Application de traçage des contacts - Belgique

Analyse d'impact relative à la protection des données (AIPD)

Sommaire

Ce document est une traduction de la version néerlandaise de l'analyse d'impact sur la protection des données. La version néerlandaise est le document original.

Notions

Accord de coopération d'exécution	Accord de coopération d'exécution du XXX entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano. (CET ACCORD SERA PUBLIÉ PROCHAINEMENT).
Analyse d'impact relative à la protection des données (AIPD)	Si un traitement de données risque de s'accompagner de risques élevés en ce qui concerne les droits et libertés des personnes physiques, le responsable du traitement ou le sous-traitant sont responsables de la réalisation d'une analyse d'impact relative à la protection des données afin d'évaluer l'origine, la nature, le caractère spécifique et la gravité de ce risque. Il convient de tenir compte du résultat de cette analyse pour déterminer les mesures adéquates devant être prises pour démontrer que l'AIPD est respectée lors du traitement des données à caractère personnel.
Anonymisation des données	Le traitement des données à caractère personnel d'une manière telle que ces données ne puissent plus être reliées à une personne spécifique et ne soient donc plus des données à caractère personnel.
API	Application Programming Interface. Cette interface fait en sorte que le logiciel puisse communiquer avec des logiciels types.
AR d'exécution	Arrêté royal du XXX portant exécution de l'Arrêté royal n°44 du 26 juin 2020 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano. (CET AR SERA PUBLIÉ PROCHAINEMENT).
Arrêté royal n°44	Arrêté royal n° 44 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano.
Base de données V	La Base de données V visée à l'Arrêté royal n° 44, qui reçoit le journal central des enregistrements des différents utilisateurs et qui est ultérieurement distribuées par CDN.
Base de données VI	Une base de données pour laquelle Sciensano est le responsable du traitement et dans laquelle sont enregistrés, de manière très

	temporaire, les résultats du test ainsi que le code du test, la date du prélèvement et la date à laquelle l'utilisateur est devenu contagieux, conformément au processus décrit à l'article 2, § 1er, 3° de l'AR d'exécution.
Clé chiffrée	Une clé chiffrée qui, après installation de l'appli, est générée quotidiennement et enregistrée sur le smartphone sur lequel l'appli a été installée. Cette clé est appelée Temporary Exposure Key (TEK) dans la documentation d'Apple et Google.
Code d'autorisation	Le code d'autorisation anonyme créé par la Base de données VI afin de permettre à l'utilisateur dont le test s'est révélé positif de charger les clés sécurisées dans la Base de données V.
Code de test	Un code qui se compose de chiffres aléatoires et qui est créé par l'appli lors de la demande d'un test.
Contact	Pour la recherche de contacts, un contact est un utilisateur qui a pris part à une interaction avec un utilisateur testé positif au virus, interaction dont la durée et la distance constituent un risque important de contamination.
Contact à risque	Un contact pendant au moins quinze minutes à moins de deux mètres de distance avec une personne infectée; ce contact est établi lorsqu'un numéro de série temporaire non personnalisé correspondant à un numéro de série non personnalisé émis par le smartphone d'un utilisateur infecté est trouvé sur un smartphone.
Content Delivery Network (CDN)	Un content delivery network, ou réseau de diffusion de contenu (RDC), est un réseau de serveurs périphériques déployés géographiquement qui proposent des informations au départ d'un point central aux utilisateurs finaux de ces informations. Son but est d'offrir une grande disponibilité et de hautes prestations en distribuant le service géographiquement pour les utilisateurs finaux.
Données à caractère personnel	Toute information se rapportant à une personne physique identifiée ou identifiable (la «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identificateur tel que : nom, numéro d'identification, données de localisation, identificateur en ligne ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
Données concernant la santé	Les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.
DP-3T (=Distributed Privacy-Preserving Proximity Tracking)	Un système sources ouvertes qui a été développé par suite du COVID-19 par un groupe paneuropéen d'universitaires spécialisés entre autres dans le cryptage, la sécurisation de l'information, la protection de la vie privée et l'épidémiologie, dans le but de faciliter le traçage de contacts par voie numérique.
Numéro de série temporaire non personnalisé	Combinaison aléatoire de uns et de zéros, émise par un smartphone sur lequel l'appli a été installée au moyen d'une balise Bluetooth qui se compose d'un chiffre aléatoire et du

	chiffrement de données anonymes du smartphone, comme la puissance du signal émis.
Personne concernée	La personne identifiée ou identifiable dont les données à caractère personnel sont traitées.
Pseudonymisation de données	Le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.
Responsable du traitement	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; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.
RGPD	Le Règlement général sur la protection des données (RGPD) (en anglais: General Data Protection Regulation (GDPR)) est un règlement européen (donc avec effet immédiat) qui standardise les règles de traitement des données à caractère personnel par les entreprises privées et les instances publiques dans l'ensemble de l'Union européenne. Son but n'est pas uniquement de garantir la protection des données à caractère personnel au sein de l'Union européenne mais également de garantir la libre circulation des données sur le marché interne européen.
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.
Traçage manuel des contacts	En cas de traçage manuel des contacts, les personnes ayant été en contact avec une personne (présumée) infectée par le Covid-19 sont tracées à l'aide d'interviews téléphoniques ou face à face par des acteurs autorisés (p. ex. les inspecteurs sanitaires).
Violation des données à caractère personnel/fuite de données	Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Cadre général

Le 11 mars 2020, l'organisation mondiale de la santé (OMS) a décrété que le virus SARS-CoV-2 était une pandémie. Le virus SARS-CoV-2 est un virus très contagieux à l'origine de la maladie COVID-19, qui cause des problèmes médicaux graves ou peut entraîner la mort principalement chez les personnes plus âgées et les personnes à antécédents médicaux.

La Belgique n'a pas été épargnée par cette pandémie et dans le cadre de la crise sanitaire liée au COVID-19 et afin d'endiguer la propagation de la maladie, un Conseil national de sécurité a été créé, dans lequel les responsables des autorités fédérales et des Etats fédérés se concertent afin de prendre des mesures harmonisées dans le but de limiter la propagation du COVID-19.

Dans le courant des mois de mars et avril 2020, tant les autorités fédérales que les gouvernements régionaux ont pris différentes mesures afin d'endiguer la propagation du COVID-19. Les mesures prises alors avaient principalement pour but de réduire au strict nécessaire les contacts physiques entre personnes afin de limiter la propagation du virus (le fameux 'lock-down light').

Par la suite, la crise du COVID-19 est entrée dans une nouvelle phase, au cours de laquelle le nombre d'hospitalisations et le nombre de décès dus au COVID-19 ont amorcé une tendance à la baisse. C'est pour cette raison que, sur la base de l'avis du Groupe d'experts en charge de l'exit strategy (GEES), le Conseil national de sécurité du 24 avril 2020 a établi un plan d'assouplissement graduel des contacts physiques autorisés entre les personnes et de déconfinement (l'exit strategy').

L'assouplissement des mesures, permettant à nouveau davantage de contacts physiques entre les personnes, entraîne évidemment un risque de voir augmenter à nouveau le nombre de cas de COVID-19. Témoin le début d'une deuxième vague en juillet 2020. Il est donc nécessaire que chaque nouvelle phase d'assouplissement s'accompagne des mesures nécessaires permettant d'éviter une nouvelle propagation du virus.

L'une de ces mesures concerne le traçage précoce des personnes ayant été infectées ou pour lesquelles il existe une probabilité qu'elles l'aient été, afin de pouvoir leur donner les recommandations nécessaires (quarantaine, télétravail, etc.) pour éviter qu'elles ne contaminent d'autres personnes avec le virus SARS-CoV-2.

Etant donné la contagiosité du virus SARS-CoV-2, il est conseillé de pouvoir détecter les personnes avec lesquelles la personne (présumée) contaminée a été en contact ('traçage des contacts'). Cela permet de donner à ces personnes les recommandations nécessaires (se faire tester, limiter les contacts, etc.) afin d'éviter une plus grande propagation du COVID-19.

Depuis que le virus SARS-CoV-2 a commencé à se répandre dans l'ensemble de l'Europe, les débats publics et politiques se sont de plus en plus concentrés sur une solution technologique à ce problème extrêmement urgent.

Une appli de traçage de contacts sur le smartphone de tout un chacun peut-elle permettre d'endiguer la pandémie ? Ces systèmes enregistreraient automatiquement les contacts interpersonnels entre tous les utilisateurs, permettant ainsi de tracer rapidement les signes d'infection. Par la suite, les personnes potentiellement exposées pourraient être tracées efficacement et pourraient donc être informées au stade précoce de l'infection et s'isoler.

Dans son avis, l'Autorité de protection des données (APD) insiste sur le fait que toute application de traçage doit répondre aux règles et spécifications fixées par l'EDPB (European Data Protection Board),

qui a publié des orientations et des outils ayant été utilisés dans la résolution du problème de sécurité et pour la rédaction de cette analyse de l'impact de la protection des données.

La Belgique a d'abord opté pour un traçage manuel des contacts comme cela était le cas jusqu'à présent pour les autres maladies infectieuses. Etant donné qu'il a été décidé par la suite de passer à une appli de traçage, la rédaction de la présente analyse d'impact relative à la protection des données s'est avérée nécessaire.

Introduction

Pour une bonne compréhension de la présente analyse d'impact relative à la protection des données, il est important de donner tout d'abord un aperçu succinct des plateformes et des traitements de données impliqués. Une description plus détaillée de l'architecture et des flux de données suivra plus loin (voir point 2.3.).

Le système de traçage numérique des contacts consiste d'une part en une application mobile que l'utilisateur (un citoyen) peut installer volontairement sur son téléphone (*GSM, smartphone*) et utiliser.. Au moyen d'une activation correcte de l'appli, un utilisateur peut, à l'aide de numéros de série temporaires non personnalisés Bluetooth (ou ID secrets), effectuer des échanges avec d'autres utilisateurs de l'appli avec lesquels il entre en contact rapproché. Ces contacts sont conservés temporairement dans l'appli pour que des alertes puissent être envoyées en cas de contamination. D'autre part, le système comporte une infrastructure de serveurs correspondante qui facilite la consultation d'un résultat de test personnel et l'envoi anonyme d'alertes aux contacts à risque d'une personne ayant un test de laboratoire positif.

L'infrastructure de serveurs se compose de deux bases de données (abrégé BD). Il s'agit des deux bases de données suivantes.

- **La base de données des résultats des tests (=Base de données VI):** une base de données permettant d'échanger avec l'utilisateur de l'application les résultats des tests labo COVID-19 réalisés et de lui conférer un code de test. Le code de test est nécessaire pour une communication fiable sur les contaminations avec la base de données centrale.
- **La base de données centrale avec le journal central des enregistrements de l'application de traçage (=Base de données V):** une base de données destinée à l'échange des clés chiffrées pour alerter d'autres citoyens qu'ils sont entrés en contact avec une personne infectée. Dans le cas d'une contamination confirmée, l'utilisateur peut choisir de partager avec la base de données centrale sa liste de clés chiffrées représentative des journées où l'utilisateur était contagieux.

En d'autres termes, il existe deux plateformes où des données peuvent être traitées : 1) une application mobile et 2) une infrastructure de serveurs avec bases de données. Comme il apparaîtra plus loin, l'utilisateur de l'appareil conserve son autonomie. Il décide lui-même de l'installation et de l'utilisation de l'application et il décide également d'échanger ou non des données avec l'infrastructure de serveurs. L'utilisateur a également toujours la possibilité de désactiver temporairement l'application sans devoir pour autant désactiver le Bluetooth de l'appareil.

Tableau 1. Aperçu des plateformes et des traitements de données

	App *(= proposée par les entités fédérées, gestion volontaire par l'utilisateur)*	Plateforme centrale *(= infrastructure de serveurs gérée par Sciensano)*
Echange de contacts	-Création de clés chiffrées -Création d'ID aléatoires temporaires -Envoi d'ID aléatoires temporaires -Réception de jetons Bluetooth et stockage de ces jetons avec des données complémentaires	
Demande de testing COVID	-Création code de test R1 -Polling de la base de données pour les résultats -Chargement de clés chiffrées pertinentes vers la base de données centrale	-Rendre disponibles les résultats du test COVID -Suppression des résultats -Création code d'autorisation -Réception des clés chiffrées
Traçage des contacts	-Téléchargement des clés chiffrées des personnes infectées -Calcul des contacts à risque sur la base des clés chiffrées et des ID aléatoires enregistrés en relation avec la durée et la distance des contacts	-Distribution des clés chiffrées via CDN

Pour des raisons de cohérence, cette analyse d'impact relative à la protection des données utilise la même terminologie que le cadre juridique pour le traçage des contacts. Ce cadre juridique régule tant les bases de données du traçage manuel que les bases de données du traçage numérique. Il est question au total de six bases de données définies par un numéro (pour plus de détails, voir les définitions de l'AR n°44, l'Accord de coopération, l'AR d'exécution et l'Accord de coopération d'exécution). Comme indiqué, seules les bases de données V et VI font partie de l'application de traçage des contacts. Voici à titre d'information complémentaire une description succincte des quatre autres bases de données créées pour l'organisation du traçage de contacts manuel:

- Base de données I reprenant les données de contact et de santé des personnes avec une infection (présumée) communiquée par les hôpitaux, les laboratoires, les médecins généralistes et les collaborateurs du centre de contact. Il s'agit d'une base de données centrale gérée par Sciensano qui alimente les bases de données II, III et VI.
- Base de données II de Sciensano reprenant les données pseudonymisées pour la recherche épidémiologique en matière de propagation du COVID-19.
- Base de données III des entités fédérées reprenant les instructions d'appel destinées aux collaborateurs du centre de contacts des entités fédérées.
- Base de données IV des entités fédérées reprenant les coordonnées des médecins ou des responsables administratifs des collectivités (p. ex. écoles, crèches, ateliers, etc.) visant à les informer des risques de contamination.

Même si toutes ces bases de données sont reprises dans un même cadre juridique, il est important de mentionner qu'il existe des différences strictes dans la gestion de ces bases de données distinctes.

Section I: Identification de la nécessité d'une analyse d'impact relative à la protection des données

L'application belge de traçage des contacts et l'infrastructure de serveurs correspondante offrent un support pour la communication relative aux contaminations (*p. ex. résultats des tests labo*), aux risques sanitaires (*contacts rapprochés avec un patient COVID-19*) et aux mesures de prévention visant à lutter contre la propagation du virus (*p. ex. quarantaine*).

Vu

- l'article 35 du RGPD,
- la liste des types de traitements pour lesquels une analyse d'impact relative à la protection des données (en abrégé AIPD) est toujours obligatoire comme stipulé par l'Autorité belge de la protection des données et la Vlaamse Toezichtcommissie ;
- la Standard Operating Procedure (SOP) I/00/24/N Data Protection Impact Assessment de Sciensano et
- les orientations du Groupe de travail Article 29 pour les analyses d'impact relatives à la protection des données ou un traitement « impliquant probablement un risque élevé » au sens du Règlement 2016/679

il est estimé que les traitements de données relatifs à l'architecture de l'application de traçage des contacts exigent une AIPD.

La décision de la nécessité de procéder à une AIPD se base en particulier sur les éléments suivants :

- l'architecture du système de traçage numérique des contacts permet un traitement à grande échelle d'une catégorie particulière de données à caractère personnel, à savoir les données concernant la santé. Il s'agit de données liées à des contaminations et/ou à des risques en matière de contamination par le coronavirus COVID-19 (voir point 2.2). L'appli est proposée sur une base volontaire à toutes les personnes habitant en Belgique et possédant un smartphone. Attention: 'A grande échelle' dépend toutefois du nombre d'utilisateurs de l'application ainsi que du nombre de contaminations.
- L'application de traçage a l'ambition d'être accessible. Tout citoyen belge à partir de 13 ans, en possession d'un smartphone, devrait en principe avoir la possibilité d'installer l'application de traçage sur son smartphone s'il le souhaite et d'échanger des données. Cela concerne également les personnes vulnérables comme les enfants (à partir de 13 ans), les travailleurs, les malades mentaux, les demandeurs d'asile, les personnes âgées, etc.
- C'est la technologie Cloud qui est utilisée pour le traitement. L'infrastructure des serveurs fait en effet appel aux services cloud d'AWS pour conserver temporairement des données.
- Utilisation ou implémentation innovantes de nouvelles solutions technologiques et organisationnelles : utilisation de la technologie Bluetooth permettant de calculer la proximité d'autres personnes dans le cadre de l'identification de contacts à risque.

La présente AIPD ne concerne pas les traitements de données pour le traçage manuel des contacts effectué via les centres de contact, les inspecteurs sanitaires et les équipes mobiles des entités fédérées.

Section II: Description des traitements de données

2.1. Données à caractère personnel

Les personnes dont les données sont traitées sont les utilisateurs de l'application de traçage des contacts. Il s'agit des citoyens qui téléchargent et activent cette appli volontairement sur leur smartphone. En fonction du traitement et de la plateforme de traitement, elles peuvent avoir différentes qualités ; par exemple :

- personne qui vient à proximité d'un autre utilisateur de l'appli et reçoit de ce fait des signaux Bluetooth qui sont enregistrés temporairement par l'appli.
- Personne qui fait effectuer un test labo COVID-19 par un médecin et qui demande le résultat de ce test via son appli.
- Personne qui envoie le résultat positif du test et une liste d'enregistrements via son appli vers une base de données centrale pour alerter du risque de contamination d'autres personnes avec lesquelles elle a été en contact. Lors du traitement de ces données, celles-ci sont pseudonymisées d'une manière telle qu'il est pratiquement impossible de savoir qui est la personne infectée.
- Personne qui reçoit via son appli une alerte l'avertissant qu'elle a été en contact avec une personne infectée, ainsi que des instructions d'action (p. ex. se faire tester, s'isoler, se rendre chez le médecin).

Il s'agit de données d'identification pseudonymisées et si d'application, de données concernant la santé et relatives à un séjour à l'étranger.

Données d'identification pseudonymisées

Une application de traçage de contacts numérique basée sur le système DP-3T ne stocke que des données pseudonymisées, sur l'appareil de l'utilisateur, à savoir des clés chiffrées et des numéros de séries temporaires non personnalisés, sans renvoyer à l'identité des personnes avec lesquelles le contact a eu lieu, ni l'endroit où ce contact a eu lieu. La date à laquelle le contact a eu lieu est en revanche conservée parce qu'elle est nécessaire pour pouvoir constater si le contact a eu lieu entre le début de la contagiosité et la constatation de l'infection.

D'un point de vue technique, on pourrait affirmer que les clés chiffrées qui sont utilisées sur l'appareil de l'utilisateur et qui sont propres à un utilisateur pourraient encore (et uniquement en faisant appel à des techniques de hacking) permettre de décoder les numéros de série partagés de ce même utilisateur et de les relier à cet utilisateur. Donc, même si c'est plutôt théorique par nature, il existe donc encore une clé et c'est la raison pour laquelle les données doivent être considérées comme pseudonymisées plutôt que comme anonymisées. L'accès à ces clés chiffrées est protégé, également pour l'utilisateur. Ce n'est que moyennant un accès aux appareils et l'utilisation des techniques de hacking nécessaires qu'il est éventuellement possible de réussir à déchiffrer la clé. Et la seule chose que cela dévoilerait, c'est si l'utilisateur s'est identifié comme un utilisateur infecté ou non. Au niveau central, aucun déchiffrage n'est toutefois possible. Les autres utilisateurs non plus ne sont pas en mesure de relier de quelque manière que ce soit à un individu les numéros de série partagés.

Données concernant la santé

Si un utilisateur de l'application fait effectuer un test labo COVID-19 (ou se rend chez un médecin en raison de symptômes COVID-19), les données suivantes seront traitées:

- code de test ;
- date probable à laquelle l'utilisateur est devenu contagieux;
- date de prélèvement pour le test labo COVID-19 (ou consultation) ;
- résultat du test labo;
- forte présomption de contamination de la part du médecin (malgré un test labo négatif ou en cas d'impossibilité de réaliser un test).

Plusieurs de ces variables doivent actuellement déjà être obligatoirement enregistrées par les médecins et par les laboratoires dans le cadre du traçage manuel des contacts, dans le cadre duquel le centre de contact des Etats fédérés utilise de telles données pour organiser les missions téléphoniques ou les visites sur le terrain[1] . Les variables 'code de test' et 'date probable à laquelle l'utilisateur est devenu contagieux' sont ajoutées pour les utilisateurs de l'application de traçage dans les systèmes d'enregistrement existants des médecins pour soutenir de cette façon certaines fonctions de l'application (voir point 2.3.2.)..

Données relatives à un séjour à l'étranger: pays de l'EEE

Un utilisateur contaminé qui veut alerter les personnes avec lesquelles il a été en contact étroit a la possibilité de communiquer les pays de l'Espace économique européen (EEE) où il a séjourné pendant l'infection afin qu'une interaction avec les applications de traçage de ces pays soit possible.

2.2. Parties impliquées

Sciensano

Sciensano, institution publique sui generis dotée de la personnalité juridique, inscrite à la Banque-carrefour des Entreprises sous le numéro 0693.876.830, ayant son siège social rue Juliette Wytsman 14 à 1050 Ixelles, est une institution publique qui remplit des missions de support à la politique sanitaire pour différents niveaux politiques. Ces missions concernent entre autres la recherche scientifique, les avis d'experts et la gestion des risques. Dans le cadre de ces missions, il est expérimenté dans l'application de principes de protection des données pour les données concernant la santé et dans l'implémentation de méthodes de sécurisation et de pseudonymisation de données.

