Recommandation n° 05/2017 du 24 mai 2017

Objet : recommandation d'initiative concernant le traitement de données de santé par GENetic DIAgnostic Network (ci-après GENDIA) (CO-AR-2017-012)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier l'article 30 ;

Vu le rapport de Monsieur Dirk Van Der Kelen ;

Émet, le 24 mai 2017, la recommandation suivante :

I. REMARQUE PRÉALABLE

1. La Commission attire l'attention sur le fait qu'une nouvelle réglementation européenne relative à la protection des données à caractère personnel a été promulguée récemment : le Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et la Directive Police et Justice. Ces textes ont été publiés au journal officiel de l'Union européenne le 4 mai 2016[1].

2. Le Règlement, couramment appelé GDPR (General Data Protection Regulation), est entré en vigueur vingt jours après sa publication, soit le 24 mai 2016, et sera automatiquement d'application deux ans plus tard, soit le 25 mai 2018. La Directive Police et Justice doit être transposée dans la législation nationale au plus tard le 6 mai 2018.

3. Pour le Règlement, cela signifie qu'à partir du 24 mai 2016, pendant le délai d'exécution de deux ans, les États membres ont d'une part une obligation positive de prendre toutes les dispositions d'exécution nécessaires, et d'autre part aussi une obligation négative, appelée "devoir d'abstention". Cette dernière obligation implique l'interdiction de promulguer une législation nationale qui compromettrait gravement le résultat visé par le Règlement. Des principes similaires s'appliquent également pour la Directive.

4. Il est dès lors recommandé d'anticiper éventuellement dès à présent ces textes. Et c'est en premier lieu aux responsables du traitement qu'il incombe d'en tenir compte dans leurs projets. Dans la présente recommandation, la Commission a d'ores et déjà veillé, dans la mesure du possible et sous réserve d'éventuels points de vue complémentaires ultérieurs, au respect de l'obligation négative précitée dans le chef des États membres.

II. OBJET, CONTEXTE ET ANTÉCÉDENTS PROCÉDURAUX DE LA RECOMMANDATION

5. Fin de l'année dernière, GENDIA a été mis en cause dans la presse car il avait réutilisé des données collectées dans le cadre d'un test DPNI (Dépistage Prénatal Non-Invasif, test prénatal

---

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (règlement général sur la protection des données)

Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil*

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2016:119:TOC.

visant à détecter des anomalies congénitales) afin de proposer un nouveau test de risques de cancer à des patientes - pour autant que celles-ci aient indiqué qu'il y avait eu des cancers dans la famille.

6. Dans ce contexte GENDIA (P. Willems) a été invité à fournir des explications à ce sujet le 20 décembre 2016 dans les locaux de la Commission, en particulier concernant la manière dont GENDIA traite (ultérieurement) des données à caractère personnel (qui concernent généralement la santé).

7. Suite à l'entretien susmentionné et à sa discussion en séance plénière de la Commission du 1er février dernier, GENDIA a été officiellement mis en demeure pour plusieurs violations constatées de la LVP, notamment de l'article 4, § 1, 2° et 3° de la LVP.
En effet, dans la mesure où GENDIA réutilise ultérieurement des données à caractère personnel collectées dans le cadre d'un test DPNI pour proposer un autre test génétique visant à détecter des risques de cancer, il se rend coupable d'une réutilisation incompatible et donc illicite des données à caractère personnel des personnes concernées.
Dans le cadre du test DPNI, GENDIA collecte en outre plus de données à caractère personnel que celles qui sont nécessaires à la réalisation de ce test. Les informations de santé relatives à la famille de la personne concernée, en particulier celles concernant d'autres affections héréditaires que celles qui sont dépistées par le test DPNI, n'y contribuent en aucune manière et sont donc excessives dans le cadre de ce test.

