DS NEWSLETTER savoir, faire

NEWSLETTER – INFORMATIONS JURIDIQUES PROPOSÉES PAR LE CABINET DS AVOCATS

[CHINE] DONNEES PERSONNELLES : QUELLES SONT LES « BONNES PRATIQUES » ATTENDUES DES AUTORITES ?

ASIE

Le 1er février 2019, le Comité technique national de normalisation de la sécurité de l'information (le « TC 260 ») a publié un projet de modifications du standard actuel GB/T 35273-2017 (le « *Standard* ») qui est en vigueur depuis le 1er mai 2018. Ce projet a été soumis à la consultation du public jusqu'au 3 mars 2019 (le « *Projet* »).

Bien que juridiquement non contraignant, le Standard donne des lignes directrices pour l'interprétation de la loi Cybersécurité et les « bonnes pratiques » attendues par les autorités régulatrices en matière de collecte et de traitement des données personnelles.

La version finalisée de ce nouveau Standard devrait voir le jour dans les prochaines semaines.

En attendant, nous avons synthétisé ci-dessous les principales modifications apportées par le Projet. Celles-ci concernent notamment:

(i) l'interdiction du consentement groupé,
(ii) les exceptions dans lesquelles le recueil du consentement n'est pas requis,
(iii) les informations devant être insérées dans les politiques de protection des données personnelles (Privacy policies),
(iv) les exigences requises en cas de fourniture de contenu personnalisé,
(v) la gestion des accès aux données personnelles par des tiers (par le biais d'API notamment),
(vi) la tenue d'un registre des traitements de données personnelles ; et
(vii) les seuils à partir desquels un Data Protection Officer devrait être désigné.

INTERDICTION DE LA COLLECTE FORCÉE DE DONNÉES PERSONNELLES ET DU CONSENTEMENT GROUPÉ (NOUVEL ARTICLE 5.3)

En complément des dispositions déjà existantes en matière de recueil du consentement, le Projet interdit au responsable de traitement[1] qui fournit un produit ou service avec de multiples fonctions qui nécessitent la collecte de données personnelles, de forcer les personnes concernées à accepter les fonctions offertes par ledit produit ou service et de consentir ainsi à la collecte de leurs données personnelles pour l'ensemble des fonctions proposées.

Par principe, le responsable de traitement ne pourrait pas obtenir en une seule fois le consentement de la personne concernée[2] à la collecte de ses données, en regroupant toutes les fonctions de son produit ou tous ses services. Seules des actions positives et volontaires de la personne concernée pourraient permettre d'activer les différentes fonctions dudit produit ou service ou d'enclencher la collecte de données personnelles, par exemple, en cochant une case, en cliquant sur une icône « I Agree » ou « Next », en remplissant volontairement un formulaire, etc. (« *Systèmes d'opt in* »).

De même, le responsable de traitement devrait fournir des mécanismes de désinscription (« *Systèmes d'opt-out* ») aisément accessibles et aussi simples d'utilisation que les Systemes d'opt-in.

Le Projet prévoit, en outre, que si la personne concernée refusait de s'inscrire à certains services ou d'activer certaines fonctions, le responsable de traitement ne pourrait pas solliciter de nouveau, à tout le moins, de façon fréquente, le consentement de la personne et il lui serait interdit de suspendre les autres fonctions ou services choisis par la personne concernée ou de diminuer la qualité des fonctions ou services auxquels il a déjà été souscrit.

[1] Les responsables de traitement sont les personnes morales ou physiques qui décident des moyens et finalités de traitement des données personnelles.

[2] Les personnes concernées sont les personnes physiques dont les données personnelles sont collectées

Le Projet introduit, toutefois, une distinction, en annexe C, entre les fonctions de base/essentielles des produits ou services (« basic business functions ») et les fonctions additionnelles (« extended business functions »). Cette distinction qui vise principalement les applications permettrait, dans certains cas, au responsable de traitement d'obtenir un consentement groupé à la collecte de données personnelles.

Les fonctions de base seraient définies comme les fonctions attendues par la personne concernée, celles pour lesquelles elle a choisi le produit ou service et qui répondraient à ses principaux besoins. En revanche, l'amélioration de l'expérience utilisateur ou le développement d'un nouveau produit par exemple ne saurait être considérée comme une fonction de base.

Pour les fonctions de base, la personne concernée devrait (i) être préalablement informée (par exemple, par le biais d'une fenêtre pop-up dans l'interface de l'application) du type de données personnelles collectées par lesdites fonctions ainsi que des conséquences de son refus de consentir à la collecte de ses données, et (ii) consentir explicitement à la collecte de ses données. Par consentement explicite, le Standard précise qu'il devrait s'agir d'une expression de volonté spécifique et non ambiguë qui peut résulter soit d'un écrit soit d'un acte positif de la personne. Si la personne concernée ne consentait pas à la collecte de ses données, le responsable de traitement serait en droit de refuser de lui fournir lesdites fonctions de base/essentielles.