Comme stipulé à l'Arrêté royal n°44 et dans le futur Accord de coopération[2], Sciensano est le responsable du traitement pour la base de données contenant la liste d'enregistrements centrale de l'application de traçage (Base de données V) . A côté de cette base de données avec journal central

[1] *Pour plus d'informations sur les traitements de données dans le cadre du traçage manuel des contacts : voir Déclaration de confidentialité :*
https://www.sciensano.be/sites/default/files/20200701_kennisgeving_burgers_centrale_database_sciensano_v4_fr.pdf

[2] *Accord de coopération du XXX entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano. (CET ACCORD SERA PUBLIÉ PROCHAINEMENT).*

des enregistrements, Sciensano est également responsable du traitement pour la base de données des résultats de tests (Base de données VI) pour laquelle il fournit un nombre limité de données via la base de données qu'il possède déjà pour le traçage manuel des contacts (Base de données I).

Le service healthdata.be de Sciensano est chargé de la gestion des bases de données en question. Ce service dont les missions concernent la facilitation technique de bases de données (de santé) est indépendant des services de Sciensano chargés de la recherche épidémiologique. Sciensano veille à ce qu'aucun croisement ne soit établi avec les autres bases de données qu'il gère.[3]

Administrations (sanitaires) des entités fédérées

Etant donné les règles de partage des compétences en matière de soins de santé préventifs, l'art. 14 § 3 du futur Accord de coopération stipule que les entités fédérées sont responsables de la mise à disposition de l'application de traçage des contacts.

Les administrations concernées des entités fédérées sont les suivantes:

- Vlaams Agentschap Zorg en Gezondheid (VAZG), inscrite à la Banque-carrefour des Entreprises sous le numéro 0316.380.841, dont les bureaux sont situés boulevard du Roi Albert II 35, boîte 33, 1030 Bruxelles.
- Agence Wallonne pour une Vie de Qualité (AVIQ), inscrite à la Banque-carrefour des Entreprises sous le numéro 0646.877.855, dont les bureaux sont situés rue de la Rivelaine 21, 6061 Charleroi.
- Les Services du Collège réuni (SCR) de la Commission communautaire commune (Cocom), inscrite à la Banque-carrefour des Entreprises sous le numéro 0240.682.833, dont les bureaux sont situés rue Belliard 71, boîte 1, 1040 Bruxelles.
- Le Ministerium der Deutschsprachigen Gemeinschaft (MDG), inscrit à la Banque-carrefour des Entreprises sous le numéro 0332.582.613, dont les bureaux sont situés Gospertstrasse 1, 4700 Eupen.

Sous-traitants

Pour le développement, la mise en production, l'entretien et les activités de support de l'appli et le back-office de l'application de traçage, un cahier des charges a été émis: https://www.corona-tracking.info/wp-content/uploads/2020/07/Smals-BB-001-031-2020.pdf

- Les entités fédérées ont attribué le marché à la firme DEVSIDE inscrite à la Banque-carrefour des Entreprises sous le numéro 0892.864.907, dont les bureaux sont situés avenue J.F. Debecker 107, 1200 Woluwe-Saint-Lambert, avec pour sous-traitant IXOR inscrit à la Banque-carrefour des Entreprises sous le numéro 0478.493.179, dont les bureaux sont situés Schuttersvest 75, 2800 Mechelen.

Pour l'infrastructure de serveurs, Sciensano fera appel dans le cadre de l'application de traçage au Cloud AWS d'Amazon via le fournisseur SoftwareONE, inscrit à la Banque-carrefour des Entreprises sous le numéro BE 0844.127.058, dont les bureaux sont situés Esplanade 1 boîte 3, Suite 315, 1020

[3] *Voir entre autres également les explications générales de l'AR n°44 relatives à la Base de données V : « Sciensano doit s'assurer que les mesures techniques et organisationnelles nécessaires ont été prises pour protéger le journal des enregistrements, et que les données de celui-ci ne sont pas croisées avec d'autres bases de données ».*

Bruxelles. Amazon et leur fournisseur conserveront temporairement les données pour le compte de Sciensano en tant que sous-traitants.

Médecins généralistes, médecins hospitaliers et médecins actifs dans les postes de triage

Dans le cadre du fonctionnement de l'application de traçage des contacts, les médecins devront, en plus des enregistrements déjà obligatoires dans le cadre du traçage manuel, également enregistrer et communiquer des données supplémentaires à Sciensano via les canaux existants (entre autres eForms)[4]. Ces données supplémentaires sont un code de test et la date probable de l'infection.

Apple et Google

Les candidats-utilisateurs de l'application de traçage doivent, en fonction du type de smartphone qu'ils utilisent, la télécharger au départ de l'Apple App Store (iOS) ou du Google Play Store (Android). Les deux environnements de téléchargement sont accessibles au public.

Apple et Google ont développé une interface API pour permettre le développement d'applications de traçage sur la base du protocole DP-3T et pour le faire fonctionner sur leur système d'exploitation (IOS ou Android). La conception de l'API et le système dont l'API fait partie empêchent que Apple et Google aient accès aux données relatives aux utilisateurs. Voir aussi la note "Exposure Notification. Frequently Asked Questions" d'Apple et Google: *"In keeping with our privacy guidelines, Apple and Google will not receive identifying information about the user, location data, or information about any other devices the user has been in proximity of."*

https://blog.google/documents/73/Exposure_Notification_-_FAQ_v1.1.pdf

Pour faciliter l'utilisation de l'interface API de notification d'exposition de Google et d'Apple, l'utilisation de couches sous-jacentes du système d'exploitation peut s'avérer nécessaire. C'est ainsi que sur Android, l'API reposera sur « Google Play Services » qui fournira un certain nombre de services de base à l'application de traçage des contacts comme c'est le cas pour d'autres applis sur l'appareil. Lors de l'utilisation de ces services, Google collectera des données sur l'appareil, les applications, la localisation et les services. Le traitement de ces données ne fait à proprement parler pas partie des traitements de l'application de traçage des contacts et il est concerné par un consentement donné par l'utilisateur au moment de configurer son compte Google ou au moment de la mise en service de son appareil. Il convient de faire remarquer que les données collectées ne contiennent pas de données relatives au contenu de l'application de traçage des contacts.

Commission européenne et autorités sanitaires concernées des pays membres de l'EEE

Les pays membres de la Commission européenne ont signé un accord pour permettre l'échange de données entre les applications nationales de traçage des contacts. De ce fait, les citoyens qui utilisent l'application belge de traçage des contacts peuvent également, pendant ou après un séjour dans un autre pays de l'Espace économique européen, détecter des contacts et en cas de contamination, les alerter. A cet effet, la Commission européenne propose une passerelle de fédération. Cette passerelle se compose d'une infrastructure IT sécurisée qui prévoit une interface commune où les autorités

[4] Pour plus d'infos: voir Délibération n°20/132 du 3 mai 2020, modifiée le 13 mai 2020, le 2 juin 2020, le 7 juillet 2020 et le 31 juillet 2020 du Comité de sécurité de l'information Chambre Sécurité sociale et santé, relative à la communication de données à caractère personnel par divers prestataires de soins ou organisations actives dans le domaine de la santé ou des soins à Sciensano et à leur communication ultérieure dans le cadre de la lutte contre la propagation du coronavirus Sars-cov-2.

sanitaires de pays de l'Espace économique européen peuvent échanger une collecte minimale de données (voir point 2.3.3.).

En tant que fournisseur de solutions techniques et organisationnelles pour la passerelle de fédération, la Commission traite des données à caractère personnel pseudonymisées au nom des autorités sanitaires concernées des pays membres qui participent en tant que responsables du traitement communs à la passerelle de fédération et elle est à ce titre un sous-traitant. Ces rôles sont décrits à l'article 7 bis de la *Décision d'exécution (UE) 2020/1023 de la Commission du 15 juillet 2020 modifiant la décision d'exécution (UE) 2019/1765 en ce qui concerne l'échange transfrontière de données entre les applications mobiles nationales de suivi de contacts et d'alerte dans le cadre de la lutte contre la pandémie de COVID-19 .*

2.3. Traitements des données

Cette section fournit une description et une illustration étape par étape des opérations de traitement des données.

2.3.1. Traitements des données en cas de contacts avec un autre citoyen

Le citoyen a installé avec succès l'application de traçage ou 'Appli Coronalert' sur son téléphone et il a activé tous les paramètres permettant un bon fonctionnement de l'appli. Désormais, le module "notifications d'exposition au COVID-19[5]" (également connu comme exposure logging) est actif en combinaison avec l'appli, en arrière-plan. (Attention: l'utilisateur peut toujours s'il le souhaite désactiver temporairement ce module, sans pour autant devoir désactiver le Bluetooth sur son appareil) (Voir également les écrans d'activation de l'appli dans la présentation corresponsante).

Les actions suivantes sont exécutées en arrière-plan :

- chaque jour, l'appli crée une nouvelle clé chiffrée temporaire[6] (TEK / Temporary Exposure Key) et la conserve sur le téléphone pour une période de 14 jours avec la date ;
- toutes les 10 à 20 minutes, l'appli crée un ID aléatoire[7] sur la base de la clé chiffrée ;
- chaque 0,5 seconde, l'appareil émet via Bluetooth les numéros de série temporaires non personnalisés (jetons Bluetooth) vers les autres smartphones dans les environs qui utilisent l'Appli Coronalert ;
- chaque appareil équipé d'une appli de notification reçoit les numéros de série temporaires non personnalisés toutes les 2,5 à 5 minutes pendant 4 secondes et il conserve ces ID aléatoires sur le téléphone pour une période de 14 jours avec la date et la force du signal Bluetooth.

[5] Les notifications d'exposition au COVID-19 se trouvent dans les paramètres du téléphone. Pour Android: Paramètres > Paramètres Google > Notifications d'exposition au COVID-19 ; pour iOS: Paramètres > Privacy > Santé ou Bluetooth > Exposition au COVID-19.
[6] Texte aléatoire (texte et chiffres) de 128 bits
[7] Numéro aléatoire de 128 bits

Schéma échange ID aléatoires:

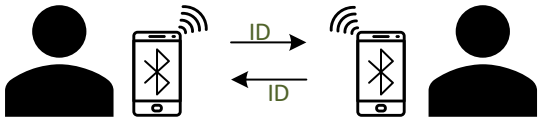


Schéma liste des ID envoyés et reçus:

SEND ID		
DAY→	KEY→	ID
D01	K-A	ID 01 ID ... ID 72
D...	K-..	ID 01 ID ... ID 72
D14	K-N	ID 01 ID ... ID 72

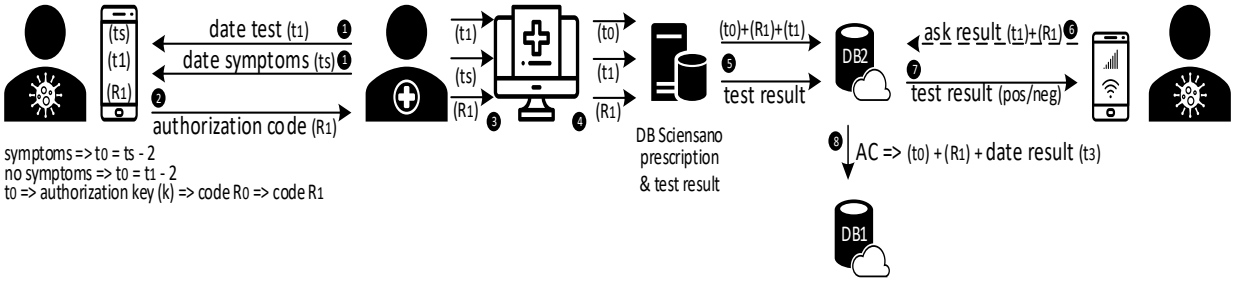
RECEIVED ID		
DAY→	ID →	SIGNAL
D01	ID X ID Y ID ..	-68 -68 -...
D...	ID X ID Y ID ..	-70 -73 -...
D14	ID X ID Y ID ..	-90 -76 -...

L'appli utilise le module "notifications d'exposition au COVID-19" de Google et Apple. Plus d'informations sur ce module de Google et Apple:
Google: https://www.google.com/covid19/exposurenotifications/
Apple: https://www.apple.com/covid19/contacttraçage

L'appli belge de notification du coronavirus est capable d'émettre des numéros de série temporaires non personnalisés (jetons Bluetooth) vers et d'en recevoir des applis de notification d'autres pays de l'Espace économique européen (EEE). La condition est toutefois que ces applis utilisent également le protocole DP-3T Protocol (Distributed Privacy-Preserving Proximity Tracking) et le module de Google et Apple.

2.3.2. Traitements des données lors d'un test COVID-19

Schéma réalisation d'un test COVID-19 jusqu'à réception du résultat du test



Aperçu des abréviations

dates

t0 = date probable de l'infection
- en cas de symptômes = date du début des symptômes (ts) - 2
- si asymptomatique = date test (t1) - 2

t1 = date à laquelle le test a été réalisé (ou la date de la consultation au cours de laquelle une demande de labo a été rédigée)

t2 = date à laquelle le labo communique le résultat du test à Sciensano

t3 = date à laquelle l'appli traite la notification du résultat du test

ts = date de début des symptômes

clés

TEK (Temporary Exposure Key) = clé chiffrée (change tous les jours) pour créer des ID aléatoires

K = clé d'autorisation secrète unique créée dans l'appli

codes

ID = code aléatoire créé sur la base de la clé chiffrée (TEK)

R0 = numéro de test personnel créé dans l'appli sur la base de la clé secrète unique (K)

R1 = code de test partagé créé dans l'appli sur la base du numéro de test personnel (R0)

AC = code d'autorisation composé d'une signature numérique sur le code de test et des données pertinentes

Bases de données gérées par Sciensano

BD Sciensano = base de données pour le traçage manuel des contacts (contenant entre autres des prescriptions et des résultats de tests labo pour le COVID-19). Cette base de données fournit des données à la plateforme sans en faire elle-même partie

BD1 = base de données destinée à l'échange de clés chiffrées, dans le but d'alerter d'autres citoyens qu'ils ont été en contact avec une personne infectée, appelée également Base de données V

BD2 = base de données destinée à l'échange de l'évaluation du résultat du test, appelée également Base de données IV, dans le but d'informer la personne infectée et de créer un code d'autorisation (CA) et de l'envoyer à la BD1

Information du citoyen quant aux possibilités de l'appli

Le citoyen fait réaliser un test COVID-19 chez un prestataire de soins. Le médecin qui prescrit un test de dépistage pour le COVID-19 demande au citoyen s'il utilise l'application de traçage des contacts. Si le citoyen dispose de l'appli, le médecin lui explique brièvement qu'il est possible de recevoir dans l'application une notification du résultat du test. Et qu'en cas de résultat positif, le citoyen a le choix d'alerter anonymement via l'appli les personnes avec lesquelles il a été en contact. Pour soutenir le processus d'information, des formations sont organisées pour les (organisations de) médecins, des brochures d'information sont distribuées et un site web (www.coronalert.be) a été lancé. Les écrans de l'application, qui ont été testés sur le plan de la facilité d'utilisation, contiennent également les explications nécessaires.

Création du code de test partagé

Si le citoyen souhaite utiliser l'appli à cet effet, le médecin vérifie s'il y a des symptômes. En cas de symptômes, le médecin détermine en accord avec son patient à quelle date ces symptômes ont commencé (ts). En l'absence de symptômes, cette date n'est pas déterminée. Le médecin demande au citoyen d'introduire la date du test (t1) dans l'appli et en cas de symptômes, d'introduire également la date de leur début (ts). A l'arrière-plan, l'application détermine la date probable de l'infection (t0). En cas de symptômes, on retire 2 jours de cette date de début des symptômes (ts). En l'absence de symptômes, 2 jours sont retirés de la date du test (t1). Ensuite, l'application crée une clé d'autorisation secrète unique (K) et ensuite, sur la base de cette clé, un numéro de test personnel (RO). L'application crée ensuite un code de test partagé (R1) et le rend visible dans l'appli. Le citoyen partage ce code avec le médecin. Cela peut se faire au cours d'un entretien, peut être lu à l'écran ou le médecin peut également le scanner.

Communication du code de test à Sciensano

Le médecin enregistre le code de test (R1), la date du test (ou de la consultation) (t1) et en cas de symptômes, la date de leur début (ts) dans un eForm (eFormulaire). La date probable de l'infection (t0) est, tout comme dans l'appli, calculée sur la base des informations saisies. Ce formulaire est envoyé à Sciensano. Par défaut, cet eFormulaire est "Notification et demande d'analyse de laboratoire pour suspicion d'infection au SARS-COV-2". Sciensano traite et conserve les informations dans la base de données qu'il possède déjà pour les prescriptions et les résultats de tests (DB Sciensano prescription & test result).

Le médecin a également la possibilité de déclarer qu'il est question d'une infection COVID-19 sans devoir attendre le résultat du test. Dans ce cas, le médecin enregistre le code de test (R1), la date probable de l'infection (t0) et la date du test (ou de la consultation) (t1) dans l'eFormulaire "Demande directe de suivi de contacts pour une suspicion très forte de COVID-19 indépendamment du résultat du test". C'est également possible en combinaison avec l'eFormulaire "Notification et demande d'analyse de laboratoire pour suspicion d'infection au SARS-COV-2".

Exécution du processus du test PCR pour le COVID-19

Le processus du test PCR donne lieu à l'obtention d'un résultat de test positif ou négatif. Ce processus consiste à prélever un échantillon pour test PCR (médecin généraliste/poste de triage/hôpital), à l'envoyer à un laboratoire, à traiter le test en laboratoire et à en partager le résultat avec Sciensano et le médecin généraliste.

Traitement du résultat du test chez Sciensano

Dès que Sciensano reçoit un résultat de test d'un laboratoire, débute un processus de traitement destiné à soutenir la recherche manuelle des contacts et ensuite, l'application. Pour l'appli, commence un processus de traitement dans le cadre duquel Sciensano copie le résultat du test (positif/négatif) dans la base de données VI (BD2/DB2 dans le schéma). Après cette action, Sciensano supprime le code de test partagé (R1) dans sa base de données (BD Sciensano). Le citoyen est identifié sur la base du code de test partagé (R1) et de la date probable de l'infection (t0).

Consultation du résultat du test dans l'appli

Toutes les 2 heures, l'appli pose une question, à l'arrière-plan et automatiquement, à la Base de données VI (BD2/DB2 dans le schéma) de Sciensano pour connaître le résultat du test. Pouréviter que des notifications de résultats de tests soient envoyées à des mauvaises personnes, l'appli envoie le code de test partagé (R1) et la date du test (t1) avec la question. En langage technique, l'ensemble de ce processus porte le nom de « polling » et dans le schéma, ceci est décrit comme "ask result (t0) + (R1)".

La Base de données VI (BD2/DB2 dans le schéma) dispose de trois réponses possibles à la question posée par l'appli :

- le résultat du test n'est pas encore disponible
- le résultat du test est disponible et a été estimé négatif
- le résultat du test est disponible et a été estimé positif

En cas de résultat négatif, le médecin a la possibilité de le 'remplacer' par un résultat de test positif. Le médecin enregistre cette donnée via l'eFormulaire "Demande de suivi de contacts pour un résultat de test négatif". Ce processus de remplacement d'un résultat de test négatif est décrit en détail dans le document suivant: https://covid-19.sciensano.be/sites/default/files/Covid19/COVID-19_procedure_GP_FR.pdf

Le cadre technologique de l'appli ne permet pas directement de faire modifier un résultat négatif en un résultat positif. La procédure prévue est que le médecin doit demander à la personne infectée de créer un nouveau code de test partagé et de le transmettre. Le médecin remplit l'eFormulaire "Demande directe de suivi de contacts pour une suspicion très forte de COVID-19 indépendamment du résultat du test" et l'envoie à Sciensano. Quelques heures plus tard, la personne infectée recevra une nouvelle notification, cette fois avec pour message qu'il y a un résultat de test positif. Si le médecin n'applique pas cette procédure, le traçage manuel reste d'application et la personne infectée n'aura pas la possibilité d'alerter d'autres citoyens via l'appli.

Que se passe-t-il si un citoyen passe un test sans consulter un médecin ? Via un site web distinct, les citoyens, en possession d'un code spécial (par exemple au retour d'une zone rouge), pourront enregistrer un test ainsi que la date du test de prélèvement (t1) et/ou la date d'apparition des symptômes (ts), suivie du code d'autorisation partagée (R1).

2.3.3. Traitements après la réception de la notification du résultat du test

Lorsque le citoyen reçoit une notification dans l'appli avec estimation du résultat du test, il peut alerter via l'appli les citoyens qui ont été en contact avec lui. Cette possibilité est active dans l'appli pendant une période de 24 heures. Ensuite, cette option est désactivée et sont exécutées les actions prévues dans « Non-alerte des citoyens via l'appli ».

L'alerte est envoyée aux citoyens qui utilisent l'appli de notification du corona belge, ou une appli de notification du corona proposée par un autre pays de l'Espace économique européen (EEE). La condition est toutefois que ces applis utilisent également le protocole DP-3T (Distributed Privacy-Preserving Proximity Tracking).

