les banques domestiques

Révision totale et modification d'autres actes législatifs concernant la protection des données

Les banques domestiques se prononcent en principe en faveur du projet de loi sur la protection des données voté par le Conseil national (P-LPD) et privilégient une entrée en vigueur rapide. Il faut encore l'adapter à certains égards afin d'aboutir à une loi suisse sur la protection des données moderne et efficace qui ne compromette pas l'équivalence avec le Règlement général sur la protection des données de l'Union européenne (RGPD-UE) et ne charge pas l'économie par un « Swiss finish » inutile.

Les banques domestiques soutiennent le projet de loi sur la protection des données moderne adopté par le Conseil national. Elles se prononcent particulièrement en faveur des points suivants, décidés par le Conseil national :

- Coordination des définitions importantes avec le RGPD-UE (not. concernant le profilage) pour créer un espace de protection des données uniforme et éviter les doublons coûteux.
- Sécurité du droit en matière de droit d'accès, not. par la limitation aux « données personnelles à proprement parler ».
- Pas d'interdiction de la vérification de la solvabilité.

Les principaux **besoins d'adaptation** se trouvent du point de vue des banques domestiques dans les domaines suivants :

1. Introduire la définition du « profilage à haut risque »

Le profilage signifie la collecte et le traitement automatisés de données électroniques afin de mieux analyser les clientes et les clients. Il s'agit d'un processus quotidien largement répandu auprès des banques qui traitent les données clients. Ce processus est aussi utilisé pour la protection de la clientèle, par ex. en cas de dépenses frappantes au moyen d'une carte de crédit. Le profilage fait, à juste titre, partie de la loi sur la protection des données. Il est cependant important de réglementer le profilage de manière différenciée afin de ne pas alourdir disproportionnellement les processus quotidiens de traitement des données. Il faut donc différencier la définition du « profilage à haut risque » du « profilage normal », qui sert typiquement à mieux conseiller ou protéger le client, par ex. contre les agissements frauduleux. À cette fin, il faut des critères efficaces qui permettent une différentiation effective. Ainsi, il faut aussi régler de manière strictement différenciée les exigences qui y sont liées (art. 5 al. 7 et art. 27 al. 2 lit. c ch. 1 P-LPD).

2. Renforcer les compétences du conseiller à la protection des données

Selon la disposition de l'art. 9 P-LPD, les responsables privés de données peuvent nommer un conseiller à la protection des données. Dans la version du Conseil national, cette fonction a du sens et doit être saluée. En contrepartie, une entreprise qui assume cette fonction doit logiquement aussi être libérée de certaines obligations not. à l'égard du Préposé fédéral à la protection des données et à la transparence (PFPDT). Cela promeut la création de la fonction du conseiller à la protection des données par l'entreprise et décharge par la même occasion le PFPDT.

3. Conception favorable à l'économie et praticable des devoirs d'information

Pour les divulgations de données à l'étranger, un consentement volontaire doit suffire ; il faut renoncer au critère du caractère expresse (cf. art. 14 al. 1 lit. a P-LPD). La Suisse est un pays d'exportation à succès ; de nombreuses marchandises et données personnelles passent la frontière chaque jour. Un consentement expresse en cas de divulgation des données à l'étranger compliquerait beaucoup ces processus et ne serait pas pratiques.

La mise à disposition d'informations selon l'art. 17 al. 2 P-LPD devrait être simplifiée. D'une part, la mise à disposition d'une communication généralement disponible, que la personne concernée peut demander ou consulter, doit suffire. D'autre part, de telles communications doivent aussi pouvoir être fournies par voie électronique. Cette modernisation réalise un concept qui est déjà ancré dans d'autres nouvelles lois (par ex. la loi sur les services financiers).

De plus, selon l'art. 17 al. 4 P-LPD, l'information concernant l'étranger ne devrait pas se faire de manière détaillée et spécifique au pays à chaque transaction transfrontalière. Un document de l'entreprise qui informe au sujet de la nécessité d'un flux de données et des risques typiques qui y sont liés doit suffire, avec un effet pour un secteur d'activité déterminé, par ex. l'achat et la vente de placements. Le client reçoit ainsi un aperçu transparent, adéquat, « digeste » et donc compréhensible, des risques potentiels du secteur d'activité en question. Cette réglementation doit en outre uniquement s'appliquer aux données qui n'ont pas été obtenues directement auprès de la personne concernée. Dans le cas contraire, on créerait un « Swiss finish » qui dépasserait les exigences correspondantes à l'UE (cf. art. 14 al. 1 lit. f RGPD-UE).

Quant à la libération de l'obligation d'information en cas de décision unique automatisée (art. 19 al. 3 lit. b P-LPD), un consentement volontaire de la personne doit suffire ; il faut ici également renoncer au critère du caractère expresse. L'obligation d'obtenir un consentement expresse ou d'informer la personne concernée de chaque décision unique automatisée limiterait l'économie de manière disproportionnée, compliquerait et renchérirait sans raison les processus, empêchant leur numérisation. Cela affaiblirait encore une fois la force d'innovation et l'attractivité du site économique suisse.

4. Ne pas étendre sans raison la divulgation des données aux tiers

Ce sont précisément les entreprises et les banques de petite taille qui ont intérêt à ce que l'outsourcing ne soit pas empêché inutilement. Selon des bases légales déjà existantes, ce genre de collaboration est déjà réglé en détail au niveau contractuel. Les partenaires d'outsourcing ne doivent donc pas être considérés comme des tiers au sens du droit sur la protection des données, afin que l'échange des données pour des motifs de gestion interne demeure possible sans entraves. Tel doit aussi être le cas pour l'échange de données entre entreprises d'un même groupe. Des exceptions dans ce sens sont nécessaires aux art. 18 al. 3 lit. c, 24 al. 2 lit. a et 27 al. 2 lit. b P-LPD ainsi qu'à l'art. 34 al. 2 LBA.

5. Diriger le système de sanctions contre les entreprises et passer à des sanctions administratives

Au niveau du régime des sanctions (art. 54 ss P-LPD), il faut remplacer les sanctions à l'égard des personnes physiques par une punissabilité primaire des entreprises et une punissabilité subsidiaire des personnes physiques en cas d'actes intentionnels directs (cf. art. 58 P-LPD). À moyen terme, le système de sanctions dans le domaine de la protection des données doit être dirigé contre les entreprises, passant à des sanctions administratives. Nous soutenons donc le postulat 18.4100 de la CIP-E concernant le « Régime général de sanctions administratives pécuniaires ».