_swissprivacy.law

Fuite de données hautement sensibles : amende salée pour le sous-traitant

Zarmine Hussain, le 19 juin 2022

À la suite d'une fuite massive de données médicales hautement sensibles, la CNIL sanctionne, par décision du 15 avril 2022, la société Dedalus Biologie pour manquement à ses obligations de protection des données en qualité de sous-traitant.

Délibération de la formation restreinte n° SAN-2022–009 du 15 avril 2022 concernant la société DEDALUS BIOLOGIE.

Le 23 février 2021, le journal Libération révèle une fuite de données « d'une ampleur inédite en France » concernant des données médico-administratives d'environ 500'000 personnes.

Parmi les données piratées et diffusées en ligne, figurent des données de patients hautement sensibles, notamment des données relatives à des pathologies (p. ex. VIH, cancer et maladies génétiques), à la grossesse, à des traitements médicamenteux ainsi qu'à des données génétiques.

À la suite de ces révélations, la Commission Nationale de l'Informatique et des Libertés (CNIL) mène une enquête et contrôle la société Dedalus Biologie, qui commercialise des solutions logicielles de gestion de laboratoire médical. En parallèle, en date du 1er mars 2021, la CNIL saisit le Tribunal Judiciaire de Paris afin de bloquer l'accès au site web sur lequel figure les données piratées, ce qui permet de limiter les conséquences de la fuite.

Au cours des enquêtes, il ressort que la fuite provient d'une intrusion au sein d'un serveur informatique de Dedalus Biologie, qui a eu lieu lors de la migration de données.

Ainsi, le 15 avril 2022, la CNIL conclut à la violation par Dedalus Biologie de ses obligations en qualité de sous-traitant (au sens des art. 28 par. 3, 29 et 32 RGPD) et prononce une amende contre la société susmentionnée d'un montant de EUR 1,5 million.

Contrat de sous-traitance

Premièrement, en qualifiant Dedalus Biologie de sous-traitant au sens de l'art. 4 par. 8 RGPD et en considérant que les conditions générales de vente et que le contrat de maintenance

transmis par cette dernière à ses clients font office de cadre contractuel au sens de l'art. 28 par. 3 RGPD, la CNIL reproche à Dedalus Biologie l'absence des mentions prévues par l'art. 28 par. 3 let. a à h RGPD.

Dedalus Biologie soutient que le responsable de traitement est également tenu de prévoir un contrat de sous-traitance qui répond aux conditions de l'art. 28 par. 3 RGPD. La CNIL considère toutefois que cette double responsabilité n'exonère pas le sous-traitant d'une responsabilité propre de prévoir un tel contrat. Partant, Dedalus Biologie a violé ses obligations au sens de l'art. 28 par. 3 RGPD.

Traitement sur instructions du responsable de traitement

Deuxièmement, lorsqu'à la demande de deux laboratoires, qualifiés de responsables du traitement, Dedalus Biologie migre des données d'une solution informatique vers une autre, elle extrait un volume de données excédant les instructions de ses clients, en violation de l'art. 29 RGPD. La CNIL considère que l'utilisation par le sous-traitant d'une solution informatique inadaptée ne justifie pas l'outrepassement des instructions des responsables de traitement, et que des mesures de suppression des données auraient, au moins, dû être prises.

Sécurité des données

Troisièmement, la CNIL constate que malgré des alertes provenant d'un ancien salarié en mars 2020 et de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en novembre 2020, Dedalus Biologie a omis d'instaurer des mesures de sécurité suffisantes pour encadrer son serveur « FTP MEGABUS », ce qui a finalement permis aux tiers non autorisés d'accéder aux données, ainsi que de les diffuser.

En précisant que les données sensibles nécessitent de par leur nature des mesures de sécurité particulières, la CNIL reproche à Dedalus Biologie notamment l'absence : (i) de procédure spécifique s'agissant des opérations de migration de données ; (ii) de chiffrement des données à caractère personnel figurant sur le serveur FTP MEGABUS ; (iii) d'effacement automatique des données du premier logiciel suite à la migration ; (iv) d'authentification nécessaire afin d'accéder à la zone publique du serveur depuis Internet ; et (vi) de procédure de contrôle et de remontée d'alertes de sécurité sur le serveur. Elle lui reproche également l'utilisation par plusieurs salariés de comptes utilisateurs partagés sur la zone privée du serveur.

Par conséquent, la CNIL considère qu'en raison de ces défauts de sécurité à l'origine de

l'intrusion sur son serveur FTP MEGABUS, Dedalus Biologie a violé ses obligations d'assurer la sécurité des données au sens de l'art. 32 RGPD.

Analyse sous l'angle du droit suisse

Bien que les obligations du sous-traitant soient moins détaillées dans la LPD qu'à l'art. 28 par. 3 RGPD, l'art. 10a LPD ainsi que l'art. 9 al. 1 nLPD prévoient également (entre autres) la mise en place d'une convention au sujet de la sous-traitance des traitements de données.

Selon l'art. 10a al. 2 LPD, le responsable du traitement a une obligation de diligence, et doit s'assurer que le sous-traitant respecte le standard de sécurité nécessaire. Le sous-traitant a également l'obligation de respecter les mêmes normes que le responsable du traitement en matière de sécurité des données (art. 8 OLPD).

En outre, l'art. 8 al. 1 nLPD prévoit expressément l'obligation du sous-traitant d'assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données par rapport au risque encouru.

Bien que le droit actuel ne prévoie pas d'amende pénale pour une telle violation de sécurité par le sous-traitant, sur plainte, l'art. 61 let. c nLPD prévoit une amende pénale en cas de violation intentionnelle des exigences minimales en matière de sécurité des données édictées par le Conseil fédéral au sens de l'art. 8 al. 3 nLPD.

Dans la mesure où l'art. 8 al. 1 nLPD prévoit une responsabilité propre du sous-traitant d'assurer un niveau de sécurité adéquat des données qui lui sont confiées, le sous-traitant qui viole intentionnellement les exigences minimales de sécurité risque également d'être sujet à une amende au sens de l'art. 61 let. c nLPD.

Finalement, bien que cet aspect ne soit pas adressé dans la décision de la CNIL, on ne saurait faire abstraction de la responsabilité pénale du responsable du traitement dans un cas similaire au cas d'espèce. En effet, l'art. 61 let. b nLPD prévoit une amende pénale dans l'hypothèse où un responsable du traitement confie intentionnellement le traitement de données personnelles à un sous-traitant sans s'assurer que ce dernier soit en mesure de garantir la sécurité des données (art. 9 al. 2 nLPD). Cette infraction trouve son origine dans le fait que tant le RGPD (art. 28 par. 1) que la LPD (art. 10a al. 2) et que la nLPD (art. 9 al. 2) imposent au responsable du traitement de s'assurer que le sous-traitant garantisse la sécurité des données. Ainsi, dans une telle situation, le responsable du traitement pourrait être sanctionné pénalement pour un éventuel manquement à ses propres obligations vis-à-vis du

sous-traitant.

Proposition de citation : Zarmine Hussain, Fuite de données hautement sensibles : amende salée pour le sous-traitant, 19 juin 2022 *in* www.swissprivacy.law/153