Avis n° 34/2020 du 28 avril 2020

Objet: Demande d'avis concernant un avant-projet d'arrêté royal n° XXX portant exécution de l'article 5, § 1, 1°, de la loi du 27 mars 2020 habilitant le Roi à prendre des mesures de lutte contre la propagation du coronavirus COVID-19 (II), dans le cadre de l'utilisation d'applications numériques de dépistage de contacts par mesure de prévention contre la propagation du coronavirus COVID-19 parmi la population (CO-A-2020-041)

L'Autorité de protection des données (ci-après « l'Autorité »);

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA »);

Vu le 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* (ci-après « RGPD »);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD »);

Vu la demande d'avis du Ministre de l'Agenda numérique, des Télécommunications et de la Poste, chargé de la Simplification administrative, de la Lutte contre la fraude sociale, de la Protection de la vie privée et de la Mer du Nord, Monsieur Philippe De Backer, reçue le 23 avril 2020;

Vu le rapport de Madame Alexandra Jaspar, Directrice du Centre de Connaissances de l'Autorité de protection des données ;

Vu l'extrême urgence de la demande d'avis ;

Émet, le 28 avril 2020, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le Ministre de l'Agenda numérique, des Télécommunications et de la Poste, chargé de la Simplification administrative, de la Lutte contre la fraude sociale, de la Protection de la vie privée et de la Mer du Nord, Monsieur Philippe De Backer (ci-après « le demandeur »), a sollicité, en extrême urgence, l'avis de l'Autorité concernant un avant-projet d'arrêté royal n° XXX portant exécution de l'article 5, § 1, 1°, de la loi du 27 mars 2020 habilitant le Roi à prendre des mesures de lutte contre la propagation du coronavirus COVID-19 (II), dans le cadre de l'utilisation d'applications numériques de dépistage de contacts par mesure de prévention contre la propagation du coronavirus COVID-19 parmi la population (ci-après « l'avant-projet »).

2. Dans le contexte de la mise en place d'une stratégie de déconfinement, il semble nécessaire d'être en mesure de rompre la chaine de contaminations. Dans la note au Gouvernement accompagnant l'avant-projet et dans le Rapport au Roi, le demandeur indique que les éléments suivants pourront y contribuer:
    - Des tests systématiques et répétitifs afin de dépister les personnes contaminées et de les encourager à s'auto-isoler.
    - Le dépistage des contacts qu'ont eues les personnes contaminées, qui seront eux-aussi encourager à s'auto-isoler et « pourront être testés »..

3. À cette fin, certains experts sont d'avis qu'il serait utile de pouvoir utiliser des applications numériques de dépistages de contacts. La note au Gouvernement précise que « *les régions sont compétentes et responsables pour le dépistage des contacts des personnes contaminées. […] Le Gouvernement fédéral est compétent pour le cadre juridique et la protection de la vie privée dans lequel les applications de dépistages sont développés et utilisées* ». L'avant-projet entend déterminer ce cadre juridique.

4. L'Autorité souligne que son avis a été émis en extrême urgence et uniquement sur base des informations dont elle dispose et sous réserve d'éventuelles considérations futures. Elle insiste pour que toute évolution du système et/ou du cadre mis en place lui soit soumis pour avis avant sa mise en place.

5. Dans la mesure où des réflexions similaires ont lieu dans un grand nombre de Etats européens, les autorités de protection des données de ces Etats ont émis ensemble, au travers du Comité européen de la protection des données (ci-après « CEPD »), des lignes directrices[i] sur les applications de tracing. L'Autorité insiste sur la nécessité de veiller à leur respect.

II. REMARQUES INTRODUCTIVES

A. Quant à la nécessité et à la proportionnalité des traitements de données à caractère personnel qui sont envisagés

6. L'Autorité rappelle, tout d'abord, que tout traitement de données à caractère personnel constitue une ingérence dans le droit au respect de la vie privée des personnes concernées. Or toute ingérence dans le droit au respect de la vie privée, en particulier lorsque l'ingérence s'avère importante, n'est admissible que **si elle est nécessaire et proportionnée à l'objectif d'intérêt général** qu'elle poursuit.