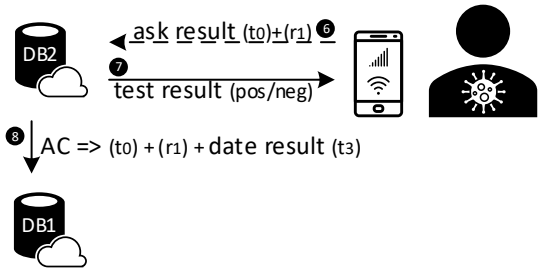
Envoi d'une signature de la BD2 à la BD 1

Dès que l'appli reçoit la notification, la BD2 enregistre la date (t3) de cette action[8]. Pour une estimation positive du résultat du test, la Base de données VI (BD2) informe la base de données V (BD1) de Sciensano. A cet effet, la Base de données VI crée une signature unique, composée du code de test partagé (R1) du citoyen, la date probable de l'infection (t0) et la date à laquelle le résultat du test a été demandé par l'appli (t3).

Une fois que l'appli a créé et envoyé la signature, Sciensano supprime de sa Base de données VI (BD2/DB2 dans le schéma) la date probable de l'infection (t0), le code de test partagé (R1) et le résultat du test.

[8] Cette action a lieu 1 fois par heure.

Schéma de l'envoi de la signature de la BD2 à la BD1



Non-alerte des citoyens via l'appli

Si le citoyen indique ne pas vouloir alerter ses concitoyens, l'appli supprime les informations suivantes :

- la date probable de l'infection (t0)
- le numéro de test personnel (R0)
- le code de test partagé (R1)
- la date à laquelle le test a été effectué (t1)
- la clé d'autorisation secrète unique (K) (qui a été utilisée pour créer le numéro de test personnel (R0))
- la date à laquelle l'appli a reçu la notification (t3)

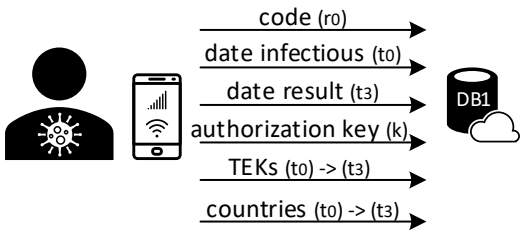
Alerte des citoyens via l'appli

Si le citoyen indique vouloir alerter ses concitoyens, l'appli demande en première instance dans quels pays il a séjourné pendant la période autour de la date de l'infection présumée jusqu'à la réception de la notification. Ensuite, l'appli partage les informations suivantes avec la base de données 1 (BD1) de Sciensano:

- la date probable de l'infection (t0)
- le numéro de test personnel (R0)
- la clé d'autorisation secrète unique (K) (qui a été utilisée pour créer le numéro de test personnel (R0))
- la date à laquelle l'appli a reçu la notification (t3)
- les clés chiffrées (TEK) des jours entre la date probable de l'infection (t0) et la date à laquelle l'appli a reçu la notification (t3)

Une fois la dernière clé chiffrée (TEK) envoyée, l'appli supprime la date probable de l'infection (t0), le numéro de test personnel (R0), le code de test partagé (R1), la date à laquelle le test a été effectué (t1), la clé d'autorisation secrète unique (K) et la date à laquelle l'appli a reçu la notification (t3).

Schéma de l'envoi des informations à la BD1 de Sciensano pour alerter les autres citoyens



Traitement de la demande d'alerte (Sciensano)

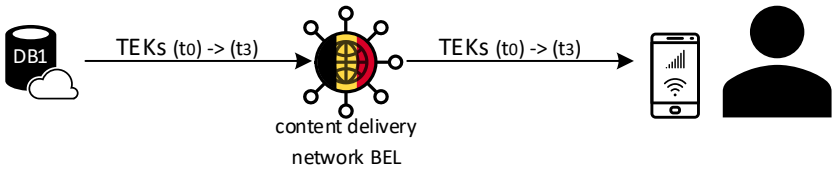
La base de données V (BD1/DB1 dans le schéma) de Sciensano traite toutes les 2 heures toutes les informations reçues et effectue un contrôle d'autorisation. Seuls les citoyens ayant une estimation positive du résultat du test sont autorisés à alerter leurs concitoyens. Ce contrôle se déroule selon les étapes suivantes:

- calcul du code de test partagé (R1), à l'aide de la date probable de l'infection (t0), de la clé d'autorisation secrète unique (K) et du numéro de test personnel (R0) ;
- création de la signature unique (AC), composée du code de test partagé (R1), de la date probable de l'infection (t0), et de la date à laquelle l'appli a reçu la notification (t3) ;
- vérifier s'il existe une signature (AC) dans la liste (des 48 dernières heures) que la base de données VI (BD2/DB2 dans le schéma) a transmise.

Alerte de citoyens qui utilisent une application de notification du coronavirus

S'il existe un code d'autorisation (CA), la Base de données V (BD1/DB1 dans le schéma) de Sciensano envoie les clés chiffrées (clés TEK) des jours entre la date probable de l'infection (t0) et la date à laquelle l'appli a reçu la notification (t3) au Content delivery network (CDN) de Belgique. Cette partie technique fait en sorte que tous les citoyens qui utilisent l'appli de notification du coronavirus reçoivent ces clés. Par la suite, l'appli effectuera une recherche, pour vérifier si elle dispose de tous les ID aléatoires qui ont été créés avec ces clés. S'il y a une correspondance, l'appli vérifie combien de temps le contact a duré et quelle était la distance entre l'utilisateur et une personne contagieuse (L'algorithme appliqué à cet effet est documenté au chapitre 5.3. de https://www.esat.kuleuven.be/cosic/sites/corona-app/wp content/uploads/sites/8/2020/08/coronalert_belgium_description_v1_2.pdf). En fonction de la réponse, l'appli enverra une notification au citoyen et lui conseillera l'attitude à adopter.

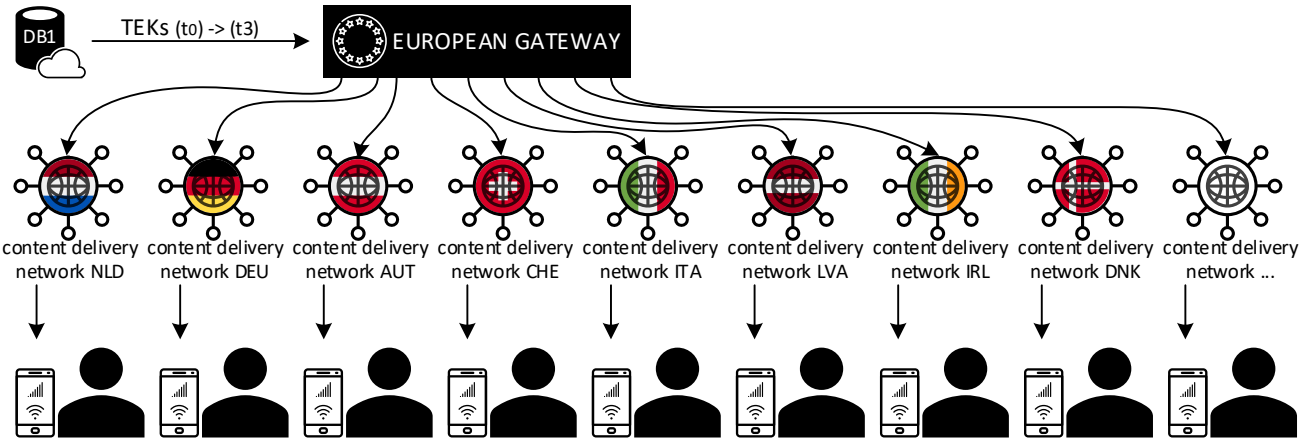
Schéma d'alerte des citoyens en Belgique



Si le citoyen a indiqué avoir séjourné dans un autre pays européen, la Base de données V (BD1/DB1 dans le schéma) de Sciensano partagera les clés chiffrées (TEK) des jours entre la date probable de l'infection (t0) et la date à laquelle l'appli a reçu la notification (t3) avec un service passerelle européen[9] de la Commission européenne. Cette passerelle partagera les informations avec le content delivery network des pays indiqués, pour ainsi pouvoir alerter les citoyens. Toute application de notification du coronavirus ira chercher les clés au moins 1 fois par jour via le content delivery network.

[9] https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_1043

Schéma d'alerte des citoyens dans d'autres pays européens



2.4. Finalités du traitement

- Comme stipulé à l'art. 14 § 4 de l'AR n°44 et dans le futur Accord de coopération, l'application numérique de traçage des contacts destinée à éviter la propagation du coronavirus COVID-19 parmi la population a pour but d'informer les utilisateurs qu'ils ont eu un contact à risque avec un autre utilisateur infecté, sans que l'utilisateur infecté soit identifié par l'application numérique de traçage des contacts et avec pour autre but que l'utilisateur alerté entreprenne volontairement les démarches nécessaires, sur la base des recommandations de Sciensano et des entités fédérées compétentes, pour éviter une propagation du coronavirus COVID-19.

2.5. Intérêts liés au traitement des données

Les intérêts des autorités concernées se situent aux niveaux suivants :

- confiance du citoyen dans le fait que les traitements de données poursuivent un but de valeur ;
- mise à disposition d'un produit de qualité qui assure les traitements de données ;
- contexte médical favorable pour les objectifs poursuivis par les traitements des données.

Confiance auprès du grand public

La valeur de l'appli doit être correctement positionnée: l'utilisation de l'appli aide en première instance l'ensemble de la société à sortir plus rapidement du confinement (ou à éviter un nouveau confinement) mais n'aide l'utilisateur lui-même qu'accessoirement (permet de constater plus rapidement un risque d'infection). Son utilisation est un signe de civisme et de solidarité: si vous êtes infecté, l'application permet d'alerter les personnes avec lesquelles vous avez été en contact et d'éviter ainsi une propagation du virus.

Exigences de qualité

L'application doit répondre à des exigences élevées en matière de qualité: elle doit être facile à installer et à utiliser, ne pas utiliser trop de batterie pour permettre les traitements des données. En matière de convivialité, des tests de 'usability & experience' ont été effectués.

L'infrastructure des serveurs doit également répondre à des exigences de qualité élevées : bonnes performances, résister aux attaques. L'infrastructure doit pouvoir être aussi rapidement que possible être rendue interopérable avec l'infrastructure à l'étranger.

L'importance de la qualité est également valable vis-à-vis de la réputation des sous-traitants des autorités impliquées.

Au niveau médical

L'effectivité du conseil sanitaire: communication claire sur les implications des risques et ce que le citoyen doit faire *(contacter son généralistes, test, quarantaine).*

Le nombre de nouvelles contaminations par jour ne peut pas être trop élevé.

Suffisamment de tests doivent être disponibles et les résultats de ces tests doivent être disponibles aussi vite que possible (idéalement <48u).

Les données des laboratoires et des médecins généralistes doivent être fiables.

2.6. Endroits où les traitements ont lieu

Les données relatives au traçage numérique des contacts sont traitées au sein de l'UE.

Des traitements ont lieu d'une part sur l'appareil de l'utilisateur et d'autre part dans l'infrastructure des serveurs (voir tableau pp. 7-8).

L'infrastructure des serveurs se trouve en Allemagne.

Comme indiqué au chapitre 2.2., le fournisseur de services peut, pour l'utilisation d'une couche de services du système d'exploitation, prévoir des traitements supplémentaires pour la télémétrie. En fonction des conditions de Google ou Apple, le traitement de ces données peut avoir lieu en dehors de l'Europe. Il convient de faire remarquer que les données collectées ne contiennent pas de données relatives au contenu de l'appli et que ces traitements sont effectués avec le consentement du propriétaire du smartphone.

2.7. Techniques et méthodes des traitements de données

L'application de la protection des données sur le plan de la conception, des paramétrages types et des principes du Règlement général sur la protection des données a occupé une place centrale dans le développement d'une application numérique de traçage des contacts. Le Comité européen de la protection des données recommande dans ce cadre des applications numériques de traçage des contacts faisant appel à Bluetooth et travaillant d'une manière décentralisée.

DP-3T[10] est un accord de coopération entre chercheurs de l'Europe entière qui ont uni leurs forces pour créer une solution technique ouverte de traçage des contacts dans le cadre de l'épidémie du COVID-19 qui respecte la vie privée. La solution DP-3T répond aux exigences susmentionnées.

L'implémentation open source la plus récente repose sur l'API Google/Apple[11]. L'intégration spécifique avec l'infrastructure sanitaire doit être développée pour chaque pays séparément ; des modèles ont également été prévus à cet effet.

La solution DP-3T est décentralisée, ce qui signifie que les informations relatives aux contacts restent conservées localement sur le smartphone et que la décision de considérer que le citoyen court un risque ou non est également prise sur le smartphone lui-même. Il existe un registre central qui ne contient que des clés aléatoires et une période de validité. L'utilisation d'une architecture décentralisée est une condition indispensable pour avoir accès à l'API de Google/Apple.

2.8. Cadre juridique & politique

Le cadre juridique et politique se déroule à trois niveaux: européen, (inter)fédéral et régional. Ci-après une liste des principales réglementations, recommandations ou initiatives politiques.

Union européenne

- *Recommandation (UE) 2020/518 de la Commission du 8 avril 2020 concernant une boîte à outils commune au niveau de l'Union en vue de l'utilisation des technologies et des données pour lutter contre la crise de la COVID-19 et sortir de cette crise, notamment en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées.*
- *Lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19 Adoptées le 21 avril 2020.*
- *Communication de la Commission Orientations sur les applications soutenant la lutte contre la pandémie de COVID-19 en ce qui concerne la protection des données 2020/C 124 I/01).*
- *Décision d'exécution (UE) 2020/1023 de la Commission du 15 juillet 2020 modifiant la décision d'exécution (UE) 2019/1765 en ce qui concerne l'échange transfrontière de données entre les applications mobiles nationales de suivi de contacts et d'alerte dans le cadre de la lutte contre la pandémie de COVID-19.*

Niveaux fédéral et interfédéral

- *Arrêté royal n° 44 du 26 juin 2020 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano.*
- *Accord de coopération du XXX entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts des personnes*

[10] https://github.com/DP-3T/documents
[11] Application Programming Interface: définit les interactions entre plusieurs composantes d'un logiciel.

(présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano.

- *Arrêté royal du xxx d'exécution de l'Arrêté royal n° 44 du 26 juin 2020 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano.*
- *Loi du 25 février 2018 portant création de Sciensano.*
- *Avis et activités du Groupe de travail en charge de l'Exit strategy (GEES) et du Comité interfédéral Tracing et Testing Covid-19.*

Il est important de faire remarquer que l'AR n°44 fait l'objet d'un recours en annulation auprès du Conseil d'Etat. Dès qu'ils seront connus, les résultats de ce recours en annulation seront intégrés dans une version actualisée de la présente AIPD.

Niveau des entités fédérées

- *Décret du 21 novembre 2003 relatif à la politique de santé préventive (pour la Flandre).*
- *Décret du 2 mai 2019 modifiant le Code wallon de l'Action sociale et de la Santé en ce qui concerne la prévention et la promotion de la santé (pour la Wallonie).*
- *Ordonnance du 19 juillet 2007 relative à la politique de prévention en santé et l'arrêté du 23 avril 2009 du Collège réuni de la Commission communautaire commune relatif à la prophylaxie des maladies transmissibles (pour Bruxelles).*
- *Décret du Parlement de la Communauté germanophone du 1er juin 2004 relatif à la promotion de la santé et à la prévention médicale.*

2.9. Délais de conservation

Les délais de conservation maximaux sont définis par la loi.

- Toutes les données relatives aux contacts entre utilisateurs, stockées sur l'appareil de l'utilisateur, sont effacées au plus tard trois semaines après avoir été générées sur l'appareil de l'utilisateur d'une application numérique de traçage des contacts. Afin de pouvoir garantir au maximum le droit d'autodétermination de l'utilisateur, la désactivation de l'application numérique de traçage des contacts est effectuée par l'utilisateur lui-même sur son appareil.
- Les données qui se retrouvent dans la base de données contenant le journal central des enregistrements ne peuvent plus être utilisées par l'application mobile de l'application numérique de traçage des contacts sur l'appareil de l'utilisateur. Les informations conservées dans cette base de données doivent être effacées au plus tard trois semaines après avoir été reprises dans cette base de données. Etant donné la période d'incubation du coronavirus COVID-19, un délai de trois semaines est opportun. Cette base de données est désactivée au plus tard vingt-et-un jours après la publication de l'Arrêté royal annonçant la fin de l'épidémie du coronavirus COVID-19.

Comme le fait apparaître la description des flux de données, les données pseudonymisées pour les notifications aux contacts rapprochés ne sont conservées que pendant 14 jours au lieu du délai maximal prévu de trois semaines. Les données de la base de données des résultats des tests (BD2) et

certaines données de la base de données pour le traçage manuel des contacts (BD) seront supprimées immédiatement après certaines actions. Voir description du flux de données au point 2.3.:

- Une fois que l'estimation du résultat du test (positif/négatif) a été copiée dans la base de données des résultats des tests, Sciensano supprime le code de test partagé (R1) de sa base de données pour le traçage manuel des contacts (BD Sciensano).
- Une fois que l'appli a téléchargé les données et que BD2 (Base de données VI) a créé le code d'autorisation, Sciensano supprime la date probable de l'infection (t0), le test de code partagé (R1) et le résultat du test de la base de données des résultats des tests. La même opération est effectuée lorsqu'un citoyen ayant un résultat de test positif indique ne pas vouloir alerter.

Section III: Processus de consultation

Le 28 avril 2020, des auditions se sont tenues à la Commission Economie de la Chambre avec des experts issus du secteur universitaire, de la société civile et des autorités en matière d'ICT, de vie privée, de droits de l'homme et de (cyber)sécurité.[12] Le débat parlementaire a eu pour résultat une proposition de loi sur laquelle un avis a été demandé à l'Autorité de protection des données.

- Avis n°43/2020 du 26 mai 2020 concernant une proposition de loi relative à 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-2020-049)

Une élaboration plus approfondie des exigences (*entre autres juridiques, techniques, épidémiologiques)* a eu lieu au sein de Groupe de travail interfédéral Testing et Tracing. Ce groupe de travail est composé de représentants des administrations (sanitaires) fédérales et régionales ainsi que d'experts en informatique et en maladies infectieuses. Lors de cette élaboration, des éléments du processus de consultation ont été pris en compte (*Voir par exemple les références à l'avis de l'APD dans le cadre légal de l'application de traçage des contacts).*

Le Groupe de travail interfédéral a également estimé important d'organiser une consultation publique accordant une attention particulière aux questions suivantes:

- A quel âge les mineurs doivent-ils pouvoir décider avec autonomie de l'utilisation de l'appli ?
- Comment faire en sorte que l'appli soit inclusive et qu'elle atteigne autant de personnes que possible dans la société ?
- Comment augmenter la confiance de la population dans l'appli ainsi que sa compréhension de l'appli ?
- La déclaration de confidentialité est-elle claire et suffisante ?
- Comment augmenter la facilité d'utilisation de l'appli ?
- Comment les professionnels du monde médical peuvent-ils jouer un rôle dans la stimulation de l'utilisation de l'appli ?
- Qui doit faire partie d'une commission de contrôle indépendante ?

La consultation publique a pour but d'identifier, dans le grand public et chez les stakeholders pertinents, les principaux défis juridiques, éthiques, sociaux, techniques et de sécurité liés au développement d'une application Bluetooth de traçage des contacts en Belgique: voir https://www.esat.kuleuven.be/cosic/sites/corona-app/fr/ . Elle s'adresse :

[12] https://www.lachambre.be/FLWB/PDF/55/1182/55K1182005.pdf

- aux experts universitaires en droit, sciences sociales, technique, informatique, médecine, etc. ;
- aux experts non universitaires et aux professionnels en matière de développement d'applications, de cybersécurité, de protection des données et de la vie privée, de santé publique, de médecine, d'e-inclusion ;
- à la société civile ;
- aux communes;
- aux citoyens inquiets.

La consultation est coordonnée par le Groupe de recherche COSIC (KU Leuven) et se tient du 5 août au 31 août 2020 inclus. Au cours de cette période a eu lieu une consultation publique au sujet des documents techniques et juridiques liés à l'application (https://www.esat.kuleuven.be/cosic/sites/corona-app/). Les résultats de cette consultation seront rendus publics dans un rapport qui paraîtra dans la première moitié du mois de septembre.

Section IV: Evaluation de la nécessité & de la proportionnalité

4.1. Licéité du traitement

Les traitements mentionnés dans la présente AIPD sont licites parce qu'ils sont «nécessaire au respect d'une obligation légale à laquelle le(s) responsable(s) du traitement est/sont soumis» (art. 6, 1, c) RGPD). Cette base légale est la suivante:

- *Arrêté royal n° 44 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano.*
- *Accord de coopération du XXX entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune, concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les entités fédérées compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano.*

L'Accord de coopération prévoit que Sciensano est le responsable du traitement pour la base de données contenant le journal central des enregistrements de l'application de traçage. Le cadre légal est indispensable mais ne peut pas être confondu avec le libre choix du citoyen d'installer, d'utiliser et de désinstaller une application numérique de traçage des contacts.

4.2. Catégories particulières de données à caractère personnel

L'interdiction de traiter des données relatives à la santé ne s'applique pas aux présents traitements étant donné que les objectifs sont liés à des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé (art. 9 § 2 i) RGPD).