S'agissant des fonctions additionnelles, celles-ci ne pourraient être activées qu'une par une, après information préalable de la personne concernée et obtention de son consentement pour chaque fonction additionnelle. En revanche, si la personne concernée ne consentait pas à la collecte de ses données, elle ne pourrait pas utiliser lesdites fonctions additionnelles mais le responsable de traitement ne pourrait pas refuser de lui fournir les fonctions de base/essentielles ou ne pourrait pas diminuer la qualité de service de ces fonctions.

EXCEPTIONS POUR LESQUELLES LE CONSENTEMENT N'EST PAS REQUIS (NOUVEL ARTICLE 5.7)

L'actuel article 5.4 du Standard a été déplacé en 5.7 et le Projet a ajouté comme exception l'exigence de conformité du responsable de traitement aux obligations prescrites par les lois et règlements. En revanche, l'ancienne exception relative à l'exécution des contrats a été supprimée. Désormais, le responsable de traitement ne pourrait donc plus utiliser comme base légale l'exécution d'un contrat à laquelle la personne concernée est partie pour justifier la collecte et le traitement de données personnelles.

INFORMATIONS SUPPLÉMENTAIRES À INSÉRER AU SEIN DES POLITIQUES DE PROTECTION DES DONNÉES PERSONNELLES (ARTICLE 5.6 MODIFIÉ)

L'actuel article 5.6 précise déjà toute une série d'informations devant être insérées au sein des politiques de protection des données personnelles (*Privacy policies*) et portées à la connaissance des personnes dont les données sont collectées et traitées.

Dans sa nouvelle version, l'article 5.6 ajoute que le responsable de traitement devra informer les personnes concernées des catégories de données personnelles collectées par chaque fonction/service en distinguant entre les données collectées par les fonctions de base/essentielles et celles collectées par les fonctions additionnelles.

NOUVELLES EXIGENCES EN MATIÈRE DE CONTENU PERSONNALISÉ (NOUVEL ARTICLE 7.4)

Le Projet prévoit de nouvelles exigences en cas de contenu personnalisé :

(i) Pour les fournisseurs de contenu qui diffusent des actualités en mode « push » ou des services d'information: ceux-ci devraient l'indiquer de façon apparente par des mentions telles que « contenu personnalisé » ou « push ciblé» et fournir aux personnes concernées des mécanismes simples et intuitifs de désactivation du mode contenu personnalisé.

(ii) Pour les opérateurs e-commerce qui fournissent des contenus personnalisés en fonction des intérêts de la personne concernée, de ses loisirs, de ses habitudes de consommation, ou d'autres caractéristiques, ceux-ci devraient permettre aux personnes concernées de désactiver le ciblage en fonction de ses caractéristiques personnelles.

En outre, le Projet recommande aux responsables de traitement de mettre en place un mécanisme permettant à la personne concernée de gérer ses préférences dans la réception de contenu personnalisé et de pouvoir supprimer ou anonymiser les données personnelles sur la base desquelles le contenu personnalisé a été adressé.

GESTION DE L'ACCÈS AUX DONNÉES PAR DES TIERS – CAS DES APIS (NOUVEL ARTICLE 8.7)

Le Projet prévoit également que, dans les cas où le responsable de traitement permettrait à des tiers, par le biais de leurs produits ou services, par exemple d'APIs (Application Programming Interfaces) de collecter des données personnelles et que ces tiers n'auraient pas la qualité de sous-traitant (c'est-à-dire n'agissant pas sur les instructions du responsable de traitement) ou de coresponsable de traitement, le responsable de traitement serait tenu de prendre plusieurs mesures, à savoir :

- Etablir un mécanisme de gestion des accès et un work-flow de l'accès au produit ou service du tiers ;
- Prévoir contractuellement les obligations de chaque partie en termes de sécurité et de confidentialité ;
- Informer les personnes concernées que le produit ou service est fourni par un tiers ;
- Exiger du tiers qu'il obtienne le consentement des personnes concernées à la collecte de leurs données et vérifier les mécanismes de recueil du consentement adoptés par ce tiers ;
- S'assurer que le tiers a mis en place un mécanisme de gestion des demandes des personnes concernées
- Contrôler le respect par le tiers de ses obligations de sécurité et de confidentialité et désactiver l'interface avec le produit du tiers si nécessaire ;
- Inspecter et auditer la collecte de données personnelles par des outils automatisés (tels que les scripts, algorithmes, kits de développement de logiciels (SDK), applets, etc.) afin de s'assurer de la conformité de la collecte aux exigences convenues entre les parties et couper les accès en cas de violation.