8. Par e-mail du 20 février dernier, P. Willems de GENDIA a déclaré qu'il donnerait suite à la mise en demeure précitée par la Commission, et en particulier :
   - qu'il cesserait immédiatement le traitement ultérieur illicite des données à caractère personnel collectées en vue du test DPNI pour proposer un test de risques de cancer ;
   - qu'il supprimerait de sa banque de données (tant sur papier qu'en version numérique) les données à caractère personnel collectées de manière excessive dans le cadre du test DPNI concernant les anomalies héréditaires autres que celles qui sont détectées à l'aide du test DPNI, et aussi
   - qu'il adapterait le formulaire de demande de DPNI en ce sens.

9. Dans le contexte de la mise en demeure précitée, il avait également été annoncé que plusieurs autres aspects relatifs à la manière dont GENDIA traite des données à caractère personnel, comme le délai de conservation, l'organisation de la sécurité de l'information, le transfert de données à des pays tiers, ... feraient l'objet d'une recommandation ultérieure de la Commission, conformément à l'article 30 de la LVP.

III. EXAMEN QUANT AU FOND

A. Finalité et licéité du traitement

10. En vertu de l'article 4, § 1, 1° de la LVP, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables.

11. Le traitement de données à caractère personnel relatives à la santé ne peut être effectué que dans le cadre des cas énumérés de manière limitative à l'article 7, § 2 de la LVP, notamment
    - lorsque la personne concernée a donné son consentement par écrit (article 7, § 2, a)) et
    - aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé (article 7, § 2, j)).

12. Dans la mesure où GENDIA réutilise ultérieurement des données à caractère personnel, collectées dans le cadre d'un test génétique bien déterminé, pour proposer un autre test génétique, il se rend coupable d'une réutilisation incompatible et donc illicite des données à caractère personnel des personnes concernées.

13. Cette réutilisation illicite n'est aucunement couverte par une phrase à ajouter au formulaire de demande d'un test bien défini *"Je souhaite aussi que GENDIA continue à m'informer des nouvelles recherches génétiques pouvant éventuellement être importantes pour moi ou ma famille." X Oui - Non"* - comme l'avait fait GENDIA pour le test DPNI - car celle-ci ne correspond en aucun cas à un consentement libre, spécifique et informé de l'intéressé (voir l'article 1, § 8 de la LVP).

B. Proportionnalité

14. Conformément à l'article 4, § 1, 3° de la LVP, les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.

15. Dans le cadre du test DPNI, GENDIA a collecté plus de données à caractère personnel que celles qui sont nécessaires à la réalisation de ce test. Les informations de santé relatives à la famille de la personne concernée, en particulier celles concernant d'autres affections héréditaires que celles qui sont dépistées par le test DPNI, n'y contribuent en aucune manière et sont donc excessives dans le cadre de ce test.

16. La Commission recommande à GENDIA de confronter également l'autre test génétique qu'il propose ainsi que les formulaires de demande respectifs au principe de proportionnalité susmentionné. GENDIA se livrera ici au même exercice que pour le test DPNI, à savoir supprimer de sa banque de données les données à caractère personnel collectées de manière excessive et, le cas échéant, adapter les formulaires de demande dans le même sens.

C. Délai de conservation

17. En vertu de l'article 4, § 1, 5° de la LVP, les données à caractère personnel peuvent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement.

18. D'après l'explication de P. Willems de GENDIA lors de l'entretien du 20 décembre 2016 dans les locaux de la Commission, en ce qui concerne le test DPNI, les échantillons sont détruits par le laboratoire chargé du test, et ce après analyse.
Les données à caractère personnel collectées et générées à cette occasion (formulaire de demande, correspondance e-mail et résultats des tests) sont conservées définitivement, donc pour une durée indéterminée, par GENDIA. Les résultats des tests seraient également conservés pour une durée indéterminée par le laboratoire chargé des tests (généralement situé à l'étranger, assez fréquemment dans des pays tiers).
Ceci est incontestablement contraire à l'article 4, § 1, 5° de la LVP.

19. La Commission recommande à GENDIA de fixer un délai de conservation maximal, compte tenu de la nécessité de conservation qui se fonde en la matière sur la finalité des tests génétiques respectifs pour lesquels les données à caractères personnel sont obtenues ou traitées. Une fois ce délai de conservation maximal écoulé, ces données à caractère personnel doivent être détruites dans les meilleurs délais.

