Les sites internet utilisant un protocole « http » à bannir

Pauline Meyer, le 26 septembre 2022

Le laboratoire d'analyses médicales qui fournit l'accès en ligne aux résultats de patients sur un site utilisant un protocole « http » et non « https » viole son obligation de sécurité.

Autorité belge de protection des données, décision de la chambre contentieuse 127/2022 du 19 août 2022

Une personne ayant plusieurs relations avec un laboratoire d'analyses médicales dépose plainte après s'être rendu compte que le site internet du laboratoire d'analyses médicales contient une page d'accès aux données d'analyse pour les médecins utilisant un protocole http non sécurisé. En outre, le plaignant reproche au laboratoire de ne pas avoir effectué d'analyse d'impact sur la protection des données et de ne pas avoir informé correctement les personnes concernées.

Pour commencer, l'Autorité belge de protection des données (*Gegevensbeschermingsautoriteit*) établit la qualité de responsable du traitement. Le laboratoire d'analyses médicales, niant d'abord cette qualité, s'y accommode finalement, dans la mesure où il détermine les finalités et les moyens du traitement (art. 4 ch. 7 RGPD).

La page d'accueil du site du laboratoire renvoie à une autre de ses pages sous la rubrique « Consulter les résultats », qui renvoie à son serveur de résultats en ligne, le « Cyberlab ». Ce serveur permet aux médecins de consulter en temps réel les résultats et l'historique des analyses de leurs patients. Le site web de la défenderesse ne contient pas de chiffrement car il utilise un protocole « http » (*Hyper Text Transfer Protocol*) au lieu d'un protocole chiffré « https » (*Hyper Text Transfer Protocol Secure*). Partant, les identifiants et mots de passe sont collectés et transmis en clair. L'utilisation de ce type de protocole entraîne un risque d'attaque du type *man-in-the-middle*. L'utilisation du protocole « http » est considérée par l'Autorité belge de protection des données comme une violation du principe et des obligations de sécurité des données auxquelles est soumise la défenderesse (art. 5 par. 1 let. f concrétisé à l'art. 32 RGPD).

Parallèlement à la violation du principe et de ses obligations de sécurité des données, l'Autorité considère que le laboratoire a violé son obligation d'analyse d'impact relative à la

protection des données (art. 35 par. 1 et par. 3 RGPD). En raison de la pandémie de COVID-19, le nombre d'analyses traitées par la défenderesse a fortement augmenté, ce qui permet de déduire de son activité un traitement à « grande échelle » de données relatives à la santé impliquant une obligation de mener une analyse d'impact. Bien que la notion de « grande échelle » est sujette à interprétation par les autorités de contrôle, l'Autorité affirme que le traitement effectué par le laboratoire est effectivement de grande échelle (se fondant sur son guide d'analyse d'impact relative à la protection des données, qui tient compte des lignes directrices du Groupe de travail Article 29 (G29) concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement « est susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2017/679). L'autorité belge admet que l'on pourrait également fonder l'obligation d'analyse d'impact sur l'échange systématique de données relatives à la santé entre la défenderesse et d'autres responsables du traitement (les médecins) comme prévu par le point 6.5) de la décision n° 01/2019 du Secrétariat général du 16 janvier 2019.

Finalement, le laboratoire est considéré comme ayant violé son devoir d'information (art. 12 à 14 RGPD). Il dispose d'affichages relatifs aux traitements de données personnels dans ses centres, mais cette mesure est à elle seule insuffisante, dans la mesure où seul un cercle limité de patients n'y est confronté. En outre, toute entreprise disposant d'un site web devrait publier une politique de confidentialité sur son site internet (en accord avec les lignes directrices du G29 sur la transparence au sens du règlement (UE) 2016/679).

L'amende, fixée à EUR 20'000 et infligée en tenant compte des critères de l'art. 83 RGPD, représente 0.07% du chiffre d'affaires de la défenderesse. Elle est déterminée en prenant en considération d'une part les circonstances aggravantes tel le traitement par la défenderesse d'une catégorie spéciale de données personnelles ou les incohérences dans sa défense. D'autre part, l'Autorité belge tient compte de circonstances atténuantes, dont notamment le fait que le laboratoire n'a par le passé vraisemblablement commis aucune infraction ou encore le fait qu'il a fait en sorte de se conformer à ses obligations depuis l'ouverture de la procédure.

Protocoles « http » vs « https »

Certains sites internet traitant des données personnelles continuent à utiliser le protocole « http » (non sécurisé car non chiffré). Ce protocole fait encourir des risques importants pour les personnes concernées en augmentant considérablement le risque d'attaques du type *man-in-the-middle* (ou de l'homme du milieu). Ce type d'attaque consiste en l'immission

d'une personne tierce non autorisée entre l'utilisateur d'un site et le site même en vue d'intercepter, modifier et voler des données, ou de rediriger l'utilisateur sur une page piégée ou malveillante. L'un des moyens classiques et simples à mettre en place pour diminuer drastiquement ce type d'attaque est d'utiliser un protocole « https », soit un protocole chiffré reposant sur TLS (*Transport Layer Security*, successeur du SSL (*Secure Sockets Layer*) permettant le chiffrement des données transférées à un navigateur), permettant d'assurer la confidentialité et l'intégrité des informations collectées et échangés ainsi que l'authenticité du serveur contacté. En d'autres termes, ce protocole permet que les différents identifiants, mots de passe et coordonnées des personnes concernées ne soient pas collectés et transmis en clair et, ainsi, que ces données courent un risque moins élevé d'être interceptées.

Certaines autorités sur le plan européen ont émis des recommandations afin que les diverses entités traitant des données personnelles mettent en place TLS et le protocole « https », comme par exemple le Contrôleur européen de la protection des données (CEPD) avec ses lignes directrices sur la protection des données personnelles traitées par des services internet fournis par les autorités européennes. Il insiste sur la nécessité de recourir à l'utilisation de TLS peu importe les catégories de données personnelles transmises par internet. En parallèle, en France, la Commission nationale française de l'informatique et des libertés (CNIL) a émis des recommandations en vue de sécuriser les sites internet, prévoyant notamment l'utilisation du protocole TLS pour toutes les pages où sont affichées ou transmises des données personnelles non publiques, se basant également sur la recommandation pour la mise en œuvre d'un site web de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui préconise d'ailleurs aujourd'hui l'utilisation d'un « http » *Strict Transport Security* (« hsts »), étape suivant une utilisation pérenne du protocole « https ».

En Suisse, le Préposé fédéral à la protection des données et à la transparence (PFPDT) s'est également prononcé en allant déjà en 2015 également dans le sens d'une utilisation de protocoles de communication sécurisés tel TLS afin d'assurer d'une part une communication chiffrée sécurisée entre un client et un serveur et, d'autre part, une authentification des parties. Partant, à notre avis, l'utilisation d'un protocole « http » comme une mesure ne permet pas d'assurer la sécurité des données en droit suisse (art. 7 LPD, 8 nLPD).

Proposition de citation : Pauline Meyer, Les sites internet utilisant un protocole « http » à bannir, 26 septembre 2022 *in* www.swissprivacy.law/173

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.