Pour nous contacter
–
Equipe IP/IT & Data Protection
ebarbry@racine.eu | (+33) 6.13.28.91.28
Equipe Réglementation bancaire, financière et assurantielle
dmasson@racine.eu | (+33) 6.30.95.80.09

Sanction par la CNIL de la société SLIMPAY à hauteur de 180 000 euros

L'essor du numérique et des nouvelles technologies a radicalement bouleversé le paysage des pratiques professionnelles. Le secteur bancaire n'y échappera pas tandis que les moyens de paiement, pléthores et toujours plus complexes, sont devenus la pierre angulaire de la fidélisation clients. Mais les prestataires de services de paiement ne sont pas les seuls maîtres à bord et la Cnil contrôle également ces entités avec attention pour garantir le strict respect des données personnelles dans un secteur usant de données souvent sensibles.

La décision du 28 décembre 2021 rendue par la formation restreinte et condamnant le prestataire de services de paiement **Slimpay** à une amende de 180.000 euros pour manquements au Règlement général sur la protection des données personnelles[1] (« **RGPD »**) en est une parfaite illustration.

Dans les faits, Slimpay est un établissement de paiement agréé par l'Autorité de Contrôle Prudentiel et de Résolution (« **ACPR** ») qui propose des solutions de gestion des abonnements et des paiements récurrents SEPA à ses clients, des marchands.

Au cours de l'année 2015, Slimpay a effectué un projet de recherche interne lors duquel elle a utilisé les données personnelles contenues dans ses bases de données. Lorsque le projet s'est terminé en juillet 2016, les données sont restées stockées sur un serveur non sécurisé et librement accessible sur Internet. Or, ce n'est qu'en février 2020 que Slimpay s'est aperçue de la violation de données, concernant 12 478 819 ressortissants européens et a averti la Cnil en conséquence.

Dans le cadre de sa mission de contrôle sur pièces diligentée et agissant en autorité chef de file de plusieurs autorités européennes, la Cnil a constaté divers manquements de Slimpay au RGPD et l'a condamnée en conséquence par une décision rendue publique.

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE

Après avoir analysé les différents manquements reprochés à Slimpay par la Cnil (**1 à 3**), nous nous intéresserons aux critères de détermination du quantum de l'amende imposée à Slimpay par la Cnil, qui ne sont pas sans rappeler ceux sur lesquels s'appuie la Commission des Sanctions de l'ACPR (**4.**).

1. Slimpay responsable des sous-traitants ultérieurs (article 28 du RGPD)

Avant tout propos, la Cnil commence par identifier la qualité de Slimpay qui intervient en tant que sous-traitant pour les services réalisés au profit de ses clients dans la mesure où elle ne détermine pas les finalités de traitement des données. Lorsqu'elle décide de mettre en œuvre un projet de recherche interne à l'origine de la fuite de données, Slimpay agi alors en qualité de responsable de traitement puisqu'elle détermine seule les finalités et les moyens du traitement des données clients.

Dès lors, s'agissant des sous-traitants ultérieurs de Slimpay, la formation restreinte rappelle qu'un encadrement juridique adéquat suppose la conclusion d'un acte juridique (généralement un contrat) transposant l'ensemble des clauses de l'article 28 paragraphe 3 du RGPD.

En effet, il convient d'imposer aux sous-traitants ultérieurs « *les mêmes obligations en matière de protection des données que celles fixées dans le contrat entre le responsable de traitement et le sous-traitant (…) de manière à ce que le traitement réponde aux exigences du règlement* » (RGPD, article 28 paragraphe 4).

Si à première lecture de la décision, les moyens mis en œuvre par Slimpay semblent tout à sait satisfaire aux exigences du RGPD, la Cnil réalise un audit poussé de la documentation fournie et consacre une lecture coercitive de l'article 28 du RGPD en estimant notamment que les questionnaires de conformité proposés par Slimpay n'étaient pas suffisants pour s'assurer que les sous-traitants ultérieurs présentaient les garanties suffisantes requises. Pire encore, les contrats conclus entre Slimpay et ses sous-traitants ne contenaient pas les clauses obligatoires au sens du RGPD.

2. Le préjudice avéré sans conséquences sur l'obligation de sécurité (article 32 du RGPD)

La Cnil condamne également Slimpay sur le volet de l'obligation de sécurité au sens de l'article 32 du RGPD qui dispose que « *compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable de traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque*.».

La Cnil relève que l'accès au serveur Slimpay n'était encadré d'aucune mesure de restriction d'accès satisfaisante puisqu'il était possible d'y accéder à partir d'Internet entre novembre 2015 et février 2020, soit pendant près de 5 ans, et aucune mesure de journalisation, pourtant si souvent recommandées par la Cnil, n'était mise en œuvre.

C'est précisément à partir de ce constat que le verdict de la Cnil est sans appel : les données bancaires (état civil, adresses, BIC/IBAN, etc.) de 12 478 819 ressortissants européens ont été compromises.

L'argument de Slimpay tendant opposer le fait que les données n'ont probablement pas été utilisées frauduleusement reste sourd.

La formation restreinte considère que l'absence de préjudice avéré pour les personnes concernées est sans incidence sur la caractérisation du manquement à l'obligation de sécurité dans la mesure où les données de nombreuses personnes ont été rendues accessibles à des tiers non autorisés.

