Décision MED-2021-093 du 4 octobre 2021

Commission Nationale de l'Informatique et des Libertés Etat juridique : En vigueur

Date de publication sur Légifrance : Jeudi 14 octobre 2021

Décision n°MED-2021-093 du 4 octobre 2021 mettant en demeure la société FRANCETEST

La Présidente de la Commission nationale de l'informatique et des libertés,

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 son article 20 ;

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° 2021-197C du 1er septembre 2021 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le Secrétaire général de procéder ou de faire procéder à une mission de vérification auprès de la société FRANCETEST ;

Vu le procès-verbal de contrôle sur place n° 2021-197/1 du 9 septembre 2021 ;

Vu les autres pièces du dossier,

I. Contexte et procédure

1. Présentation de la société et du contexte d'engagement de la procédure de contrôle

Créée en août 2021, la société FRANCETEST (ci-après, la "société"), dont les locaux sont situés 6, boulevard de la Marne, à Strasbourg (67000), comporte un associé unique et n'emploie aucun salarié.

Elle développe un service, opérationnel depuis mars 2021, à destination des pharmacies qui effectuent des tests antigéniques au SARS-CoV-2 (ci-après, le "service Francetest") en leur permettant de simplifier la collecte des données à caractère personnel des patients ayant effectué un test et leur acheminement vers le Système d'information national de dépistage, soit le traitement mis en œuvre par le ministère des solidarités et de la santé centralisant les résultats de ces tests (ci-après, "la plateforme SI-DEP"). Dans ce cadre, elle met notamment en œuvre le site web "francetest.fr" qui permet de remplir les deux objectifs énoncés ci-avant.

A la suite d'un signalement anonyme auprès des services de la CNIL le 27 août 2021 faisant état d'une faille de sécurité affectant le site web "francetest.fr", des vérifications en ligne conduites le jour même ont permis de constater l'effectivité et l'ampleur de la violation de données et, le 9 septembre 2021, une délégation a procédé à une mission de contrôle sur place dans les locaux de la société dans le but de vérifier la conformité des traitements de données à caractère personnel mis en œuvre par cette dernière avec le règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel (ci-après, le "RGPD") et 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"), en application de la décision no 2021-197C du 1er septembre 2021 de la Présidente de la Commission.

2. Fonctionnement du service Francetest

La société propose soit son service directement aux pharmacies, soit au travers de sociétés intermédiaires qui le distribuent auprès des pharmacies dans le cadre d'une prestation plus large d'accompagnement à la réalisation des tests antigéniques (fourniture d'une tente dédiée aux prélèvements et mise à disposition de personnel en charge de la réalisation des prélèvements, notamment).

La société est en relation d'affaires avec environ 350 pharmacies au total (en relation directe avec 200 pharmacies et en relation indirecte, via les sociétés intermédiaires mentionnées ci-avant, avec environ 150 pharmacies).

Dans les deux hypothèses, les pharmacies recourant au service doivent créer un compte sur le site web "francetest.fr" et renseigner leur numéro d'identification au répertoire partagé des professionnels de santé (RPPS) consistant en un identifiant unique et pérenne.

Le patient souhaitant faire un test antigénique dans une pharmacie recourant au service devra d'abord scanner, avec son terminal mobile, un code à réponse rapide (ci-après, "code QR") affiché à l'entrée des officines ou du lieu où le test est effectué. Ce code QR le renverra vers un formulaire en ligne à remplir et dans lequel il devra renseigner son nom, son prénom, son adresse courriel, son numéro de téléphone, sa date de naissance, son numéro d'inscription au répertoire national d'identification des personnes physiques (soit le numéro de sécurité sociale, ci-après "NIR"), l'adresse de son domicile ainsi que, le cas échéant, la date d'apparition des premiers symptômes. Ce formulaire en ligne est hébergé sur le site web "francetest.fr" .

Une fois le test effectué, le pharmacien devra renseigner le résultat du test dans son interface en ligne sur le service Francetest et valider la transmission de ce résultat vers la plateforme SI-DEP depuis l'application mobile qui permet l'authentification auprès des services liés à sa carte d'identité professionnelle électronique (ci-après, "l'application e-CPS"). Le service Francetest transmet alors au patient un courriel contenant un lien permettant d'accéder à ses résultats.

En synthèse, le service Francetest a un rôle d'intermédiaire et de facilitateur pour les pharmacies dans la collecte et le traitement des données à caractère personnel des patients testés et dans leur acheminement vers la plateforme SI-DEP.

Selon les constatations effectuées par la délégation de contrôle le 9 septembre 2021, 436 972 tests concernant 386 970 personnes uniques étaient présents dans sa base de données.