7. Pour rappel, un traitement de données à caractère personnel est considéré comme étant **nécessaire** s'il constitue la mesure la moins attentatoire pour atteindre l'objectif (d'intérêt général) qu'il poursuit. Il faut donc :
   - premièrement, que le traitement de données permette effectivement d'atteindre l'objectif poursuivi. Il faut donc démontrer, sur base d'éléments factuels et objectifs, **l'efficacité** du traitement de données à caractère personnel pour atteindre l'objectif recherché ;
   - deuxièmement, que ce traitement de données à caractère personnel constitue **la mesure la moins intrusive** au regard du droit à la protection de la vie privée. Cela signifie que s'il est possible d'atteindre l'objectif recherché au moyen d'une mesure moins intrusive pour le droit au respect de la vie privée ou le droit à la protection des données à caractère personnel, le traitement de données initialement envisagé ne pourra pas être mis en place. Il faut, à cette fin, détailler et être en mesure de démontrer, à l'aide d'éléments de preuves factuels et objectifs, les raisons pour lesquelles les autres mesures moins intrusives ne sont pas suffisantes pour atteindre l'objectif recherché.

8. Si la nécessité du traitement de données à caractère personnel est démontrée, il faut encore démontrer que celui-ci est **proportionné (au sens strict)** à l'objectif qu'il poursuit, c'est-à-dire qu'il faut démontrer qu'il existe un juste équilibre entre les différents intérêts en présence, droits et libertés des personnes concernées. En d'autres termes, il faut qu'il y ait un équilibre entre l'ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel et l'objectif que poursuit – et permet effectivement d'atteindre – ce traitement. Les avantages qui découlent du traitement de données en question doivent donc être plus importants que les inconvénients qu'il génère pour les personnes concernées. À nouveau, il faut être en mesure de démontrer que cette analyse a bien été réalisée avant la mise en œuvre du traitement.

9. L'Autorité constate que si le projet d'arrêté royal, la note au Gouvernement et le Rapport au Roi démontrent en quoi l'utilisation d'applications numériques de dépistage de contacts est moins intrusive

que le système existant faisant un usage exclusif de call-centers (et utilisé dans le cadre de la lutte contre d'autres épidémies), ils ne démontrent pas de manière suffisante l'efficacité et donc la nécessité et la proportionnalité de cette utilisation. Une estimation du pourcentage de la population qui en fera usage, sur base de sondages récents d'intention ainsi qu'une étude relative au taux d'utilisation requis pour que le système produise des résultats contribueraient à convaincre quant à ces points. Une campagne de test de l'efficacité des mesures envisagées nous semble également indispensable, notamment afin d'éviter au maximum les faux positifs et le stress injustement généré chez les personnes contactées à tort.

10. A cet égard, l'efficacité des applications numériques de dépistage de contacts ne peut pas être pensée en isolation de la politique globale de santé publique visant à lutter contre la propagation du coronavirus COVID-19 parmi la population.

11. L'Autorité rappelle que, dans ses lignes directrices précitées, le CEPD, a souligné que « *The efficiency of the contribution of contact tracing applications to the management of the pandemic depends on many factors (e.g., percentage of people who would need to install it; definition of a "contact" in terms of closeness and duration.). Moreover, such applications need to be part of a comprehensive public health strategy to fight the pandemic, including, inter alia, testing and subsequent manual contact tracing for the purpose of doubt removal. Their deployment should be accompanied by supporting measures to ensure that the information provided to the users is contextualized, and that alerts can be of use to the public health system. Otherwise, these applications might not reach their full impact*»[1].

B. Quant à la possible multiplication des applications de traçage

12. Certains risques liées à une possible reconstitution de données sont largement mitigés par le protocole que le gouvernement propose d'adopter via le projet d'arrêté royal. D'autres risques (en ce compris la possibilité donnée à un utilisateur de déterminer qui l'a infecté) doivent néanmoins également être mitigés au niveau de l'application de traçage elle-même. Si l 'Autorité comprend la volonté de ne pas réserver la création d'une application à un opérateur unique, elle attire néanmoins l'attention du demandeur sur le fait rappelle que la multiplication des applications augmente dès lors également ce risque puisque leur contrôle en devient plus ardu. L'encouragement des citoyens à utiliser une seule et unique application labellisée diminuerait ce risque ainsi que le risque d'apparition d'applications non certifiées présentant des risques importants pour le respect de la confidentialité des données des citoyens. L'Autorité recommande donc à tout le moins (et à côté de la gestion de ce risque dans le cadre de l'analyse d'impact à effectuer) d'imposer via l'arrêté royal la publication du code-source de chacune des applications de tracing dans un délai

raisonnable avant sa mise à disposition (qui pourrait être d'environ une semaine), afin que ses algorithmes puissent être audités par des experts indépendants.

