Délibération SAN-2022-009 du 15 avril 2022

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Etat juridique : En vigueur

Date de publication sur Légifrance : Jeudi 21 avril 2022

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

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Monsieur Alexandre LINDEN, président, Monsieur Philippe-Pierre CABOURDIN, vice-président, Madame Anne DEBET, Madame Christine MAUGÜÉ, Monsieur Bertrand du MARAIS et Monsieur Alain DRU, membres ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants ;

Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2021-028C de la présidente de la Commission nationale de l'informatique et des libertés du 24 février 2021 de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification de tout traitement accessible à partir des domaines […] ou portant sur des données à caractère personnel collectées à partir de ces derniers ;

Vu la décision n° 2021-029C de la présidente de la Commission nationale de l'informatique et des libertés du 25 février 2021 de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification auprès des sociétés DEDALUS FRANCE et DEDALUS BIOLOGIE ;

Vu la décision n° 2021-031C de la présidente de la Commission nationale de l'informatique et des libertés du 2 mars 2021 de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification de tout traitement de données à caractère personnel accessible en ligne et qui serait en lien avec les faits relatés par le journal Libération dans son article intitulé Les informations confidentielles de 500 000 patients français dérobées à des laboratoires ;

Vu la décision n° 2021-034C de la présidente de la Commission nationale de l'informatique et des libertés du 5 mars 2021 de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification auprès de la société […] ;

Vu la décision n° 2021-035C de la présidente de la Commission nationale de l'informatique et des libertés du 5 mars 2021 de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification auprès de la société […] ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 6 octobre 2021 ;

Vu le rapport de Monsieur François PELLEGRINI, commissaire rapporteur, notifié à la société DEDALUS BIOLOGIE le 9 décembre 2021 ;

Vu les observations écrites versées par le conseil de la société DEDALUS BIOLOGIE le 24 janvier 2022 ;

Vu la réponse du rapporteur à ces observations notifiée le 7 février 2022 au conseil de la société ;

Vu les observations écrites versées par le conseil de la société DEDALUS BIOLOGIE reçues le 21 février 2022 ;

Vu les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 10 mars 2022 :

- Monsieur François PELLEGRINI, commissaire, entendu en son rapport ;

En qualité de représentants de la société DEDALUS BIOLOGIE :

- […]

La société DEDALUS BIOLOGIE ayant eu la parole en dernier ;

Après en avoir délibéré, la formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La société DEDALUS BIOLOGIE (ci-après " la société ") est une société par actions simplifiée à associé unique immatriculée au registre du commerce et des sociétés de Strasbourg sous le numéro 348 585 233 depuis le 1er décembre 1988. Elle a pour activité l'édition de logiciels applicatifs. Elle compte entre dix et dix-neuf salariés.

2. La société DEDALUS BIOLOGIE fait partie du groupe DEDALUS, qui emploie environ neuf cents personnes et qui est composé, en France, de cinq sociétés.

3. La société DEDALUS BIOLOGIE commercialise des solutions logicielles à destination de laboratoires d'analyses médicales, appelées solutions de gestion de laboratoire. Environ trois mille laboratoires de biologie médicale privés et entre trente et cinquante laboratoires d'analyses d'établissements publics de santé sont équipés des solutions éditées par la société DEDALUS BIOLOGIE.

4. À ce jour, cinq logiciels sont commercialisés, parmi lesquels le logiciel KALISIL. Deux solutions auparavant commercialisées par la société DEDALUS BIOLOGIE ne sont plus maintenues et sont considérées comme obsolètes, parmi lesquelles MEGABUS, dont la " fin de vie " a été atteinte en septembre 2019 selon la société. Les clients utilisateurs de la solution MEGABUS ont été destinataires d'un courrier adressé par la société NETIKA (ancienne dénomination de DEDALUS BIOLOGIE) en 2018 pour les informer de l'" arrêt définitif de la maintenance " de cette solution.

5. Pour l'utilisation des logiciels commercialisés par les sociétés DEDALUS FRANCE et DEDALUS BIOLOGIE, les clients font l'acquisition d'une licence. La société DEDALUS BIOLOGIE assure également des prestations d'installation, de démarrage et d'accompagnement des clients à l'utilisation du logiciel. Un contrat de maintenance est en règle générale conclu pour assurer les mises à jour des solutions, lesquelles incluent notamment de nouvelles fonctionnalités et permettent de maintenir les solutions en conformité avec les normes en vigueur.

