_swissprivacy.law

Violation de données : La CNIL sanctionne les sociétés FREE MOBILE et FREE à hauteur de 42 millions d'euros

Clarence Tocchio, le 4 mars 2026

À la suite d'une violation de données massive touchant 24 millions de contrats d'abonnés, de nombreuses plaintes, ainsi qu'à un contrôle mené par la CNIL, cette dernière a prononcé deux sanctions à l'égard des sociétés FREE MOBILE et FREE.

Les montants particulièrement élevés sont motivés par la conservation excessive de données de contrats résiliés, des mesures de sécurité insuffisantes pour prévenir et détecter les accès non autorisés, ainsi que par une information incomplète transmise aux personnes concernées.

Délibération de la formation restreinte n° SAN-2026–002 du 8 janvier 2026 prononçant une sanction pécuniaire à l'encontre de la société FREE

Délibération de la formation restreinte n° SAN-2026–001 du 8 janvier 2026 prononçant une sanction pécuniaire à l'encontre de la société FREE MOBILE

Introduction

La Commission nationale de l'informatique et des libertés (« CNIL ») revient dans cette sanction sur des articles emblématiques du RGPD en précisant les exigences attendues dans la mise en œuvre de ces derniers. Plus spécifiquement, l'Autorité offre une analyse des articles relatifs à la conservation des données (art. 5 para. 1 let. e RGPD), à la sécurité du traitement (art. 32 RGPD) et à la communication à la personne concernée d'une violation de données à caractère personnel (art. 34 RGPD).

Pour rappel, le manquement à l'art. 5 para. 1 let. e RGPD, qui consacre l'un des principes clés du RGPD, est susceptible de faire l'objet d'une amende administrative pouvant s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel. Le manquement aux art. 32 et 34 RGPD est, quant à lui, susceptible de faire l'objet d'une amende administrative pouvant s'élever jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel. Le montant de l'amende doit toutefois être proportionné et dissuasif au regard des responsabilités et capacités financières de l'organisme mis en cause.

Faits

La société FREE a été alertée par un attaquant de la compromission de la confidentialité des données des abonnés de ses sociétés FREE MOBILE et FREE (« sociétés »). À la suite d'investigations, les sociétés ont confirmé la survenance d'une violation de données survenue.

En effet, l'attaquant a réussi à se connecter au réseau privé virtuel (VPN), puis à l'outil de gestion des abonnés des sociétés, et à accéder à des données à caractère personnel (données d'identité, de contact, contractuelles). En ce qui concerne les clients convergents, soit ceux qui sont abonnés à la fois à FREE MOBILE et à FREE, l'attaquant a également pu accéder à leur IBAN. Au total, l'attaquant a exfiltré les données relatives à plusieurs dizaines de millions de contrats.

La société FREE a notifié cette violation de données à la CNIL. Les sociétés ont ensuite informé par courriel les personnes concernées.

Lors de la notification du rapport de sanction à la société, la CNIL avait reçu plusieurs milliers de plaintes de personnes concernées par cette violation de données.

Ultérieurement, un contrôle a été réalisé dans les locaux des sociétés afin de vérifier leur conformité à la loi n° 78–17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (« LIL ») et au RGPD.

Dans le cadre de la procédure, la présidente de la CNIL a décidé de disjoindre la procédure de sanction initialement engagée à l'égard des deux sociétés afin de les poursuivre dans le cadre de procédures distinctes.

Il est ainsi reproché à ces sociétés, un manquement aux art. 32 (sécurité du traitement) et 34 (communication à la personne concernée d'une violation de données à caractère personnel) RGPD. Un manquement à l'art. 5 para. 1 let. e (conservation des données à caractère personnel) RGPD est également reproché à la société FREE MOBILE.

Droit

La CNIL détaille son analyse en quatre parties : (i) la qualité de responsable de traitement de la société, (ii) le manquement à l'obligation de conserver les données pour une durée proportionnée à la finalité du traitement, (iii) le manquement à l'obligation d'assurer la sécurité des

données, et (iv) le manquement à l'obligation de communiquer aux personnes concernées la survenance d'une violation de données.

