traitées dans les 15 jours ouvrables.
- Demande de suppression : Supprimer les Données personnelles si la conservation n'est plus nécessaire, si le consentement est retiré ou si le traitement est illégal.
- Désactivation des décisions automatisées : permettre aux utilisateurs de refuser le profilage ou d'exiger une intervention humaine.

Les réponses doivent être claires, intervenir dans le délai imparti et gratuites. Les refus nécessitent des justifications juridiques détaillées.

Q8 : Comment gérer l'historique des activités de traitement ?

R : Les responsables de traitement doivent :

- Examiner les systèmes existants : identifier les pratiques non conformes (par exemple, les mécanismes de consentement obsolètes, la conservation excessive des Données personnelles).
- Supprimer les données : supprimer les Données personnelles historiques inutiles sans fondement légal.
- Renouveler le consentement : dans la mesure du possible, obtenir un nouveau consentement pour le traitement continu des Données personnelles existantes.
- Documenter tous les efforts de remédiation pour démontrer une conformité proactive lors des audits.

Conclusion

Les Mesures fournissent un cadre solide pour garantir la protection des données en Chine, avec des domaines clés couvrant le consentement, les différents scénarios de traitement de données la sécurité et les droits des tiers. Il est recommandé aux entreprises, notamment aux entreprises à capitaux étrangers, de se préparer à ces audits en effectuant des autocontrôles à l'avance, en se concentrant sur le transfert transfrontalier et la gestion des données sensibles, afin de transformer les défis réglementaires en avantages concurrentiels sur le marché chinois..

Contactez-nous pour des conseils personnalisés.

Pour toute information complémentaire, merci de contacter :

Isabelle DOYON
Senior Associate- Shanghai Office
doyon@dsavocats.com

ZHANG Beibei
Senior Associate - Shanghai Office
beibeizhang@dsavocats.com

2 Avril 2025