Indépendamment de cette exception à l'interdiction en matière de traitement des données à caractère personnel, il reste important d'insister sur le libre choix du citoyen de traiter ou non les données (de santé) via l'application ou l'infrastructure de serveurs correspondante. Les utilisateurs de l'application de traçage des contacts ont la possibilité de se déclarer ou non d'accord avec la consultation d'un résultat de test et avec le chargement des données nécessaires (comme la date probable de l'infection) s'ils souhaitent alerter leurs contacts.

4.3. Limitation des finalités

L'explication du cadre juridique de l'application de traçage des contacts indique d'une manière claire les limites d'utilisation de cette application et du traitement des données correspondant. L'unique but est d'alerter les citoyens sur une base volontaire d'une éventuelle exposition au virus. Ces missions sont décrites dans les AR et accords de coopération respectifs.

Les traitements effectués par la plateforme se limitent aux traitements tels que décrits au chapitre 2.3 de la présente AIPD.

Les données ne sont traitées comme décrit au chapitre 2.3 que si la personne concernée est d'accord. Ces données ne sont ni extrapolées ni traitées avec des données provenant d'autres sources, à l'exception des résultats des tests. L'utilisateur doit également donner son accord pour le traitement de ces résultats de tests.

Aucun autre traitement n'est effectué avec les données à caractère personnel reçues.

4.4. Nécessité et proportionnalité

L'application Coronalert fonctionne sans identification directe de personnes. Seules les informations pertinentes et absolument nécessaires sont collectées :

- numéros de série temporaires non personnalisés (via jetons Bluetooth): indispensables pour alerter de manière anonyme les utilisateurs de l'appli qu'ils sont entrés en contact avec une personne infectée ;
- résultat test labo: indispensable pour initier ou non les actions nécessaires pour alerter les contacts des risques de contamination ;
- date probable de l'infection: indispensable pour estimer d'un point de vue médical pour quels contacts il existe un risque de contamination ;
- codes de test: indispensables pour éviter que de fausses notifications (malveillantes) soient envoyées en matière de risques d'infection ;
- séjour dans un pays d'Europe: indispensable pour envoyer une notification aux personnes avec lesquelles la personne infectée a été en contact en dehors de la Belgique.

L'application Coronalert ne traite aucune donnée de localisation des utilisateurs individuels. Pour mesurer la proximité entre personnes, il n'est en effet pas nécessaire de connaître leur localisation. Le système ne stocke pas non plus les adresses IP des utilisateurs.

Pour limiter au maximum les risques pour les personnes concernées, les données stockées dans la base de données centrale ne peuvent pas être comparées aux autres bases de données.

4.5. Droits des personnes concernées

Sous les conditions du RGPD, les utilisateurs ont un droit d'accès à leurs données à caractère personnel, pour demander la rectification, l'effacement ou la limitation du traitement ou pour s'opposer au traitement de leurs données à caractère personnel ("droits de la personne concernée").

Sciensano ne pourra réagir à la requête d'un utilisateur que lorsqu'il sera possible de lier à cet utilisateur spécifique les données traitées dans le cadre de l'application de traçage des contacts. Pour lier les données à l'utilisateur, Sciensano aurait besoin de données supplémentaires. Etant donné que l'application de traçage des contacts est basée sur une technologie qui doit protéger autant que possible la vie privée des utilisateurs, il n'est pas souhaitable que Sciensano traite des données complémentaires permettant d'identifier l'utilisateur. En vertu de l'article 11 du RGPD, Scienscano ne peut pas être obligé de traiter de telles données complémentaires pour identifier l'utilisateur dans le seul but de respecter les droits de la personne concernée conformément au RGPD. Cela signifie que dans la pratique, les utilisateurs ne seront pas capables d'exercer leurs droits de personnes concernées, sauf si des informations complémentaires sont fournies à Sciensano.

Ces informations seront communiquées dans la Déclaration de confidentialité destinée aux personnes concernées. Pour la Base de données V, Sciensano ne peut pas non plus contrôler la légitimité d'une demande relative aux droits (p. ex. consultation ou suppression) parce que les clés ne peuvent pas être ramenées à un individu.

Bien que l'exercice de ces droits soit rendu difficile en raison du degré élevé de pseudonymisation, les données sont protégées par les courts délais de conservation (14 jours au maximum) et par l'autonomie intégrée pour l'utilisateur en ce qui concerne les traitements de données. Le téléchargement d'un résultat de test fait par exemple automatiquement en sorte que les données sont supprimées de la Base de données VI. L'utilisateur peut en outre, via les fonctions de l'application, décider lui-même s'il souhaite (faire) traiter ou non ses données *(p. ex. résultats de test, pays où il a séjourné ou clés)*.

Section V: Sécurité de l'information

5.1. Sécurité de l'information infrastructure de serveurs

Résumé

L'application Coronalert a été conçue, construite, hébergée et entretenue avec la sécurité comme une des principales priorités.

La décision d'héberger le back-end chez AWS se base également sur cette grande importance accordée à l'aspect sécurité. Etant donné qu'AWS peut être considéré comme un cloud public, il est important de formuler d'une manière très claire et très précise les mesures de sécurisation qui sont prises. Ces mesures sont les suivantes :

1. La mise en place de l'architecture complète de l'application se base sur le principe 'security by design'. Quelques-unes des caractéristiques de l'architecture de l'application sont:
    1. Les serveurs sontétablis en Europe (Frankfort)
    2. Les "Data at rest" sont cryptées (AES-256)
    3. Les "Data in transit" sont toujours cryptées (TLS)

2. La gestion des informations et de l'architecture des données a lieu dans le respect de la sécurité et de la vie privée :
    1. Seules des données pseudonymisées sont stockées sur les systèmes back-end.
    2. Le code de 15 chiffres donnant accès aux résultats d'un test et permettant à la personne concernée de recevoir son résultat ne contient aucune donnée pouvant être ramenée à l'utilisateur ou à son téléphone.
    3. Le code de 15 chiffres est supprimé du back-end dès que l'utilisateur a reçu le résultat de son test.
    4. Les informations sont supprimées des systèmes de back-end une fois qu'elles ne sont plus nécessaires (une fois que l'utilisateur a reçu ses résultats ou au plus tard 14 jours après la date probable de l'infection).
3. Des outils AWS spécifiques sont implémentés en support de:
    1. Rate limiting
    2. Certificate pinning
    3. Mesures anti DDoS
    4. Une série de contrôles de sécurité pour protéger les données d'un accès, d'une modification ou d'une suppression non autorisés.

Architecture

- La plateforme est installée dans 3 AZ (Availability Zones) dans 1 endroit central en UE (Frankort).
- Tous les services sont installés au moins dans chaque AZ.
- S3, CloudFront et ALB *sont très évolutifs*.
- Les "Data at rest" sont cryptées (AES-256).
- Les "Data in transit" sont toujours cryptées (TLS).
- Le SLA est de 99.999%. AWS garantit 99.9% pour la plupart des services mais en raison de l'exécution multiple dans 3 AZ, la disponibilité totale a été calculée à 1 - (0.001^3).
- Back-ups avec Point In Time Recovery.

Architecture des données

- Seules les données pseudonymisées stockées dans le back-end.
- R1 est un code de 15 chiffres qui lie un test déterminé (et son résultat) à un appareil mobile. Il ne contient aucune information sur l'utilisateur du téléphone. Il est généré sur le téléphone et communiqué au médecin.
- Ces informations sont également supprimées du back-end dès qu'un résultat de test est téléchargé.
- Rate limiting, certificate pinning, mesures anti DDoS, proof-of-work sont appliqués.
- Les données sont supprimées du back-end une fois qu'elles ne sont plus nécessaires (une fois que les résultats ont été téléchargés ou après t0+14).

Les informations suivantes sont conservées :

Verification Service
R1 (code de 17 chiffres qui lie un test déterminé (et son résultat) à un appareil mobile
t0 (date à laquelle l'utilisateur a probablement été infecté)
t3 (date à laquelle les résultats ont été téléchargés)

Résultat du test (positif/négatif)
Test channel (lab/arts)
Code d'autorisation AC (signature numérique) – conservé temporairement jusqu'à l'envoi (submission service)
Submission Service
Code d'autorisation AC (signature numérique) pour valider les clés chiffrées
TEK: clé chiffrée
Pays pour la TEK
Distribution Service
TEK chargées (période de conservation de 14 jours, tant les TEK pertinentes que les factices)t
Keys & Certificates
• Clé de signature qui est utilisée par le service de distribution pour signer les clés de diagnostic. • Public key pour connexion TLS avec la base de données.

Pour une analyse de sécurité détaillée, consulter le lien suivant : https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Upload%20Authorisation%20Analysis%20and%20Guidelines.pdf section 3 - Data Bound Auth Codes

Contrôles de sécurisation sélectionnés dans AWS

Le cloud public AWS propose toute une série de contrôles de sécurité permettant de protéger les données d'un accès, d'une modification ou d'une suppression non autorisés.

Ci-dessous une liste de services de sécurisation utilisés pour l'environnement du back-office. Les contrôles de sécurisation ont été groupés par type de service selon la structure de l'*Overview of Security Processes* whitepaper, et qui se concentrent sur les services qui sont utilisés pour la solution. Vous trouverez plus d'informations dans le livre blanc et sur le portail de documentation d'AWS.

- Sécurité de l'infrastructure
- Services informatiques
- Services réseau
- Services de stockage
- Services de bases de données
- (Gestion application – non applicable)
- Services de déploiement et de management

Des informations supplémentaires sont disponibles dans la documentation relative aux contrôles de sécurité AWS sélectionnés pour l'infrastructure des serveurs.

Les données à protéger sont composées des clés sécurisées de Coronalert et des résultats de test d'un utilisateur (informations publiques).

Mesures organisatoires de Sciensano

Seul un nombre limité de collaborateurs de Sciensano ont accès aux bases de données concernées. Tous les collaborateurs internes et externes, temporaires ou de longue durée, ont signé avec Sciensano un Accord de confidentialité.

5.2. Sécurité de l'information application

L'application est basée sur le principe DP-3T qui prévoit déjà une forte protection de la vie privée des utilisateurs. Les points suivants sont au minimum repris dans les exigences de sécurité de l'appli:

- application des principes de DP-3T;
- la communication entre l'appli et les serveurs doit être cryptée ;
- les informations sont effacées après le délai de traitement prévu ;
- protection de la confidentialité et de l'intégrité, de sorte que les clés et les moyens d'authentification soient protégés de fuites de données ou d'une adaptation pratiquée par d'autres applications présentes sur l'appareil ou par des hackers.

L'infrastructure sous-jacente de l'application est le smartphone/gsm sur lequel l'appli est installée. L'utilisateur devra au moins être informé des risques qui y sont liés.

5.3. Contrôle de la sécurité de l'information

L'adjudication pour le développement de l'appli prévoit également un volet "Audit de la sécurité". (Lot 2 : Audit de sécurité de l'application et du back office développés dans le Lot 1 de l'adjudication "Procédure négociée sans publication préalable Smals-BB-001.031/2020").

Cet audit doit réaliser une estimation pour des évaluations complémentaires du besoin de corrections de bugs et de réparation d'éventuelles failles.

L'audit poursuit entre autres les objectifs suivants:

- l'application mobile doit être auditée quant à l'intégrité des données (at-rest of in-motion), afin que la manipulation des clés générées ou la validation du code de test ne puissent pas être mal utilisées pour générer de fausses infections COVID-19 et une manipulation ou une suppression des clés stockées (sur l'architecture mobile ou centrale).
- L'audit doit contrôler si l'application n'est pas sensible à des vecteurs d'attaque connus basés sur Bluetooth.
- L'audit doit contrôler si le transfert sécurisé de clés liées à l'infection ne peut pas être intercepté.
- L'audit doit contrôler le fonctionnement sécurisé de l'application mobile, y compris les attaques basées sur la validation ou l'injection d'input.

Les parties obligatoires de l'audit ont été définies comme suit :

- Planning
- Security Architecture Review (chaque sprint)
- Modèles de menaces (chaque sprint)
- Analyse composition logiciel (chaque sprint)

- Evaluation des écrans d'application et de la validation d'input (audit final)
- Examen dynamique de la vulnérabilité (chaque sprint)
- Analyse statique
- Détermination manuelle des codes
- Analyse des codes malicieux
- Rapportage

Section VI : Description et évaluation des risques pour les personnes concernées et mesures envisagées

Pour l'estimation des risques d'atteinte à la vie privée liés à la corruption des données de l'application Coronalert, cette AIPD utilise les outils d'analyse de risque de la haute-école Thomas More et de la Banque Carrefour de la Sécurité sociale.

Ci-dessous, les risques sont regroupés en fonction des objectifs.

- D01. Respect du droit à la transparence du traitement des données
- D02. Respect de la limitation de la finalité du traitement des données
- D03. Respect de la minimisation des données
- D04. Garantie de la qualité des données à caractère personnel
- D05. Respect des exigences en matière de limitation de la conservation
- D06. Respect du droit à la protection de la confidentialité et de la sécurité du traitement des données
- D07. Licéité du traitement des données à caractère personnel
- D08. Respect du droit à l'information (sur le traitement des données)
- D09. Respect du droit de rectification et d'effacement des données à caractère personnel
- D10. Respect du droit à la portabilité des données
- D11. Respect du droit d'opposition
- D12. Respect du régime relatif aux décisions individuelles automatisées
- D13. Respect des obligations (techniques) relatives à l'organisation du traitement
- D14. Respect des obligations organisationnelles

La description du risque décrit la probabilité (improbable/probable/très probable) et l'impact (limité/moyen/grand) d'un risque. On obtient ainsi un score de risque global, selon le tableau ci-dessous.

				IMPACT		
				Limitée	Moyen	Grand
				1	2	3
				Les droits et libertés de la personne concernée sont pleinement sauvegardés	Les droits et libertés des personnes concernées sont régulièrement affectés	Les droits et libertés de la personne concernée sont toujours, ou très souvent, affectés
PROBABILITÉ Quelle est la probabilité que cela se produise ?	Peu probable	#	L'événement ne se produit pas ou seulement dans certaines circonstances	**Acceptable Risque FAIBLE 1**	**Acceptable Risque FAIBLE 1**	**Acceptable Risque MOYEN 2**
	Probable	#	L'événement peut se produire à un certain moment	**Acceptable Risque FAIBLE 1**	**Acceptable Risque MOYEN 2**	**NON-Acceptable Risque HAUT 3**
	Très probable	#	L'événement aura lieu à un moment donné	**Acceptable Risque MOYEN 2**	**NON-Acceptable Risque HAUT 3**	**NON-Acceptable Risque EXTRÊME 4**

D01. Respect du droit à la transparence du traitement des données

Principe Dites à la personne concernée quelles informations vous collectez, ce que vous allez en faire et quelles sont les conséquences du traitement des données

Résumé Comment informez-vous la personne concernée du traitement des données ? Ou est-ce si évident que vous n'avez pas à l'expliquer ? Si vous n'êtes pas transparent avec eux sur ce que vous faites, laquelle des exceptions vous autorise à ne pas communiquer à ce sujet ?

Lien RGPD Article 5 a) licéité, loyauté et transparence du traitement

R01. Informer à propos du traitement

R01. Informer à propos du traitement	
Vulnérabilité	
La personne concernée n'a pas été/n'a pas été pleinement/suffisamment informée du fait que des données à caractère personnel sont collectées, utilisées, consultées ou traitées d'une autre manière.	
Commentaire explicatif	
Le RGPD exige que l'utilisateur soit informé d'une manière simple sur le traitement de ses données à caractère personnel. Si l'information n'est pas facilement accessible, l'utilisateur peut involontairement mettre ses données à disposition.	
Mesures	
Rédaction d'une Déclaration de confidentialité (application + infrastructure de serveur). Campagnes de promotion pour l'application. Exposition médiatique. Mention du site spécifique www.coronalert.be. Informations supplémentaires données par le prestataire de soins à l'utilisateur lorsqu'un échantillon est prélevé pour un test.	
Risque résiduel	
Malgré le fait que les mesures proposées couvrent un large éventail de médias, il peut arriver que l'utilisateur ne soit pas pleinement informé et marque donc involontairement son accord .	
Score de risque	
Probabilité après mesures	1
Impact après mesures	2

R01. Informer à propos du traitement	
Risque	FAIBLE

R02. Informer à propos de la finalité du traitement des données

R02. Informer à propos de la finalité du traitement des données
Vulnérabilité
La personne concernée n'a pas été/n'a pas été pleinement/suffisamment informée de la finalité du traitement des données.
Commentaire explicatif
Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (« licéité, loyauté, transparence »). La transparence exige que la personne concernée soit informée de toutes les opérations de traitement qui seront effectuées sur ses données.
Mesures
Rédaction d'une Déclaration de confidentialité (application + infrastructure de serveur). Campagnes de promotion pour l'application. Exposition médiatique. L'AIPD sera rendue publique.
Risque résiduel
Malgré le fait que les mesures proposées couvrent un large éventail de médias, il peut arriver que l'utilisateur ne soit pas pleinement informé et ne sache donc pas exactement quels traitements seront effectués.
Score de risque

Probabilité après mesures	1
Impact après mesures	2
Risque	FAIBLE

R03. Décisions automatisées

R03. Décisions automatisées
Vulnérabilité
L'algorithme probabiliste sous-jacent aux procédures de décision automatisées n'est pas ou pas suffisamment clair et l'exactitude des conclusions de la machine ne peut donc pas être évaluée.
Commentaire explicatif
L'application détermine si les contacts sont à risque sur la base des numéros de série temporaires non personnalisés reçus et des clés chiffrées des personnes infectées reçues. Si cet algorithme n'est pas clair ou ne peut être contrôlé, la personne concernée peut être informée à tort qu'il y a eu un contact à haut risque et donc être invitée à se mettre en quarantaine.
Mesures
La seule partie de l'application où il est question d'une décision automatique est sur le téléphone mobile. Ce calcul fait l'objet d'une description transparente au chapitre 5.3 de la note « Coronalert: A Distributed Privacy-Friendly Contact Tracing App for Belgium ». Cet algorithme a été largement testé par les chercheurs du Consortium DP-3T, de la Fraunhofer-Gesellschaft et de l'Institut Robert Koch. En outre, en cas de signalement d'un contact à risque, la personne concernée peut contacter un médecin pour subir un test susceptible de lever la quarantaine en cas de résultat négatif.
Risque résiduel
Si l'algorithme prescrit n'est pas appliqué correctement, la personne concernée peut toujours recevoir des informations incorrectes qui peuvent entraîner une demande de quarantaine

R03. Décisions automatisées	
injustifiée. La durée de la quarantaine peut être limitée en permettant à la personne concernée de se soumettre à un test.	
Score de risque	
Probabilité après mesures	1
Impact après mesures	3
Risque	MOYEN

D02. Respect de la limitation de la finalité du traitement des données

Principe	Utilisez les données pour la finalité pour laquelle vous les avez collectées, à moins qu'une exception ne s'applique.
Résumé	Soyez clair quant à la finalité de la collecte et de l'utilisation des données. Cela correspond-il bien aux attentes de la personne ? Les utilisez-vous dans une autre finalité que celle pour laquelle vous les avez collectées ? Si oui, y a-t-il une exception qui justifie cette utilisation ?
Lien RGPD	Article 5 b) : collectées pour des finalités déterminées, explicites et légitimes

R04. Finalité spécifiée

R04. Finalité spécifiée
Vulnérabilité
La finalité du traitement des données n'est pas précisée. Il n'est pas stipulé que les données collectées ne seront utilisées que pour un objectif ou un service spécifique.
Commentaire explicatif
Le type et la quantité de données à caractère personnel qu'une entreprise/organisation est autorisée à traiter dépend des raisons du traitement (raison juridique utilisée) et de l'utilisation visée des données à caractère personnel. L'entreprise/l'organisation doit respecter plusieurs règles importantes, dont : • les données à caractère personnel doivent être traitées d'une manière licite et transparente et la loyauté vis-à-vis de la personne dont les données à caractère personnel sont traitées doit être garantie (« licéité, loyauté et transparence ») ; • le traitement des données doit avoir des finalités spécifiques et l'entreprise/l'organisation doit expliquer ces finalités aux personnes dont les données à caractère personnel sont collectées. Une entreprise/organisation ne peut pas collecter des données à caractère personnel pour des finalités non définies (« limitation des finalités ») ; • l'entreprise/l'organisation n'est autorisée à collecter et à traiter que les données à caractère personnel nécessaires pour atteindre cette finalité. •
Mesures
L'utilisation de l'application couvre exclusivement la finalité prévue au titre de « l'Arrêté royal n°44 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano » et sera reprise dans le futur Accord de coopération. Cet arrêté énonce la base juridique pour atteindre les finalités suivantes (voir rapport au Roi): • en premier lieu, une application de traçage numérique des contacts doit enregistrer les contacts entre utilisateurs de manière automatisée et sans possibilité de retrouver l'identité des utilisateurs ; • en deuxième lieu, une application de traçage numérique des contacts doit permettre à l'utilisateur dont l'infection au COVID-19 a été constatée de signaler volontairement sa

R04. Finalité spécifiée
contamination de manière autorisée et contrôlée afin d'éviter tout signalement faux ou erroné ; • le signalement de l'infection doit alors permettre aux autres utilisateurs qui ont été en contact avec l'utilisateur infecté par le COVID-19 pendant la période d'infection d'être informés qu'ils se trouvaient à proximité de cette personne infectée, sans donner le nom, le lieu ou le moment exact de l'infection.
Risque résiduel
La description est suffisamment claire et a été reprise dans l'accord de coopération entre les différentes autorités, ce qui limite le risque ici. L'impact potentiel est activement réduit par le cadre légal qui définit les finalités.
Score de risque