C. Quant à la concentration des données utilisées entre les mains d'un opérateur unique

13. L'avant-projet prévoit que Sciensano détiendrait et gèrerait :
    - plusieurs bases de données constituées dans le cadre de ce projet (contenant notamment les numéros de téléphone des utilisateurs ayant été testés « positifs » les noms et numéros de téléphone des « contacts » des personnes infectées à appeler, la date et la durée de leurs contacts etc) ; ainsi que
    - d'autres bases de données constituées dans le cadre de l'exercice de ses missions, en ce compris une base de données dont un second arrêté royal prévoit la constitution par Sciensano, sur base de sources diverses, et contenant une grande quantité de données à caractère personnel (y compris relatives à la santé) relatives à des personnes pour lesquelles le médecin présume une infection, pour lesquelles un test a été prescrit, qui ont subi un test ou ont été hospitalisées et relatives à leurs contacts et à leur médecin.

14. L'Autorité s'inquiète du fait que le second arrêté royal en projet prévoie une centralisation de toutes ces données au sein d'une seule et unique base de données constituée et gérée par Sciensano. Alors même que le Rapport au Roi relatif à l'arrêté royal en projet (qui fait l'objet du présent avis) indique qu'une « garantie supplémentaire est l'impossibilité de croiser des données sauvegardées ». L'Autorité insiste dès lors pour que le projet soit revu et que les mesures nécessaires soient prises afin d'empêcher toute possibilité de recoupement entre ces différents sets de données détenus par le même organisme (ou par tout tiers auquel le projet donne accès à la fois à la liste des utilisateurs et au code qui leur est attribué pour uploader les clefs et au serveur reprenant le code et les clefs. Une transparence optimale quant à la concentration de ces données entre les mains d'un organisme unique devra par ailleurs être assurée.

15. L'Autorité insiste également pour que les agents du call-center soient soumis à l'autorité hiérarchique ou du moins fonctionnelle du responsable des traitements de données à caractère personnel qu'ils seront amenés à effectuer, qu'ils soient soumis à une obligation stricte du respect de la confidentialité des données qu'ils seront amené à manipuler et que des contrôles effectifs soient réalisés.

16. Enfin, vu la sensibilité des données traitées dans le cadre du projet faisant l'objet du projet d'arrêté royal, l'Autorité rappelle la nécessité de respecter scrupuleusement les règles du RGPD en matière de sous-traitance de données et la responsabilité du responsable du traitement en matière de sélection de son/ses

sous-traitants et de contrôle de ses opérations ainsi que la responsabilité qui lui incombe en cas de défaillance.

III. COMMENTAIRES DE CERTAINS ARTICLES DU PROJET

- **Article 3 § 1, tirets 1 et 2 : « *Les applications numériques de dépistage de contacts se limitent au traitement des données permettant de :***

  - ***Pouvoir confirmer une contamination COVID-19 d'un utilisateur d'une application numérique de dépistage de contacts ;***
  - ***Prévenir les utilisateurs d'une application numérique de dépistage de contacts que pendant un certain temps ils ont été à proximité d'une personne contaminée du COVID-19* » ;**

17. L'Autorité rappelle qu'un système par lequel les personnes avec qui une personne infectée a été en contact pendant la période déterminée par le projet d'arrêté (ci-après les « contacts ») serait contrainte de s'auto-isoler ou de se faire tester, sans intervention d'un professionnel de la santé (y compris dans le cadre d'un appel d'un agent du call-center), constituerait une décision « *fondée exclusivement sur un traitement automatisé […] produisant des effets juridiques […] concernant [la personne concernée] ou l'affectant de manière significative de façon similaire* » au sens de l'article 22 du RGPD. Or, le CEPD, a souligné dans ses lignes directrices, que « *It is the EDPB's understanding that such apps cannot replace, but only support, manual contact tracing performed by qualified public health personnel, who can sort out whether close contacts are likely to result in virus transmission or not (e.g., when interacting with someone protected by adequate equipment – cashiers, etc. -- or not). The EDPB underlines that procedures and processes including respective algorithms implemented by the contact tracing apps should work under the strict supervision of qualified personnel in order to limit the occurrence of any false positives and negatives. In particular, the task of providing advice on next steps should not be based solely on automated processing*»[ii].