D. Confidentialité et sécurité de l'information

20. L'article 16, § 4 de la LVP oblige le responsable du traitement (et le cas échéant son sous-traitant) à prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel. Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.
Pour une interprétation concrète de cette disposition, la Commission renvoie à la recommandation[2] qu'elle a émise visant à prévenir les fuites de données et aux mesures de référence[3] qui devraient être respectées dans le cadre de tout traitement de données à caractère personnel.

21. Les données à caractère personnel sensibles, dont celles relatives à la santé, sont de nature à légitimer des mesures de sécurité plus strictes. En vertu de l'article 25 de l'arrêté royal du 13 février 2001 portant exécution de la LVP, le responsable du traitement de telles données à caractère personnel doit prendre les mesures de sécurité supplémentaires suivantes :
- désigner les catégories de personnes, ayant accès aux données à caractère personnel, avec une description précise de leur fonction par rapport au traitement des données visées ;
- tenir la liste des catégories des personnes ainsi désignées à la disposition de la Commission ;
- veiller à ce que ces personnes désignées soient tenues par une obligation légale ou statutaire ou par une disposition contractuelle au respect du caractère confidentiel des données visées.

22. D'après l'explication de P. Willems de GENDIA lors de l'entretien du 20 décembre 2016 dans les locaux de la Commission, les résultats des tests sont toujours communiqués électroniquement/par e-mail à GENDIA par le laboratoire chargé des tests. Les données sont parfois cryptées mais cela est plutôt perçu comme un inconvénient que comme une plus-value selon P. Willems. Pour l'envoi d'échantillons, accompagnés du formulaire de demande (traduit), par GENDIA au laboratoire chargé des tests, on a recours à DHL.

---

[2] Voir :https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2013_0.pdf.

[3] Voir : http://www.privacycommission.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel_0.pdf .

23. Pour le traitement/l'envoi de données à caractère personnel sensibles, telles que celles qui concernent la santé, le cryptage est néanmoins considéré comme une mesure standard en matière de sécurité de l'information afin de protéger la confidentialité, l'authenticité et/ou l'intégrité des données à caractère personnel[4].

24. La Commission recommande à GENDIA de veiller scrupuleusement à ce que les mesures et les directives précitées en matière de sécurité de l'information soient en tout temps respectées lors du traitement de données à caractère personnel collectées ou générées lors de la réalisation des tests génétiques qu'il propose.

E. Transfert international à des pays tiers

25. Selon son site Internet[5] et d'après l'explication de P. Willems de GENDIA lors de l'entretien du 20 décembre 2016 dans les locaux de la Commission, GENDIA est un "réseau" international composé de plus de 100 laboratoires situés en Europe, aux États-Unis, en Asie et en Australie, avec Anvers comme "laboratoire central". Cela signifie que des données à caractère personnel sont régulièrement envoyées vers des pays "tiers" (en dehors de l'UE) qui n'appliquent pas nécessairement un même niveau de protection (élevé et adéquat) des données à caractère personnel qu'en Europe.
P. Willems déclare uniquement à ce propos que pour le test DPNI, les personnes concernées sont informées par la mention sur le site Internet du fait que le test sera effectué par le laboratoire américain ARIOSA[6].

26. En vertu de l'article 21 de la LVP, des données à caractère personnel ne peuvent en principe être transférées vers des pays non membres de l'Union européenne que si les pays en question assurent un niveau de protection adéquat de ces données. Afin d'apprécier le caractère adéquat du niveau de protection, il est notamment tenu compte de la nature des données, de la finalité et de la durée du ou des traitements envisagés, des pays d'origine et de destination finale, des règles de droit, générales et sectorielles, en vigueur dans le pays en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées.
La Commission européenne a déjà reconnu le niveau de protection adéquat des pays suivants : la Suisse, le Canada (pour les traitements soumis au "Personal Information Protection and Electronic Act" canadien), Andorre, l'Argentine, les États-Unis (pour les entreprises certifiées

---

[4] Voir : https://www.privacycommission.be/sites/privacycommission/files/documents/Richtsnoeren_CBPL_V%202%200%20FR_TRA.pdf en https://www.ehealth.fgov.be/sites/default/files/assets/nl/pdf/sector_committee/2014/11-052-n142-derdebetalersregeling-gewijzigd_op_16_september_2014.pdf (point. 32).