La qualité de responsable de traitement

En premier lieu, la CNIL rappelle qu'aux termes de l'art. 4 al. 7 RGPD, le responsable de traitement est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».

Dans le cas d'espèce, si les sociétés ne contestent pas être responsables du traitement, elles reprochent au rapporteur d'imputer indistinctement des manquements aux sociétés sans prendre en compte leurs traitements et leurs responsabilités respectifs. Sur ce point, la formation restreinte de la CNIL précise que les sociétés sont des filiales du même groupe et que certaines mesures de sécurité étaient communes aux deux sociétés.

Toutefois, comme les manquements reprochés auxdites sociétés concernent des traitements dont elles sont seules responsables (gestion des abonnés mobiles), deux procédures de sanction autonomes ont été engagées à l'encontre des sociétés FREE MOBILE et FREE.

L'obligation de conserver les données pour une durée proportionnée à la finalité du traitement (art. 5 para. 1 let. e RGPD)

Lors du contrôle de la société FREE MOBILE, il a été relevé que la société n'avait pas mis en place de mesures permettant de trier les données de ses anciens abonnés et que cette dernière conservait les données à caractère personnel de millions d'anciens abonnés pendant une durée excessive. Au titre de l'art. 5 para. 1 let. e RGPD, les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. La CNIL précise également qu'il incombe au responsable du traitement de définir une durée de conservation conforme à la finalité du traitement et que, lorsque cette finalité est atteinte, les données doivent être supprimées, anonymisées ou faire l'objet d'un archivage intermédiaire.

En l'espèce, FREE MOBILE avance qu'elle conservait les données à caractère personnel de ses abonnés tant qu'un contrat, principal ou accessoire, était en cours et qu'elle conservait les données pendant dix ans pour s'acquitter d'obligations comptables, tel que le recommande le référentiel relatif aux traitements mis en œuvre aux fins de gestion des activités

commerciales publié par la CNIL en 2021. Toutefois, la société reconnaît que son mécanisme de purge des données n'était pas pleinement opérationnel et que l'architecture de son système d'information s'accordait difficilement avec des opérations de purge à grande échelle.

La formation restreinte précise alors que des difficultés ou défaillances techniques n'exonèrent pas la société de sa responsabilité de s'assurer du tri ou de la suppression des données aux échéances de leurs durées de conservation telles qu'elle les a elle-même définies. De plus, les données des abonnées conservées pour s'acquitter d'obligations comptables et les données des contrats après la résiliation de ces derniers étaient toutes deux, conservés pendant des durées supérieures à dix et cinq ans, sans justification, ce qui est manifestement excessif et constitue un manquement à l'art. 5 para. 1 let. e RGPD.

L'obligation d'assurer la sécurité des données (art. 32 RGPD)

En premier lieu, la formation restreinte rappelle l'analyse de la CJUE retenant que le RGPD instaure un régime de gestion des risques et qu'il ne prétend nullement éliminer les risques de violations des données à caractère personnel (*cf.* C-340/21 « VB » du 14 décembre 2023, points 29 à 31, commentée *in* swissprivacy.law/230/).

En ce sens, l'art. 32 du RGPD impose une obligation de moyens au responsable de traitement, qui est tenu de prendre des mesures permettant à la fois de réduire la probabilité de la survenance d'une violation de données et, cas échéant, d'en atténuer la gravité (*cf.* Guide de la sécurité des données personnelles de la CNIL ; Guide d'hygiène informatique de l'ANSSI). La CJUE précise que cette obligation de moyens doit s'apprécier en deux temps. Dans un premier temps, identifier les risques de violation des données à caractère personnel induits par le traitement concerné et leurs éventuelles conséquences pour les droits et libertés des personnes physiques. Dans un second temps, vérifier si les mesures mises en œuvre par le responsable de traitement sont adaptées à ces risques compte tenu de l'état des connaissances, des coûts de mise en œuvre ainsi que de la nature, de la portée, du contexte et des finalités de ce traitement (cf. C-340/21 « VB » du 14 décembre 2023, point 42).