- **Article 3 § 1, tiret 3 : « *Les applications numériques de dépistage de contacts se limitent au traitement des données permettant de […]***
  - ***Effectuer des rechercher épidémiologiques sur des données pseudonymisées, notamment de rechercher le taux de contact de l'épidémie COVID*-19 ».**

18. Cette utilisation de données pseudonymisées ne peut être envisagée que si ces études épidémiologiques ne peuvent être effectuées sur base de données anonymisées. Le projet devrait aborder cette question. Par ailleurs, le projet actuel ne fournit pas d'informations suffisantes pour permettre d'évaluer le niveau de

risque de ré-identification des données en question (risque majeur puisqu'il donnerait lieu à la centralisation, à la transmission et à l'utilisation de données à caractère personnel relatives à la santé).

19. Il y a lieu, afin que le respect du principe de proportionnalité puisse être analysé, de préciser s'il s'agit-il uniquement de recherches sur le COVID-19 (symptômes, incubation, évolution, …) ou également de recherches plus larges portant sur les personnes non contaminées ou contaminées autrement ou sur les médecins qui sont consultés et demandent ou non des tests, ou sur des personnes de contact et où elles résident (voire la communication de données de personnes dont le test est « négatif » ou qui sont seulement « suspectées » d'être contaminées, informations relatives aux médecins, aux contacts). La note au Conseil des Ministres semble limiter la réutilisation des données à des recherches épidémiologiques « sur la propagation du COVID-19 ». Si tel est le cas, il convient de la préciser dans le projet.

- **Article 4, alinéa 1: « *L'installation, l'utilisation et la désinstallation d'une application numérique de dépistage de contacts se fait uniquement sur base volontaire* »**

20. L'Autorité souhaite qu'il soit spécifié qu'il doit être fait en sorte que la désinstallation des applications soit une opération aussi simple que son installation.

- **Article 4, alinéa 2 : *« La non installation, la non utilisation et la non désinstallation d'une application numérique de dépistage de contacts ne peut en aucun cas donner lieu à une mesure civile ou pénale, ni à quelconque action discriminatoire* »**

21. L'Autorité recommande :
    - ✓ d'ajouter que les citoyens/individus qui refuseraient d'utiliser l'application ne peuvent souffrir d'aucun désavantage quelconque (tel un refus d'accès à un bien ou à un service) ; et
    - ✓ de prévoir des sanctions civiles et/ou administratives et/ou pénales pour les personnes qui lieraient l'accès à un bien ou à un service à l'utilisation de cette application (ex : entrée dans un magasin, un cinéma, reprise du travail etc.)

- **Article 5 § 1er : « *Le responsable du traitement dans le sens de l'art. 4, 7° du RGPD pour les objectifs visés à l'art. 3 est l'organisme de recherche Sciensano* »**

22. Premièrement, l'Autorité souligne qu'une personne/entité est responsable d'un traitement de données et non d'une finalité. Il convient donc de revoir la désignation du responsable du traitement à l'article 5 du projet. L'Autorité rappelle, par ailleurs, que la désignation du responsable du traitement doit être adéquate

au regard du RGPD. Tant le Groupe de travail 29 – prédécesseur du CEPD – que l'Autorité ont insisté sur la nécessité d'approcher le concept du responsable du traitement dans une perspective factuelle. En d'autres termes, lorsque la (les) finalité(s) du traitement est déterminée(s) par une norme, comme c'est le cas en l'espèce, le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, dans les faits, poursuit cette (ces) finalité(s) et assure la maitrise du traitement. Si c'est Sciensano qui est désignée comme le responsable du traitement, c'est donc parce que c'est cette institution qui poursuivra les finalités des traitements de données envisagés et qui en assurera la maitrise.

23. Par ailleurs, l'Autorité rappelle que si c'est Sciensano qui agit en tant que responsable des traitements visés par le présent projet d'arrêté, il lui appartient d'assumer les responsabilités qui lui incombent en cette qualité, en ce compris:
    - ✓ de faire le choix de/des applications qui seront proposées ;
    - ✓ de conclure les instruments contractuels nécessaires avec les sous-traitants de données ;
    - ✓ de garantir le respect du présent arrêté, en ce compris (1) le fait que les données à caractère personnel dont le traitement y est envisagé ne soient traitées qu'afin de réaliser les finalités décrites à l'article 3§1 et (2) le fait que ces applications n'effectuent pas la collecte d'autres données à caractère personnel que celles qui sont prévues par le présent arrêté
    - ✓ de vérifier que ce soit toujours le cas suite à d'éventuelles mises à jour de ces applications
    - ✓ de réaliser une analyse d'impact (AIPD)

