Mauvaise utilisation du pixel Meta : fuite de données bancaires et lourde amende pour une banque

Alexandre Jotterand, le 8 juillet 2024

Pixel Meta : l'autorité suédoise de protection des données (IMY) sanctionne une banque pour une fuite de données bancaires causée par la mauvaise configuration du pixel Metal sur son site web et application d'e-banking.

Décision du 24 juin 2024 de l'autorité suédoise de protection des données (IMY) contre Avanza Bank AB, DI-2021–5544 Avanza Bank

L'Autorité suédoise de protection des données (IMY) a infligé une amende de 15 000 000 SEK (environ 1 287 000 francs suisses) à Avanza Bank AB pour un pixel Meta mal configuré.

La banque a utilisé l'outil d'analyse Facebook pixel (qui s'appelle désormais « pixel Meta ») à la fois sur son site web et dans son application d'e-banking afin d'optimiser le marketing de la banque. Dans le contexte du suivi en ligne, un « pixel » est un petit élément graphique invisible intégré dans une page web (ou un email) pour suivre le comportement des utilisateurs et collecter des données sur leurs interactions avec le contenu web.

Avant l'intégration de ce pixel, un processus d'approbation impliquant les fonctions de risque, de conformité, du juridique et de la sécurité de l'information de la banque a été mené. Dans ce cadre, les questions du secret bancaire et du traitement des données personnelles ont été abordées. Les seules données qui devaient être traitées pour la finalité en question étaient celles relatives aux pages web visitées par les utilisateurs, l'adresse IP et les informations sur certains événements uniques, tels que les choix de produits et les recherches sur le site web.

Toutefois, une erreur de paramétrage (qui n'a jamais été élucidée) a conduit à l'activation accidentelle par la banque de deux sous-fonctionnalités du pixel Meta : « AAM » (*Automatic Advanced Matching*) et « EA » (*Automatic Events*). Ces sous-fonctionnalités ont entrainé le transfert des données personnelles de près d'un million de clients de la banque à Meta pendant une longue période (novembre 2019 à juin 2021). Les informations transmises de cette manière portaient notamment sur les avoirs et la valeur des titres, les montants des prêts, les numéros de compte, les adresses email et les numéros de sécurité sociale.

Une grande partie de ces données provenaient d'éléments (boutons, formulaires, etc.) intégrés sur des pages disponibles après la connexion à l'e-banking. Ils ne concernaient donc que de clients liés par une relation d'affaires préexistante avec la banque. Dans tous les cas, la transmission ne pouvait intervenir que si l'utilisateur avait accepté les cookies marketing de la banque (*opt-in*).

Dès que la banque a eu connaissance de l'incident, elle a désactivé le pixel Meta et a demandé à Meta de supprimer les données collectées via le pixel, ce que Meta a confirmé avoir fait. La banque a également adapté ses procédures internes pour garantir un traitement correct et sécurisé des données personnelles. Elle a en particulier mis en place un processus de gestion des scripts de tiers et a déplacé les scripts des fournisseurs tiers vers ses systèmes afin d'éviter que des modifications puissent être apportées à son insu.

Estimant qu'il s'agissait d'une violation de données à caractère personnelles au sens de l'art. 4(12) RGPD, la banque a notifié cet incident à l'autorité de surveillance conformément à l'art. 33 RGPD (*Notification à l'autorité de contrôle d'une violation de données à caractère personnel*).

Les considérations de l'autorité

Premièrement, l'autorité retient que le RGPD est applicable au cas d'espèce et que la banque agit comme responsable du traitement en lien avec la collecte et le transfert des données des utilisateurs via les pixels qu'elle a intégrés à ses solutions numériques.

L'autorité rappelle ensuite qu'en vertu de l'art. 32 RGPD, la banque est tenue de protéger les données à caractère personnel qu'elle traite en mettant en œuvre des mesures techniques et organisationnelles appropriées. Les données concernées (données bancaires soumises au secret) nécessitaient une protection particulière.