Les données des personnes enregistrées en base contenaient le numéro identifiant, le nom, le prénom, l'adresse courriel, le téléphone, la date de naissance, le résultat du test (positif ou négatif) de 386 970 personnes et, pour 322 337 d'entre elles, également le NIR.

3. Architecture technique du service Francetest

Il ressort des déclarations du contrôle sur place que le service est proposé à partir du site web "francestest.fr" , qui repose sur un système de gestion de contenu Z installé sur un serveur web hébergé sur un serveur de la société X.

Le service fonctionne grâce à deux bases de données principales :

- une base "clients" , qui contient les données des pharmaciens disposant d'un compte et qui est hébergée sur un serveur de la société X ; et

- une base "patients" , qui contient les données des patients ayant effectué les tests et qui est également hébergée sur les serveurs de la société Y.

4. Sur la vulnérabilité à l'origine de la violation de données et les suites apportées par la société

Le représentant de la société a précisé qu'après avoir été alerté le 27 août 2021 par un journaliste que des données à caractère personnel étaient librement accessibles dans l'arborescence du site web "francetest.fr" , il a relevé que la vulnérabilité était due à un défaut de configuration du serveur web.

Celui-ci permettait d'accéder au contenu du répertoire du module Z "francetest" permettant de gérer les différents services de la société. Dans le répertoire du site était accessible le code source du service, qui contenait notamment les identifiants de connexion à la base de données patients hébergée sur Y ainsi que des extraits au format CSV de cette base, c'est-à-dire dans un format texte directement lisible.

Ces extraits comprenaient toutes les données renseignées par les personnes lors de la réalisation d'un test, évoquées ci-avant. La présence de ces fichiers dans un répertoire du site web s'explique par un dysfonctionnement d'une des fonctionnalités du site permettant aux pharmaciens de réaliser des exports des données de leurs patients ayant réalisé des tests.

Lorsqu'il a été alerté de la vulnérabilité, le représentant de la société a indiqué avoir éteint et redémarré le serveur web du service "Francetest" et corrigé la vulnérabilité en rendant le dossier inaccessible. Il a modifié le mot de passe de connexion aux bases de données hébergées chez X et Y. Il a également ajouté des règles de pare-feu pour empêcher la connexion à la base de données depuis d'autres serveurs que ceux dédiés au service "Francetest" .

Le 30 août 2021, la société a notifié la violation de données à caractère personnel à la CNIL.

5. Suites de la procédure de contrôle

Par un courrier électronique du 15 septembre 2021, la société a communiqué à la CNIL les éléments complémentaires demandés par la délégation dans le cadre du contrôle sur place, à savoir les documents encadrant sa relation contractuelle avec les sociétés X et Y ainsi que des documents démontrant sa relation commerciale avec les sociétés intermédiaires. Par ailleurs, la société a également communiqué d'autres documents, tels que la dernière version de ses conditions générales de vente.

II. Sur la qualité de la société FRANCETEST vis-à-vis du traitement en question

Au titre de l'article 4, paragraphe 8, du RGPD, est sous-traitant *"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 "*.

En l'espèce, depuis l'arrêté du 26 octobre 2020 modifiant l'arrêté du 10 juillet 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de Covid-19 dans le cadre de l'état d'urgence sanitaire du ministre des Solidarités et de la Santé, les pharmaciens d'officine peuvent procéder à des tests antigéniques nasopharyngés pour la détection du SARS-CoV-2. Il en résulte que la réalisation des tests s'effectue sous la responsabilité des pharmacies, y compris la mise en œuvre opérationnelle impliquant, outre le test en lui-même, la collecte des données des patients et leur transmission vers la plateforme SI-DEP. Ainsi, ce sont les seules pharmacies qui

ont décidé des moyens et des finalités concernant le traitement lié à l'organisation des tests antigéniques, à savoir le recours à un dispositif simplifiant la collecte des données à caractère personnel des patients en vue de leur acheminement vers la plateforme SI-DEP.

Par ailleurs, dès lors que, dans le cadre du service qu'elle propose aux pharmacies, la société Francetest, d'une part, ne fait que mettre à disposition les outils, notamment informatiques, choisis par les pharmacies pour faciliter la mise en œuvre du traitement et, d'autre part, agit uniquement au nom et sous la responsabilité des pharmacies, que ce soit lorsque le service leur a été directement proposé ou lorsqu'il a été distribué aux pharmacies par les sociétés intermédiaires mentionnées, elle doit être regardée comme sous-traitante de ces dernières au sens de l'article 4, paragraphe 8 précité.