Probabilité après mesures	1
Impact après mesures	2
Risque	FAIBLE

R05. Lien entre finalité et données

R05. Lien entre finalité et données
Vulnérabilité
Les données qui ne sont conservées et traitées que pour une finalité spécifique ne sont pas conformément marquées et/ou gérées.
Commentaire explicatif
Il s'agit d'une mesure de sécurité qui empêche que les données détenues sur les différents systèmes soient utilisées à tort pour un traitement autre que celui pour lequel elles ont été collectées, sans que le gestionnaire de l'information n'en ait l'intention.
Mesures
L'application utilise des numéros de série temporaires non personnalisés et des clés chiffrées; seules les clés chiffrées aboutissent dans le système central. Comme ces clés sont pseudonymisées et qu'il est donc difficile de remonter jusqu'à l'individu, l'impact pour la personne concernée sera faible. Pour l'échange des résultats des tests, on utilise un code de test R1 qui ne contient aucune donnée permettant de remonter jusqu'au téléphone de l'utilisateur ou jusqu'à l'utilisateur lui-même. Par conséquent, l'impact du traitement ultérieur de ces données est limité. Les opérations de traitement sur les systèmes utilisés pour gérer les données ci-dessus sont limitées à celles de la plateforme. En ce sens, il est clair que les données présentes sur ces plateformes ne peuvent être utilisées que pour des traitements relatifs au traçage numérique de contacts.
Risque résiduel
Les mesures prévues offrent une sécurité suffisante pour réduire à la fois la probabilité et l'impact.
Score de risque

Probabilité après mesures	1
Impact après mesures	2
Risque	FAIBLE

R06. Utilisation des données hors de la finalité

R06. Utilisation des données hors de la finalité
Vulnérabilité

R06. Utilisation des données hors de la finalité
Les données collectées sont traitées à des fins autres que celles pour lesquelles elles ont été initialement recueillies. Ces différentes finalités ne sont pas compatibles avec la finalité initiale.
Commentaire explicatif
Comme stipulé dans des AIPD étrangères : (i) Les données conservées peuvent être utilisées pour l'application des règles de distanciation et des bulles sociales, en plus des objectifs épidémiologiques. Si cela s'opère de façon anonyme (statistique), cela peut conduire à un profilage socio-économique, ce qui entraîne des mesures sélectives influençant le sujet. Si cela se fait de manière individualisée, cela peut donner lieu à des poursuites en cas de violation des mesures, voire à une réduction des soins (« cette personne a été tellement négligente que nous utilisons le respirateur pour quelqu'un d'autre »). (ii) L'infrastructure mise en place pour le traçage des contacts peut être utilisée pour identifier les relations de criminels présumés. Des pressions politiques peuvent entraîner une modification de la loi, permettant à l'application d'être utilisée comme un outil dans les enquêtes criminelles dans certains cas (comme la recherche de réseaux terroristes). L'impact sur la vie privée des utilisateurs dépend de la conception technique de l'application.
Mesures
Les finalités de l'application sont clairement définies dans « l'Arrêté royal n°44 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano » et seront reprises dans le futur Accord de coopération. En outre, l'application prévoit une pseudonymisation des informations via des clés chiffrées pour l'échange des informations sur les contacts. Outre le fait que ces clés chiffrées ne contiennent pas d'informations de géolocalisation, les risques susmentionnés seront limités puisque les contacts ne sont identifiés que par l'application. De plus, les données sont supprimées une fois que les résultats des tests ont été téléchargés ou après 14 jours (clés). La détection des contacts est effectuée localement par l'application et non pas centralement.
Risque résiduel
L'utilisation de l'application est cruciale pour limiter autant que possible la propagation du coronavirus. Etant donné que la confiance dans l'application est cruciale, le législateur a exclu d'autres finalités. Les mesures techniques sur la plateforme limitent l'impact du traitement ultérieur des données. Ces données sont en effet pseudonymisées et il est presque impossible de remonter jusqu'à l'utilisateur ou à ses appareils. Etant donné que les données ne sont disponibles que pendant peu de temps, le risque qu'elles soient utilisées en dehors de la finalité est limité. Comme les informations présentes sur le système central ne contiennent pas d'informations sur les contacts, la possibilité de les utiliser pour d'autres finalités est également limitée.

Score de risque	
Probabilité après mesures	1
Impact après mesures	2
Risque	FAIBLE

D03. Respect de la minimisation des données

Principe	Ne recueillez des informations personnelles que lorsque vous en avez réellement besoin.
Résumé	Identifiez chaque élément de données à caractère personnel que vous utilisez et vérifiez s'il est nécessaire au traitement. Quel est l'objectif de la collecte des données à caractère personnel dont il est question ici ? Comment l'organisation

peut-elle faire ce qu'elle doit faire ? Ne recueillez-vous que ce dont vous avez réellement besoin ? Par exemple, avez-vous vraiment besoin de connaître la « date de naissance », ou pouvez-vous vous contenter de « l'âge » ou de l'information « plus de 18 ans » ?

Lien RGPD Article 5 c) : données adéquates, pertinentes et limitées

R07. Collecte de données non pertinentes

R07. Collecte de données non pertinentes
Vulnérabilité
La personne concernée doit fournir des données à caractère personnel qui ne sont pas pertinentes au regard de la finalité déclarée du traitement.
Commentaire explicatif
Les données collectées doivent être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (« minimisation des données »). Cela signifie que même si la personne concernée donne son accord sur la transmission de ses données, elle doit avoir la garantie que la communication de ses données sera limitée au maximum. L'application elle-même comporte deux composantes distinctes : une application « client » qui est gérée par l'autorité nationale de santé publique et le service de Google/Apple Notification d'exposition (GAEN), qui sur les appareils Android est gérée par Google et fait partie des services Google Play. Les informations collectées par l'appli sont décrites dans le cahier des charges destiné au développement de l'appli. En ce qui concerne les services Google Play, ceux-ci prennent contact, dans une configuration « respectant la vie privée », toutes les 20 minutes avec les serveurs de Google, permettant ainsi par exemple de suivre la localisation via l'adresse IP. De plus, les services Google Play partagent également avec Google l'IMEI du téléphone, le numéro de série du hardware, le numéro de série de la carte SIM, le numéro de téléphone de l'appareil, l'adresse MAC Wi-fi et l'adresse e-mail de l'utilisateur, ainsi que les données très fines relatives aux applications qui tournent sur le téléphone. Cette collecte de données est propre au fonctionnement d'Android et ne peut être évitée sans devoir désactiver toutes les applis de Google. Il convient de faire remarquer que Google n'a pas accès aux données collectées par l'application.
Mesures
Les spécifications de l'application ont été rendues publiques et sont reprises dans le cahier des charges pour le développement de l'application. Les données échangées concernent les clés chiffrées (entre l'application et l'infrastructure centrale) et le numéro de série temporaire non personnalisé entre les appareils des utilisateurs. Ces deux types d'informations sont au minimum nécessaires pour la détermination d'un contact à risque. L'algorithme de détermination des contacts et du risque de contact n'utilise que les informations qui ont été échangées. Lors de l'enregistrement de numéros de série temporaires non personnalisés, l'application enregistre des informations supplémentaires (durée et intensité du signal), mais comme les clés chiffrées et les numéros de série temporaires non personnalisés sont pseudonymisés, il est presque impossible de remonter jusqu'à une personne depuis ces informations. Un deuxième type de données concerne les résultats du test, qui sont une partie essentielle des traitements exécutés par l'application et la plateforme centrale. Pour le fonctionnement de l'application est appliqué le principe de la minimisation des données. La description de l'application indique quelles informations sont échangées. Ces informations sont limitées à ce qui est strictement nécessaire pour l'enregistrement des contacts et la durée et la distance respectives pour le traçage des contacts. À chaque nouvelle version de l'application, Google et Apple vérifient si l'application traite les informations de géolocalisation ; si c'est le cas, l'application n'accède pas à l'interface Exposure Notification de Google/Apple et ne sera plus fonctionnelle.

R07. Collecte de données non pertinentes	
Pour p. ex. l'utilisation d'Android, le service « Google Play Services » ne peut pas être désactivé. Aucune politique de confidentialité spécifique n'est disponible mais la Déclaration de confidentialité générale de Google informe l'utilisateur que l'appareil collecte les informations. Il convient de faire remarquer que l'application Coronalert ne fonctionnera pas sans « Google Play Services ».	
Risque résiduel	
Les spécifications de l'application ont été stipulées dans différents documents et prévoient la minimisation des données traitées. Etant donné que l'application utilise des services sous-jacents de la plateforme Android et doit de ce fait utiliser les services Google Play, il n'est pas possible d'éviter que le fournisseur du système d'exploitation collecte des informations supplémentaires non indispensables aux opérations visées. Google récoltera ainsi des informations sur la localisation sur la base de la position GPS, des adresses IP et des informations sur le Wi-fi, des balises Bluetooth et des informations sur les capteurs.	
Score de risque	
Probabilité après mesures	1
Impact après mesures	3
Risque	MOYEN

R08. Utilisation minimale des données

R08. Utilisation minimale des données
Vulnérabilité
Aucune mesure n'est prise pour garantir que seules les données pertinentes sont traitées, d'une part, et que leur traitement se limite à la finalité énoncée, d'autre part.
Commentaire explicatif
La collecte de données traitées doit se limiter à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (« minimisation des données »). Cela signifie qu'aucune donnée qui n'est pas nécessaire aux finalités prévues ne peut être traitée sur la plateforme ou via l'application, par extrapolation ou tout autre mécanisme d'acquisition de données.
Mesures
Pour l'échange des résultats des tests, la plateforme doit obtenir ces informations à partir d'une autre base de données de Sciensano. Ces données ne sont fournies qu'avec la date probable de l'infection et un code de test. Cette date et ce code ne contiennent aucune information qui pourrait permettre de relier les résultats à l'appareil de l'utilisateur ou à l'utilisateur lui-même, limitant ainsi la possibilité d'utiliser les données obtenues pour d'autres finalités. L'échange de ces données est toutefois essentiel pour le traitement visé. Les clés chiffrées sont également chargées au moyen d'un échange de codes secrets qui ne permettent pas de remonter jusqu'à l'appareil de l'utilisateur ou jusqu'à l'utilisateur lui-même. L'échange de ces codes est également essentiel au fonctionnement de la plateforme. Les deux traitements susmentionnés sont décrits dans l'Arrêté royal n°44 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano, avec leurs limitations, ainsi que dans le futur Accord de coopération. L'application elle-même traitera les clés chiffrées obtenues ainsi que les numéros de série temporaires non personnalisés pour déterminer le risque du contact, en tenant compte aussi de la distance et de la durée. Ce traitement a été documenté et rendu public. Afin de garantir au maximum le respect de la vie privée des personnes concernées, le traitement se limite aux données essentielles au fonctionnement du traçage des contacts.

R08. Utilisation minimale des données	
Risque résiduel	
Les données de l'application ne permettent pas facilement de remonter jusqu'aux personnes physiques, ce qui limite l'impact du traitement de données non pertinentes et limite très fortement la possibilité de traiter ces données pour d'autres finalités. La plateforme a été conçue de manière à limiter le risque d'un traitement de données autres que les données prévues. Le cas échéant, ce traitement n'aurait que peu d'impact pour la personne concernée, car toutes les données sont pseudonymisées et les bases de données de la plateforme ne contiennent pas d'informations de contact identifiables.	
Score de risque	
Probabilité après mesures	1
Impact après mesures	2
Risque	FAIBLE

D04. Garantie de la qualité des données à caractère personnel

Principe	Assurez-vous que vos données à caractère personnel sont exactes, pertinentes et à jour avant de les utiliser.
Résumé	Des mesures raisonnables sont prises pour assurer la qualité, en fonction des informations concernées. Les questions pertinentes ici sont notamment les suivantes : quel est le processus mis en place pour vérifier l'exactitude des informations ? Les informations ont-elles été fournies directement par la personne ? Ont-elles été vérifiées directement auprès de la personne ? Est-il question d'une vérification automatisée ou d'un jugement humain ? Quel est le préjudice pour l'individu si les informations sont fausses ou trompeuses ? (plus le préjudice est grand, plus les étapes de vérification de l'exactitude doivent être étendues)
Lien RGPD	Article 5 d) : les données doivent être exactes et, si nécessaire, tenues à jour.

R09. Exhaustivité et exactitude des données

R09. Exhaustivité et exactitude des données
Vulnérabilité
L'exhaustivité et l'exactitude des données ne sont pas suffisamment vérifiées lors de la collecte de celles-ci.
Commentaire explicatif
(i) Il existe un risque de faux positifs en raison d'une saisie erronée des prestataires de soins de santé dans la base de données de Sciensano qui sert de source authentique pour la plateforme. Si un résultat de test a été copié sur la plateforme de traçage numérique des contacts, il n'est plus possible de le modifier, tandis que la personne concernée ne peut être identifiée. (ii) Le signal BT (Bluetooth) traverse les murs et peut donc être indûment reçu par les voisins d'une personne index, les passagers d'autres wagons, les personnes se trouvant dans des voitures proches, ou encore les passants le long de la maison d'une personne index. (iii) Il existe un risque de fausses alertes pour les prestataires de soins qui utilisent l'appli Coronalert. Ils entrent en effet en contact avec de nombreux patients à risque mais ils portent des vêtements de protection. (iv) Il y a un risque de faux positifs introduits par les utilisateurs s'ils devaient charger leurs clés. L'impact sera alors que d'autres utilisateurs pourront recevoir, sans raison aucune, une alerte sur un contact à risque.
Mesures

R09. Exhaustivité et exactitude des données
i) Contrôle de la qualité des données par Sciensano. Ce contrôle ne peut s'effectuer qu'au niveau macro et non au niveau individuel du patient. Le Risk Assesment Group a émis un avis pour aider les microbiologistes et les cliniciens dans l'interprétation de résultats PCR faiblement positifs. Un suivi et une objectivation sur l'ordre de grandeur des faux positifs ainsi qu'une communication à ce sujet seront suivis au sein du Groupe interfédéral Testing et Tracing. (ii) Le protocole DP-3T prévoit dans sa détermination des contacts à risque une prise en compte des facteurs de distance et de durée du contact. Ceci permet d'éviter le problème, par exemple, d'un train qui passe : ces contacts sont de durée nettement plus courte que celle indiquée dans les spécifications. Le signal BT est par ailleurs atténué lorsqu'il traverse des murs ou des cloisons de séparation de wagons par exemple, ce qui entraînera une exclusion dans le calcul d'un contact à risque. Des tests et mesures approfondis ont été effectués pour garantir la fiabilité des estimations de la durée et de la distance. (iii) L'application Coronalert prévoit que l'utilisateur puisse arrêter temporairement l'envoi et la réception de jetons Bluetooth pour le traçage des contacts (sans désactiver Bluetooth sur le téléphone). Cela peut par exemple être le cas lorsqu'une personne du secteur médical portant un équipement de protection traite des patients infectés ou lorsqu'une personne laisse son smartphone dans un locker d'une pièce commune. iv) L'utilisateur ne peut pas charger de clés chiffrées autres que celles valables pour la période d'infectiosité. Ce contrôle est assuré par la création d'un code d'autorisation par la plateforme lorsqu'un test s'avère positif.
Risque résiduel
i) Comme le contrôle de qualité ne peut pas être effectué au niveau du patient *(sauf par des microbiologistes et des cliniciens),* les probabilités ne sont pas complètement éliminées par les mesures proposées. Par ailleurs, vu les mesures de sécurité de la plateforme, un patient et utilisateur de l'application ne peut pas être averti lorsque son résultat s'avère erroné. Cet utilisateur et d'autres peuvent donc être invités à tort à se placer en quarantaine. Pour les utilisateurs qui n'ont reçu qu'un avertissement, la durée de la quarantaine proposée peut être limitée en demandant un test COVID. Néanmoins, l'utilisateur sera confronté à un risque potentiel de quarantaine inutile s'il souhaite se tenir strictement aux mesures proposées. (ii) La probabilité de cette vulnérabilité est limitée par le fait que l'algorithme traite des paramètres supplémentaires pour déterminer si un contact était risqué ou non. (iv) La probabilité qu'un utilisateur puisse importer des clés chiffrées de manière incorrecte est limitée par le système du code d'autorisation. Si cela devait se produire, l'impact sur les contacts à risque, c'est-à-dire la quarantaine temporaire, n'est pas faible. Il correspond toutefois – compte tenu de l'état actuel de la science – à tous les modes de traçage des contacts (y compris le traçage manuel des contacts) selon lesquels les contacts à risque ne donnent lieu à une contamination qu'avec une chance de 10 à 15 %. Dans le cas du traçage numérique des contacts également, le citoyen devra accepter une éventuelle quarantaine temporaire injustifiée. C'est pourquoi l'impact est qualifié de « moyen ».

Score de risque	
Probabilité après mesures	2
Impact après mesures	2
Risque	MOYEN

R10. Caractère précis et à jour des données

R10. Caractère précis et à jour des données	
Vulnérabilité	
Aucune procédure n'a été mise en place pour vérifier régulièrement si les données à caractère personnel sont exactes et à jour.	
Commentaire explicatif	
Les données disponibles sur la plateforme et sur l'appareil de l'utilisateur seront utilisées pour informer l'utilisateur de l'appli d'éventuels contacts à risque. Si ces données ne sont pas correctes, un utilisateur pourra éventuellement recevoir des informations fautives sur des contacts à risque. Si un contact à risque n'est pas jugé comme tel, l'utilisateur ne demandera pas de test et il ne prendra pas non plus les mesures qui s'imposent. Si un contact est jugé à tort comme étant à risque, parce que les données ne sont pas précises, l'utilisateur demandera un test et s'il suit littéralement l'avis donné par l'appli, il se mettra en quarantaine alors que ce n'est pas nécessaire.	
Mesures	
Une fois que les données ont été chargées dans la plateforme, elles ne peuvent pas être contrôlées quant à leur précision en raison de leur pseudonymisation. Il n'existe pas non plus de mécanisme prévoyant que les données collectées par l'appli puissent être contrôlées ultérieurement. Le concept de l'application prévoit que les données mises à disposition sont téléchargées et consommées régulièrement. L'application et la plateforme prévoient également que les données seront supprimées après une période de 14 jours.	
Risque résiduel	
Etant donné que les données ne peuvent être contrôlées ni quant à leur précision, ni quant à leur caractère actuel pour le traitement, le risque reste au même niveau que pour R.09.	
Score de risque	
Probabilité après mesures	2
Impact après mesures	2
Risque	MOYEN

R11. Enrichissement des données

R11. Enrichissement des données	
Vulnérabilité	
Les profils personnels et identifiables des personnes concernées sont enrichis d'informations inexactes par des algorithmes probabilistes.	
Commentaire explicatif	
Les données suivantes sont échangées : • clés chiffrées • numéro de série temporaire non personnalisé • résultats des tests en laboratoire, protégés par un code de test Aucun de ces codes, numéros de série et clés ne contient d'informations permettant de remonter jusqu'à un utilisateur. Par conséquent, la vulnérabilité mentionnée ne s'applique pas à ces données. Cependant, les journaux contenant les activités d'un utilisateur peuvent permettre d'identifier l'utilisateur et sont sujets à cette vulnérabilité.	
Mesures	
Les journaux d'enregistrements peuvent contenir des informations qui permettent au fournisseur de services (le sous-traitant étant ici AWS) , de récupérer des données relatives à l'utilisateur sur la	

R11. Enrichissement des données
base d'une adresse IP et des serveurs contactés. Par conséquent, l'application fournit des informations « factices » (par exemple, le chargement de fausses clés) afin qu'aucune conclusion ne puisse être tirée de cette activité. En outre, il est prévu au sein de la plateforme centrale qu'aucune combinaison de données ne peut se produire entre les journaux (par exemple, l'adresse IP) et l'activité (par exemple, l'obtention de résultats de tests).
Risque résiduel
Chaque jour, environ 20 % des utilisateurs téléchargeront un faux résultat de test pour ensuite importer une fausse clé chiffrée (c'est-à-dire sans code d'autorisation). En moyenne, 0,1 à 0,2 % des utilisateurs par jour seront effectivement testés. Une clé chiffrée n'est jamais importée en cas de test négatif. Elle l'est généralement (mais pas toujours) en cas de test positif. Cela signifie que pour 100 résultats, il y aura un seul résultat authentique, lequel laissera échapper une très petite quantité d'informations qui sera noyée dans l'ensemble (vu le grand nombre de faux résultats de tests).

