**FAITS** : la société DEDALUS BIOLOGIE commercialise des solutions logicielles à destination de laboratoires d'analyses médicales, ces logiciels visent à faciliter le traitement des données médicales des patients. La société est sous-traitante des données médicales de ses clients, et les laboratoires d'analyses médicales clients sont responsables de traitements de données. Le 23 février 2021 un article de presse révèle que les informations médicales de près de 500 000 patients français ont été volées à des laboratoires d'analyses clients de la société DEDALUS BIOLOGIE et ont été diffusées en ligne

**PROCEDURE** : Le 24 février la CNIL (Commission nationale de l'informatique et des libertés) effectue une mission de contrôle en ligne au cours de laquelle elle constate que de nombreuses données personnelles sensibles (numéro de mutuelles des patients, noms, prénoms, adresses, pathologies…) sont disponibles sur le net. Le 1er mars 2021 une mission de contrôle sur place dans les locaux de la société est effectuée par les agents de la CNIL et elle fait délivrer une assignation en référé d'heure à heure aux fournisseurs d'accès Internet français afin que le fichier internet contenant ces données ne soit plus librement accessible en ligne. La présidente de la CNIL désigne, le 6 octobre 2021 mr Pellegrini en qualité de rapporteur sur cette affaire, il notifie la société DEDALUS BIOLOGIE le 9 décembre 2021 d'un rapport détaillant les manquements aux RGPD qu'il estimait constitués par la situation présente. C'est finalement le 15 avril 2022 qu'est tenue la séance de la formation restreinte de la CNIL statuant sur les potentiels manquements aux obligations du RPGD dont la société DEDALUS BIOLOGIE se serait rendue coupable et sur les potentiels sanctions à adopter.

**PROBLEMES DE DROIT** : Quelles sont, pour le sous-traitant, les conséquences du manque d'encadrement juridique des traitements effectués pour le compte d'un responsable de traitement ?

Quid des conséquences du traitement d'un volume excessif de données ?

Quelles sont les conséquences de manquements à l'obligation d'assurer la sécurité des données ?

Quel est le montant maximal encouru pour des violations multiples du RPGD dans le traitement de données sensibles ?

**SOLUTION** : La CNIL constate dans sa délibération du 15 avril 2022 plusieurs manquements aux obligations du RPGD, plus précisément aux articles 28 paragraphe 3 relatif à l'obligation de mettre en place un contrat entre le responsable de traitement et son sous-traitant, l'article 29 relatif aux traitements effectués sous autorité du responsable de traitement de données et enfin l'article 32 relatif lui à la sécurité de ces traitements. En conséquence de ces multiples et graves manquements aux obligations du RPGD la CNIL sanctionne la société DEDALUS BIOLOGIE à une amende de 1 500 000 euros et à la publicité nominative de cette délibération pendant 2 années à compter du jour de la publication de cette délibération.

**SOURCES :**

Article 9 RGPD - Traitement portant sur des catégories particulières de données à caractère personnel

Article 28 RGPD - Sous-traitant

Article 29 RGPD- Traitement effectué sous l'autorité du responsable du traitement ou du sous-traitant

Article 32 RGPD - Sécurité du traitement

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article28

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

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000045614368

« Délibération de la CNIL du 15 avril 2022, sanction de 1,5 millions d'euros pour un éditeur-intégrateur de progiciel à destination des laboratoires d'analyse médicale »

DUJARDIN EVE-ANNE, QUINIOU VALENTINE, Simon associés, publié le 12/05/2022

https://www.simonassocies.com/deliberation-de-la-cnil-du-15-avril-2022-sanction-de-15-millions-deuros-pour-un-editeur-integrateur-de-progiciel-a-destination-des-laboratoires-danalyse-medicale/

« délibération CNIL 15 avril 2022 un leak de données sensibles »

Marc-Antoine LEDIEU Publié le 25/05/2022

https://technique-et-droit-du-numerique.fr/deliberation-cnil-15-avril-2022-un-leak-de-donnees-sensibles-suite-a-une-cyber-attaque/

**NOTE** :

Il s'agit ici d'une affaire majeure à plusieurs niveaux, que ce soit en matière d'illustration des changements qu'apporte la nécessité de se conformer aux règles du RGPD pour les sous-traitant de données, les risques encourus en cas de brèche de sécurité dans les logiciels de traitements de données et enfin le durcissement de la jurisprudence de la CNIL en cas de non-conformité répétée aux règles du RGPD.

***Le non-respect des mentions écrites (28 RGPD) et le non-respect par le sous-traitant des instructions du responsable de traitement (29 RGPD)***

La CNIL constate tout d'abord la qualité de sous-traitant de données informatiques de la société DEDALUS BIOLOGIE, puis rappelle que le fait d'être sous-traitant n'exempte pas cette dernière de suivre toutes les recommandations du RPGD en matière de traitement de données (proportionnalité, sécurité, loyauté…), surtout quand il s'agit de données définies comme « sensibles » par l'article 9 du RGPD qui précise que ces la fuite de ces données (médicales en l'espèce) pourraient porter un grave préjudice morale aux personnes concernées en plus de les exposer à de potentielles usurpations d'identités ou divers chantages.