Par conséquent, la simple survenance d'une violation de données ne caractérise pas à elle seule, un manquement à l'art. 32 RGPD. Toutefois, si celle-ci a été rendue possible ou facilitée par l'absence ou l'insuffisance des mesures de sécurité mises en œuvre par le responsable de traitement, ce dernier peut être sanctionné au titre de cette disposition. En complément, la CNIL ajoute que le Conseil d'État a confirmé à plusieurs reprises que le manque-

ment à l'art. 32 RGPD peut être caractérisé à la lumière des recommandations de l'Autorité (*cf.* CE, n°472864 « Commune de Beaucaire » du 30 avril 2024).

Sur les risques du traitement pour les personnes concernées, les sociétés estiment que les traitements ne présentaient pas de risque élevé puisqu'ils ne concernaient pas des données sensibles (art. 9 RGPD) et que la compromission des IBAN seuls, ne permet pas de réaliser des prélèvements frauduleux. *A contrario*, la CNIL ne partage pas complètement cet avis et précise que l'accès non autorisé ou la divulgation des données traitées par les sociétés est de nature à créer un préjudice moral et matériel pour les personnes concernées tel que la revente de leurs données, une usurpation d'identité ou des tentatives d'hameçonnage. La formation restreinte ajoute que les IBAN sont des données « hautement » personnelles et qu'une personne disposant d'un IBAN usurpé, peut tout de même procéder à un paiement frauduleux sur un site internet par l'intermédiaire d'une simple case à cocher.

Sur le niveau de sécurité déployé par les sociétés, l'ANSSI rappelle que les entités doivent adopter des mesures spécifiques au nomadisme dans leurs politiques de sécurité du système d'information. Pour cela, il est nécessaire de mettre en œuvre un VPN entre le poste nomade et le système d'information interne de l'entité et de prévoir une authentification multifacteur forte des utilisateurs. En l'espèce, l'absence de mise en œuvre de ces mesures est reprochée aux deux sociétés.

En outre, sur l'absence de détection des comportements anormaux, la CNIL et l'ANSSI rappellent que la mise en place d'un dispositif de journalisation est un prérequis indispensable en ce qu'il participe au respect de l'obligation de sécurisation de tout traitement de données à caractère personnel et permet de détecter, d'analyser et de répondre aux incidents de sécurité (*cf.* Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation ; Guide ANSSI, Recommandations de sécurité pour l'architecture d'un système de journalisation). En l'espèce, bien que les sociétés aient pris des mesures au cours de la procédure permettant de mettre fin aux manquements constatés, les mesures mises en œuvre par ces dernières pour détecter les connexions frauduleuses à leur VPN et les comportements suspects sur leurs réseaux internes, étaient insuffisantes au jour du contrôle.

En complément, il est reproché à la société FREE MOBILE de ne pas avoir pris les mesures nécessaires pour assurer la confidentialité du stockage des mots de passe des utilisateurs de son outil de gestion clientèle, bien que cette vulnérabilité n'ait pas été exploitée par l'attaquant dans le cadre de la violation (*cf.* Délibération n° 2022-100 du 21 juillet 2022

portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés, et abrogeant la délibération n°2017–012 du 19 janvier 2017 ; Guide ANSSI, Recommandations relatives à l'authentification multifacteur et aux mots de passe).

Par conséquent, ces différents manquements ont facilité la survenance de cette violation de données et constituent une violation des dispositions de l'art. 32 RGPD.

L'obligation de communiquer aux personnes concernées la survenance d'une violation de données (art. 34 RGPD)

Il est reproché aux sociétés que le courriel d'information adressé aux personnes concernées par la violation de données ne fournissait aucune indication sur les mesures de remédiation déployées, les conséquences probables de la violation de données, ou les précautions à adopter par les personnes concernées pour atténuer les risques induits.

En ce sens, l'art. 34 para. 1 RGPD précise 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. » et le para. 2 ajoute les mentions qui doivent obligatoirement figurer dans le contenu de cette communication en renvoyant à l'art. 33 para. 3 let. b, c et d RGPD.