Score de risque	
Probabilité après mesures	1
Impact après mesures	2
Risque	FAIBLE

D05. Respect des exigences en matière de limitation de la conservation

Principe	Supprimez les données dès que vous n'en avez plus besoin.
Résumé	Pendant combien de temps comptez-vous conserver les informations ? Existe-t-il des obligations de conserver les informations pendant une certaine période, par exemple en vertu de la réglementation ou de la législation ? Si de telles obligations n'existent pas, quelle serait la durée raisonnable de conservation des informations ? Qu'en est-il des procédures de recours et des délais de prescription ? Comment allez-vous procéder ? Si des informations sont partagées avec un tiers, il convient de réfléchir à la durée de conservation des informations et aux mesures à prendre pour s'assurer que le tiers en question dispose de renseignements personnels uniquement s'il répond aux exigences techniques et organisationnelles.
Lien RGPD	Article 5 e)

R12. Suppression des données

R12. Suppression des données
Vulnérabilité
Les données à caractère personnel et les données de sauvegarde correspondantes ne sont pas supprimées ou rendues anonymes alors que leur conservation n'est plus nécessaire pour la finalité spécifiée. Absence de politique ou de mécanisme d'effacement des données.
Commentaire explicatif
Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais devraient être fixés par le responsable du traitement pour leur effacement ou pour un examen périodique. En l'absence d'une politique adéquate à cet égard, le principe de minimisation des données est bafoué.
Mesures
Les données sont conservées sur 2 plateformes : • Plateforme centrale :

R12. Suppression des données
○ Données de test : les données de test sont effacées une fois qu'elles ont été téléchargées par la personne concernée. ○ Clés chiffrées : elles sont supprimées au plus tard 3 semaines après la date de contamination. Le délai pour la plateforme est fixé à 14 jours. • Appli : ○ Numéro de série temporaire non personnalisé: supprimé après une période de 14 jours. ○ Clés chiffrées : elles sont supprimées au plus tard 3 semaines après la date de contamination. Le délai pour la plateforme est fixé à 14 jours. ○ En cas de suppression de l'appli de l'appareil de l'utilisateur, les numéros de série temporaires non personnalisés et les clés chiffrées sont encore conservés jusqu'à ce que la période de 14 jours soit écoulée. Les données de tests reçues sont supprimées de l'appareil lorsque l'appli est désinstallée. Toutes les données sur les deux plateformes sont pseudonymisées ou protégées par un code qui ne permet pas de remonter jusqu'à un utilisateur ou son appareil.
Risque résiduel
Étant donné que les spécifications de l'application et de la plateforme contiennent des périodes de conservation claires et que celles-ci font l'objet d'une mise en œuvre technique, la probabilité est faible. Comme les données ne peuvent pas être rattachées à un utilisateur ou à son appareil, l'impact qu'un utilisateur peut subir est plutôt limité.
Score de risque

Probabilité après mesures	1
Impact après mesures	2
Risque	FAIBLE

R13. Utilisation de données non supprimées

R13. Utilisation de données non supprimées
Vulnérabilité
Des données à caractère personnel qui ne sont plus nécessaires pour la finalité spécifiée, mais qui ne peuvent être supprimées en raison des règles de conservation, ne peuvent être exclues du traitement régulier des données.
Commentaire explicatif
Aucune règle de conservation exigeant que les données soient conservées plus longtemps que nécessaire au traitement n'a été définie pour la plateforme ou l'application. Cela n'aurait en définitive aucun sens, puisque les informations sur les deux plateformes ne permettent pas de remonter jusqu'à l'utilisateur ou son appareil.
Mesures
Les données stockées sur les différentes plateformes sont pseudonymisées et ne permettent que très difficilement de remonter aux personnes concernées. Le pseudonyme utilisé pour décrire un utilisateur changera quotidiennement en cas de clé chiffrée ou sera unique dans le cas du code de test.
Risque résiduel
Etant donné que les données ne permettent quasiment pas de remonter à la personne concernée, le risque d'un traitement ayant un impact sur la personne concernée est très faible, même si ces données n'étaient pas supprimées. Etant donné qu'un pseudonyme n'est jamais utilisé plusieurs fois pour une même personne concernée, le risque d'une nouvelle identification en cas de combinaison de données reste très faible.

R13. Utilisation de données non supprimées	
Etant donné qu'il s'agit de données médicales, l'impact peut être grand si lors du traitement, les données peuvent permettre de remonter à la personne concernée.	
Score de risque	
Probabilité après mesures	1
Impact après mesures	3
Risque	MOYEN

O06. Respect du droit à la protection de la confidentialité et de la sécurité du traitement des données

Principe	Traitez les données en votre possession avec soin et protégez-les contre la perte, l'accès et l'utilisation non autorisés, l'altération ou la divulgation et toute autre utilisation abusive.
Résumé	Il peut exister un certain nombre de méthodes pour vous aider à protéger les informations personnelles que vous détenez, telles que des politiques et des codes de conduite régissant la manière dont les employés traitent les informations personnelles, ou des contrôles physiques ou techniques destinés à protéger les informations. Il est utile de se référer directement aux documents ou aux informations disponibles à l'appui. Les garanties peuvent comprendre : la sécurité physique, la sécurité informatique, la formation du personnel, la politique à suivre par les employés, les clauses de confidentialité dans les contrats avec les prestataires externes, etc. Voyez s'il existe des vulnérabilités à chaque niveau de la chaîne de traitement de l'information – identifiez les maillons faibles.
Lien RGPD	Article 5 f) : garantir une sécurité appropriée des données à caractère personnel.

R14. Accès non autorisé aux données

R14. Accès non autorisé aux données
Vulnérabilité
Les données étant insuffisamment sécurisées, des données à caractère personnel peuvent être volées ou consultées par une personne qui n'est pas autorisée ou habilitée à le faire.
Commentaire explicatif
Les données sont disponibles sur 2 plateformes, à savoir l'application et la plateforme centrale. Les vulnérabilités suivantes sont valables pour l'application (également citées dans les AIPD étrangères concernant l'application de traçage des contacts) : i) les distributeurs de l'application (Google Play, Apple Store) collectent des métadonnées lors de l'installation et de la désinstallation de l'application de traçage des contacts, conformément aux stipulations de leur modèle d'exploitation. Cela comprend des données à caractère personnel liées à l'application ; ii) des numéros de série temporaires non personnalisés peuvent être récupérés et liés à une personne, ce qui permet de retracer celle-ci ; iii) le smartphone de l'utilisateur n'est pas suffisamment sécurisé. Les vulnérabilités suivantes s'appliquent à la plateforme centrale : i) le contrôle d'accès à la plateforme n'est pas suffisamment fort ; ii) l'accès aux journaux d'enregistrement (infrastructure) n'est pas suffisamment sécurisé ; iii) il n'existe pas de mécanisme de détection des fuites de données ; iv) la plateforme elle-même n'est pas suffisamment sécurisée.

R14. Accès non autorisé aux données
Pour la communication entre l'appli et la plateforme, il convient de veiller à ce que les données ne puissent pas être interceptées.
Mesures
Toutes les informations disponibles sur la plateforme et sur les applications sont toujours pseudonymisées et il est très difficile de remonter jusqu'à la personne concernée. Les mesures supplémentaires suivantes valent en ce qui concerne l'application : • Les informations collectées par l'application ne sont pas accessibles aux utilisateurs. • . • Le numéro de série temporaire non personnalisé change toutes les 10 minutes, ce qui rend difficile le traçage d'une personne. • Il n'y a pas d'échange de clés chiffrées directement entre les appareils. • Dans le traitement d'un risque précédent, il a été question de la collecte de données par les distributeurs de l'application. Comme indiqué, aucun accès aux données de l'appli n'a été prévu pour les distributeurs de l'application. La plateforme centrale est soumise aux mesures de sécurité prévues dans l'architecture. (Voir la description des mesures de sécurité AWS) La communication entre l'appli et la plateforme se déroule d'une manière sécurisée et de ce fait, les données ne peuvent pas être interceptées.
Risque résiduel
Malgré les accords passés avec les fournisseurs Google et Apple, il subsiste le risque que ces derniers puissent transférer régulièrement les données collectées par l'application vers leurs serveurs centraux. Comme indiqué dans les commentaires relatifs à un risque précédent, il est prévu que ces fournisseurs n'aient aucun accès à ces informations. Tant pour l'application que pour la plateforme centrale, la principale protection est que les données ne permettent pas de remonter jusqu'à une personne physique. En cas de fuite, l'impact sera toujours faible ou limité. En raison des mesures de sécurité prévues, la probabilité sera également faible, sauf pour les smartphones mal sécurisés.

Score de risque	
Probabilité après mesures	1
Impact après mesures	3
Risque	MOYEN

R15. Pseudonymisation des données

R15. Pseudonymisation des données
Vulnérabilité
Les données ne sont pas anonymisées ni pseudonymisées, de sorte que des données à caractère personnel peuvent être directement liées à la personne concernée.
Commentaire explicatif
i) L'adresse IP et d'autres métadonnées, ainsi que l'adresse MAC et d'autres données relatives à l'appareil, peuvent être utilisées par le sous-traitant pour identifier une personne testée positive, ainsi que son historique de contact. ii) Chez les utilisateurs ayant un nombre limité de contacts, une nouvelle identification peut se produire lorsqu'un des contacts signale une contamination pour laquelle une notification sera donnée via l'appli.
Mesures

R15. Pseudonymisation des données
i) Le protocole DP-3T se concentre principalement sur la pseudonymisation des données nécessaires pour déterminer les contacts à risque et pour obtenir les résultats d'un test. Dans la conception de la plateforme, une séparation est prévue pour l'accès aux journaux d'enregistrements avec l'adresse IP et le résultat obtenu, entre autres. En outre, l'importation de « clés factices » permet difficilement de tirer des conclusions sur le trafic des données. Cette possibilité a déjà été évoquée plus haut. ii) Pour les personnes ayant un nombre limité de contacts, il est important que les conférences de presse de la Cellule de crise nationale continuent de répéter que tous les groupes de la population, quels que soient l'âge, la race, la croyance, le sexe ou les antécédents médicaux peuvent être confrontés au COVID-19 et qu'une contamination n'est que temporaire et ne peut pas être une raison de stigmatiser ou d'exclure socialement une personne.
Risque résiduel
i)Vu la pseudonymisation prévue dans le protocole DP-3T, les données opérationnelles sont d'ores et déjà protégées. Un risque résiduel réside principalement dans les données rendues disponibles par les mesures supplémentaires de sécurité de l'information. Par exemple, un WAF offrira la possibilité de vérifier le contenu du trafic et des informations seront transmises au sous-traitant. Ces mesures de sécurité étant déterminantes pour la disponibilité de la plateforme, il est recommandé de les maintenir, sans pour autant laisser le sous-traitant y recourir. Il est également possible de collecter secrètement des balises Bluetooth avec un smartphone et votre propre application ; cela fonctionne à environ 10-20 m, mais grâce à une antenne spéciale, vous pouvez étendre la portée jusqu'à 100 m. En combinant ce procédé avec un appareil photo numérique, il serait alors possible de relier les balises aux utilisateurs. Si l'un de ces utilisateurs est contaminé et qu'il importe ses clés chiffrées, il peut être déterminé que cet utilisateur particulier a été testé positif. Ces actions exigent toutefois un effort considérable et la probabilité est jugée plutôt faible. ii) Bien qu'une identification ne puisse pas totalement être exclue dans le cadre d'un petit réseau social et peut avoir un impact important, nous estimons la probabilité en matière d'augmentation de la stigmatisation par l'introduction de l'appli plutôt faible en raison des connaissances plus larges qu'a la population générale sur le COVID-19.

Score de risque	
Probabilité après mesures	1
Impact après mesures	3
Risque	MOYEN

R16. Perte de données

R16. Perte de données
Vulnérabilité
Aucune mesure n'est prise pour garantir qu'il peut être remédié à la disparition (perte, destruction ou détérioration accidentelle) ou à l'indisponibilité de données à caractère personnel.
Commentaire explicatif
En raison de l'absence de mesures de redondance suffisantes, la plateforme peut être temporairement indisponible en cas d'endommagement ou de destruction des données, intentionnellement, en raison d'une erreur humaine ou de la défaillance d'un appareil. L'impact pour les personnes concernées est alors que les résultats d'un test ne peuvent plus être obtenus par l'intermédiaire de l'application. L'impact pour la société est encore plus grand, puisque cette application devrait permettre aux citoyens d'être mieux et plus rapidement informés des contacts à risque potentiel. À défaut, les citoyens pourraient être confrontés à des mesures renforcées pour lutter contre la propagation du coronavirus.

R16. Perte de données

Afin de limiter ce risque, il convient de s'intéresser tout particulièrement à l'application au niveau de la plateforme centrale et à l'infrastructure sous-jacente.
 	
• Application :
  ○ Une adaptation logicielle rend les bases de données inaccessibles
  ○ Le volume de la base de données dépasse les limites du système
  ○ Le code source de l'application disparaît
• Infrastructure
  ○ La disponibilité de la plateforme n'est pas suffisamment garantie
  ○ La disponibilité du réseau n'est pas suffisamment garantie
  ○ La capacité de la plateforme n'est pas suffisante pour un traitement correct
  ○ La plateforme subit une attaque de l'extérieur, ce qui entraîne une indisponibilité
  ○ Une faille au niveau de composants essentiels de la plateforme provoque une interruption du service et entraîne la perte de données
L'impact en cas de perte de données dans l'application sera limité pour la personne concernée. En effet, cela signifierait que la clé pour charger sur la plateforme si la personne concernée s'avérait infectée, ne sera plus disponible.

Mesures
• Les données sont sécurisées au moyen d'une sauvegarde avec point de restauration • Le service est installé dans 3 zones de disponibilité d'AWS • En retenant AWS comme fournisseur, de la capacité peut facilement être ajoutée à la plateforme si nécessaire • Sauvegardes avec Point-In-Time Recovery • Protection via Web Application Firewall (WAF) et systèmes de mitigation DDoS • Répartition de la charge à l'aide de dispositifs dédiés
Risque résiduel
Les mesures de sécurité prévues dans les mesures limitent l'impact d'une perte de données. En utilisant différentes zones de disponibilité, l'impact sur la disponibilité sera limité en cas de perte d'une zone de disponibilité, que ce soit pour les systèmes de calcul ou pour les systèmes de réseau. En utilisant des sauvegardes de la base de données, les données perdues peuvent être récupérées et la disponibilité de la plateforme et de ses données reste garantie au maximum pour l'utilisateur, tandis que l'impact d'une panne est limité. Si un utilisateur perd les données de son application, il devra retomber sur le traçage manuel des contacts.
Score de risque

Probabilité après mesures	1
Impact après mesures	2
Risque	FAIBLE

R17. Détection de fuites de données

R17. Détection de fuites de données
Vulnérabilité
Aucun mécanisme ne détecte automatiquement les fuites de données.
Commentaire explicatif
Les données traitées contiennent des informations qui peuvent être utilisées pour déterminer les contacts à risque (informations médicales) et des informations sur les résultats des tests demandés. Au niveau de la plateforme centrale, il faut s'intéresser aux éventuelles fuites de résultats de tests.

R17. Détection de fuites de données
Au niveau de l'application, il convient d'examiner les éventuelles fuites d'informations sur les contacts. Une fois que les clés chiffrées ont été importées par un utilisateur, ces données sont publiques. Une fuite de ces données ne représente pas de risque pour les personnes concernées.
Mesures
Ni la plateforme ni l'application ne disposent d'un système permettant de détecter des fuites de données.
Risque résiduel
Même si les fuites de données ne pourront pas être détectées, l'impact d'une fuite depuis la plateforme centrale restera limité. Les données confidentielles concernent le code de test qui protège l'accès au résultat du test et celui-ci ne contient aucune information permettant de remonter à la personne ou à son appareil. De ce fait, le risque d'impact est faible pour la personne concernée. Les éventuelles fuites d'une application individuelle auront un impact limité en raison du volume, mais surtout parce que cela ne concernera que le numéro de série temporaire non personnalisé, qui doit être considéré comme une information pseudonymisée qui ne peut être que difficilement reliée à une personne concernée.

Score de risque	
Probabilité après mesures	2
Impact après mesures	1
Risque	FAIBLE

R18. Test des mesures de sécurité

R18. Test des mesures de sécurité
Vulnérabilité
Les mesures de sécurité mises en œuvre ne sont pas régulièrement testées, évaluées ou appréciées ?
Commentaire explicatif
Des mesures de sécurité sont nécessaires pour garantir la protection des données à caractère personnel présentes sur la plateforme et sur les smartphones des utilisateurs. Étant donné leur importance, il convient de les tester à intervalles réguliers pour en apprécier l'efficacité.
Mesures
La mesure la plus importante pour la protection des données est l'application du protocole DP-3T. Les données sont ainsi pseudonymisées et ne permettent pas de remonter jusqu'à la personne concernée ou à son appareil. Comme mentionné précédemment, l'impact d'une fuite sera limité. En outre, l'architecture de la plateforme assure la disponibilité sur plusieurs zones de disponibilité, tandis qu'une sauvegarde est configurée pour garantir une disponibilité maximale de la plateforme. La protection de la plateforme elle-même est assurée par les services de sécurité du sous-traitant (AWS). La sécurité des smartphones ne peut être vérifiée, car elle relève de la responsabilité de l'utilisateur. Pendant le développement de l'application et de la plateforme, il est prévu que le développeur teste les aspects fonctionnels et non fonctionnels de l'application. Un auditeur testera en outre le logiciel développé sur les points de sécurité.
Risque résiduel
La confidentialité des informations est protégée par la pseudonymisation des données. Ce mécanisme est prévu au sein de l'architecture et la plateforme est testée au niveau de ses vulnérabilités après chaque mise à jour, ce qui réduit les risques d'incident.

R18. Test des mesures de sécurité	
Concernant la plateforme, un test régulier est également crucial. La sortie du logiciel s'accompagnera d'un test de pénétration visant à évaluer la vulnérabilité de la plateforme. Il demeure une vulnérabilité concernant la disponibilité, principalement en termes de basculement et de restauration des données.	
Score de risque	
Probabilité après mesures	2
Impact après mesures	2
Risque	MOYEN

R19. Procédure en cas de fuites de données

R19. Procédure en cas de fuites de données
Vulnérabilité
Il n'existe pas de procédure pour informer les personnes concernées en cas de fuite de données.
Commentaire explicatif
Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais. Cette communication à la personne concernée n'est pas nécessaire si : • des mesures de protection techniques et organisationnelles appropriées ont été mises en place ; • elle exigerait des efforts disproportionnés.
Mesures
Bien que la prévention des fuites et le traitement de ces fuites doivent être décrits dans une politique de lutte contre les fuites de données, la pseudonymisation de toutes les données garantit que l'information divulguée ne peut permettre de remonter jusqu'à une personne physique. Les données étant pseudonymisées et le responsable du traitement de laplateforme centrale ne pouvant pas remonter jusqu'à une personne physique, aucun avertissement individuel ne peut être émis à l'égard de la personne dont les données ont fait l'objet d'une fuite. Ces deux remarques valent tant pour les clés de sécurité importées que pour les résultats de test. Il convient toutefois de noter que les clés chiffrées deviennent des informations publiques une fois importées. Une fuite à ce niveau n'aurait donc pas d'impact pour la personne concernée, ces informations étant déjà publiques.
Risque résiduel
Le risque résiduel pour la personne concernée est principalement la fuite d'informations médicales, pour laquelle elle ne peut être avertie. Toutefois, les informations étant pseudonymisées, l'impact pour la personne concernée est limité et le risque peut être évalué comme faible.
Score de risque

Probabilité après mesures	1
Impact après mesures	2
Risque	FAIBLE

R42. Exposition de données à des tiers

R42. Exposition de données à des tiers
Vulnérabilité

R42. Exposition de données à des tiers
Des données ne relevant pas de l'examen des contacts seront exposées à des tiers suite à l'utilisation de l'application.
Commentaire explicatif
Comme indiqué dans des AIPD d'autres pays à propos des applications de traçage des contacts : i) L'activation permanente du Bluetooth (BT) permet aux pirates d'abuser des fuites de sécurité BT existantes et connues – l'intrusion automatisée via ces fuites est possible lorsqu'un hacker se trouve à faible distance de sa cible. Il n'est pas possible d'exiger la version la plus récente (et la plus sécurisée) de Bluetooth, car cela exclurait des utilisateurs. ii) Les centres commerciaux, les aéroports, les gares, etc. sont déjà équipés d'une infrastructure de traçage par BT pour suivre le comportement des clients, comme la durée du séjour, l'itinéraire suivi dans les locaux et le taux de retour. Les personnes ayant lancé l'application de traçage des contacts Coronalert ne peuvent pas désactiver leur BT, et de grandes quantités de données peuvent donc tomber entre les mains de tiers.
Mesures
Les vulnérabilités propres à l'utilisation de Bluetooth comme moyen d'échanger le numéro de série temporaire non personnalisé sont spécifiques à l'utilisation de Bluetooth et non à l'application. En ce sens, aucune mesure supplémentaire ne peut être prévue au sein de l'application pour éliminer ces vulnérabilités. Il est et sera stipulé dans « l'Arrêté royal N°44 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano » et le futur Accord de coopération que le citoyen ne peut en aucun cas être tenu d'installer l'application. Par conséquent, le citoyen qui estime le risque susmentionné trop important est libre de ne pas installer l'application.
Risque résiduel
Le risque décrit ci-dessus ne peut être éliminé avec l'application. La seule mesure pour éliminer cette vulnérabilité est d'éteindre l'application. Le risque de traçage par le biais de Bluetooth reste présent lors de l'utilisation de l'application, tout comme il l'est lors de toute utilisation d'appareils audio connectés via Bluetooth.