6. Le 23 février 2021, un article de presse intitulé " Les informations confidentielles de 500 000 patients français dérobées à des laboratoires et diffusées en ligne " a été publié par le journal Libération. Cet article faisait état de la présence sur un forum d'un lien de téléchargement vers un fichier contenant les données médico-administratives de près de 500 000 personnes : " Selon les spécialistes, la fuite est d'une ampleur inédite en France pour des données ayant trait à la santé. Le fichier en question, que " CheckNews " a pu consulter, contient l'identité complète de près d'un demi-million de Français, souvent accompagnée de données critiques, comme des informations sur leur état de santé ou même leur mot de passe. Initialement partagée sur des forums de pirates informatiques, cette base de données est de plus en plus largement diffusée ".

7. En application de la décision n° 2021-028C de la présidente de la Commission nationale de l'informatique et des libertés (ci-après la " Commission " ou la " CNIL ") du 24 février 2021, la CNIL a effectué une mission de contrôle en ligne afin de vérifier la conformité à la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après la " loi Informatique et Libertés ") et au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le " RGPD " ou le " Règlement ") de tout traitement accessible à partir des domaines […] ou portant sur des données à caractère personnel collectées à partir de ces derniers.

8. Dans le cadre du contrôle en ligne diligenté, le fichier contenant les données médico-administratives a été téléchargé. Il est apparu que les données à caractère personnel de 491 840 patients y figuraient, parmi lesquelles :

- des données d'identification : numéro de sécurité sociale, nom, prénoms, sexe, adresse postale, numéro de téléphone, adresse électronique, date de la dernière visite médicale, date de naissance ;

- deux colonnes de commentaires libres contenant notamment des informations relatives aux pathologies des patients (VIH, cancers, maladies génétiques), à l'état de grossesse, aux traitements médicamenteux suivis par le patient ou encore des données génétiques ;

- des données d'identification du médecin prescripteur : nom, prénom, adresse postale, numéro de téléphone, adresse électronique ;

- des données relatives au préleveur : nom, prénom, adresse, numéro de téléphone ;

- des données relatives à la mutuelle du patient : " Id tiers payant " (suite de chiffres), adresse postale, numéro de téléphone ;

- une colonne " Identifiant SR " et une colonne " MP ", correspondant, au regard de son contenu, aux identifiants et mots de passe utilisés par le patient pour se connecter à son espace.

9. En application de la décision n° 2021-029C de la présidente de la Commission du 25 février 2021, la CNIL a effectué une mission de contrôle sur pièces auprès des sociétés DEDALUS FRANCE et DEDALUS BIOLOGIE, afin de vérifier la conformité à la loi Informatique et Libertés et au RGPD des traitements mis en œuvre par des laboratoires d'analyses médicales au moyen des solutions ou services commercialisés par ces sociétés. Cette mission s'est effectuée par l'envoi d'un questionnaire à la société DEDALUS FRANCE, adressé par courriel le 25 février 2021.

10. Le 26 février suivant, la société a transmis des éléments de réponse à la CNIL, notamment les noms et adresses des laboratoires d'analyses médicales concernés par la violation de données susvisée.

11. En application de la même décision, une délégation de la CNIL a procédé, le 1er mars 2021, à une mission de contrôle sur place dans les locaux de DEDALUS FRANCE, situés 22, avenue Galilée au PLESSIS-ROBINSON (92350), après information du procureur de la République territorialement compétent et de la déléguée à la protection des données de DEDALUS FRANCE et DEDALUS BIOLOGIE.

12. Les 5 mars, 10 mars, 1er avril, 6 avril et 19 avril 2021, les sociétés DEDALUS FRANCE et DEDALUS BIOLOGIE ont transmis les éléments complémentaires sollicités par la délégation lors du contrôle sur place.

13. En parallèle, le 1er mars 2021, la CNIL a fait délivrer une assignation en référé d'heure à heure aux différents fournisseurs d'accès à Internet, afin que soit assuré le blocage effectif du fichier contenant les données de près de 500 000 patients.

14. En application de la décision n° 2021-031C de la présidente de la Commission du 2 mars 2021, la CNIL a effectué une mission de contrôle en ligne le jour même, afin de vérifier la présence du fichier litigieux en ligne, en le recherchant à partir de différents moteurs de recherche.

15. Par ordonnance du 4 mars 2021, le juge des référés du tribunal judiciaire de PARIS a enjoint " à la SA ORANGE, la SAS FREE, la SA SFR et la SA BOUYGUES TELECOM de mettre en œuvre ou de faire mettre en œuvre, sans délai et pour une période de 18 mois à compter de la présente décision toutes mesures les plus adaptées et les plus efficaces de surveillance ciblées de nature à assurer le blocage effectif du service de communication au public en ligne " […] " sur leurs réseaux ".

