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

Où en êtes-vous avec votre Politique de Confidentialité des Données ?

CHINE

Le traitement de données à caractère personnel est incontournable de nos jours pour les organisations dans le cadre de leurs activités quotidiennes. Il peut s'agir de données personnelles de salariés, de consommateurs, de clients ou de partenaires commerciaux. Les entreprises B2C peuvent avoir déjà mis à jour leurs politiques de confidentialité à plusieurs reprises en raison des exigences sans cesse renouvelées de la loi et des réglementations sur la protection des données personnelles.

Quel que soit le mode de collecte des données à caractère personnel, une politique de confidentialité conforme aux exigences légales et régulièrement mise à jour doit être fournie aux personnes concernées («personnes concernées») avant le début du traitement de leurs données. Par exemple, les responsables du traitement peuvent envisager de collecter des données à caractère personnel par des canaux en ligne tels qu'une page web, une application, un mini-programme Wechat ou via des canaux hors ligne tel que des formulaires de candidature, etc. Il convient de noter que le mode de collecte des données à caractère personnel ne dispense pas les responsables du traitement de l'obligation d'information, c'est-à-dire de la politique de confidentialité des données.

En cette 3eme année d'application de la *Loi sur la Protection des données personnelles* en Chine, nous constatons que les entreprises accordent plus d'attention à la protection des données personnelles qu'elles ne le faisaient auparavant. Toutefois, les exigences légales en constante évolution obligent les responsables du traitement des données à affiner sans cesse leurs mesures de protection des données. L'une des tâches importantes consiste à disposer d'une politique de confidentialité actualisée et valide. Dans la pratique, il subsiste encore souvent des politiques de confidentialité incomplètes dont les clauses restent vagues, voire totalement inexistantes et ce manquement ne peut donner satisfaction aux responsables du traitement des données car dans le pire des cas, elles peuvent les exposer à des risques et entraîner des coûts élevés en cas de non-conformité.

L'année dernière, un groupe universitaire chinois de renom a été condamné à une amende de 50 millions de RMB par l'Administration du cyberespace de Chine pour traitement illégal de données personnelles et violation de la loi sur la cybersécurité et de la loi sur les protection des données personnelles.. Concrètement, il était exploité 14 applications avec des politiques de confidentialité incomplètes, voire sans politique de confidentialité. En conséquence, les responsables de traitement ont été condamnés à des amendes pour avoir collecté des catégories de données personnelles inutiles, sans consentement, sans divulguer/fournir les règles de traitement de ces données à caractère personnel et, pour avoir omis d'insérer un lien de désinscription, pour avoir omis de supprimer les données, etc.

Pour éviter ces risques, voici quelques conseils sur les étapes nécessaires à l'élaboration d'une bonne politique de confidentialité des données (scénarios B2C) :

√ Étape 1 : Connaître TOUS les secteurs de votre entreprise qui traitent des données à caractère personnel et savoir exactement quelles catégories de données à caractère personnel sont nécessaires.

Cette étape consiste à collecter les éléments liés au traitement des données à caractère personnel. Tout d'abord, le département commercial (et/ou d'autres personnes dont les fonctions sont liées) doit décrire en détail les activités de collecte et de traitement des données qui sont prévues par le responsable du traitement. En d'autres termes, cette étape doit permettre d'identifier la finalité de chaque traitement, les modalités du traitement et les catégories de données personnelles traitées. La minimisation des données doit être appliquée afin d'exclure les catégories de données à caractère personnel non nécessaires. À cette fin, les responsables du traitement doivent distinguer les catégories de données à caractère personnel collectées pour les fonctions nécessaires (produit/service de base) de celles pour les autres fonctions étendues des produits/services.

Un guide officiel pour les applications mobiles publié en 2021, constitue une bonne référence, (*Scope of Necessary Personal Information for Common Types of Mobile Internet Applications*) . Selon ce guide, les personnes concernées devraient avoir le droit de refuser de fournir des catégories inutiles de données à caractère personnel et ce refus ne devrait pas empêcher l'utilisation de la fonction essentielle/de base des produits/services fournis pa le responsable du traitement des données.

√ Étape 2: Élaborer une politique de confidentialité des données équilibrée entre les objectifs de l'entreprise et les exigences de conformité .

Le projet de politique de confidentialité devrait être examiné en détail par des professionnels, puis finalisé et confirmé par l'ensemble des membres de l'équipe (qu'ils soient internes ou non, y compris l'équipe connaissant les exigences légales, les objectifs commerciaux, les activités réelles de traitement des données et les professionnels technique/de l'informatique qui fournissent l'assistance nécessaire dans le domaine de la sécurité). Cette étape devrait être gérée, par les responsables du traitement, plus attentivement s'ils traitent des données personnelles sensibles et/ou si des transferts de données transfrontaliers peuvent avoir lieu.

√ Étape 3 : Faire évoluer la politique de confidentialité comme un document « vivant » .

L'obligation d'information des responsables du traitement à l'égard de la personne concernée ne prend pas fin avec la publication d'une politique de confidentialité, mais elle commence à partir de ce moment-là. Dans la pratique, les responsables du traitement ignorent parfois que la politique de confidentialité doit être maintenue et mise à jour régulièrement conformément aux lois applicables. Ils doivent superviser l'activité de traitement des données et adapter la politique de confidentialité et/ou l'activité si nécessaire. De plus, lors de la mise à jour/amendement d'une politique de confidentialité, il existe également des règles à suivre sur la manière d'afficher les versions précédentes et les versions mises à jour.

