Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 79/2020 van 7 september 2020

Onderwerp: advies over een ontwerp van koninklijk besluit tot uitvoering van het koninklijk besluit nr. 44 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden of door de bevoegde agentschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn op basis van een gegevensbank bij Sciensano en een ontwerp van een uitvoerend samenwerkingsakkoord van tussen de Federale staat, de Vlaamse Gemeenschap, het Waalse Gewest, de Duitstalige Gemeenschap en de Gemeenschappelijke Gemeenschapscommissie, betreffende de digitale contactopsporingsapplicatie(s), overeenkomstig artikel 92bis, §1, derde lid, van de Bijzondere wet van 8 augustus 1980 tot hervorming der instellingen (CO-A-2020-099)

De Gegevensbeschermingsautoriteit (hierna "de Autoriteit");

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, inzonderheid op de artikelen 23 en 26 (hierna "WOG");

Gelet op de Verordening (EU) 2016/679 *van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn* 95/46/EG (hierna "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVP");

Gelet op de adviesaanvraag van minister van Sociale Zaken en Volksgezondheid, en van Asiel en Migratie, mevrouw Maggie De Block, ontvangen op 26 augustus 2020;

Gelet op de vraag om dringend advies;

Gelet op het verslag van mevrouw Alexandra Jaspar, Directeur van het Kenniscentrum van de Gegevensbeschermingsautoriteit;

Brengt , op 7 september 2020, het volgende advies uit:

I. VOORWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. De minister van Sociale Zaken en Volksgezondheid, en van Asiel en Migratie, mevrouw Maggie De Block (hierna "de aanvrager") heeft de Gegevensbeschermingsautoriteit (hierna "de Autoriteit") gevraagd dringend advies te verstrekken over (i) een ontwerp van koninklijk besluit tot uitvoering van het koninklijk besluit nr. 44 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden of door de bevoegde agentschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn op basis van een gegevensbank bij Sciensano (hierna "**het ontwerp van koninklijk uitvoeringsbesluit**") en (ii) een ontwerp van een uitvoerend samenwerkingsakkoord van tussen de Federale staat, de Vlaamse Gemeenschap, het Waalse Gewest, de Duitstalige Gemeenschap en de Gemeenschappelijke Gemeenschapscommissie, betreffende de digitale contactopsporingsapplicatie(s), overeenkomstig artikel 92bis, §1, derde lid, van de Bijzondere wet van 8 augustus 1980 tot hervorming der instellingen (hierna het "**ontwerp van uitvoerend samenwerkingsakkoord**"[1], samen "**de ontwerpen**")

2. Het ontwerp van uitvoerend samenwerkingsakkoord beoogt de uitvoering van het ontwerp van samenwerkingsakkoord tussen de federale staat, de Vlaamse Gemeenschap, het Waalse Gewest, de Duitstalige Gemeenschap en de Gemeenschappelijke Gemeenschapscommissie betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden of door de bevoegde agentschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn op basis van een gegevensbank bij Sciensano, dat voor advies aan de Autoriteit werd voorgelegd **(advies nr. 64/2020 van 20 juli 2020[2]**). Volgens de door aanvrager verstrekte informatie werd dit samenwerkingsakkoord op 21 augustus 2020 goedgekeurd door het Overlegcomité.

[1] Met betrekking tot het ontwerp van samenwerkingsakkoord wordt de adviesaanvraag ingediend in naam van de verschillende regeringen die partij zijn bij het ontwerp.

[2] Advies nr. 64/2020 van 20 juli 2020 over een ontwerp van samenwerkingsakkoord tussen de federale staat, de Vlaamse Gemeenschap, het Waalse Gewest, de Duitstalige Gemeenschap en de Gemeenschappelijke Gemeenschapscommissie betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden of door de bevoegde agentschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn op basis van een gegevensbank bij Sciensano,

3. Daarnaast beoogt het ontwerp van koninklijk uitvoeringsbesluit de uitvoering van koninklijk besluit nr. 44 van 26 juni 2020 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden of door de bevoegde agentschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn op basis van een gegevensbank bij Sciensano (hierna "**het koninklijk besluit nr. 44**"). Het koninklijk besluit nr. 44 (waarvan de inhoud zeer dicht aanleunt bij het bovengenoemde ontwerp van samenwerkingsakkoord) werd niet voor advies aan de Autoriteit voorgelegd. Het ontwerp van koninklijk uitvoeringsbesluit bepaalt dat dit ophoudt uitwerking te hebben op de dag waarop een samenwerkingsakkoord tussen de federale staat en de gefedereerde entiteiten in werking treedt of, uiterlijk, op 15 oktober 2020 (datum waarop het koninklijk besluit nr. 44 eveneens ophoudt van kracht te zijn).