LA TENUE D'UN REGISTRE DES TRAITEMENTS (NOUVEL ARTICLE 10.2)

Le Projet prévoit que les responsables de traitement devraient maintenir un registre des différents traitements de données personnelles opérés au sein de leur organisation.

Il est précisé que le registre des traitements devrait notamment inclure :

1. Le type, le volume de données personnelles et les sources de collecte de ces données (par exemple directe ou indirecte, par l'intermédiaire de tiers) ;
2. Les finalités du traitement (ex : gestion de la paie, envoi de newsletters, suivi des retours clients, etc.), si les données personnelles font l'objet d'une sous-traitance, si elles sont transférées à l'étranger, etc. ;
3. Les systèmes de collecte et de traitement des données (ex : un outil de CRM) et les destinataires des données personnelles en interne (le personnel au sein de l'entreprise) et en externe (à des tiers).

LA DÉSIGNATION D'UN DATA PROTECTION OFFICER (ARTICLE 10.1 MODIFIÉ)

L'actuel article 10.1 recommande la désignation d'une personne en charge de la protection des données personnelles (« *Data Protection Officer* ») à plein temps, si l'un des deux seuils suivants est atteint, à savoir si l'entreprise compte plus de 200 salariés ou si l'entreprise traite les données personnelles de plus de 500 000 personnes. Dans sa nouvelle version, le Projet augmente le second seuil et le fait passer à 1 000 000 personnes.

Les missions du Data Protection Officer incluent notamment la mise en œuvre de la stratégie globale de sécurité des données personnelles au sein de l'entreprise, l'élaboration, la publication et la mise à jour régulière des privacy policies et des procédures associées, l'élaboration et la mise à jour du registre des traitements de données de l'entreprise, la réalisation - lorsque cela est nécessaire - d'études d'impact, l'organisation de formations/trainings en matière de sécurité des données personnelles, la réalisation de tests sur les produits ou services avant d'être mis en ligne, la gestion des demandes d'accès et des plaintes par les personnes concernées, la communication et le reporting des incidents de sécurité.

En conclusion, bien que les différents textes d'application de la loi Cybersécurité ne soient pas encore tous entrés en vigueur (l'on pense notamment à celui relatif aux transferts de données personnelles hors de Chine), ceux-ci sont attendus prochainement, la protection des données personnelles faisant partie des priorités du gouvernement en 2019.

Les autorités ont d'ailleurs déjà entamé des campagnes de contrôle à travers tout le pays, que les entreprises soient chinoises ou étrangères. Il ressort des inspections menées dans le domaine que **les principaux points de contrôle des autorités sont, à ce jour, la mise en œuvre par les entreprises de privacy policies et de procédures associées destinées à assurer la sécurité des données personnelles.** Si le Projet était adopté en l'état, les entreprises se verraient également devoir établir un registre des traitements de données personnelles.

Nous recommandons, en conséquence, aux entreprises, si cela n'a pas déjà été initié, de se mettre en conformité, en commençant par procéder à un audit de l'existant. En fonction des résultats de celui-ci et de l'analyse des écarts entre la situation actuelle de l'entreprise et les exigences de la loi, une feuille de route pourrait être établie afin (i) d'identifier les différentes actions de régularisation à entreprendre, (ii) de les prioriser et (iii) de documenter (à des fins de preuve en cas de contrôle) les actions ayant effectivement mises en œuvre.

COMMENT DS AVOCATS PEUT VOUS AIDER ?

Quel que soit votre secteur d'activités, quel que soit le type de données personnelles que vous traitez (données clients, données de santé, données des salariés, etc.), DS peut **vous accompagner dans vos projets de mise en conformité** en mettant à votre service une **équipe d'avocats dédiée, réactive, pragmatique**, disposant d'un savoir-faire transversal et ayant une parfaite connaissance de l'écosystème numérique chinois. Nous disposons de bureaux à Pekin, Shanghai et Canton.

Notre intervention, à vos côtés, peut être plus ou moins étendue, selon votre situation actuelle et selon vos besoins : (i) assistance pour une mise en conformité complète (audit de l'existant, analyse des écarts, feuille de route, actions de mise en conformité), (ii) accompagnement de votre DPO interne dans votre mise en conformité (ex : formalisation du référentiel sécurité, assistance à l'élaboration des procédures internes, au registre des traitements de données, à la réalisation d'une étude d'impact, etc.), (iii) accompagnement sur un projet en particulier (ex : mise en œuvre de nouveaux outils, transferts de données, etc.), (iv) accompagnement dans le cadre de vos relations avec les autorités de contrôle, (v) séances de sensibilisation/ de formation « Données personnelles » à destination de vos équipes, et/ou (vi) assistance dans le cadre de litige (en collaboration avec des avocats chinois).