- **Article 5 § 2 : « *Le responsable du traitement fournit sur son site les informations à l'utilisateur, comme visé à l'art. 13 du RGPD* »**

24. La fourniture de cette information sur le site web de Sciensano ne suffit pas pour que les utilisateurs potentiels des applications soient informés de manière certaine et transparente au sujet, notamment, des objectifs du système mis en place, des traitements de données auquel il donnera lieu et des parties impliquées. Une information simple et courte à ce sujet doit être fournie à l'utilisateur potentiel dans le cadre de l'opération de téléchargement de l'application. Une possibilité d'accès à une information beaucoup plus détaillée (lui permettant de comprendre le fonctionnement du système, les flux de données, ses droits etc.) doit également être prévue et renseignée à cette occasion.

- **Article 6 § 1er : « *Les applications numériques de dépistage de contacts traitent uniquement les clés secrètes, les numéros de série temporaires non personnalisés générés par les applications, un fuseau horaire comprenant une date et une partie de la journée de six heures dans laquelle un contact entre utilisateurs a eu lieu, ainsi que la distance et la durée de ce contact* »**

25. Il convient de revoir la formulation de cette disposition. En effet, l'utilisation de l'application implique nécessairement le traitement des données visées au 6 § 1 alors que l'utilisateur peut également partager d'autres données et informations (sur base volontaire) en plus des données identifiées au § 1.

- **Article 6 § 2, 1er et 2ème tirets: « *L'utilisateur peut communiquer volontairement les données suivantes au responsable du traitement :***
  - ***la contamination de COVID-19 constatée ;***
  - ***le numéro de téléphone de l'utilisateur* »**

26. D'après les informations qui nous ont été communiquées, il demandé à l'utilisateur de transmettre son numéro de téléphone à Sciensano lorsque l'utilisateur est informé être infecté et qu'il décide de permettre la recherche de ses contacts. Ceci ne ressort néanmoins pas du projet d'arrêté et devrait être précisé.

27. Par ailleurs, dans la note au Gouvernement, il est indiqué que « *Le tracing call center téléphone le patient contaminé, détermine la date présumée de la contamination et demande d'indiquer dans l'application qu'il est contaminé. A ce moment, l'utilisateur peut encore toujours décider de ne pas le faire* ». Mais rien n'est indiqué dans le projet quant aux modalités et à l'objectif de cet appel. L'Autorité souligne, en outre, que cet appel "encourageant" la personne infectée à indiquer son statut dans l'application risque de porter atteinte au caractère « volontaire » de la communication de cette information avec l'application.

- **Article 6 § 2, 3ème tiret : « *L'utilisateur peut communiquer volontairement les données suivantes au responsable du traitement : […]***
  - ✓ ***pour chacune des personnes contaminée du COVID-19 avec qui l'utilisateur a été en contact : la clé secrète de la personne en question, le nombre de rencontres que l'utilisateur a eu avec cette personne et pour chacune des rencontres le nombre de jours depuis la date de contamination du COVID-19 de la personne en question où la date à laquelle la contamination a été constaté* »**

28. Ici aussi, nous comprenons que ces données sont transmises à Sciensano dans l'hypothèse où l'utilisateur est informé être infecté et qu'il décide de permettre la recherche de ses contacts (pour autant que ces derniers fassent également usage de l'application ou d'une application interopérable)? Ceci devrait être précisé.

29. Nous ne sommes par ailleurs pas certains que la formulation soit adéquate car, si notre compréhension est correcte, dans cette hypothèse, l'utilisateur ne transmet (« meedeelt ») aucune de ces données mais il autorise (en activant la fonctionnalité indiquant qu'il est infecté et souhaite que ses contacts soient avertis) que le système géré par Sciensano génère ces données. Et ce, sur base de la volonté exprimée préalablement par ces contacts (manifestée par leur téléchargement de l'application). De ce fait, l'utilisateur infecté ne transmet à Sciensano et donc ne traite aucune donnée (à caractère personnel ou non) relative à ces contacts.