Dans l'environnement juridique actuel, il serait difficile de pouvoir justifier un traitement illégal de données à caractère personnel, en particulier pour ce qui est de l'obtention du consentement via les politiques de confidentialité . En effet,, les réponses et les approches sont toutes fournies par les normes nationales. Nous répertorions ci-dessous certaines des plus récentes à titre de référence :

Code	Nom de la norme nationale	Date de sortie	Date d'entrée en vigueur
GB/T 43506-2023	*Exigences en matière de protection des données personnelles des utilisateurs*	2023-12-28	2024-04-01
GB/T 42574-2023	*Lignes directrices pour la mise en œuvre des notifications et du consentement dans le cadre du traitement des données à caractère personnel.*	2023-05-23	2023-12-01
GB/T 42582-2023	*Spécification de test et d 'évaluation de la sécurité des informations personnelles dans les applications Internet mobiles (App)*	2023-05-23	2023-12-01
GB/T 41391-2022	*Exigences de base pour la collected 'informations personnelles dans les applications Internet mobiles*	2022-04-15	2022-11-01

Par ailleurs, nous résumons comme suit, à titre de référence, certaines «choses à ne pas faire» basées sur des cas de sanctions administratives concernant le traitement des données à caractère personnel au cours des dernières années et sur notre expérience propre :

- Aucune politique de confidentialité n'est fournie; ou le lien vers la politique de confidentialité est fourni mais ne fonctionne pas.

- La politique de confidentialité est affichée et accessible, mais elle n'inclut pas/ne clarifie pas les éléments suivants :
  - les règles de collecte des données personnelles ;
  - les informations de base du responsable du traitement ;
  - durée/date d'entrée en vigueur de la politique de confidentialité ;
  - avis de mise à jour (le cas échéant) ;
  - les règles de traitement des données à caractère personnel (objectifs, méthodes et champs d'application) du SDK tiers (kit de développement logiciel); ou,
  - la durée de conservation des données et méthode d'élimination après la période de conservation.

- La politique de confidentialité est affichée et accessible, mais elle n'est pas :
  - en chinois simplifié ;
  - dans un langage simple (facile à lire) ; ou,
  - facilement accessible par les personnes concernées (plus de 4 clics nécessaires dans les applications mobiles).

- Par rapport aux droits des personnes concernées:
  - ne pas répondre aux droits des personnes concernées ou tarder à répondre aux personnes concernées ;
  - ne pas fournir aux personnes concernées un mécanisme de dépôt de plainte ou des informations de contact ; ou
  - le droit de désinscription du compte d'utilisateur n'est pas prévu/prévu mais déraisonnablement compliqué .

- Autres scénarios:
  - les activités de traitement des données ne sont pas conformes à la politique de confidentialité et violent le principes de minimisation, de nécessité et de transparence des données ;
  - les données personnelles sensibles ne sont pas marquées séparément, et les finalités, les méthodes et l'étendue des catégories de traitement des données personnelles sensibles ne sont pas énumérées ;
  - fournir des données à caractère personnel à un tiers sans le consentement des personnes concernées ou sans anonymisation des données à caractère personnel ;
  - collecter et/ou traiter des données à caractère personnel avant que les personnes concernées n'aient lu la politique de confidentialité et donné leur consentement ; ou,
  - les données à caractère personnel ne sont pas supprimées après la désinscription de la personne concernée de son compte d'utilisateur.

Outre les violations courantes mentionnées ci-dessus, il est conseillé aux responsables du traitement des données, en particulier à ceux qui traitent des données à caractère personnel par l'intermédiaire d'applications mobiles et du mini-programme Wechat, d'accorder une plus grande attention aux normes nationales relatives aux exigences en matière de collecte et de traitement des données à caractère personnel. Des chiffres et des règles plus détaillés sont fournis en ce qui concerne les clics des utilisateurs, la fréquence des demandes de consentement pour un certain scénario de traitement, la période de conservation, etc.

En un mot, une politique de confidentialité digne de confiance ne se contente pas de respecter les principes fondamentaux établis par les lois applicables, mais contribue également à la réalisation des objectifs commerciaux tout en réduisant l'impact sur les personnes concernées. Son texte principal transmettra les informations au cours de la première interface présentée aux personnes concernées, et des «alertes » au moment de traitements de données peuvent rappeler les principes aux personnes concernées. Par exemple, une notification contextuelle peu avant la collecte de données personnelles sensibles (caméra pour la reconnaissance faciale, microphone, fourniture de données GPS et de données de santé, etc.) Plus le responsable du traitement souhaite obtenir de données à caractère personnel (en particulier des données à caractère personnel sensibles), plus il doit s'efforcer d'élaborer une politique de confidentialité et des notifications dans le cadre des activités de traitement des données à caractère personnel.

Remarques finales

Une politique de confidentialité des données est censée montrer la responsabilité du responsable du traitement des données en notifiant aux personnes concernées les règles de traitement des données à caractère personnel. En cas de contestation par les personnes concernées, le responsable du traitement des données peut utiliser la politique de confidentialité comme preuve juridique pour justifier le traitement des données à caractère personnel. Toutefois, si une politique de confidentialité des données n'est pas fondée sur des faits et/ou est trompeuse, elle pourrait également être utilisée par les personnes concernées comme preuve contre le responsable du traitement dans le cadre d'une plainte administrative ou d'autres actions en justice, ce qui se retournerait contre le responsable du traitement des données.

Pour toute information complémentaire, merci de contacter :

Isabelle DOYON
Associate - Shanghai Office
doyon@dsavocats.com

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

11, Avril 2024