4. De inhoud van beide ontwerpen is identiek[3], zodat de Autoriteit één advies uitbrengt voor beide ontwerpen. De Autoriteit wijst erop dat zij, naast bovengenoemd advies nr. 64/2020, onlangs twee andere adviezen heeft uitgebracht over ontwerpen van normen betreffende contactopsporing met behulp van digitale opsporingsapplicaties (op een moment dat blijkbaar nog de mogelijkheid werd open gelaten om meerdere operatoren de kans te geven om onder hun verantwoordelijkheid een door hen ontwikkelde applicatie aan te bieden), namelijk:

- **Advies nr. 34/2020 van 28 april 2020** betreffende het voorontwerp van koninklijk besluit nr. XXX tot uitvoering van artikel 5, § 1, 1°, van de wet van 27 maart 2020 die machtiging verleent aan de Koning om maatregelen te nemen in de strijd tegen de verspreiding van het coronavirus COVID-19 (II), met het oog op het gebruik van digitale contactopsporingsapplicaties ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking;
- **Advies nr. 43/2020 van 26 mei 2020** betreffende een wetsvoorstel betreffende het gebruik van digitale contactopsporingsapplicaties ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking.

5. De Autoriteit verwijst naar deze adviezen voor de aspecten die niet in dit advies aan de orde komen en die desalniettemin nog relevant zouden zijn. Zij benadrukt dat haar advies dringend werd gevraagd en is uitgebracht, waardoor zij niet in staat was de in deze vorige adviezen gemaakte opmerkingen samen te brengen, opmerkingen die nog steeds van toepassing zijn.

[3] Met uitzondering van artikel 2, §1, 2°, b). Het ontwerp van het uitvoeringsbesluit bepaalt inderdaad dat "de testcode op initiatief van de gebruiker samen met de datum van staalname en de datum waarop de gebruiker besmettelijk is geworden, opgeslagen wordt in Gegevensbank I", terwijl het ontwerp van uitvoeringsakkoord niet voorziet in de bewoording "op initiatief van de gebruiker". Deze leemte zou in het ontwerp van uitvoerend samenwerkingsakkoord opgevuld moeten worden.

I. ONDERZOEK VAN DE AANVRAAG

6. De Autoriteit wijst erop dat haar rol, in het kader van het uitbrengen van adviezen door het Kenniscentrum, er niet in bestaat te bepalen of de door de aanvrager voorgestelde digitale opsporingsapplicatie functioneel of voldoende beveiligd is noch of zij de beste dergelijke applicatie is, maar wel om na te gaan of de persoonsgegevens die in het kader van het aanbod en het gebruik van deze applicatie verwerkt worden, (1) in een passende norm en (2) op een voldoende duidelijke, nauwkeurige en voorzienbare wijze beschreven worden, zodat de betrokkenen duidelijk de verwerkingen kunnen zien die door de verwerkingsverantwoordelijke uitgevoerd zullen worden in het kader van de digitale contactopsporing en, in voorkomend geval, in het kader van andere doeleinden en (3) of deze verwerkingen nodig en evenredig zijn in het licht van deze doeleinden.

7. Zoals aangekondigd en zoals vereist geven de ontwerpen een gedetailleerde beschrijving van de werkingswijze van de digitale opsporingsapplicatie die ter beschikking zal worden gesteld en van de gegevenscommunicatie die zal plaatsvinden tussen de applicatie en de Gegevensbanken I[4], V[5] en VI[6] enerzijds en tussen de Gegevensbanken onderling anderzijds. De ontwerpen voorzien ook in een interoperabiliteit met opsporingsapplicaties die ontwikkeld zijn door andere staten die de gebruiker eventueel heeft bezocht. Ze bieden garanties voor de naleving van de informatieplicht van de verwerkingsverantwoordelijke en voorzien in een controle van de applicatie achteraf. Uit de ontwerpen blijkt thans duidelijk dat slechts één digitale contactopsporingsapplicatie in aanmerking komt (zie onze vorige aanbeveling in die zin) en dat deze door de gefedereerde entiteiten ter beschikking gesteld zal worden, zodat privéactoren zich niet op het uitvoerend samenwerkingsakkoord zullen kunnen beroepen om gegevens te verwerken in het kader van het aanbod van digitale contactopsporingsapplicaties die zij zouden ontwikkelen.

a. Noodzaak en evenredigheid van de digitale opsporingsapplicatie

8. De Autoriteit heeft er in haar advies nr. 43/2020 al op gewezen en heeft in haar advies nr. 64/2020 herhaald dat de evenredigheid van de door het gebruik van een digitale opsporingsapplicatie veroorzaakte inmenging afhangt van de garanties die het regelgevingskader voor digitale tracering biedt. Bovendien hangt de noodzaak van een dergelijke inmenging af van externe factoren die rechtvaardigen in hoeverre het gebruik van digitale traceringstoepassingen daadwerkelijk helpt het nagestreefde doel te bereiken, en wel op een wijze die minder inbreuk maakt op de eerbiediging van de persoonlijke levenssfeer dan andere maatregelen die even doeltreffend zijn.

---

[4] De Gegevensbank I bedoeld in artikel 1, §1, 6° van het samenwerkingsakkoord.