30. Enfin, selon les explications qui nous ont été fournies, un utilisateur d'une application de traçage qui a été en contact avec un autre utilisateur déclaré infecté, recevra une notification lui indiquant qu'il a vraisemblablement été en contact avec une personne porteuse du virus. Selon ces explications toujours, il lui sera fourni, dans le cadre de cette notification, toutes informations nécessaires afin qu'il puisse décider du comportement à adopter (s'auto-isoler, consulter un médecin en cas de symptômes, permettre un appel du call-center). Il reste donc libre de décider de rester entièrement anonyme en ne communiquant pas son numéro de téléphone (ni le fait qu'il ait reçu une telle notification) à Sciensano. Il ne sera pas invité à appeler le call-center. L'Autorité insiste pour que ceci (et surtout le fait que ce « contact » puisse déterminer librement s'il pourra faire l'objet d'un appel du call-center ou pas) soit précisé dans l'arrêté royal.

- **Article 6 § 2, 4ème tiret : « *L'utilisateur peut communiquer volontairement les données suivantes au responsable du traitement : […]***
  - ***le nombre de numéros de série uniques non personnalisées de personnes contaminées* »**

31. Même remarque qu'au point précédent.

- **Article 7 : « *§ 1er Nonobstant le deuxième jusqu'au quatrième paragraphe, les clés secrètes, les numéros de série temporaires non personnalisés, le fuseau horaire dans lequel le contact entre utilisateurs a eu lieu, ainsi que la distance et la durée du contact sont sauvegardés exclusivement dans l'équipement terminal de l'utilisateur.***
  § 2. La clé secrète ou les clés secrètes d'un utilisateur dont la contamination avec le COVID-19 a été constatée et ensuite validée au moyen d'un code d'autorisation ainsi que le fuseau horaire dans lequel un contact entre utilisateurs a eu lieu peuvent être téléchargés dans une liste log centrale et sauvegardés auprès du responsable du traitement.
  § 3. Les données visées à l'art. 6, § 2 peuvent être téléchargées et sauvegardées dans une banque de données centrale auprès du responsable du traitement.
  Ces données sont téléchargeables séparément de la liste log visée au deuxième paragraphe et la banque de données visée au quatrième paragraphe.
  § 4. Le responsable du traitement peut télécharger et sauvegarder dans une banque de données centrale les données visées à l'article 6, § 2, premier, troisième et quatrième point, pour analyse épidémiologique sur la propagation du coronavirus COVID-19.
  ***Ces données doivent être sauvegardées séparément de la liste log visée au deuxième paragraphe et de la banque de données visée au troisième paragraphe*. »**

32. A des fins de lisibilité, de clarté et dès lors de transparence, l'Autorité souhaite que le texte en projet indique, pour chacune des trois finalités, quelles clés, numéros de série et autres données sont utilisées et conservées et par qui.

- **Article 8 § 1er : « *Les données collectées ne peuvent pas être sauvegardées plus longtemps que nécessaire pour l'accomplissement des objectifs visés à l'art. 3, § 1* »**

33. Ce paragraphe répète le principe de la limitation de la durée de conservation des données personnelles et n'a dès lors aucune valeur juridique ajoutée par rapport à l'article 5.1.e) du RGPD. En outre, telle que formulée, cette disposition viole l'interdiction de retranscription du RGPD[iii] et elle doit dès lors être supprimée. Les délais de conservation des données doivent, par contre, être spécifiés.

- **Article 8 § 2 : « § 2. *Les clés secrètes, les numéros de série temporaires non personnalisés, le fuseau horaire dans lequel un contact a eu lieu entre utilisateurs ainsi que la distance et la durée du contact doivent être effacés au plus tard trois semaines après être générés dans l'équipement final de l'utilisateur d'une application numérique de dépistage de contacts.***

  ***La contamination de COVID-19 constatée, ainsi que le numéro de téléphone, pour autant que ces données sont traitées en application de l'art. 6, § 2, doivent être effacés immédiatement après leur traitement* ».**

34. Nous comprenons que la durée de 3 semaines correspond à la période pendant laquelle les contacts d'un utilisateur infecté sont recherchés, et ce, au motif qu'une personne infectée est contagieuse pendant trois semaines au maximum. Le Rapport au Roi mentionne la durée de 14 jours. Une harmonisation des textes est requise sur ce point. Il convient de justifier la durée de conservation choisie, étant donné que celle-ci doit être strictement limitée à ce qui est nécessaire pour atteindre l'objectif poursuivi.

