



CH-3003 Berne

POST CH AG
PFPDT; EDÖB-A-DEDA3401/2

Envoi en annexe

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Votre référence :
Notre référence : EDÖB-A-DEDA3401/2
Dossier traité par : [REDACTED]
Berne, le 18 novembre 2024

Ämterkonsultation : AsP Technologie-Entscheid für die initiale Umsetzung der E-ID-Vertrauensinfrastruktur

Madame, Monsieur,

Nous vous remercions de la possibilité de nous prononcer sur le sujet cité en titre ainsi que de l'intérêt porté à la protection des données.

Après avoir analysé le document "*AsP_Technologie-Entscheid_E-ID-Vertrauensinfrastruktur.docx*", nous prenons note que le DFJP recommande de privilégier la variante d'une « introduction technique échelonnée dans le temps » (stipulé au chiffre 5.1). A cet égard, le PFPDT se permet d'apporter les remarques suivantes :

La protection de la sphère privée est ancrée dans la Constitution fédérale (article 13) et est considérée comme un principe important de la protection des données, qui garantit que les activités des utilisateurs ne peuvent pas être suivies ou surveillées au-delà du nécessaire. La loi sur la protection des données (LPD, RS : 235.1) aborde ce principe plus en détail à l'article 7 LPD en prévoyant des mesures techniques et paramétrages favorables à la protection des données. Dans le cas présent, il convient donc de s'assurer dès la conception que les transactions ne peuvent pas être attribuées/liées aux utilisateurs. Cela se fait en utilisant des technologies modernes et respectueuses de la protection des données afin de garantir l'impossibilité d'établir des liens.

L'introduction prévue de l'E-ID en deux phases représente à notre avis un risque du point de vue de la protection des données, notamment en ce qui concerne la probabilité que le système, initialement conçu comme provisoire, soit établi de manière durable. Dans la pratique, on constate souvent que les systèmes et processus techniques introduits provisoirement développent une constance considérable qui rend difficile les adaptations ultérieures. Cela est principalement dû à la dépendance du chemin. Cela signifie que les autorités et les prestataires de services adaptent leurs systèmes aux structures existantes et aux processus de travail établis, qui reposent sur la possibilité de relier l'E-ID. Plus ces systèmes sont en service depuis longtemps, plus il est difficile et coûteux de les modifier.



A cela s'ajoute un effet de dépendance qu'il ne faut pas sous-estimer. Les autorités pourraient s'habituer aux possibilités élargies de mise en relation des données et défendre le statu quo en arguant que « cela fonctionne ainsi jusqu'à présent ». Cela pourrait atténuer la pression sur la mise en œuvre de la deuxième phase et réduire la volonté d'adaptation nécessaire. Du point de vue du PFPDT, les questions pratiques de ressources jouent également un rôle décisif. La transition nécessite des ressources financières et humaines. Compte tenu d'autres projets éventuellement plus urgents et de la pression sur les coûts, cela pourrait entraîner des retards.

L'apparition d'un « système à deux vitesses » en matière de protection de la sphère privée constitue un autre problème. Alors que les utilisateurs de la nouvelle version de l'E-ID bénéficieraient d'une meilleure protection des données grâce à l'absence de lien, les détenteurs de la version initiale devraient s'accommoder d'un niveau de protection moins élevé. Le passage à la nouvelle version entraîne en outre des difficultés pratiques qui devraient être prises en compte dans la planification de la mise en œuvre. Les citoyens devraient donc s'efforcer activement d'obtenir un nouveau E-ID, ce qui pourrait entraîner des coûts et des efforts supplémentaires. Cela pourrait à son tour conduire à ce que beaucoup restent par commodité avec l'ancienne version - du moins jusqu'à ce qu'ils soient contraints à une « mise à niveau ».

Le PFPDT recommande donc d'attendre que les technologies respectueuses de la protection des données soient mises en œuvre pour garantir la dissociabilité (empêcher de faire les liens) avant d'introduire l'infrastructure de confiance. Ainsi, la protection des données par la technique serait garantie dès le début selon l'état de la technique. Nous comprenons qu'il est regrettable qu'un projet si important prenne du retard, mais cela ne doit pas se faire au détriment de la protection des données des citoyens. C'est pourquoi, le **PFPDT recommande de privilégier l'option du report de la date d'introduction.**

Si la variante « report de la date d'introduction » ne devait pas s'imposer, le PFPDT estime qu'il faudrait fixer un calendrier contraignant pour la deuxième phase afin de minimiser les risques. En outre, des rapports publics réguliers sur l'état d'avancement devraient être établis, la deuxième phase devrait être budgétée suffisamment tôt et une instance de surveillance indépendante devrait être mise en place.

Nous souhaitons également ajouter que nous sommes tout à fait disposés à organiser une réunion pour toute question ou discussion sur le sujet. Vous pouvez sans autre contacter Madame [redacted], chef de team 2 et responsable adjointe du domaine de direction Protection des données ([\[redacted\]@edoeb.admin.ch](mailto:[redacted]@edoeb.admin.ch)) ou [redacted], juriste team 2 ([\[redacted\]@edoeb.admin.ch](mailto:[redacted]@edoeb.admin.ch)).

Nous vous prions d'agréer, Madame/Monsieur, nos salutations distinguées

[redacted] e
Leiterin Team 2
Stv. Leiterin Direktionsbereich Datenschutz
[redacted]