L'autorité retient que la banque – en violation de ses propres directives internes – a activé (à son insu) des fonctionnalités qui ont conduit à la divulgation des données à des tiers non autorisés (*data breach*). L'autorité reproche également à la banque de n'avoir pas mis en place les contrôles techniques qui lui auraient permis de constater et corriger l'erreur plus rapidement. Elle retient en conséquence que la banque a violé l'art. 32 RGPD, en manquant à l'obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté des données personnelles des visiteurs du site web et des utilisateurs de l'application. L'autorité n'accorde aucune importance au fait que seules les données des utilisateurs ayant consenti à l'utilisation des cookies de marketing de

la banque aient été transmises ; ce fait n'est pas de nature à remédier aux manquements en matière de sécurité.

L'autorité retient par contre la banque n'a pas violé les dispositions nationales implémentant la Directive « vie privée et communications électroniques » (*ePrivacy Directive*). En effet, à la différence des cookies, la technologie des pixels de suivi n'implique pas le stockage d'informations sur le poste de l'utilisateur, de sorte que cette législation n'est pas applicable au cas d'espèce.

Compte tenu de la gravité des violations constatées, l'autorité estime qu'une amende de 15 000 000 SEK (environ 1 287 000 francs suisses) est justifiée.

Enseignements

Cette décision souligne l'importance pour les entreprises de bien comprendre et gérer les outils numériques qu'elles utilisent. Il faut rappeler qu'en droit suisse, les manquements aux exigences minimales en matière de sécurité peuvent conduire à des sanctions pénales (art. 61 let. c LPD). Les banques suisses sont au demeurant tenues au respect du secret bancaire et à la réglementation prudentielle, qui exigent notamment de prendre des mesures pour protéger les données bancaires (et plus particulièrement les données qualifiées de *critiques* au sens du point 7 de la Circulaire FINMA 2023/01) et notifier les incidents, que cela soit en vertu des Communications FINMA 05/2020 et 03/2024, que très prochainement en vertu des art. 74a ss de la loi fédérale sur la sécurité de l'information). Nous relevons en particulier les enseignements suivants :

1. Mesures basées sur les risques : c'est une évidence, mais les mesures de sécurité requises dépendent notamment de la sensibilité des données traitées. Dans le cas d'espèce, bien qu'il ne s'agissait pas de données sensibles au sens de la loi (catégories particulières de données à caractère personnel), un haut niveau de sécurité était attendu.
2. Vigilance dans l'intégration des outils tiers : l'utilisation de solutions numériques tierces, comme les pixels de suivi dans le cas d'espèce, nécessite une attention particulière. Les entreprises doivent s'assurer que les fonctionnalités de ces outils sont entièrement comprises et correctement configurées avant leur déploiement.
3. Gestion des changements : il faut en particulier pouvoir s'assurer que le fournisseur de l'outil ne peut pas en modifier les fonctionnalités sans que l'entreprise en soit informée. Dans notre cas, cette réalisation tardive a conduit la banque, suite à l'incident, à mettre en place un processus de gestion des scripts de tiers et à déplacer les scripts des four-

nisseurs tiers vers ses propres systèmes afin d'éviter que des modifications puissent être apportées à son insu.

4. Processus de contrôle (*monitoring*) : il est également important de disposer de contrôles techniques pour surveiller les outils intégrés. La banque aurait pu éviter ou limiter l'impact de cette violation si elle avait mis en place des mécanismes permettant de détecter rapidement les flux de données ou l'activation involontaire de fonctionnalités supplémentaires.
5. Respect des règles internes : enfin, s'il est naturellement utile de mettre en place des directives et procédures internes, encore faut-il pouvoir s'assurer de les suivre en pratique. Tel n'a pas été le cas en l'espèce.

Proposition de citation : Alexandre JOTTERAND, Mauvaise utilisation du pixel Meta : fuite de données bancaires et lourde amende pour une banque, 8 juillet 2024 *in* www.swissprivacy.law/309