III. Le manquement à l'article 32 du RGPD

Aux termes de l'article 32, paragraphe 1, du RGPD, *"le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque"* .

Les a) et b) de ce même paragraphe 1 prévoient qu'en fonction notamment de *"la portée, du contexte et des finalités du traitement ainsi que des risques"* pour les personnes concernées, le responsable de traitement met en œuvre *"le chiffrement des données à caractère personnel"* et *"des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement"* .

A la lumière du considérant 75 du RGPD, qui éclaire la portée à donner à cet article, lorsque le traitement en cause porte sur des catégories particulières de données à caractère personnel, comme des données de santé, le traitement doit bénéficier de mesures de sécurité renforcées.

Au titre de ces mesures de sécurité renforcées, l'article L. 1111-8 du code de la santé publique prévoit que les données de santé doivent être hébergées chez un hébergeur disposant d'un agrément délivré par le ministère des Solidarités et de la Santé (ci-après, "agrément HDS").

En l'espèce, la délégation de contrôle a constaté lors du contrôle sur place que si la société a pris certaines mesures pour corriger le défaut de sécurité qui était à l'origine de la violation de données lorsqu'elle en a eu connaissance (extinction et redémarrage du serveur web du service Francetest, correction de la vulnérabilité en rendant le dossier inaccessible, modification du mot de passe de connexion aux bases de données hébergées chez X et Y, ajout de règles de pare-feu ; voir Point 4 ci-dessus), le service Francetest souffrait encore d'autres insuffisances en matière de sécurité, qui n'avaient pas été corrigés, et qui continuaient de faire peser un risque sur la confidentialité des données à caractère personnel traitées.

De multiples insuffisances en termes de sécurité ont été constatées et concernent, notamment, l'hébergement de données de santé chez un prestataire ne disposant pas d'un agrément HDS, le recours à des processus d'authentification insuffisamment robustes, l'utilisation d'une fonction de hachage faible et une journalisation lacunaire des activités des serveurs du service Francetest. Le détail de ces défauts de sécurité, constituant le manquement à l'article 32 du RGPD, n'est pas décrit dans la présente mise en demeure afin de ne pas exposer la sécurité du traitement à de nouveaux risques. Il a cependant été communiqué de façon confidentielle et sécurisée au sous-traitant, afin qu'il prenne les mesures de mise en conformité correspondantes.

Il convient de souligner que la caractérisation du manquement à la sécurité relevé s'effectue tant au regard de la nature des données concernées – comportant des données de santé, qui sont des données dites "sensibles" qui nécessitent une protection particulière en application de l'article 9 du RGPD – du volume de données objet de la violation ainsi que des risques qu'une telle violation fait peser sur les personnes.

En effet, ces personnes ont encouru le risque que leurs données directement identifiantes fassent l'objet d'un accès illicite, revendues à des tiers et réutilisées dans d'autres schémas d'attaques, notamment l'hameçonnage (ou *"phishing"*), technique consistant à se faire passer pour un organisme officiel (organisme de sécurité sociale, banque, etc.) qui demande à sa "proie" de confirmer ses données bancaires. En outre, ces personnes sont particulièrement exposées à des risques d'usurpation d'identité.

L'ensemble de ces faits constitue un manquement à l'obligation d'assurer la sécurité des données traitées prévue à l'article 32 du RGPD. Il revient à la société de mettre en place plusieurs mesures visant à garantir la sécurité des données à caractère personnel qu'elle traite pour le compte des pharmacies.

En conséquence, la société FRANCETEST, sise 6, boulevard de la Marne, à Strasbourg (67000), est mise en demeure sous un délai de deux (2) mois à compter de la notification de la présente décision et sous réserve des mesures qu'elle aurait déjà pu adopter, de :

- prendre toute mesure pour garantir la sécurité et la confidentialité des données à caractère personnel traitées et, en particulier, celles visées en annexe de la présente mise en demeure ;

- justifier auprès de la CNIL que l'ensemble des demandes précitées a bien été respecté, et ce dans le délai imparti.

A l'issue de ce délai, si la société FRANCETEST s'est conformée à la présente mise en demeure, il sera considéré que la présente procédure de mise en demeure est close et un courrier lui sera adressé en ce sens.

A l'inverse, si elle ne s'est pas conformée à la présente mise en demeure, un rapporteur sera désigné qui pourra demander à la formation restreinte de prononcer l'une des mesures prévues par l'article 20 de la loi du 6 janvier 1978 modifiée au regard du manquement précité et, le cas échéant, d'éventuels autres manquements constatés.

La Présidente

Marie-Laure DENIS