ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

La Commission

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08, F +41 26 305 59 72
www.fr.ch/atprd

—

Réf: LS/RPA/coc 2017-PrD-50 et 2017-Trans-12
Courriel: secretariatatprd@fr.ch

Autorité cantonale de la transparence et de la protection des données
Rue des Chanoines 2, 1700 Fribourg

Chancellerie d'Etat
Madame Danielle Gagnaux
Chancelière d'Etat et
Monsieur Stéphane Schwab
Responsable du secrétariat de
cyberadministration
Rue des Chanoines 17
1700 Fribourg
Céans

Fribourg, le 24 avril 2017

Loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID) – consultation fédérale

Madame la Chancelière d'Etat,
Monsieur le Responsable du secrétariat de cyberadministration,

Nous nous référons au courriel du 21 mars 2017 adressé à notre Autorité concernant l'objet cité en marge et vous remercions de nous avoir consultés à ce sujet.

I. Sous l'angle de la protection des données

D'une manière générale, la Commission se permet de signaler que l'utilisation de l'e-ID dans le cadre de l'activité étatique ne peut pas concerner plus de données personnelles que dans le monde « réel ».

La Commission fait les remarques suivantes :

Ad article 2

Il manque la définition du titulaire d'un e-ID.

Ad article 4

De manière globale, nous saluons les efforts de mise en œuvre d'un système d'identification électronique permettant de réduire les risques d'usurpation d'identité dans le cadre de relations commerciales ou avec l'Etat. Par contre, l'établissement de documents d'identité doit rester une tâche étatique, et cela vaut aussi pour l'identification électronique. Cette tâche ne peut pas être attribuée, dans le cas d'un outsourcing, à des fournisseurs d'identités privés. L'Etat doit en rester le principal fournisseur. Les arguments relatifs au changement de paradigme, à savoir que des sociétés privées figurent comme fournisseuses d'identité, ne convainquent pas. La tâche publique, la transparence ainsi que la confiance du citoyen envers l'Etat exigent que celui-ci prenne la responsabilité de mettre en place les structures et les finances nécessaires.

Ad article 7

Le catalogue des données d'identification personnelle nous semble long et contient des données biométriques, qui sont des données sensibles. Les raisons pour lesquelles le traitement de ce nombre important de données est nécessaire ne sont pas compréhensibles. Vu que cette liste n'est pas exhaustive, laissant la possibilité d'ajouter des données, la norme ne répond pas au principe de la proportionnalité. Il y a lieu de constater que des données en réserve sont collectées et interconnectées.

Les données énumérées dans l'article 7 sont destinées à être transmises aux fournisseurs d'identité. Même si le consentement de la personne concernée est requis, la transmission de données envisagée reste disproportionnée. Les fournisseurs des services reçoivent un nombre de données personnelles beaucoup plus important que dans le cadre du déroulement actuel des opérations commerciales. En résumé, il s'agit pour l'instant de transmissions non admissibles de données personnelles venant des registres de personnes tels qu'ISA, SYMIC, Infostar ou CdC-UPI à des particuliers.

Ad article 9 - numéro AVS

L'avant-projet prévoit l'utilisation systématique du NAVS13 par le service d'identité à des fins d'identification de personnes dans le cadre de l'échange électronique de données avec les registres de personnes (ISA, SYMIC, Infostar, CdC-UPI). Comme le rapport le soulève, l'utilisation du NAVS13 comporte un grand risque d'interconnexions de données personnelles dans les différents systèmes. Contrairement à ce qu'affirme le rapport, ce risque est augmenté si une utilisation systématique est envisagée. Une telle utilisation est également exercée par les fournisseurs. Nous exigeons que le numéro AVS ne soit pas accessible à des particuliers et ne soit ni transmis aux fournisseurs ni stocké dans leurs systèmes et bases de données. Le numéro AVS a été initialement prévu pour être utilisé dans le domaine des assurances sociales. En principe, son utilisation systématique devrait être autorisée uniquement aux organes et services chargés des tâches dans ce domaine. Le projet ne se prononce pas sur les limites de l'utilisation du numéro AVS, problématique sous l'angle de la protection de données. En effet, ce projet élargit considérablement l'utilisation de cet élément comme identificateur unique et général, contredisant les intentions initiales du champ d'application de ce numéro. L'unique argument avancé pour une telle utilisation est – comme pour l'outsourcing d'ailleurs – celui relatif à la question des coûts d'investissement, qui ne tient pas compte du fait que la tâche étatique n'est pas un service commercial.

Ad article 10

Selon le rapport accompagnant l'avant-projet, l'article 10 vise à régler le traitement des données, notamment leur transmission. Cependant, le texte est peu clair et laisse une marge d'appréciation trop large aux fournisseurs d'identité. Nous exigeons donc une interdiction stricte de l'utilisation des données à d'autres fins. Des normes et sanctions pénales en cas d'abus devraient être incluses dans le projet.

Ad article 11

Les mesures en cas de faillite ou de cessation de l'activité du fournisseur d'identité sont insuffisantes. Selon l'avant-projet, le système e-ID est insaisissable, mais il ne se prononce pas sur le sort des données personnelles et du numéro AVS. Qu'en est-il ? L'article 11 al. 2 de l'avant-projet, qui laisse au fournisseur d'identité le choix des mesures à entreprendre en cas de faillite ou

de cessation d'activité, ne satisfait pas les exigences de la protection des données. L'article 11 al. 3 ouvre la porte à une commercialisation des données personnelles, ce qui est inadmissible. La réglementation prévue conduit d'une manière indirecte à une commercialisation des données personnelles.

Dans ce contexte, nous relevons que les droits des personnes concernées, les titulaires d'un e-ID, ne sont pas mentionnés. La personne concernée devrait pouvoir accéder à ses données et retirer à tout moment son consentement. Ainsi, elle doit être informée en cas de faillite ou de cessation d'activité du fournisseur ou de la reprise du système par un autre fournisseur.

II. Sous l'angle de la transparence

La Commission n'a pas de remarque particulière à vous transmettre.

Nous vous prions de recevoir, Madame la Chancelière d'Etat, Monsieur le Responsable du secrétariat de cyberadministration, l'expression de nos salutations les meilleures.

Laurent Schneuwly
Président