16. En application des décisions n° 2021-034C et n° 2021-035C de la présidente de la Commission du 5 mars 2021, la CNIL a effectué des missions de contrôle sur place auprès des sociétés […] et […] le 10 mars 2021.

17. Les deux laboratoires ayant été concernés par la violation de données susvisée, il s'agissait de vérifier le respect par ces deux sociétés des dispositions de la loi Informatique et Libertés et du RGPD.

18. Par courriel du 11 juin 2021 adressé à la déléguée à la protection des données des sociétés DEDALUS FRANCE et DEDALUS BIOLOGIE, la délégation de la CNIL a sollicité des éléments complémentaires auprès de ces sociétés, lesquels ont été transmis le 24 juin 2021.

19. Aux fins d'instruction de ce dossier, la présidente de la Commission a, le 6 octobre 2021, désigné Monsieur François PELLEGRINI en qualité de rapporteur sur le fondement de l'article 39 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi du 6 janvier 1978 modifiée.

20. À l'issue de son instruction, le rapporteur a, le 9 décembre 2021, fait notifier à la société DEDALUS BIOLOGIE un rapport détaillant les manquements au RGPD qu'il estimait constitués en l'espèce.

21. Ce rapport proposait à la formation restreinte de la Commission de prononcer à l'encontre de la société une amende administrative, au regard des manquements constitués aux articles 28 paragraphe 3, 29 et 32 du RGPD. Il proposait également que la décision de sanction soit rendue publique, mais qu'il ne soit plus possible d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

22. Par courrier du 10 décembre 2021, la société, par l'intermédiaire de son conseil, a sollicité un délai supplémentaire pour fournir ses observations en réponse. Par courrier du 15 décembre 2021, le président de la formation restreinte lui a accordé un délai supplémentaire jusqu'au 24 janvier 2022.

23. Le 24 janvier 2022, la société a produit des observations en réponse au rapport de sanction.

24. Le rapporteur a répondu aux observations de la société le 7 février 2022. Un courrier était également remis à la société, l'informant que le dossier était inscrit à l'ordre du jour de la formation restreinte du 10 mars 2022.

25. Le 21 février 2022, la société a produit de nouvelles observations en réponse à celles du rapporteur.

26. La société et le rapporteur ont présenté des observations orales lors de la séance de la formation restreinte.

II. Motifs de la décision

A. Sur la qualité de la société à l'égard des traitements en cause

27. Aux termes de l'article 4 du RGPD, le responsable de traitement est défini comme " 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 " (point 7) et le sous-traitant est " la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement " (point 8).

28. Le rapporteur relève que la société DEDALUS BIOLOGIE commercialise des solutions logicielles à destination de laboratoires d'analyses médicales. Dans le cadre du service qu'elle propose aux laboratoires, la société ne fait, d'une part, que mettre à disposition des laboratoires les outils, notamment informatiques, pour faciliter la mise en œuvre des traitements et, d'autre part, agit uniquement au nom et sous la responsabilité des laboratoires pour la maintenance du logiciel et, le cas échéant, la migration vers un autre logiciel par exemple. La société doit donc être regardée comme agissant en tant que sous-traitant des laboratoires au sens de l'article 4, point 8, du RGPD selon le rapporteur.

29. En défense, la société ne conteste pas l'analyse du rapporteur sur ce point.

30. La formation restreinte considère que les notions de responsable de traitement et de sous-traitant doivent faire l'objet d'une appréciation concrète prenant en compte l'ensemble des éléments permettant d'attribuer l'une ou l'autre de ces

qualités à une entité. À ce titre, elle relève qu'il ressort des éléments communiqués à la CNIL que la société DEDALUS BIOLOGIE agit en qualité de sous-traitant des traitements mis en œuvre pour le compte de ses clients, les laboratoires, qui sont responsables de traitement, dans la mesure où elle met à disposition des laboratoires des outils informatiques leur permettant de mettre en œuvre leurs traitements et qu'elle agit, de manière générale, uniquement sur la base de leurs instructions.

31. Il appartient dès lors à la formation restreinte d'examiner, au regard de cette qualité, les griefs formulés par le rapporteur à l'encontre de la société.

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

32. Aux termes de l'article 28, paragraphe 3, du RGPD, " 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, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis ; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;

c) prend toutes les mesures requises en vertu de l'article 32 ;

d) respecte les conditions visées aux paragraphes 2 et 4 pour recruter un autre sous-traitant ; […] ".

33. Le rapporteur considère qu'il ressort des éléments transmis par la société DEDALUS BIOLOGIE que les différents documents encadrant les relations contractuelles entre la société sous-traitante et les laboratoires ne comportent pas les mentions requises par l'article 28 du RGPD. Il relève que les conditions générales de vente proposées par DEDALUS BIOLOGIE au moment où les laboratoires acceptent sa prestation ne comportent aucune des mentions requises par cet article. De même, il note que les mentions requises ne figurent pas non plus dans les contrats de maintenance conclus entre la société et les laboratoires, tels que transmis à la CNIL.