35. Il y a également lieu de préciser ce qui est entendu par « *immédiatement après leur traitement* ». Par ailleurs, de quels traitement parle-t-on ?

- **Article 8 § 3 : « *Les clés secrètes et le fuseau horaire dans lequel un contact a eu lieu entre utilisateurs d'une application numérique de dépistage de contacts qui sont sauvegardés dans la liste log visée à l'art. 7, § 2, doivent être effacés au plus tard trois semaines après être repris dans la liste log* »**

36. À nouveau, il convient de justifier cette durée de conservation de trois semaines ou 14 jours.

- **Article 8 § 4 : *« Les données sauvegardées dans la banque de données visée à l'art. 7, § 3 doivent être effacées au plus tard trois semaines après être reprises dans la banque de données* »**

37. À nouveau, il convient de justifier cette durée de conservation de trois semaines ou 14 jours.

- **Article 8 § 5 : « *Les applications numériques de dépistage de contacts sont désactivées par le responsable du traitement aussitôt que le ministre de la Santé publique déclare la fin de la crise COVID-19.***
  ***La désactivation des applications numériques de dépistage de contacts ne doit pas dépendre de la désinstallation par l'utilisateur* »**

38. Dans la mesure où il n'est pas du tout établi que la Ministre de la santé (s'agit-il par ailleurs de la Ministre fédérale ?) décrétera effectivement un jour « la fin de la crise », cette formulation ne permet pas de déterminer avec certitude le moment auquel cette désactivation aura. Il y a donc lieu de repenser la détermination de ce moment/délai. Par exemple via une référence à la publication d'un arrêté reprenant une formulation spécifique et certaine.

- **Article 9, alinéa 1er : « *Les données sauvegardées dans la liste log visée à l'art. 7, § 2 ne peuvent pas être communiquées à des tiers* »**

39. L'Autorité recommande de préciser qu'aucun accès ne peut par ailleurs être donné à ces tiers.

- **Article 9, alinéa 2 : « *La banque de données visée à l'art. 7, § 3 peut uniquement être consultée par les autorités compétentes des régions et exclusivement pour l'objectif visé à l'art. 3, § 1, deuxième point* »**

40. Il y a lieu de préciser qui sont ces « autorités compétentes des régions »

- **Article 11, dernier alinéa : « *Les logs sont sauvegardés pendant [5] ans* »**

41. Une durée de conservation de 10 ans peut sembler appropriée au vu de la nature pénale des peines attachées à l'accès non autorisé aux données et de la durée de prescription de ce type d'infractions.

- **Article 12, alinéa 1er : « *Les instances qui, en vertu de l'art. 9, deuxième alinéa, ont un droit d'accès, prennent toutes les mesures techniques et organisationnelles, sous leur responsabilité exclusive, pour garantir que :***
  - ***l'utilisateur individuel est compétent pour exercer le droit d'accès ;***
  - ***chaque accès est exercé conformément à l'objectif visé à l'art. 3, § 1, deuxième point ;***
  - ***l'exactitude des données soit assurée ;***
  - ***la confidentialité des données reçues soit respectée et qu'ensuite ces données ne sont pas utilisées, remaniées ou dispersées à des fins incompatibles avec l'objectif visé à l'art. 3, § 1, deuxième point, sauf dispositions légales contraires* »**

42. Premièrement, il ne peut pas être prévu que le responsable du traitement (Sciensano) soit totalement déchargé de sa responsabilité. Il lui revient de vérifier que les « autorités compétentes » ayant accès aux bases de données ont bien pris les mesures techniques et organisationnelles nécessaires, conformément au RGPD.

43. Ensuite, si par « utilisateur individuel » on vise la personne physique qui télécharge et utilise l'application (ce que nous comprenons), nous supposons qu'il ne faut pas le déclarer qu'il doit être rendu « compétent » (« bevoegd ») pour exercer son droit d'accès mais confirmer qu'il doit pouvoir exercer son droit d'accès auprès de ces autorités, conformément à l'article 15 du RGPD.

44. Par ailleurs, si ces instances régionales doivent garantir l'exercice de ce droit, cela signifie-t-il qu'elles deviennent responsables du traitement des données qu'elles traiteront pour leurs finalités propres ?

45. Quant au deuxième tiret, il semble ici que l'accès dont il est question n'est pas le droit d'accès visé par le RGPD, mais le droit pour des administrateurs des autorités régionales compétentes de pouvoir accéder aux données conservées par Sciensano ? Ce point devrait être reformulé pour éviter cette confusion.