[5] Voir : http://www.gendia.net/mission.html.

[6] *"Le test DPNI proposé par GENDIA (test Harmony) a été développé et est réalisé par le labo américain ARIOSA sous l'accréditation de CLIA (*Clinical Laboratory Improvement Amendments)." - voir www.DOWNsyndromeNIPT.info.

par le "Privacy Shield" UE-USA concernant la protection des données à caractère personnel)[7], Guernesey, l'île de Man, les îles Feroë, Jersey, Israël, la Nouvelle-Zélande et l'Uruguay[8].

27. Si un transfert est envisagé vers un pays "tiers" n'ayant pas été reconnu comme offrant un niveau de protection adéquat, le transfert est éventuellement possible malgré tout, pour autant que le responsable du traitement garantisse lui-même une protection adéquate via des dispositions contractuelles. Le responsable du traitement peut alors opter soit pour les modèles de contrat-type mis à disposition par la Commission européenne, soit pour un contrat propre, à condition qu'il ait été autorisé par arrêté royal, conformément au protocole signé conjointement en la matière par le ministre de la Justice et le président de la Commission vie privée[9].

28. Un responsable du traitement qui n'offre pas de garanties suffisantes, par ex. via des dispositions contractuelles appropriées, peut, en vertu de l'article 22 de la LVP, procéder "exceptionnellement" à un transfert de données à caractère personnel vers des pays "tiers" lorsque les personnes concernées ont indubitablement donné leur consentement au transfert envisagé ou lorsque le transfert est nécessaire à l'exécution d'un contrat avec la personne concernée. Ces exceptions doivent cependant être interprétées de manière restrictive et ne peuvent pas être la norme pour le transfert de données, surtout s'il s'agit de transferts massifs et répétés. Il est recommandé de rechercher ici rapidement une solution contractuelle[10].

29. La Commission recommande à GENDIA de s'abstenir de tout transfert systématique de données à caractère personnel (souvent sensibles) vers des laboratoires de tests dans des pays tiers dont le niveau de protection adéquat n'a pas été officiellement reconnu, sans qu'un niveau de protection adéquat n'ait été garanti via des dispositions contractuelles.

---

[7] Sauf erreur, tel n'est pas le cas pour le laboratoire américain ARIOSA. (Voir : https://www.privacyshield.gov/list).

[8] Voir :https://www.privacycommission.be/fr/en-dehors-ue-protection-adequate.

[9] Voir https://www.privacycommission.be/fr/en-dehors-ue-sans-protection-adequate-clauses-contractuelles.

[10] Voir :http://www.privacycommission.be/fr/en-dehors-ue-sans-protection-adequate-exceptions.

PAR CES MOTIFS,

La Commission,

Recommande à **GENDIA** :

- de s'abstenir de toute réutilisation illicite de données à caractère personnel collectées dans le cadre d'un test génétique bien déterminé pour proposer un autre test génétique (voir le point 12) ;
- d'effectuer un test de proportionnalité concernant les données à caractère personnel collectées pour tous les tests génétiques qu'il propose et, le cas échéant, de supprimer de sa banque de données les données à caractère personnel collectées de manière excessive et d'adapter dans le même sens les formulaires de demande respectifs (voir le point 16) ;
- de fixer un délai de conservation maximal au terme duquel les données à caractère personnel collectées et générées dans le cadre de l'exécution de tests génétiques seront détruites (voir le point 19) ;
- de prendre les mesures techniques et organisationnelles appropriées en matière de sécurité de l'information qui sont nécessaires pour la protection des données à caractère personnel (souvent sensibles) (qui concernent la santé) lors de leur traitement (conservation, envoi, ...) (voir le point 24) ;
- de s'abstenir de tout transfert de données à caractère personnel vers des pays tiers sans qu'un niveau de protection adéquat soit assuré via des dispositions contractuelles (voir le point 29).

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere