Lorsque la mitigation rend la notification impossible : quelles modalités à suivre pour informer d'une violation ?

Charlotte Beck et Alain Steinmann, le 30 septembre 2026

Le TAF rend une première décision sur l'obligation d'information des personnes concernées en cas de violation de la sécurité des données. Un arrêt complété par une conclusion (ambiguë) de violation du droit d'être entendu.

TAF, Arrêt A-3790/2024 du 8 avril 2026

Le Tribunal administratif fédéral (TAF) confirme, dans son arrêt, la décision du PFPDT enjoignant à un exploitant de boutique en ligne d'informer les clients dont les données ont été exposées sur un moteur de recherche. Il précise notamment qu'en cas de violation de la sécurité des données, l'impossibilité d'une information individuelle n'éteint pas l'obligation d'informer les personnes concernées mais devrait conduire au recours à la communication publique, laquelle demeure toutefois une faculté que le PFPDT ne peut pas imposer formellement.

Faits

Une société exploitant une boutique en ligne gère les retours de marchandise au moyen d'URLs individuels menant chaque client vers une page dédiée à son propre cas de support. En substance, l'URL est censé n'être connu que du client concerné. La confidentialité repose ainsi sur le seul caractère secret du lien.

Dès juin 2023, un ensemble de ces URLs est indexé par le moteur de recherche Bing, rendant accessibles les données personnelles de 19'000 clients (identité, adresse électronique, adresse postale, contenu des échanges relatifs au support, coordonnées bancaires [IBAN], photographies des produits achetés et codes de bons d'achat). Les fiches de retour devenaient dès lors accessibles par une simple recherche, sans mot de passe ni authentification.

Le 16 février 2024, la société annonce la violation au PFPDT et prend diverses mesures techniques correctives, dont notamment le blocage du crawler de Bing, la demande de suppression des URLs concernés, l'altération des IBAN et la confirmation obligatoire de l'adresse électronique avant tout accès. Elle estime en revanche qu'informer les personnes concernées

n’est pas nécessaire et représenterait un effort disproportionné, voire impossible.

Par décision du 28 mai 2024, le PFPDT ordonne à la société d’informer les personnes concernées dans les dix jours dès l’entrée en force de la décision, sous menace d’amende. À la suite de cette décision, la société recourt au TAF.

Le TAF rejette le recours et confirme la décision du PFPDT.

Droit

I. Existence d’une violation de la sécurité des données

Le TAF rappelle qu’une violation de la sécurité des données suppose l’atteinte à l’un des trois objectifs de protection, à savoir la confidentialité, la disponibilité et l’intégrité. La confidentialité est réputée atteinte dès la simple possibilité que des données personnelles soient accessibles à des tiers non autorisés.

La recourante s’emploie à relativiser la portée de l’incident. Elle fait notamment valoir que seule une petite fraction des URLs avait été indexée par le seul moteur Bing et qu’aucune conséquence dommageable ne s’était manifestée à sa connaissance. Elle en déduit l’absence de besoin de protection justifiant une information.

Le TAF conclut qu’aucun de ces éléments n’influe sur l’analyse que ce soit sur la qualification de violation, sur la nécessité d’informer ou sur l’existence d’une exception au sens de l’art. 24 al. 5 LPD.

II. Nécessité d’informer les personnes concernées

Le responsable de traitement a l’obligation d’informer la personne concernée lorsque cela est nécessaire à sa protection conformément à l’art. 24 al. 4 LPD. Cette information revêt un caractère préventif. Elle vise à permettre aux personnes de se protéger elles-mêmes sans que la preuve d’un dommage concret ne constitue une condition de cette obligation. Le critère déterminant n’est donc pas l’intensité du risque ou de la violation, mais la possibilité pour la personne d’entreprendre, sur la base de cette information, des démarches utiles pour se protéger (cf. FF 2017 6682).

Le TAF retient logiquement un besoin de protection dans le cas d’espèce. La combinaison de l’IBAN, de l’identité et de l’adresse expose notamment à l’usurpation d’identité, à l’ingénierie

sociale et aux prélèvements frauduleux, contre lesquels la personne informée peut réagir simplement en changeant par exemple ses mots de passe ou en contrôlant ses relevés.

Le TAF relève également que l'écoulement du temps ne modifie pas cette appréciation. Des données divulguées peuvent être conservées puis réutilisées ultérieurement, de sorte que le risque d'abus et donc le besoin de protection subsiste.

III. Exceptions à l'information et communication publique

Le TAF constate que l'information individuelle est en l'espèce à la fois (i) impossible dans la mesure où l'identification des personnes est devenue impraticable à la suite des mesures de blocage et (ii) disproportionnée au regard des quelque 19'000 personnes concernées.