Dans la continuité, le considérant 86 précise que cette communication doit « formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels » et comme le précise le Comité européenne de la protection des données (CEPD), « l'objectif principal [de l'art. 34 RGPD] est d'aider les personnes concernées à comprendre la nature de la violation ainsi que les mesures qu'elles peuvent mettre en place pour se protéger » (*cf.* CEPD, Lignes directrices 09/2022 sur la notification de violations de données à caractère personnel en vertu du RGPD, point 83).

Plus concrètement, les informations devant figurer *a minima* dans un premier niveau d'information d'une notification de violation de données sont les suivantes :

- la description de la nature de la violation de données, avec si possible, les catégories et le nombre approximatif de personnes concernées par la violation ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

- les conséquences probables de la violation de données à caractère personnel, et
- les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Le responsable de traitement peut également choisir de fournir des informations complémentaires à celles-ci (*cf.* CEPD, Lignes directrices 09/2022 sur la notification de violations de données à caractère personnel en vertu du RGPD, point 87).

En l'espèce, les sociétés ont adressé un premier courriel d'information, constituant un premier niveau d'information, en insérant dans ce courriel un numéro gratuit ainsi qu'un système de « ticket DPO » afin de répondre aux questions complémentaires des personnes, constituant un second niveau d'information.

Toutefois, la formation restreinte reproche aux sociétés l'utilisation de formulations trop vagues et, par conséquent, l'absence de plusieurs éléments importants, comme une description des principales mesures correctives prises pour remédier à la violation de données en cause, une mention indiquant que les comptes compromis ont été révoqués, que les vulnérabilités liées à leur outil métier ont été corrigées et que l'accès aux données à caractère personnel a été renforcé. L'Autorité ajoute qu'un renvoi vers la page dédiée du site cybermalveillance.gouv.fr aurait été plus pertinent.

Cela est d'autant plus regrettable puisque les sociétés avaient bien identifié les différents risques et recommandations à mettre en place dans leur notification initiale auprès de la CNIL et que la description des mesures de sécurité mises en œuvre par un organisme ne présente pas toutes un risque pour la sécurité d'un système d'information et peuvent, par conséquent, être partagées.

Pour ces raisons, un manquement à l'art. 34 RGPD a été caractérisé à l'encontre de ces deux sociétés.

Conclusion

Ces décisions s'inscrivent dans la continuité de la doctrine de la CNIL et illustrent qu'avant de prendre des sanctions, l'Autorité met en balance l'intégralité des manquements reprochés, leur gravité et le nombre de personnes concernées. En effet, ce que la CNIL sanctionne dans cette décision c'est l'ampleur de la violation de données en raison du nombre

très important de personnes concernées et l'insuffisance des mesures de sécurité déployées par les sociétés.

On retrouve également dans la décision à l'encontre de la société FREE MOBILE, un aveu de non-conformité. La société FREE MOBILE reconnaît que son activité a débuté en 2012, mais que la question de la suppression des données ne s'est posée que très récemment. Rappelons-le, le RGPD est entré en application le 25 mai 2018.

Cela illustre une triste réalité : les entreprises, même de grandes tailles, n'ont pris les sujets de protection des données au sérieux que très tardivement et la conformité reste souvent un sujet annexe dans la gouvernance des entreprises, au lieu d'en être le cœur.

Il y a donc une réelle nécessité d'anticiper les risques et de prévoir sa gouvernance en amont de la mise en œuvre de tout traitement, à la fois pour éviter ce type de sanction, mais surtout pour protéger la vie privée des individus. Soulignons qu'au-delà du risque de sanction financière, un préjudice réputationnel et une perte de confiance des clients sont également des risques à considérer.

En outre, il est ainsi important de retenir de ces décisions les obligations de transparence en cas de violation et d'information des personnes concernées de manière claire et complète, de mettre en place des durées de conservation adéquates afin de diminuer le risque d'attaque et la nécessité d'investir dans la détection et la réponse aux incidents.

Au surplus, notons que l'opérateur conteste la sévérité de la sanction et a annoncé avoir déposé un recours devant le Conseil d'État. A suivre …

Proposition de citation : Clarence Tocchio, Violation de données : La CNIL sanctionne les sociétés FREE MOBILE et FREE à hauteur de 42 millions d'euros, 4 mars 2026 *in* www.swissprivacy.law/397