34. En défense, si la société ne conteste pas la matérialité du manquement à l'article 28 du RGPD, elle précise que la conclusion d'un contrat de sous-traitance constitue une obligation tant pour le responsable de traitement que pour le sous-traitant. Elle en conclut que la société DEDALUS BIOLOGIE ne saurait être tenue seule responsable de ce manquement. Elle insiste en outre sur les efforts mis en œuvre pour se conformer au RGPD dès 2018 et indique que de nouveaux modèles de contrat de sous-traitance respectant les exigences de l'article 28 sont en cours de déploiement.

35. En premier lieu, la formation restreinte relève que le fait que l'obligation résultant de l'article 28, paragraphe 3, du RGPD incombe tant au responsable de traitement qu'au sous-traitant est sans incidence sur l'existence d'une responsabilité propre du sous-traitant. Elle note que c'est la société elle-même qui transmet aux laboratoires ses propres conditions générales de vente qui font office d'encadrement contractuel au titre du RGPD.

36. En deuxième lieu, la formation restreinte relève que les conditions générales de vente proposées par DEDALUS BIOLOGIE au moment où les laboratoires acceptent sa prestation, transmises par la société dans le cadre de la procédure de contrôle, ne comportent aucune des mentions requises par l'article 28 du RGPD. De même, elle note que les mentions requises ne figurent pas non plus dans les contrats de maintenance transmis à la CNIL, conclus entre la société et les laboratoires. À titre d'illustration, le contrat de maintenance conclu entre NETIKA SAS (ancienne dénomination de DEDALUS BIOLOGIE) et la société […], le 13 septembre 2019, comporte certes une partie dédiée aux données à caractère personnel, mais qui ne répond pas aux exigences de l'article 28 du RGPD et vise des dispositions obsolètes de la loi Informatique et Libertés. La formation restreinte note en outre que l'exemple de contrat d'assistance et de maintenance, remis par la société à la délégation de la CNIL lors du contrôle sur place du 1er mars 2021, ne contient pas non plus les mentions obligatoires au titre de l'article 28 du RGPD. S'il contient une partie dédiée aux données à caractère personnel, celle-ci ne répond pas aux exigences posées par cet article.

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

39. Aux termes de l'article 29 du RGPD, " Le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre ".

40. Le rapporteur relève que la société DEDALUS BIOLOGIE a extrait un volume de données plus important que celui requis dans le cadre de la migration demandée par ses clients, les laboratoires […] et […]. 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.

41. En défense, la société précise que l'outil d'extraction disponible sur l'ancien logiciel DXLAB ONE, utilisé pour ces migrations, ne permettait que de procéder à une extraction totale du fichier des patients du laboratoire concerné, sans possibilité d'ajouter des filtres sur les champs à exporter pour n'en extraire que certains. Elle ajoute que DEDALUS BIOLOGIE opérait bien la migration des données de ses clients vers une nouvelle solution logicielle en conformité avec leurs instructions, puisqu'une fois le fichier des données à migrer constitué, la société demandait toujours la validation du laboratoire concerné avant d'effectuer la migration. La société en conclut qu'elle a opéré les opérations d'extraction nécessaires à la migration et que le périmètre des données à migrer a été défini à ce titre conformément aux instructions des laboratoires concernés et compte tenu des limitations techniques des outils utilisés à l'époque pour effectuer ces migrations.

42. Dans ses dernières observations en réponse, la société indique qu'elle " n'entend pas minorer la réalité de son manquement à l'obligation de ne procéder à des traitements de données à caractère personnel, en qualité de sous-traitant, que sur les seules instructions du responsable de traitement ". Elle rappelle néanmoins les importants investissements engagés par l'entreprise, depuis plusieurs années, pour développer notamment de nouvelles solutions logicielles. Elle ajoute que c'est justement parce qu'elle était consciente du caractère obsolète du logiciel MEGABUS et des outils de migration associés qu'elle s'est attachée à développer une solution plus innovante et respectueuse des exigences du RGPD et c'est ainsi qu'elle a proposé à ses clients, dès 2018, de passer au logiciel KALISIL.

43. En premier lieu, la formation restreinte relève que, ainsi qu'il sera établi ci-après, les différents éléments recueillis dans le cadre des contrôles des laboratoires […] et […] ont permis d'établir que DEDALUS BIOLOGIE avait extrait un volume de données plus important que celui requis dans le cadre de la migration demandée par ses clients.

44. S'agissant du laboratoire […], le procès-verbal de contrôle sur place mentionne que celui-ci a sollicité, " selon les préconisations de DEDALUS ", la migration de données de la solution MEGABUS (également appelée DXLAB ONE) vers la solution KALISIL pour les patients ayant procédé à une analyse médicale après le 7 mai 2017. Or, les données extraites par la société DEDALUS BIOLOGIE pour cette migration comportaient 8 403 lignes relatives à des patients dont la date de dernière visite était antérieure au 7 mai 2017, ce qui représente 6,5 % de la volumétrie totale.

45. S'agissant du laboratoire […], la formation restreinte relève que, dans le cadre d'un changement de logiciel, le laboratoire a demandé à la société DEDALUS BIOLOGIE de procéder à une extraction de la base des données de patients contenues dans le logiciel DXLAB ONE afin de migrer vers un autre logiciel édité et maintenu par une société tierce. À cette fin, la société […] a fourni à la société DEDALUS une liste des champs à extraire afin d'être importés dans la nouvelle solution logicielle. Les colonnes " commentaire P " (contenant des informations telles que " STERILITE 100 % ", etc.) et " commentaire D " (contenant des informations telles que " TUBERCULOSE OSSEUSE SOUS RIFATER ", " XARELTO " (médicament), " DIABETE ", etc.) ont également été extraites, alors pourtant qu'elles ne figuraient pas dans la liste des champs à extraire.

46. Ainsi, la formation restreinte en conclut que les données extraites par la société DEDALUS BIOLOGIE, incluant notamment les colonnes " commentaire P " et " commentaire D " qui n'auraient pas dû l'être, couvrent un champ plus large que la demande du responsable de traitement.

47. En deuxième lieu, la formation restreinte relève que, s'agissant de la validation des extractions par les laboratoires concernés, la société produit uniquement deux documents intitulés " tickets SAV " à l'appui de ses déclarations, lesquels ne sauraient en réalité suffire à démontrer qu'elle a effectué les opérations d'extraction conformément aux instructions des laboratoires et que les laboratoires ont validé le contenu des extractions réalisées. Ces " tickets SAV " permettent seulement de rendre compte de démarches effectuées par la société DEDALUS auprès de deux laboratoires pour envoyer des fichiers avec des extractions et ne démontrent en rien une validation qui aurait été donnée par les laboratoires concernés.

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

51. Aux termes de l'article 32 du RGPD, " 1. 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 du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite […] ".

52. Le rapporteur relève que, dès mars 2020, un ancien salarié de la société DEDALUS BIOLOGIE avait fait remonter à son employeur des problèmes de sécurité. Selon le rapporteur, il est établi que celui-ci avait bel et bien effectué des signalements pertinents, ce qui ressort d'échanges internes entre […].

53. Le rapporteur note ensuite que, le 4 novembre 2020, l'Agence nationale de la sécurité des systèmes d'information (ci-après " l'ANSSI ") a observé que des données de patients du laboratoire […] étaient mises en vente sur le darknet, sous-réseau d'Internet pourvu de fonctions d'anonymisation et dans lequel toutes les ressources ne sont pas nécessairement indexées par les moteurs de recherche. L'ANSSI a transmis au laboratoire concerné un fichier contenant 56 lignes avec des données à caractère personnel de ses patients. Le jour même, le fichier ainsi que le courriel de l'ANSSI ont été transmis à la société DEDALUS BIOLOGIE par le directeur des systèmes d'information du réseau […], au sein duquel figure le laboratoire […].

54. Le rapporteur relève ensuite que, le 23 février 2021, les informations confidentielles de près de 500 000 patients ont été diffusées sur Internet. Dès le 24 février 2021, la société DEDALUS BIOLOGIE a mandaté la société […] pour mener une mission d'analyse forensique. Ladite société a rendu son rapport d'investigation le 26 mars 2021.

55. Le rapporteur note en outre qu'aux termes de ses investigations, la société DEDALUS BIOLOGIE a établi une correspondance entre les données du fichier transmis par l'ANSSI et les données présentes sur un serveur FTP hébergé sur le serveur de télémaintenance MEGABUS (MEGAEXT). Environ 90 % des données à caractère personnel du fichier objet de la violation, publié sur Internet en février 2021, étaient présentes sur le serveur FTP MEGABUS (MEGAEXT).

56. Selon le rapporteur, de nombreux manquements techniques et organisationnels en matière de sécurité ont été constatés lors des contrôles de la CNIL et peuvent être retenus à l'encontre la société DEDALUS BIOLOGIE. Il note notamment 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, l'utilisation de comptes utilisateurs partagés entre plusieurs salariés s'agissant de la zone privée de ce même serveur et l'absence de procédure de supervision et de remontée d'alertes de sécurité sur le serveur.