Score de risque	
Probabilité après mesures	2
Impact après mesures	2
Risque	MOYEN

D07. Licéité du traitement des données à caractère personnel

Principe	L'une des conditions pour que le traitement soit considéré comme licite est-elle remplie ?
Résumé	Le traitement des données à caractère personnel ne repose pas sur : une relation contractuelle, une obligation légale, un intérêt général, des intérêts légitimes, un consentement, un intérêt vital Il est question de légitimité pour le traitement de : catégories particulières de données à caractère personnel

	données à caractère personnel relatives aux condamnations pénales et aux infractions
Lien RGPD	Article 6 Licéité du traitement Article 7 Conditions applicables au consentement Article 8 Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information Article 9 Traitement portant sur des catégories particulières de données à caractère personnel Article 10 Traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions

R20. Licéité du traitement

R20. Licéité du traitement
Vulnérabilité
Le traitement des données à caractère personnel ne repose pas sur : - une relation contractuelle, - une obligation légale, - un intérêt général, - des intérêts légitimes, - un consentement, - un intérêt vital
Commentaire explicatif
Pour que les données puissent être traitées, il doit exister un fondement juridique pour la collecte et le traitement ultérieur des données. Les données à traiter sont des données médicales, ce qui signifie que les exigences énoncées aux articles 6 et 9 du RGPD doivent être respectées.
Mesures
La licéité du traitement est basée sur l'article 6.1 e du RGPD. Pour le traitement de données médicales, une exception au principe d'interdiction est obtenue par application de l'article 9.2. i du RGPD. Le cadre juridique a été élaboré au niveau fédéral, régional et communautaire. Il consiste en l'arrêté royal n°44 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano et en les dispositions complémentaires visées dans l'Accord de coopération entre les différents niveaux politiques. La lutte contre le coronavirus représentant un intérêt général pour la santé publique tout en formant un enjeu transfrontalier, l'interdiction de traitement des données médicales ne s'applique pas. L'utilisateur est par ailleurs invité à donner son consentement au traitement ultérieur de ses données lorsqu'il installe l'application et communique des données, sans que ce soit indispensable pour la licéité du traitement.
Risque résiduel
Etant donné que la finalité du traitement prévoit une base juridique licite conformément au RGPD, vu l'importance pour la santé publique de ces traitements qui prévoit une levée de l'interdiction du traitement des données médicales ainsi que les différents AR et conventions entre les différents niveaux politiques, la probabilité que cette vulnérabilité se produise est très limitée. L'impact du non-respect de cette exigence est modéré à élevé étant donné que le traitement ne pourra plus se poursuivre et que les citoyens ne seront plus avertis à temps de tout contact à risque.

R20. Licéité du traitement	
En ce qui concerne la continuité du cadre législatif, il n'est pas exclu que certains éléments soient modifiés à la suite de procédures judiciaires en cours. Le cas échéant, il est possible que les législateurs ou les régulateurs remédient aux lacunes (rapidement et/ou rétroactivement) en raison du large soutien social et politique en faveur de mesures proportionnées dans la lutte contre le COVID-19.	
Score de risque	
Probabilité après mesures	1
Impact après mesures	2
Risque	FAIBLE

R21. Consentement pour le traitement

R21. Consentement pour le traitement	
Vulnérabilité	
Si le traitement est fondé sur le consentement : un consentement explicite n'a pas été obtenu, ou a été obtenu sur la base d'informations incomplètes ou incorrectes, ou a été obtenu sur la base d'une offre d'avantage ou d'une menace de préjudice.	
Commentaire explicatif	
La licéité du traitement est basée sur l'article 6.1. e du RGPD et l'interdiction du traitement des données médicales est levée par invocation de l'article 9.2. i de ce même RGPD. Par conséquent, aucun consentement ne doit être donné par les personnes concernées pour le traitement des données.	
Mesures	
Aucune mesure supplémentaire n'est prise.	
Risque résiduel	
Etant donné que la licéité du traitement repose sur l'article 6.1. e du RGPD, la probabilité est ici très faible.	
Score de risque	
Probabilité après mesures	1
Impact après mesures	2
Risque	FAIBLE

R22. Légitimité du traitement portant sur des catégories particulières de données à caractère personnel

R22. Légitimité du traitement portant sur des catégories particulières de données à caractère personnel	
Vulnérabilité	
Le traitement portant sur des catégories particulières de données à caractère personnel n'est pas légitime.	
Commentaire explicatif	
Le RGPD stipule que les données mentionnées aux articles 9 et 10 ne peuvent pas être traitées. Or, l'application prévoit le traitement des données décrites à l'article 9, §1. Des exemptions sont toutefois prévues et le traitement est autorisé si une des conditions visées à l'article 9, §2 s'applique. Dans le cas présent, le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, comme stipulé à l'article 9, §2, i., et l'interdiction est donc levée.	
Mesures	

R22. Légitimité du traitement portant sur des catégories particulières de données à caractère personnel	
Outre l'exemption stipulée à l'article 9, §2, i. du RGPD, l'utilisateur est invité à donner son accord pour le traitement de ses données médicales lors de chaque échange de données.	
Risque résiduel	
Le risque initial est déjà faible étant donné que l'intérêt de la santé publique justifie une levée de l'interdiction du traitement des données médicales. Étant donné que l'utilisateur est également explicitement invité à donner son accord lors de l'échange des données et de leur traitement ultérieur, le risque doit être considéré comme faible.	
Score de risque	
Probabilité après mesures	1
Impact après mesures	1
Risque	FAIBLE

R23. Légitimité du traitement de données à caractère personnel juridiques

R23. Légitimité du traitement de données à caractère personnel juridiques	
Vulnérabilité	
Il n'y a pas de légitimité au traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions.	
Commentaire explicatif	
Le traitement d'informations juridiques n'est pas prévu, que ce soit au niveau de l'infrastructure ou de l'application.	
Mesures	
Non applicable	
Risque résiduel	
Non applicable (NA)	
Score de risque	
Probabilité après mesures	NA
Impact après mesures	NA
Risque	NA

R24. Traitement de données de mineurs

R24. Traitement de données de mineurs	
Vulnérabilité	
Les enfants sont probablement moins conscients des risques impliqués, des conséquences et garanties, et de leurs droits en matière de traitement des données à caractère personnel. En l'absence de mesures spécifiques, ils peuvent donc être exposés à des risques inconnus.	
Commentaire explicatif	
Lors de l'installation de l'application sur un smartphone, l'âge de l'utilisateur n'est pas vérifié. De cette manière, les enfants qui possèdent un appareil mobile peuvent donc installer l'application et de ce fait, leurs données à caractère personnel peuvent être traitées par d'autres utilisateurs ainsi que par la plateforme centrale. Les traitements visés ne s'adressent pas spécifiquement aux enfants et de ce fait, les informations fournies ne le seront pas nécessairement dans un langage entièrement compréhensible pour des enfants (Raison 58 RGPD).	
Mesures	
Le RGPD prévoit que, lorsque des données d'enfants sont traitées, ces enfants ont droit à une protection spécifique en ce qui concerne leurs données à caractère personnel étant donné qu'ils	

R24. Traitement de données de mineurs	
sont probablement moins conscients des risques impliqués, des conséquences et garanties, et de leurs droits en matière de traitement des données à caractère personnel. L'application et la plateforme centrale ont été conçues d'une manière telle qu'elles prévoient une protection suffisante des données, même si ces données sont relatives à des enfants. Une campagne de communication s'adressant aux jeunes sera mise en place à une phase ultérieure (après le test planifié avec 10.000 adultes).	
Risque résiduel	
L'application et la plateforme prévoient suffisamment de mesures pour protéger efficacement les données des enfants. Comme c'est le cas pour d'autres groupes de la population, il existe chez les enfants ayant peu de contacts sociaux un risque de nouvelle identification si ceux-ci rapportent une contamination dans le système. La probabilité est estimée à 2 pour cette dernière catégorie d'enfants et même si l'impact en R.15 a été estimé à 3, il sera réduit à 2 pour les enfants parce que l'on suppose dans ce cas que les contacts de ces enfants feront partie du cercle réduit d'un groupe de personnes de confiance.	
Score de risque	
Probabilité après mesures	2
Impact après mesures	2
Risque	MOYEN

R43. Utilisation de l'application sous la contrainte

R43. Utilisation de l'application sous la contrainte
Vulnérabilité
La personne concernée est contrainte par un tiers d'installer l'application; ou la fourniture de biens et/ou de services et/ou l'exécution d'un contrat est conditionnée par l'installation de l'application.
Commentaire explicatif
Des tiers tels que des universités, employeurs, écoles, transports publics, organismes gouvernementaux, établissements horeca, etc. peuvent introduire des restrictions d'accès pour les personnes qui n'ont pas installé l'application.
Mesures
La charte de l'application énonce ce qui suit : *L'application ne peut entraîner aucune forme de discrimination individuelle.* L'arrêté royal n°44 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano prévoit qu'il revient au citoyen de décider s'il installe et utilise ou non cette application, pour communiquer ses données en cas de contamination. Plus spécifiquement, l'AR stipule que « Sur la recommandation de l'APD dans son avis 34/2020, il est également précisé qu'un (non-) utilisateur ne peut subir aucun désavantage ou avantage de quelque manière que ce soit selon qu'il utilise ou non une application numérique de traçage de contacts. » L'Accord de coopération stipule ce qui suit : Le fait pour une autorité, une entreprise ou un individu d'obliger un autre individu à installer, utiliser et désinstaller l'application numérique de traçage des contacts sera sanctionné en vertu du droit commun (interdiction des actes discriminatoires, interdiction du traitement illicite de données...).
Risque résiduel
L'AR et l'Accord de coopération soulignent l'existence d'une protection qui limite les chances qu'un citoyen soit contraint d'installer cette application.
Score de risque

Probabilité après mesures	1

R43. Utilisation de l'application sous la contrainte	
Impact après mesures	2
Risque	FAIBLE

D08. Respect du droit à l'information (sur le traitement des données)

Principe Tout individu peut consulter ses données à caractère personnel s'il le souhaite.

Résumé Cette section doit décrire les mesures prises par l'organisation pour permettre à une personne d'accéder à ses informations et la manière dont l'organisation traite les demandes d'accès.
Le système peut-il être conçu de manière à ce qu'il soit facile de permettre aux gens d'accéder à leurs informations ?

Lien RGPD Section 1 Transparence et modalités
Article 12 Transparence des informations et des communications
Section 2 Information et accès aux données à caractère personnel
Article 13 Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée
Article 14 Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée
Article 15 Droit d'accès de la personne concernée

R25. Expliquer l'impact du traitement des données

R25. Expliquer l'impact du traitement des données	
Vulnérabilité	
L'impact du traitement des données n'a pas été suffisamment expliqué à la personne concernée.	
Commentaire explicatif	
Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 du RGPD en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique.	
Mesures	
Un avis de confidentialité sera établi avant le traitement. Celui-ci comprendra les informations utiles sur le traitement et le responsable du traitement, comme indiqué dans le RGPD. Des informations complémentaires sont mises à la disposition du public sur les sites web suivants : • https://www.corona-tracking.info/app/coronalert/ • https://www.esat.kuleuven.be/cosic/sites/corona-app/	
Risque résiduel	
Bien que des informations sur l'application soient disponibles en abondance par différents canaux, il y a toujours un risque qu'elles n'atteignent pas certains groupes de la population et des utilisateurs, soit parce que les canaux ne sont pas connus, soit parce que l'information n'est pas facile à comprendre. Pour cette raison, il est recommandé de continuer à travailler sur une description simple de toutes les informations nécessaires et pertinentes lors de la demande du consentement de l'utilisateur pour l'installation de l'application et lors de la transmission des informations. L'impact est plutôt limité en raison des contrôles effectués par les différents organismes lors du développement de l'application et de la plateforme centrale, ainsi que des mesures prévues pour protéger la confidentialité des données et la vie privée de l'utilisateur.	
Score de risque	
Probabilité après mesures	2

R25. Expliquer l'impact du traitement des données	
Impact après mesures	2
Risque	MOYEN

R26. Informations sur le service

R26. Informations sur le service
Vulnérabilité
Les informations existantes décrivant le service ne sont pas facilement accessibles pour la personne concernée, ne sont pas faciles à comprendre et/ou nécessitent des connaissances particulières pour les comprendre.
Commentaire explicatif
Conformément au RGPD, l'utilisateur doit être informé en termes compréhensibles des objectifs de l'application, des traitements qui ont lieu et des données utilisées à cette fin.
Mesures
Les informations sont mises à disposition le plus simplement possible par les différents canaux (voir R.25). Des canaux de communication seront répertoriés et utilisés autant que possible.
Risque résiduel
Il subsiste un risque que l'information n'atteigne pas certains groupes de la population et certains utilisateurs, parce qu'elle n'est pas facile à comprendre. Pour cette raison, il est recommandé de continuer à travailler sur une description simple de toutes les informations nécessaires et pertinentes lors de la demande du consentement de l'utilisateur pour l'installation de l'application et lors de la transmission des informations. L'impact est plutôt limité en raison des contrôles effectués par les différents organismes lors du développement de l'application et de la plateforme centrale, ainsi que des mesures prévues pour protéger la confidentialité des données et la vie privée de l'utilisateur.

Score de risque	
Probabilité après mesures	2
Impact après mesures	1
Risque	FAIBLE

R27. Informations sur des données complémentaires

R27. Informations sur des données complémentaires
Vulnérabilité
La personne concernée ne reçoit pas d'informations adéquates sur la provenance des données lorsque celles-ci n'ont pas été obtenues directement auprès d'elle.
Commentaire explicatif
L'article 14 du RGPD définit les informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée. Dans le cas de cette application, il est uniquement question des données à caractère personnel d'une personne concernée obtenues via la plateforme Sciensano par laquelle les résultats du test sont communiqués à la plateforme.
Mesures
Le responsable du traitement de la plateforme est Sciensano. Sciensano se charge aussi de la transmission des résultats des tests à la plateforme qui met les données à la disposition de l'application. L'avis de confidentialité, les informations sur l'application et l'AR avec les accords de coopération fournissent également les informations requises.
Risque résiduel
Le cadre législatif comporte les dispositions nécessaires, de sorte que la probabilité que le responsable du traitement ne respecte pas cette obligation est faible.

R27. Informations sur des données complémentaires	
Score de risque	
Probabilité après mesures	1
Impact après mesures	1
Risque	FAIBLE

R28. Informations sur des sous-traitants tiers

R28. Informations sur des sous-traitants tiers
Vulnérabilité
Aucune information n'est donnée sur les tiers qui reçoivent également les données de la personne concernée.
Commentaire explicatif
Le traitement des données de santé de la personne concernée est nécessaire pour des motifs d'intérêt public dans les domaines de la santé publique. Un tel traitement doit donc faire l'objet de mesures appropriées et spécifiques de façon à protéger les droits et libertés des personnes physiques. De tels traitements de données concernant la santé pour des motifs d'intérêt public ne devraient pas aboutir à ce que des données à caractère personnel soient traitées à d'autres fins par des tiers, tels que les employeurs ou les compagnies d'assurance et les banques. Dans ce cas, il convient de tenir compte de la transmission de clés secrètes vers des pays situés au sein de l'Espace économique européen, dans le cadre de laquelle des responsables du traitement supplémentaires seront identifiés lors du traitement des données.
Mesures
L'arrêté royal n°44 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano définit les finalités du traitement et interdit le traitement des données collectées à d'autres fins. Par conséquent, la transmission à des tiers n'est pas autorisée. L'application permet d'échanger des clés avec d'autres pays européens, à condition que l'utilisateur indique les pays où il a séjourné pendant la période d'infectiosité. L'exportation des clés suppose donc l'approbation de l'utilisateur. L'échange des clés n'aura lieu qu'avec les pays utilisant également le protocole DP-3T. Cet échange est prévu sur la base de données pseudonymisées. Les responsables du traitement qui recevront ultérieurement ces données sont d'une part des instances sanitaires nationales au sein de l'Espace économique européen pour la gestion et l'exploitation de l'application nationale de traçage du Coronavirus et d'autre part l'organe de coordination au sein des institutions européennes pour l'implémentation et l'exploitation de la passerelle européenne pour l'échange des informations relatives aux contaminations.
Risque résiduel
Le cadre juridique prévoit des garanties suffisantes pour que les informations ne soient pas échangées avec des tiers autres que les instances sanitaires au sein des pays européens, de sorte que les risques que cela se produise sont faibles. En outre, la plateforme ne dispose que d'informations pseudonymisées, ce qui rend difficile l'identification de la personne physique à l'aide des données, tandis que l'impact d'un tel échange est faible.

Score de risque	
Probabilité après mesures	1
Impact après mesures	1
Risque	FAIBLE

R29. Information sur l'utilisation des données

R29. Information sur l'utilisation des données	
Vulnérabilité	
Au moment de la collecte des données, la personne concernée n'a pas ou pas suffisamment été informée sur tous les points suivants : - le responsable du traitement des données - la finalité du traitement - les destinataires des données - quelles sont les données obligatoires/facultatives - l'existence d'un droit d'accès et de rectification des données la concernant	
Commentaire explicatif	
Lorsque des données personnelles sont collectées auprès de la personne concernée, le RGPD stipule que cette dernière doit être informée des points ci-dessus. Ces informations sont nécessaires pour que la personne concernée puisse décider en connaissance de cause si elle consent ou non au traitement de ses données et en évaluer les conséquences.	
Mesures	
Sciensano a rédigé une déclaration de confidentialité qui fournit les informations nécessaires. En outre, l'objectif de l'application et les différentes parties responsables sont décrits dans l'AR en la matière ainsi que dans les accords de coopération qui s'y rapportent.	
Risque résiduel	
Il subsiste un risque que l'information n'atteigne pas certains groupes de la population et certains utilisateurs, parce qu'elle n'est pas facile à comprendre. Pour cette raison, il est recommandé de continuer à travailler sur une description simple de toutes les informations nécessaires et pertinentes lors de la demande du consentement de l'utilisateur pour l'installation de l'application et lors de la transmission des informations. L'impact est plutôt limité en raison des contrôles effectués par les différents organismes lors du développement de l'application et de la plateforme centrale, ainsi que des mesures prévues pour protéger la confidentialité des données et la vie privée de l'utilisateur.	
Score de risque	
Probabilité après mesures	2
Impact après mesures	1
Risque	FAIBLE

R30. Informations individualisées sur les données traitées

R30. Informations individualisées sur les données traitées
Vulnérabilité
La personne concernée ne peut pas recevoir d'informations individualisées sur les données la concernant qui sont traitées et sur l'utilisation qui en est faite.
Commentaire explicatif
Lors du traitement de données à caractère personnel, il est prévu que la personne concernée puisse obtenir des informations personnalisées sur les données à son sujet faisant l'objet du traitement. L'architecture de cette plateforme prévoit un traitement pseudonymisé de toutes les informations, sans que le responsable du traitement puisse remonter jusqu'à la personne concernée ou son appareil. L'article 12, §2 du RGPD stipule que « Le responsable du traitement facilite l'exercice des droits conférés à la personne concernée au titre des articles 15 à 22. Dans les cas visés à l'article 11, paragraphe 2, le responsable du traitement ne refuse pas de donner suite à la demande de la personne concernée d'exercer les droits que lui confèrent les articles 15 à 22, à moins que le responsable du traitement ne démontre qu'il n'est pas en mesure d'identifier la personne

R30. Informations individualisées sur les données traitées	
concernée. » En raison de la pseudonymisation des données, le responsable du traitement ne peut pas identifier la personne concernée et cette exigence ne s'applique donc pas.	
Mesures	
Non applicable (NA)	
Risque résiduel	
Non applicable	
Score de risque	
Probabilité après mesures	NA
Impact après mesures	NA
Risques	NA

D09. Respect du droit de rectification et d'effacement des données à caractère personnel

Principe	La personne concernée peut corriger les données si elles contiennent des erreurs ou faire supprimer ses données.
Résumé	Cette section doit porter sur la manière dont l'organisation traitera une demande de correction de données à caractère personnel. Y a-t-il des limitations ? (par exemple, limites de caractères dans les champs de données ou absence de possibilité d'ajouter un marqueur indiquant que des informations pertinentes sont conservées dans un fichier physique)
Lien RGPD	Section 3 Rectification et effacement Article 16 Droit de rectification Article 17 Droit à l'effacement (« droit à l'oubli »)

R31. Modification des données

R31. Modification des données
Vulnérabilité
Il n'existe pas de procédure permettant à la personne concernée de rectifier, d'effacer ou de bloquer des données individuelles.
Commentaire explicatif
Le médecin traitant de la personne concernée et le laboratoire effectuant le test envoient un nombre limité de données à caractère personnel de la personne concernée à Sciensano, sur le serveur de résultats de tests (Base de données VI). Conformément à l'article 16 du RGPD, la personne concernée a la possibilité de rectifier ces données.
Mesures
Si les données ont déjà été envoyées et traitées par le médecin traitant et le laboratoire, elles ne peuvent plus être rectifiées dans la base de données VI de Sciensano en raison de la pseudonymisation. Voir aussi la problématique évoquée concernant les faux positifs. Des mesures supplémentaires ne peuvent pas être prises, compte tenu de l'automatisation des processus du serveur de résultats de tests et de la nécessité d'actions d'alerte rapide dans le cadre d'une lutte efficace contre la propagation du COVID-19. Cette limitation relative au droit de rectification sera mentionnée dans la déclaration de confidentialité, afin que la personne concernée en ait connaissance et puisse éventuellement décider (en cas de soupçon d'informations incorrectes) de ne pas donner suite aux alertes.
Risque résiduel
En raison de la pseudonymisation, il existe des obstacles à l'exercice du droit de rectification par le responsable du traitement.