La CNIL observe ensuite qu'il n'est nulle part fait mention des obligations listées par l'article 28 paragraphe 3 du RGPD dans les contrats conclus entre la société DEDALUS BIOLOGIE et ses clients, à savoir notamment que :

« Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement. Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant :

a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ».

La conséquence de ce manquement constaté par la CNIL est une violation flagrante de l'article 28 paragraphe 3 du RGPD. La CNIL constate également un autre manquement, celui posé par l'article 29 du RGPD et disposant que le sous-traitant ayant accès à des données à caractère personnel pour lesquelles on ne lui a demandé aucun traitement, ne peut en principe pas traiter ces données à moins d'y être obligé par le responsable de traitement ou par un Etat membre.

En l'espèce la société défenderesse à procédé au traitement de nombre de données personnelles pour lesquelles le responsable de traitement n'avait exigé aucun traitement, et en conséquence « Le rapporteur en conclut que la société DEDALUS BIOLOGIE a traité des données au-delà des instructions données par les responsables de traitement, ce qui constitue un manquement à l'article 29 du RGPD ».

L'argument avancé par la société défenderesse est qu'elle usait d'un logiciel daté technologiquement et qui ne permettait pas de séparer en catégories distinctes les différents types de données personnelles. Il n'en reste pas moins qu'elle ne pouvait procéder au traitement de ces données sans l'autorisation expresse de son responsable de traitement et aurait dû user d'un autre logiciel lui permettant de respecter l'article 29 du RGPD, ou à minima transférer toutes les données vers le document destinataire puis en supprimer les données superflues à caractère personnel.

***Le manquement à l'obligation de sécurité (32 RGPD)***

Le manquement à l'obligation de sécurité du traitement des données est la raison pour laquelle la brèche de sécurité subie par la société défenderesse s'est produite. La CNIL constate ainsi que la société DEDALUS BIOLOGIE procédait au traitement de données sensibles en « l'absence de procédure spécifique s'agissant des opérations de migration de données, l'absence de chiffrement des données à caractère personnel stockées sur le serveur FTP MEGABUS, l'absence d'effacement automatique des données après migration vers un autre logiciel, l'absence d'authentification requise depuis Internet pour accéder à la zone publique du serveur FTP MEGABUS ». Facteur aggravant, un ex-salarié ayant tenté de faire remonter ces failles de sécurité à ses supérieurs de DEDALUS BIOLOGIE en 2020 a été ignoré par sa hiérarchie qui ne semblait alors pas faire grand cas de la nécessité de se conformer aux règlements du RGPD.

L'article 32 mentionne que ces obligations de sécurité doivent être mises en œuvre proportionnellement aux moyens à dispositions et à l'importance du traitement des données, il s'agissait en l'espèce d'une société réalisant plusieurs millions d'euros de bénéfices net par exercices fiscaux et ne jugeant pas nécessaire de respecter des principes de base de sécurité informatique alors même qu'elle gère le traitement de données hautement sensibles.

***La sévérité de la sanction prononcée par la CNIL***

La CNIL précise que ce n'est pas simplement du fait des graves conséquences sur la vie de nombreux patients français que cette fuite d'information a causé que sa sanction est calculée. Elle prend

également en compte la multiplicité des violations du RGPD, leur aspect répété malgré des tentatives d'avertissement en interne, et enfin leur gravité dû au non-respect de certains principes élémentaires de sécurité dans le domaine informatique. C'est en prenant tous ces éléments en compte qu'elle inflige une amende de 1 500 000 euros à la société DEDALUS BIOLOGIE en plus d'une publicité de cette sanction mentionnant nominativement la société en question pendant 2 ans à compter de la publication de cette délibération le 15/05/2022.

C'est une amende lourde pour une société qui déclarait en bénéfices net la somme de 1 437 017 euros en 2020. Elle cherche indiscutablement à envoyer un signal fort aux entreprises offrant des services similaires à la société défenderesse et tardant à se mettre en conformité avec les règlements du RGPD, nul doute que les proportions prises par cette affaire ont aidé à sensibiliser les entreprises sur ces sujets.