57. Le rapporteur en conclut que, malgré des alertes préalables, la société DEDALUS BIOLOGIE n'a pas mis en œuvre de mesures satisfaisantes de sécurité pour encadrer le serveur FTP MEGABUS, ce qui a non seulement permis l'accès aux données concernées par des tiers non autorisés, mais également la divulgation sur des forums d'un fichier contenant les données médico-administratives de près de 500 000 personnes.

58. En défense, la société relève, s'agissant de la violation de données ayant eu lieu en février 2021, que les investigations effectuées par la société […] ont conclu à l'existence d'intrusions sur le serveur FTP de DEDALUS BIOLOGIE. Elle précise cependant que, bien que le rapport relève que 90 % du contenu du fichier circulant sur Internet était également disponible sur le serveur FTP, il convient de noter que, a contrario, le rapport de […] précisait qu'environ 10 % du fichier circulant sur Internet (soit environ 43 000 enregistrements) ne se trouvait pas sur le serveur FTP et qu'environ 50 % des données du serveur FTP ne se trouvaient pas dans le fichier circulant sur Internet. La société DEDALUS BIOLOGIE en conclut qu' " au regard des incohérences subsistantes entre les données présentes sur le serveur FTP et celles ayant circulé sur Internet, les investigations combinées de Dedalus Biologie et de […], qui se sont achevées le 26 mars 2021, n'ont pas permis à l'époque des faits de conclure avec certitude que lesdites intrusions seraient à l'origine de la cyberattaque reportée par la presse ". Enfin, la société fait état des différentes mesures de sécurité mises en place depuis lors.

59. Dans ses dernières observations en réponse, la société indique qu'elle n'entend pas contredire les constats faits par le rapporteur sur l'absence de mesures satisfaisantes de sécurité encadrant le serveur FTP MEGABUS et précise avoir conscience des défauts de l'ancienne technologie utilisée par ses équipes, mais fait à nouveau valoir les évolutions intervenues en matière de sécurité et ses importants efforts de mise en conformité.

60. En premier lieu, la formation restreinte relève qu'il ressort des constations effectuées par la CNIL que la société ne disposait pas de procédure spécifique établie s'agissant des opérations de migration de données. Aucune mesure de sécurité n'était notamment prévue pour l'envoi des données, pourtant sensibles au sens de l'article 9 du RGPD. Les fichiers d'extractions de données étaient donc envoyés " en clair " (c'est-à-dire lisibles directement, car non transformées

préalablement via une fonction de hachage), sans aucune mesure de chiffrement ou de sécurité. Or, pour assurer la sécurité des opérations de migration d'un nombre aussi important de données à caractère personnel sensibles, il convient de mettre en place des procédures spécifiques permettant de décrire étape par étape l'enchaînement des tâches à réaliser, les rôles et les responsabilités associées. De telles procédures permettent également de disposer d'un compte rendu détaillé des opérations pour les laboratoires ou clients dont les données ont été traitées et transmises. L'absence de telles procédures fait peser sur les données à caractère personnel concernées un risque de compromission pourtant facilement évitable, qui peut conduire à exposer des données relevant de la vie privée.

61. En deuxième lieu, la formation restreinte relève que plusieurs alertes successives auraient dû conduire la société à effectuer des investigations sur son système de sécurité. Si, s'agissant du signalement réalisé par l'ANSSI en novembre 2020, la société indique avoir entrepris des investigations internes pour identifier la source possible de compromission et avoir mis en œuvre plusieurs actions correctives et préventives, elle n'a pas effectué de diligences suffisantes afin d'identifier si les données d'autres laboratoires avaient pu être compromises et si des vulnérabilités existantes étaient à l'origine de la compromission. La formation restreinte considère que la société n'a pas pris la mesure des problèmes de sécurité qu'elle rencontrait à l'époque, lesquels ont fini par aboutir à la violation de données de février 2021 ayant concerné près de 500 000 personnes.

62. En troisième lieu, la formation restreinte note que plusieurs mesures de sécurité élémentaires en matière de sécurité faisaient défaut en l'espèce. La formation restreinte note d'abord que les données à caractère personnel stockées sur le serveur FTP MEGABUS n'étaient pas chiffrées et étaient donc directement lisibles, alors qu'il s'agit de données sensibles qui, de par leur nature, nécessitent des mesures de sécurité particulières.

63. En outre, dans le cadre des migrations du logiciel DXLAB ONE vers un autre logiciel, les données, une fois transférées sur le serveur, n'étaient pas effacées automatiquement. Or, la conservation des données fait encourir un risque de fuite ou de compromission desdites données.