R31. Modification des données	
Toutefois, si la personne concernée soupçonne des erreurs, elle peut choisir de ne pas importer les clés chiffrées dans la base de données V, afin d'éviter des alertes fautives. La personne concernée peut donc elle-même limiter l'éventuel impact négatif pour autrui.	
Score de risque	
Probabilité après mesures	2
Impact après mesures	2
Risque	MOYEN

R32. Informations sur des données rectifiées

R32. Informations sur des données rectifiées	
Vulnérabilité	
Le responsable n'a pas mis en place de procédure pour informer les tiers concernés que des données individuelles ont été rectifiées, supprimées ou bloquées.	
Commentaire explicatif	
Aucune donnée ne sera échangée avec des tiers en raison des restrictions imposées par l'arrêté royal (pas de traitement supplémentaire autre que les fins stipulées dans l'arrêté royal pour l'application). Concernant l'échange de clés avec des pays tiers, en raison de la pseudonymisation des données, il n'est pas possible de retrouver l'identité de la personne concernée et donc de rectifier ces données le cas échéant.	
Mesures	
Les parties concernées seront informées via la déclaration de confidentialité qu'au niveau de l'échange avec des tiers, seule une communication de données à des pays membres de l'EEE sera possible. Les obstacles aux rectifications des données seront commentés dans ce même document.	
Risque résiduel	
Toutefois, si la personne concernée soupçonne des erreurs, elle peut choisir de ne pas importer les clés dans la base de données V, afin d'éviter des alertes fautives. La personne concernée peut donc elle-même limiter l'éventuel impact négatif pour autrui.	
Score de risque	
Probabilité après mesures	2
Impact après mesures	2
Risque	MOYEN

D10. Respect du droit à la portabilité des données

Principe	La personne concernée doit être en mesure de changer de sous-traitant de manière simple.
Résumé	Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle.
Lien RGPD	Article 20 Droit à la portabilité des données

R33. Changement de responsable

R33. Changement de responsable
Vulnérabilité

R33. Changement de responsable	
La personne concernée ne peut pas changer de responsable du traitement ou doit reconstituer elle-même ses données à caractère personnel.	
Commentaire explicatif	
S'il existait un autre fournisseur d'applications, on pourrait admettre que la personne concernée pourrait faire transférer ses données à caractère personnel à ce fournisseur.	
Mesures	
Non pertinent : aucune autre application disponible pour le transfert : Google et Apple n'autorisent qu'une seule application par pays/région à utiliser l'API Google/Apple Exposure Notification. Ce risque pourra être réévalué si Google et Apple modifient leurs règles et qu'un autre fournisseur d'applications propose ses services tout en publiant son mode opératoire : par ex. quelles données utilisera-t-il ou pourra-t-il utiliser exactement ?	
Risque résiduel	
Non applicable (NA)	
Score de risque	
Probabilité après mesures	NA
Impact après mesures	NA
Risque	NA

D11. Respect du droit d'opposition

Principe	La personne concernée peut s'opposer au traitement de ses données.
Résumé	La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions.
Lien RGPD	Article 21 Droit d'opposition

R34. Opposition aux procédures de décision

R34. Opposition aux procédures de décision	
Vulnérabilité	
La personne concernée ne peut pas s'opposer aux procédures de décision automatisée utilisées dans le cadre du service offert.	
Commentaire explicatif	
Le RGPD stipule que la personne concernée peut s'opposer au traitement de ses données à caractère personnel. Les données de la personne concernée ne seront pas traitées de manière à aboutir à une procédure de décision automatisée. Le résultat du traitement est un message indiquant si la personne concernée a eu ou non un contact à risque, auquel cas il est recommandé de la mettre en quarantaine et de lui faire subir un test Covid-19. Pour cette raison, cet article n'est pas applicable.	
Mesures	
Non applicable	
Risque résiduel	
Non applicable	
Score de risque	
Probabilité après mesures	NA
Impact après mesures	NA
Risque	NA

R35. Information à propos de la transmission de données à des tiers

R35. Information à propos de la transmission de données à des tiers	
Vulnérabilité	
La personne concernée n'a pas été informée de la transmission de ses données à des tiers ni de l'utilisation de ses données à des fins de marketing direct.	
Commentaire explicatif	
L'arrêté royal n°44 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano définit les finalités du traitement et interdit le traitement des données collectées à d'autres fins. Par conséquent, la transmission à des tiers n'est pas autorisée et cet article n'est pas applicable. Seul le numéro de série temporaire non personnalisé est transféré à un autre utilisateur de l'application. Cet échange est pseudonomysé et décrit dans la déclaration de confidentialité.	
Mesures	
Non applicable (NA)	
Risque résiduel	
NA	
Score de risque	
Probabilité après mesures	NA
Impact après mesures	NA
Risque	NA

R36. Opposition au traitement de données à caractère personnel

R36. Opposition au traitement de données à caractère personnel
Vulnérabilité
Aucune procédure ne permet de s'opposer au traitement de données à caractère personnel.
Commentaire explicatif
Le RGPD stipule que la personne concernée peut s'opposer au traitement de ses données à caractère personnel. Dans le cas présent, il s'agit d'une application où les données sont collectées auprès de la personne concernée et où celle-ci donne son accord avant de les envoyer à la plateforme. Concernant les données obtenues de la source authentique auprès de Sciensano, l'utilisateur doit également donner son accord avant qu'elles puissent être générées. Pour l'utilisation de l'application, l'utilisateur doit donner son autorisation au moment de l'installation. L'échange de données via Bluetooth est donc également soumis à un consentement. On peut donc affirmer de manière générale que le traitement est basé sur le consentement et que l'opposition n'a pas de sens. Si l'utilisateur décide quand même de s'opposer après avoir donné son consentement, le responsable du traitement des données ne pourra pas répondre positivement. En effet, en raison de la pseudonymisation, les données ne peuvent plus être retracées jusqu'à la personne concernée et ne peuvent donc pas être supprimées de la plateforme. Pour les raisons susmentionnées, il est considéré que ce droit ne peut pas être exercé.
Mesures
Les droits de la personne concernée sont décrits dans la déclaration de confidentialité.
Risque résiduel
En raison de la pseudonymisation, il existe des obstacles à l'exercice de ces droits. Vu le principe du consentement, la probabilité d'un tel cas de figure est plutôt faible. L'utilisateur a été informé des

R36. Opposition au traitement de données à caractère personnel	
restrictions qui s'appliquent à l'opposition par le biais de la déclaration de confidentialité. Comme il s'agit d'un document séparé qui peut échapper à l'attention de l'utilisateur, il est également recommandé d'afficher ce message lors de toute demande d'autorisation. L'impact est limité par la pseudonymisation, qui rend très difficile la recherche de l'identité de la personne concernée. En outre, les données sont supprimées après une période de 14 jours, ce qui limite l'impact dans le temps.	
Score de risque	
Probabilité après mesures	1
Impact après mesures	1
Risque	FAIBLE

R37. Information sur l'opposition au traitement de données à caractère personnel

R37. Information sur l'opposition au traitement de données à caractère personnel	
Vulnérabilité	
L'exploitant n'a pas mis en place de procédure pour informer les tiers concernés qu'une personne concernée s'est opposée au traitement de ses données à caractère personnel.	
Commentaire explicatif	
Comme indiqué dans les chapitres précédents, aucune donnée n'est échangée avec un tiers qui traite ces données avec un impact sur la personne concernée. Seul le numéro de série temporaire non personnalisé est échangé avec d'autres utilisateurs de l'application, laquelle détermine sur la base de ces données s'il a été question d'un contact à risque.	
Mesures	
L'application nécessite le consentement de l'utilisateur lors de son installation sur le smartphone. Des informations sont par ailleurs disponibles à propos des finalités de l'application et des données qui sont échangées. Avant d'envoyer ses clés chiffrées à la plateforme et avant de créer un code de test R1 pour obtenir les résultats d'un test, l'utilisateur (la personne concernée) doit donner son consentement explicite.	
Risque résiduel	
L'utilisateur étant invité à formuler son consentement au moment de l'installation de l'application et lors de l'échange de données, le risque d'une opposition au traitement des données est assez limité. Si l'utilisateur souhaite malgré tout s'opposer au traitement de ses données, le mécanisme de pseudonymisation des données empêche de répondre favorablement à cette demande. Cependant, les données étant pseudonymisées et disponibles de façon limitée dans le temps, l'impact de cette réponse négative à la demande de suspension du traitement sera lui aussi limité.	
Score de risque	
Probabilité après mesures	1
Impact après mesures	1
Risque	FAIBLE

D12. Respect du régime relatif aux décisions individuelles automatisées

Aucune décision individuelle ayant une incidence sur la personne concernée qui fournit ses informations n'est prise. Les résultats sont soit les suites d'un test, soit la communication d'informations sur la base des conclusions à propos un contact à risque, en foi de quoi la personne concernée est invitée à maintenir certaines mesures. Les risques associés à ces aspects ont déjà été abordés au point R.03.

D13. Respect des obligations (techniques) relatives à l'organisation du traitement

Principe Afin de protéger les droits des personnes concernées, les traitements doivent prévoir des mesures de sécurité adéquates.

Résumé Lors de la conception d'applications chargées du traitement de données à caractère personnel, les mesures suivantes seront envisagées :

- Protection des données dès la conception et via des paramètres standards
- Détermination des rôles des sous-traitants
- Sécurité du traitement lorsque le personnel du responsable du traitement ou le sous-traitant intervient dans le traitement des données.

Lien RGPD Article 25
Article 26

R38. Protection de la vie privée dès la conception et par défaut

R38. Protection de la vie privée dès la conception et par défaut
Vulnérabilité
Le traitement des données n'a pas été élaboré selon les principes de conception et de paramétrage standard « dès la conception et par défaut ».
Commentaire explicatif
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, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées et à l'étendue de leur traitement.
Mesures
Le protocole DP-3T a été développé selon ces principes (et a été testé par le Comité européen de la protection des données) et est appliqué dans l'application et la plateforme sous-jacente. D'autres mesures techniques, telles que le cryptage des données au repos et des données en transit, constituent des mesures de sécurité supplémentaires. Les traitements possibles et autorisés sont clairement décrits et limités dans le prescrit de l'AR. Tout autre traitement n'est pas admis et ne sera de toute façon – étant donné la pseudonymisation des données prévue par le protocole DP-3T – pas possible ou pertinent, vu que le résultat ne pourra jamais être relié à une personne physique. La minimisation des données est prévue au sein de l'application via la conception du protocole DP-3T. L'utilisateur doit seulement donner son accord pour l'utilisation de l'application. Il n'est pas demandé à l'utilisateur de configurer les paramètres de confidentialité.
Risque résiduel
Par l'application du DP-3T et l'application des mesures de sécurité prévues, l'application de traçage est pourvue « dès la conception » de mécanismes de protection des droits des personnes concernées l'utilisant. Aussi, le risque d'utilisation abusive des données collectées pour les traitements prévus est faible.

R38. Protection de la vie privée dès la conception et par défaut	
Comme les paramètres ne peuvent pas être ajustés, la possibilité d'erreurs par l'utilisateur est également minimisée.	
Score de risque	
Probabilité après mesures	1
Impact après mesures	1
Risque	FAIBLE

D14. Respect des obligations organisationnelles

Principe	0
Résumé	0
Lien RGPD	0

R39. Détermination des rôles des sous-traitants

R39. Détermination des rôles des sous-traitants	
Vulnérabilité	
Les rôles des sous-traitants en ce qui concerne le traitement des données ne sont pas clairement définis, et la personne concernée ne peut donc pas savoir précisément qui est habilité à consulter ou à modifier les données.	
Commentaire explicatif	
Le responsable du traitement est réputé définir des instructions à l'intention du sous-traitant qui traite les données pour le compte du responsable du traitement. Dans le cas présent, la plateforme est fournie par Amazon Web Services (AWS). À l'heure d'écrire la présente AIPD, il n'existe pas d'autre responsable du traitement. Le développeur de l'application et de la plateforme ne sera pas responsable de la gestion de la plateforme. Afin de permettre au fournisseur d'intervenir sur la plateforme, une clause de confidentialité a été inscrite dans le cahier des charges (4.2.37 - 4.2.42 du cahier des charges https://www.corona-tracking.info/wp-content/uploads/2020/07/Smals-BB-001-031-2020.pdf)	
Mesures	
Le responsable du traitement prévoit la conclusion d'un contrat de sous-traitance avec son sous-traitant.	
Risque résiduel	
Vu la conclusion d'un contrat de sous-traitance et les mesures complémentaires, le risque de violation de la présente règle est faible. Toutefois, le non-respect du contrat susmentionné par le sous-traitant peut avoir un impact sur l'individu étant donné la divulgation de données. La séparation imposée des bases de données et des journaux d'enregistrement dans la conception limite cet impact, mais il reste la possibilité d'identification par l'adresse IP et de détermination des informations de contenu par la séquence d'activités d'un utilisateur.	
Score de risque	
Probabilité après mesures	1
Impact après mesures	2
Risque	MOYEN

R40. Codes de conduite ou mécanismes de certification

R40. Codes de conduite ou mécanismes de certification
Vulnérabilité
Le sous-traitant ne dispose pas d'un code de conduite ou d'un mécanisme de certification approuvé.
Commentaire explicatif

R40. Codes de conduite ou mécanismes de certification	
Le responsable du traitement est censé superviser la sécurité et le respect du RGPD par son sous-traitant dans le cadre des traitements proposés. Outre les instructions à donner par le responsable du traitement, l'organisation du sous-traitant doit veiller à ce que les mesures nécessaires soient prises pour assurer le respect du RGPD.	
Mesures	
Le contrat avec AWS reprend d'office les clauses pour la convention avec le sous-traitant. (https://aws.amazon.com/blogs/security/aws-gdpr-data-processing-addendum/) AWS stipule par ailleurs ce qui suit : • Les mesures nécessaires ont été prises dans l'organisation et sur le réseau pour garantir la sécurité et le respect du RGPD. • Un processus de notification des violations est en place pour garantir que le responsable du traitement soit informé de tout incident. • L'organisation est certifiée ISO 27001, 27017 et 27018.	
Risque résiduel	
Le risque résiduel est plutôt limité par les garanties fournies par AWS, plus précisément par sa certification ISO 27001. Comme cet audit est réalisé par une partie externe, on peut objectivement supposer que les mesures décrites ont été effectivement appliquées.	
Score de risque	
Probabilité après mesures	1
Impact après mesures	1
Risque	FAIBLE

R41. Formation des collaborateurs

R41. Formation des collaborateurs	
Vulnérabilité	
Les collaborateurs n'ont pas été suffisamment informés sur la manière de gérer le « traitement des données à caractère personnel ».	
Commentaire explicatif	
Bien que les données pour l'application de traçage des contacts aient été pseudonymisées, certains collaborateurs de Sciensano ayant des droits d'accès aux bases de données I et VI pourraient prendre des mesures d'identification.	
Mesures	
Tous les collaborateurs concernés de Sciensano ont signé un accord de confidentialité et de non-divulgation. Le service healthdata.be de Sciensano sensibilise son personnel à l'importance du traitement confidentiel des données sensibles au travers de documents de qualité, de processus d'entreprise, d'ateliers et de l'utilisation quotidienne d'outils de sécurité. L'accès aux données fait lui aussi l'objet d'un traçage.	
Risque résiduel	
Malgré le travail de sensibilisation, il ne peut être exclu à 100 % que certains collaborateurs traitent des données à caractère personnel avec de mauvaises intentions et de manière indésirable. L'accès aux données étant toutefois enregistré, cela génère un effet dissuasif et réduit la probabilité d'une utilisation illicite.	
Score de risque	
Probabilité après mesures	1
Impact après mesures	1
Risque	FAIBLE

Conclusion

L'application belge de traçage des contacts ou « Appli Coronalert » utilise le protocole DP-3T, qui se caractérise par son haut niveau de protection de la vie privée. Le fonctionnement repose sur des clés chiffrées qui empêchent toute identification des personnes contaminées. Les contacts à risque peuvent être signalés anonymement par l'utilisateur *(pas d'heure exacte, pas de lieu, pas d'identité)*. L'installation de l'application, son utilisation et l'échange des données se font sur une base volontaire. Les données ne seront échangées avec une plateforme centrale que si une personne infectée agit de son propre chef et donne donc son accord. Par rapport aux traitements de données existants pour le traçage manuel des contacts, l'application de traçage des contacts offre plus d'autonomie au citoyen, tandis que moins de données sont collectées.

Les résultats de l'analyse d'impact sur la protection des données indiquent que les recommandations du Comité européen de la protection des données *sur l'utilisation des données de localisation et des outils de traçage des contacts dans le contexte de l'épidémie COVID-19 ont été prises en compte,* telles que

- l'utilisation volontaire de l'application ;
- aucune utilisation des données de localisation ;
- utilisation exclusive d'ID aléatoires non personnels (qui sont régulièrement renouvelés) ;
- utilisation exclusive dans le but principal (à savoir avertir les personnes des risques de contamination) ;
- caractère temporaire de l'application et de l'infrastructure des serveurs (désactivation au terme de la période de crise) ;
- traitement limité aux données (de santé) strictement nécessaires ;
- mise en œuvre de mesures techniques et organisationnelles adéquates pour protéger les données (par exemple, utilisation d'un serveur proxy, de serveurs non collusoires) ; et
- protection contre la manipulation (fausses alertes sur les risques d'infection) par des utilisateurs malveillants.

En d'autres termes, il existe un cadre légal clair qui définit le fondement juridique, limite les finalités et les destinataires des données, définit les courtes périodes de conservation des données et énumère de manière exhaustive les données minimales qui peuvent être collectées (ce cadre est formé par l'arrêté royal n°44, un futur Accord de coopération et les arrêtés d'exécution). Ce cadre légal a été évalué par le Conseil d'État et l'Autorité de protection des données, pour être renforcé ou clarifié sur la base de leurs commentaires. Bien que la suppression de certaines parties du cadre légal par des procédures judiciaires en cours soit encore possible, on peut s'attendre à ce que le législateur comble les lacunes éventuelles (rapidement et/ou rétroactivement), compte tenu du soutien social et politique dont bénéficie la lutte contre le COVID-19. Le cas échéant, l'analyse d'impact sur la protection des données sera elle aussi révisée. Outre le cadre légal, l'architecture intègre des aspects tels qu'une pseudonymisation, des transferts de données cryptées, une continuité du service, le principe de protection par défaut, un effacement des données et l'autorisation des alertes.

Les modifications du cadre légal et/ou de l'architecture ayant un impact négatif sur la protection des droits et libertés des personnes concernées semblent moins réalistes en raison de la structure de gouvernance envisagée pour le suivi du fonctionnement de l'application et de l'importance accordée à la consultation publique à propos de l'application de traçage des contacts (visant notamment à accroître la confiance du public dans l'application). Le développement de l'application et de la documentation connexe (par exemple, un projet de déclaration de confidentialité) est basé sur une

approche multidisciplinaire *(juridique, conception de l'application, cybersécurité, épidémiologique, ...),* avec une consultation des différentes parties prenantes et une attention portée aux préoccupations sociales telles que l'inclusion électronique et la convivialité. Il ne s'agit pas, en d'autres termes, d'une procédure isolée. Outre l'audit technique prévu, cette approche participative permet également de contrôler la mise en œuvre et le respect des mesures de protection de la vie privée.

Concernant les risques résiduels de non-respect de la transparence pour les personnes concernées ou propres à la licéité, à la minimisation des données, à la limitation de la finalité, à la limitation de la conservation et à la protection de la confidentialité et de la sécurité, diverses mesures sont prises pour pouvoir les considérer comme faibles ou moyens. À cet égard, il convient d'accorder une attention particulière au suivi de certaines mesures telles que :

- la finalisation du cadre légal et réglementaire ;
- la mise en œuvre de la campagne de communication prévue vis-à-vis des personnes concernées ;
- le développement d'une campagne d'information axée sur les jeunes et
- les résultats de l'audit de sécurité, exigeant d'éventuelles actions.

Eu égard aux droits des personnes concernées, le degré élevé de pseudonymisation rend difficile l'exercice des droits par le responsable du traitement, Sciensano. Par exemple, la difficulté d'identifier la personne concernée empêche Sciensano de mettre en œuvre les rectifications demandées ou de donner suite à une opposition au traitement des données. Toutefois, l'impact sur la personne concernée est limité en raison de la protection de l'identité et des courtes périodes de conservation des données au sein de l'infrastructure des serveurs.

L'analyse de l'impact sur la protection des données n'a pas révélé de risques résiduels pouvant encore être qualifiés d'élevés après la mise en place des mesures envisagées. La problématique connue du risque de faux positifs dans les tests de laboratoire COVID-19 mérite cependant une attention particulière. Une alerte concernant un contact à risque basé sur un résultat faussement positif peut en effet entraîner une quarantaine inutile. Il est recommandé de continuer à sensibiliser les cliniciens à la détection des faux positifs et à informer la population au sujet de ces faux positifs afin de limiter les fausses alertes.

Vu

a) le niveau élevé de protection politique, juridique et technique des personnes concernées ;
b) la grande transparence de la documentation architecturale (par exemple, l'algorithme de calcul des risques d'exposition) ;
c) l'ensemble étendu de mesures d'atténuation des risques ;
d) l'absence de risques résiduels élevés (uniquement des risques faibles ou moyens) ;
e) la valeur ajoutée sociale de l'application de traçage des contacts ;

les délégués à la protection des données des services publics concernés *(Sciensano et les administrations sanitaires des entités fédérées)* rendent un avis positif quant aux traitements de données associés à l'application Coronalert.