Odran AMAUDRIC DU CHAFFAUT

Master 2 Droit des médias électroniques

AIX MARSEILLE UNIVERSITE IREDIC 2022

**ARRET :**

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

**B. Sur les manquements au regard du RGPD**

**1. Sur le manquement à l'obligation d'encadrer par un acte juridique formalisé les traitements effectués pour le compte du responsable de traitement**

37. En troisième lieu, la formation restreinte prend note que la société DEDALUS BIOLOGIE a déployé de nouveaux modèles de contrat de sous-traitance et a entamé des démarches pour se mettre en conformité avec les dispositions de l'article 28 du RGPD. Pour autant, il n'en demeure pas moins que la société a entamé des démarches auprès de ses clients dans le cadre de la présente procédure et qu'elle n'était pas en conformité au moment des constatations effectuées par la CNIL. Elle ne l'est d'ailleurs toujours pas s'agissant de certains contrats, puisque la société a indiqué, dans ses dernières observations, poursuivre ses actions visant à transmettre à l'ensemble de ses clients les contrats mis à jour et à les négocier le cas échéant.

38. Dès lors, au regard de l'ensemble de ces éléments, la formation restreinte considère que ces faits constituent un manquement à l'article 28, paragraphe 3, du RGPD, que la société ne conteste pas au demeurant.

(…)

**2. Sur le manquement à l'obligation pour le sous-traitant de ne traiter les données à caractère personnel que sur instruction du responsable de traitement**

48. La formation restreinte relève en outre que la société prétend, s'agissant de […], avoir eu " un " retour d'email " confirmant la conformité dudit fichier aux instructions du laboratoire ". Cette affirmation est inexacte puisque, d'après le " ticket SAV ", le " retour de mail " émane de la société […], société tierce éditant et maintenant un autre logiciel vers lequel les données extraites devaient être migrées. Ainsi, ce courriel ne saurait valoir validation de l'extraction par le client, dans la mesure où la société […] est une société tierce.

49. En troisième lieu, la formation restreinte considère que la société ne saurait se prévaloir d'un outil inadapté pour justifier d'avoir outrepassé les instructions des responsables de traitement. Elle aurait pu, par exemple, opter pour un autre outil lui permettant de respecter les instructions données par ses clients, comme elle indique le faire désormais, ou a minima supprimer toutes les données qui n'auraient pas dû être extraites.

50. Compte tenu de ces éléments, la formation restreinte considère que la société DEDALUS BIOLOGIE a traité des données au-delà des instructions données par les responsables de traitement, ce qui constitue un manquement à l'article 29 du RGPD.

(…)

**3. Sur le manquement à l'obligation d'assurer la sécurité des données**

69. Ainsi, l'absence de mise en place de mesures de sécurité protégeant le serveur en cause - notamment l'absence de chiffrement, l'absence d'effacement automatique des données après leur migration, l'absence d'authentification requise depuis Internet pour accéder à la zone publique du serveur et l'utilisation de comptes utilisateurs partagés - a conduit à rendre accessibles lesdites données à des tiers, et ce malgré des alertes préalables à la violation de données à caractère personnel ayant conduit à la divulgation d'un fichier contenant les données médico-administratives de près de 500 000 personnes.

70. Dès lors, la formation restreinte considère que la société DEDALUS BIOLOGIE a méconnu son obligation résultant des dispositions de l'article 32 du Règlement, ce que la société ne conteste pas au demeurant.

(…)

**III. Sur la sanction et la publicité**

85. La formation restreinte rappelle également que les amendes administratives doivent être dissuasives mais proportionnées. Elle considère en particulier que l'activité de la société et sa situation financière doivent être prises en compte pour la détermination de la sanction et notamment, en cas d'amende administrative, de son montant. Elle relève à ce titre que la société fait état d'un chiffre d'affaires de 18,8 millions d'euros en 2019 et de 16,3 millions d'euros en 2020, pour un résultat net s'élevant à 2 226 949 euros en 2019 et à 1 437 017 euros en 2020.

86. Au vu de ces éléments, la formation restreinte considère que le prononcé d'une amende de 1 500 000 euros apparaît justifié.

87. En troisième lieu, s'agissant de la publicité de la sanction, la société indique que la cyberattaque qui l'a impliquée a fait l'objet d'une publicité très importante, puisque plusieurs articles de presse ont été publiés, puis relayés tant dans la presse papier que télévisuelle, en France et à l'étranger. L'incident a également fait l'objet de plusieurs communications de la part de la CNIL. Elle ajoute que cette médiatisation aura des effets particulièrement néfastes pour elle, non seulement dans le cadre de son activité, mais encore sur son chiffre d'affaires.

88. Compte tenu de la gravité des manquements commis, particulièrement des manquements relatifs à la sécurité, du nombre de personnes concernées et des conséquences pour celles-ci, la formation restreinte considère que la publicité de la décision se justifie.

**PAR CES MOTIFS**

La formation restreinte de la CNIL, après en avoir délibéré, décide de :

- **prononcer à l'encontre de la société DEDALUS BIOLOGIE une amende administrative d'un montant de 1 500 000 (un million cinq cent mille) euros ;**

**- rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération, qui n'identifiera plus nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.**

Le président

Alexandre LINDEN