64. La formation restreinte relève ensuite que la zone publique du serveur, dans laquelle certaines données des laboratoires ont été stockées aux fins de migration, était accessible librement sans authentification depuis Internet. Ce n'est que le 4 novembre 2020, date à laquelle l'incident de sécurité a été signalé par l'ANSSI, que l'accès " anonyme " sans authentification au serveur FTP a été coupé et, le 23 février 2021 seulement, que ce serveur a été définitivement mis hors ligne. En outre, la zone privée du serveur était accessible avec des comptes utilisateurs partagés entre plusieurs salariés. Or, l'utilisation de comptes partagés fait peser un risque disproportionné, pourtant facilement évitable, sur la sécurité du traitement et augmente considérablement les risques de compromission, notamment du fait de la circulation du mot de passe entre plusieurs personnes. En outre, les comptes communs (ou partagés) ne permettent pas une bonne application de la politique d'habilitation, qui est pourtant un élément fondamental de la sécurité des systèmes d'information, visant à limiter les accès aux seules données dont un utilisateur a besoin.

65. La formation restreinte souligne enfin qu'aucune procédure de supervision et de remontée d'alertes de sécurité n'était mise en œuvre sur le serveur FTP. Les connexions provenant d'adresses IP suspectes n'étaient donc ni détectées ni traitées. Le rapport d'investigation numérique de la société […] confirme d'ailleurs que certaines connexions suspectes ont été identifiées, ce qui confirme que le serveur était exposé sur Internet et que des connexions non autorisées à ce serveur ont eu lieu, sans qu'elles puissent être identifiées grâce à ces procédures de supervision et de remontée d'alertes.

66. En dernier lieu, la formation restreinte relève que le manquement reproché n'est pas constitué par les violations de données en tant que telles, mais par les défauts de sécurité qui sont à l'origine de l'intrusion sur les serveurs de la société, constatés lors des contrôles effectués par la CNIL. Elle souligne que cette proposition du rapporteur, visant à sanctionner les défauts de sécurité à l'origine de violations, s'inscrit dans la lignée de décisions précédentes de la formation restreinte. Ainsi, dans sa délibération n° SAN 2019-007 du 18 juillet 2019, la formation restreinte a relevé " que les mesures élémentaires de sécurité n'avaient pas été prises en amont du développement de son site web [par la société sanctionnée], ce qui a rendu possible la survenance de la violation de données à caractère personnel ".

67. La formation restreinte souligne toutefois que les conséquences de ces défauts de sécurité ne sont pas pour autant exclues du champ de son analyse, en ce qu'elles révèlent la concrétisation du risque engendré par ces défauts de sécurité. La formation restreinte observe ainsi que les vulnérabilités existantes ont été exploitées et que plusieurs violations de données ont eu lieu : des intrusions sur le serveur FTP, suivies par la diffusion d'un fichier contenant les données médico-administratives de près de 500 000 personnes sur des forums en février 2021. À cet égard, la formation restreinte relève que les intrusions sur le serveur FTP sont avérées et qu'elles ne sont pas contestées par la société, celles-ci ayant été établies par les investigations menées par […] pour le compte de la société.

68. S'agissant de la diffusion du fichier sur les forums, si la société indique qu'il ne peut être conclu avec certitude que les intrusions sur le serveur FTP sont à l'origine de la violation de données ayant abouti à la diffusion de ce fichier, la formation restreinte observe néanmoins qu'il ressort des éléments du dossier qu'environ 90 % des données du fichier publié étaient présentes sur le serveur FTP. Le fichier diffusé sur les forums contient notamment les commentaires qui n'auraient pas dû être extraits par la société DEDALUS BIOLOGIE dans le cadre de la migration de la solution MEGABUS vers une autre solution (" commentaire P " et " commentaire D " susmentionnés). Ces différents éléments tendent bien à montrer le lien entre les données figurant dans le fichier accessible sur Internet et celles qui étaient sur le serveur FTP.

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

71. Aux termes du III de l'article 20 de la loi du 6 janvier 1978 modifiée, " Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […]

7° A l'exception des cas où le traitement est mis en œuvre par l'Etat, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83 ".

72. L'article 83 du RGPD prévoit que " chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives ", avant de préciser les éléments devant être pris en compte pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de cette amende.

73. En premier lieu, sur le principe du prononcé d'une amende, la société insiste en défense sur l'absence de violation commise précédemment, sur son importante coopération avec la CNIL, sur les mesures de remédiation mises en œuvre depuis la violation de données à caractère personnel et sur les importants efforts de remise en conformité engagés.