3. Donnée bancaires, risque élevé pour un devoir d'information accru (article 34 du RGPD)

La Cnil considère que Slimpay a méconnu ses obligations au titre de l'article 34 du RGPD relatif au devoir d'information des personnes concernées d'une violation de données personnelles en ce sens que « *Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.* »

L'argumentaire de Slimpay tendant à supposer qu'une communication publique n'aurait pas été pertinente car invisible pour ses clients ne tient pas aux yeux de la Cnil. La formation restreinte considère qu'une communication publique sur le site web de l'organisme aurait pu être un point de départ pour que l'information prenne ensuite une dimension bien plus importante.

Par ailleurs, considérant le caractère sensible des données bancaires exposées, du volume de personnes concernées, de la possibilité d'identifier les personnes touchées par la violation et par voie de conséquence, du risque d'utilisation frauduleuse de ces données notamment par hameçonnage ou usurpation d'identité, la formation restreinte estime que le risque associé à la violation devait être considéré comme élevé. Slimpay aurait dû informer toutes les personnes concernées par la violation de données.

4. Les critères relatifs à la détermination du quantum de la sanction pécuniaire imposée à Slimpay

La Cnil rappelle dans sa décision que le paragraphe 3 de l'article 83 du RGPD prévoit qu'en cas de violations multiples, comme c'est le cas en l'espèce, le montant total de l'amende ne peut excéder le montant fixé pour la violation la plus grave. Or, il est reproché à la société un manquement aux articles 28, 32 et 34 RGPD, le montant maximum de l'amende pouvant être retenu s'élève à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

La Cnil rappelle également qu'elle doit tenir compte, pour le prononcé d'une amende administrative, des critères précisés à l'article 83 du RGPD, tels que la nature, la gravité et la durée de la violation, les mesures prises par le responsable du traitement pour atténuer le dommage subi par les personnes concernées, le degré de coopération avec l'autorité de contrôle et les catégories de données à caractère personnel concernées par la violation.

Au cas présent, si la Cnil considère qu'il est proportionné de prononcer une amende administrative à l'encontre de Slimpay, elle estime nécessaire de tenir compte, pour déterminer son quantum, compte tenu des faits suivants :

- les manquements concernent un nombre très important de personnes, puisque la violation de données a concerné plus de 12 millions de débiteurs ;
- les données accessibles concernées des données qualifiées de « hautement personnelles » par le Comité Européen dela protection des données telles que l'IBAN des débiteurs ;
- les données sont restées accessibles pendant une très longue période, entre la fin de l'import des données sur le serveur en novembre 2015 et la découverte de l'incident par la société le 14 février 2020 ;
- les négligences commises en matière de sécurité par Slimpay étaient particulièrement graves.

La Cnil relève cependant qu'il est nécessaire de tenir compte de la situation économique de l'entité concernée pour déterminer une amende administrative proportionnée et qu'à la date du prononcé de la sanction, la situation financière de Slimpay était déficitaire.

Il résulte ainsi des éléments qui précèdent que Slimpay s'est vue imposer une amende de 180.000 euros.

Les critères énumérés par la Cnil dans sa décision pour déterminer le montant de l'amende administrative à imposer à Slimpay ne sont pas sans rappeler ceux sur lesquels s'appuie la Commission des Sanctions de l'ACPR.

En effet, comme l'article 83 du RGPD, l'article L. 612-40 X du Code monétaire et financier précise que le quantum de la sanction pécuniaire éventuellement prononcée doit être déterminé selon une liste de critères objectifs :

- la gravité et de la durée des manquements commis et, le cas échéant, de leurs conséquences systémiques potentielles ;
- le degré de responsabilité de l'auteur des manquements, de sa situation financière, de l'importance des gains qu'il a obtenus ou des pertes qu'il a évitées, de son degré de coopération avec l'ACPR et des manquements qu'il a précédemment commis ;
- les préjudices subis par des tiers du fait des manquements, s'ils peuvent être déterminés.

En pratique, la Commission des sanctions de l'ACPR a pu également prendre en compte la situation financière déficitaire d'un établissement pour réduire le montant de l'amende, voire pour ne pas en prononcer une. Tel était notamment le cas s'agissant de la décision rendue à l'encontre de la société Transaction Services International (« **TSI** »), par laquelle la Commission des Sanctions de l'ACPR a considéré qu'il n'y avait pas lieu à imposer une sanction pécuniaire, malgré les manquements substantiels reprochés à TSI compte tenu de sa situation financière très dégradée avec des pertes égales à plusieurs millions d'euros[2].

Il existe ainsi une convergence entre les différentes autorités de contrôle dans la mise en œuvre de leur pouvoir coercitif, lequel est soumis aux mêmes critères objectifs pour déterminer le montant des amendes administratives prononcées à l'encontre des établissements qui relèvent de leur supervision.

***

La décision de la Cnil intervient juste après la publication de son livre blanc du 6 octobre 2021 « *Quand la confiance paie : les moyens de paiement d'aujourd'hui et de demain au défi de la protection des données* ».

Coïncidence ? Rien n'est moins sûr ! La sanction prononcée à l'encontre de l'établissement de paiement Slimpay pourrait être la première application de ces recommandations.

Auteurs

Eric Barbry
Avocat associé
IP/IT & Data Protection
ebarbry@racine.eu

Sonia Oudjhani-Rogez
Avocat
Réglementation bancaire, financière et assurantielle
soudjhanirogez@racine.eu

Sabina Topcagic
Juriste
IP/IT & Data Protection
stopcagic@racine.eu

[2] Commission des sanctions de l'ACPR, décision n°2018-03 c/ Transaction Services Internation, 2 juillet 2019