46. Enfin, il y a lieu de supprimer « *et qu'ensuite ces données ne sont pas utilisées, remaniées ou dispersées à des fins incompatibles avec l'objectif visé à l'art. 3, § 1, deuxième point, sauf dispositions légales contraires* ». Une réutilisation des données visées par le présent projet de norme à des fins autres que celles listées à l'article 3§1 ne peut être envisagée.

- **Article 13 : « *L'Autorité de protection des données surveille l'exécution du présent arrêté et pour l'exécution de cette tâche elle a accès aux données traitées par le responsable du traitement* »**

47. Cette disposition doit être supprimée. Les missions et pouvoirs de l'Autorité ont définis par le RGPD et la LTD de sorte qu'il n'est pas pertinent de rappeler ici sa compétence générale de contrôle. Par ailleurs, la formulation de cette disposition donne l'impression fausse que l'Autorité effectuera nécessairement un contrôle systématique et continu du respect, par tous les acteurs concernés, du présent arrêté et de la conformité au RGPD de tous les traitements de données à caractère personnel qui seront effectués en vertu de cet arrêté.

IV. REMARQUES FINALES

48. L'Autorité rappelle :
    - La nécessité d'effectuer, conformément à l'article 35 du RGPD, une analyse d'impact relative à la protection des données avant la mise en place de tout traitement à grande échelle de données à caractère personnel relatives à la santé (voir aussi le point 39 des Guidelines précitées du CEPD) et de la soumettre pour avis à l'Autorité en cas de constatation de la subsistance de « risques résiduels » (par ailleurs, le CEPD recommande de publier cette analyse d'impact)
    - La nécessité de respecter les règles édictées par le Chapitre 5 du RGPD dans le cas où des données à caractère personnel feraient l'objet d'un transfert international (par exemple, parce que les données seraient conservées sur des serveurs situés en dehors de l'espace économique européen, ce que l'Autorité déconseille vivement dans le cadre du présent projet) ; et
    - L'obligation pour le responsable du traitement de mettre en place un système permettant aux utilisateurs du système/des applications de tracing envisagées d'exercer les droits qui leur sont conférés par le RGPD.

49. L'Autorité insiste :
    - Sur le fait qu'en aucun cas une application de traçage ne doit permettra la transmission en temps réel de l'information d'un contact avec une personne contaminée ;

50. L'Autorité attire l'attention du demandeur quant à la nécessité de stocker les données générées par le système mis en place dans une base de données distincte des bases de données (existante sou envisagées) contenant d'autres données dont la combinaison pourrait donner lieu à des utilisations illégitimes, inattendues ou illégales.

PAR CES MOTIFS,

L'Autorité estime, tout d'abord, que l'adoption de l'avant-projet et la mise en place d'un système de traçage par le biais d'applications numériques de dépistages de contact n'est possible que s'il est démontré que cette solution est strictement nécessaire et proportionnée à l'objectif de lutte contre la propagation du coronavirus COVID-19 parmi la population.

Si la nécessité et la proportionnalité de la mesure envisagée devait être démontrée, l'Autorité estime que l'avant-projet devra être adapté afin de répondre aux différentes remarques soulevées dans cet avis.

(sé) Alexandra Jaspar
Directrice du Centre de Connaissances

---

[i] Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21 April 2020.

[ii] Guidelines 04/2020on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21 April 2020, cons. 36

[iii] Pour rappel, et comme la Cour de justice de l'Union européenne l'a établi dans une jurisprudence constante, l'applicabilité directe des règlements européens emporte l'interdiction de leur retranscription dans le droit interne parce qu'un tel procédé peut "(créer) une équivoque en ce qui concerne tant la nature juridique des dispositions applicables que le moment de leur entrée en vigueur" (CJUE, 7 février 1973, Commission c. Italie (C-39/72), Recueil de jurisprudence, 1973, p. 101, § 17). Voyez, également et notamment, CJUE, 10 octobre 1973, Fratelli Variola S.p.A. c. Administration des finances italienne (C-34/73), Recueil de jurisprudence, 1973, p. 981, § 11 ; CJUE, 31 janvier 1978, Ratelli Zerbone Snc c. Amministrazione delle finanze dello Stato, Recueil de jurisprudence (C-94/77), 1978, p. 99, §§ 24-26.