74. La formation restreinte rappelle 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 et la gravité de la violation, le nombre de personnes affectées et le niveau de dommage qu'elles ont subi, le fait que la violation a été commise par négligence, 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.

75. La formation restreinte relève, tout d'abord, les nombreux défauts de sécurité encadrant le serveur FTP MEGABUS, lequel était insuffisamment protégé, ce qui a entraîné une violation de données à caractère personnel massive : de très nombreuses données concernant 491 840 personnes ont été divulguées.

76. La formation restreinte insiste, en outre, sur le caractère extrêmement dommageable de la violation pour les personnes concernées, dans la mesure où, outre des données d'état civil (civilité, nom, prénom), des coordonnées postales, électroniques et téléphoniques, des données très sensibles ont été divulguées. Le fichier objet de la violation de données à caractère personnel contient en effet des mentions relatives à l'infection au VIH, à des cancers ou des maladies génétiques, à la grossesse, aux traitements médicamenteux suivis par les patients ou encore à des données génétiques. Les données concernées par la violation sont des données de santé, lesquelles sont des catégories particulières de données au sens de l'article 9 du RGPD (dites données " sensibles "). Compte tenu de la nature des données concernées, la formation restreinte considère que la société aurait dû faire preuve d'une vigilance particulière en ce qui concerne la sécurisation de telles données, pour éviter qu'elles puissent être réutilisées par des tiers non autorisés, portant ainsi préjudice aux personnes concernées par la violation de données. Or les négligences commises en matière de sécurité ont été multiples et particulièrement graves, alors que la société traite de données sensibles et qu'elle avait d'ores et déjà été alertée sur l'existence potentielle de risques, dont certains se sont réalisés. La formation restreinte considère que le manquement ayant conduit à la violation de données est d'une particulière gravité.

77. Elle souligne en outre qu'au regard de la nature de ces données à caractère personnel, les personnes concernées par la violation sont des cibles de choix pour un hameçonnage (" phishing ") personnalisé (envoi de faux messages ou de faux documents pour récupérer des informations personnelles ou de l'argent) : d'éventuels pirates disposent désormais de leur numéro de sécurité sociale, du nom de leur médecin prescripteur, de la date de leur examen, du nom du laboratoire ou encore, dans certains cas, d'informations médicales. La nature des données à caractère personnel compilées sous-tend également des risques d'usurpation d'identité, de fausses ordonnances (qui peuvent utiliser les noms des médecins), de messages de détresse factices reprenant les problèmes de santé mentionnés.

78. La formation restreinte relève enfin que la société n'a pas pris de mesures particulières pour faire cesser la diffusion du fichier une fois qu'elle en a eu connaissance. C'est la présidente de la CNIL, et non la société DEDALUS BIOLOGIE, qui a fait délivrer une assignation en référé afin que soit assuré le blocage effectif du fichier litigieux.

79. Si la formation restreinte relève que la société a coopéré tout au long de la procédure avec les services de la CNIL, elle considère que les défauts de sécurité, qui ont permis la réalisation de la violation de données , comprenant à la fois les intrusions sur le serveur FTP et la diffusion du fichier en ligne, résultent d'une négligence des règles élémentaires de sécurité des systèmes d'information qui a conduit à rendre accessibles à des tiers non autorisés les données à caractère personnel traitées par la société.

80. La formation restreinte relève en outre que, le fait que la société DEDALUS BIOLOGIE ait traité des données à caractère personnel au-delà des instructions données par les responsables de traitement et ait donc commis un manquement à l'article 29 du RGPD a contribué à aggraver la violation, puisque des commentaires qui n'auraient pas dû être extraits se sont ensuite retrouvés dans le fichier diffusé en ligne et accessible sur les forums.

81. La formation restreinte rappelle enfin que les différents documents encadrant les relations contractuelles entre la société DEDALUS BIOLOGIE et les laboratoires ne comportent pas les mentions requises par l'article 28 du RGPD, ce qui n'est également pas de nature à assurer une protection efficace des données à caractère personnel traitées par le biais de garanties contractuelles.

82. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative au regard des manquements aux articles 28, paragraphe 3, 29 et 32 du RGPD.

83. En deuxième lieu, s'agissant du montant de l'amende, la société souligne que […]. La société insiste sur le fait que la situation financière de l'entreprise doit être prise en compte, de façon à ce que l'amende prononcée soit adaptée aux capacités contributives du responsable de traitement.

84. La formation restreinte rappelle que le paragraphe 3 de l'article 83 du Règlement 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. Dans la mesure où il est reproché à la société un manquement aux articles 28, 29 et 32 du 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.

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

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'État dans un délai de deux mois à compter de sa notification.