Dans un tel cas de figure, la communication publique au sens de l'art. 24 al. 5 let. c LPD reste l'alternative. Elle permet de remplacer l'information individuelle lorsque celle-ci est assurée de manière comparable par une annonce publique. Le TAF précise que cette disposition institue une faculté et non une obligation.

L'arrêt confirme que le PFPDT ne peut pas, dans le cadre d'une mesure administrative, ordonner formellement le recours à une communication publique. C'est du reste pour cette raison que ce moyen de communication figurait à juste titre dans les seuls considérants de la décision du PFPDT et non pas dans le dispositif (celui-ci se bornant à confirmer l'obligation légale d'informer). Le TAF rappelle toutefois que le PFPDT peut, de son propre chef, informer le public sur ses constatations et décisions, mesure qui incite en pratique le responsable de traitement à procéder lui-même à l'annonce.

Examinant la proportionnalité de la communication publique, le TAF la juge apte (il s'agit du seul moyen d'atteindre les personnes devenues non identifiables), nécessaire (aucun autre moyen n'est disponible vu que l'information individuelle est exclue) et exigible. Il est encore rappelé que, dans la pesée des intérêts, le besoin de protection des personnes concernées l'emporte sur l'intérêt de la société à éviter une atteinte à sa réputation.

IV. Droit d'être entendu

Le TAF consacre également un considérant entier sur le droit d'être entendu, considéré comme violé par la société (pour une analyse détaillée en allemand, cf. Vasella David, BVGer : Informationspflicht ggü. Betroffenen bei einem Data Breach ; schwerwiegende Verletzungen von Verfahrensrechten durch den EDÖB). En effet, le PFPDT n'aurait pas suffi-

samment motivé sa décision, ayant pour conséquence une obligation d'indemniser la société à hauteur de CHF 500.

L'art. 29 al. 2 Cst est reconnu comme violé sur un des trois griefs soulevés par la recourante. Une contradiction dans la décision du PFPDT est constatée. D'une côté, l'information individuelle des personnes concernées était considérée comme disproportionnées mais, de l'autre côté, le PFPDT niait qu'une des exceptions de l'art. 24 al. 5 LPD permettant de déroger à l'information individuelle était remplie. Aucune précision sur le moyen de notifier les personnes concernées n'a été fournie par le préposé, ce qui est d'autant plus problématique, l'injonction d'informer étant assortie d'une menace de sanction pénale.

Ce manque de motivation claire mène donc le TAF à conclure à une violation du droit d'être entendu. Cette violation est cependant guérie par la procédure de recours, ne nécessitant pas de la renvoyer en instance inférieure.

Appréciation

L'arrêt confirme une logique déjà présente dans le système de l'art. 24 LPD. L'obligation d'informer les personnes concernées ne s'éteint pas lorsque l'information individuelle devient impossible ou disproportionnée mais elle se transforme, le responsable de traitement devant recourir à la communication publique.

Curieusement, alors même que la communication publique constitue le seul moyen possible et envisageable, le PFPDT ne peut pas la contraindre faute d'obligation légale expresse. En effet, les moyens décrits à l'art. 51 LPD ne lui donne pas la possibilité de préciser la manière dont les personnes concernées doivent être informées. Cependant, cette conclusion se heurte à celle rendue dans cette même décision en lien avec le droit d'être entendu.

Le TAF affirme que le PFPDT aurait dû clarifier les modalités de notification que la société devait suivre dans sa décision, tout en démontrant que celui-ci n'a pas la compétence pour imposer lesdites modalités, amenant une ambiguïté non résolue dans cet arrêt. Le TAF lui-même ne permet pas de se déterminer sur l'obligation ou non de la communication publique, dans un manque de motivation similaire à ce qui est reproché au PFPDT.

Enfin, l'arrêt illustre un écueil pratique en gestion d'incident. En bloquant l'accès aux URLs pour protéger sa clientèle (démarche correcte qui ne peut être reprochée à la recourante), le responsable de traitement a rendu l'identification ultérieure des personnes concernées impossible, avec pour conséquence de devoir procéder à une communication publique plutôt qu'in-

dividuelle. Un des enseignements de cet arrêt (qui pourrait sembler être une évidence) est que la préservation des données nécessaires à l'identification des personnes concernées devrait être pensée en amont avant la mise en place des mesures correctives. Ceci pour se garder la possibilité de pouvoir procéder à une communication individuelle moins dommageable pour une société sur le plan réputationnel.

Proposition de citation : Charlotte Beck / Alain Steinmann, Lorsque la mitigation rend la notification impossible : quelles modalités à suivre pour informer d'une violation ?, 30 septembre 2026 *in* www.swissprivacy.law/420

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.