5 De Gegevensbank V bedoeld in artikel 1, §1, 10° van het samenwerkingsakkoord.

6 De Gegevensbank VI bedoeld in artikel 1, 4° van de ontwerpen.

9. De auteurs van het ontwerp moeten dus kunnen aantonen dat het gebruik van een digitale opsporingsapplicatie nodig is in het kader van de aangenomen algemene gezondheidsstrategie. Deze noodzaak zal ook met regelmatige tussenpozen geherevalueerd moeten worden om na te gaan of deze inmenging in het recht op de eerbiediging van de persoonlijke levenssfeer nodig blijft in het licht van de gezondheidscontext.

10. Terwijl artikel 6, eerste lid van de ontwerpen bepaalt dat de *werking* van de applicatie regelmatig wordt gecontroleerd, geëvalueerd en gecorrigeerd "onder impuls" van het Interfederaal Comité Tracing en Testing, zo nodig ondersteund door een interdisciplinaire werkgroep van wetenschappelijke deskundigen. Er moet derhalve in de ontwerpen eveneens worden bepaald dat de *noodzaak* van het aanbod door de auteurs en van het gebruik van een dergelijke applicatie tevens met regelmatige tussenpozen beoordeeld en gedocumenteerd moet worden, met name gezien de mate van inmenging van een dergelijke opsporingsmaatregel (ook al is deze vrijwillig) in het recht op privacy.

b. Doel(en)

11. Artikel 4, §3, 7° van de ontwerpen bepaalt dat "*het niet mogelijk is om het systeem of de gegevens voor andere doeleinden te gebruiken*". De Autoriteit stelt vast dat het (de) doel(en) van de voorgenomen gegevensverwerkingen niet in de ontwerpen wordt (worden) beschreven. Het enige doel van deze gegevensverwerking blijkt echter uit 14, § 1, van koninklijk besluit nr. 44 en van het ontwerp van samenwerkingsakkoord:

"*De digitale contactopsporingsapplicatie ter voorkoming van de verdere verspreiding van het coronavirus COVID-19 onder de bevolking heeft als doel de gebruikers te informeren dat zij een risicovol contact hebben gehad met een andere besmette gebruiker, zonder dat de besmette gebruiker door de digitale contactopsporingsapplicatie wordt geïdentificeerd, en met als verder doel dat de verwittigde gebruiker dan zelf vrijwillig de nodige stappen zou ondernemen, op basis van de aanbevelingen van Sciensano en de bevoegde overheden, om verdere verspreiding van het coronavirus COVID-19 te voorkomen*".

12. Het is dan ook aangewezen om dit doel op te nemen in de ontwerpen of in deze ontwerpen te verwijzen naar het bovengenoemde artikel 14, § 1, en eraan toe te voegen dat de gegevens die in het kader van het gebruik van de applicatie worden verzameld of gegenereerd niet voor enige andere doelen [7]mogen worden gebruikt.

[7] De Autoriteit veronderstelt dat de aanvragers vooraf hebben gecontroleerd in hoeverre het juridisch mogelijk is deze gegevens te onttrekken aan het gebruik door controleautoriteiten zoals politie en gerechtelijke autoriteiten (die worden vermeld in de beschrijving van de applicatie in de documenten die onderworpen zijn aan een openbare raadpleging) in het licht van de wetgevende bepalingen die hun uiterst ruime onderzoeksbevoegdheden toekennen en hun met name toestaan de overlegging te eisen van alle voor het onderzoek/hun opdracht nuttig geachte documenten).

c. Gegevensminimalisatie

13. De Autoriteit stelt vast dat de werkingswijze van de applicatie zoals in de ontwerpen beschreven wordt erop gericht is het risico van heridentificatie van de gebruikers van de applicatie minimaal te houden, met name door middel van beveiligde sleutels en van niet-gepersonaliseerde tijdelijke serienummers die door de applicatie worden gegenereerd. De Autoriteit neemt er nota van dat de ontwerpen voor dit doel een nieuwe gegevensbank hebben gecreëerd, "Gegevensbank VI", waarin zeer tijdelijk de door de gebruikers uitgevoerde opsporingsresultaten worden opgeslagen, samen met de "testcodes", de datum van staalafname en de datum waarop de gebruiker besmettelijk is geworden, om te vermijden dat de digitale applicatie in wisselwerking staat met de Gegevensbank I waarin, zoals bekend, allerhande persoonsgegevens worden verzameld.

14. De Autoriteit merkt op dat in de ontwerpen belangrijke begrippen werden gedefinieerd, wat de leesbaarheid van de teksten en de voorspelbaarheid van de beoogde gegevensverwerking verbetert. Dit is onder meer het geval voor de begrippen beveiligde sleutel, niet-gepersonaliseerd tijdelijk serienummer, autorisatiecode, testnummer, testcode en risicocontact. Het is echter aangewezen om in de Franse versies van de ontwerpen het gebruik van de termen "clé chiffrée" en "clé sécurisée" te harmoniseren (in de Nederlandse versie wordt uitsluitend de term "beveiligde sleutel" gebruikt). Voorts is het met het oog op de transparantie wenselijk om in de ontwerpen te specificeren hoe "de datum waarop de gebruiker besmettelijk is geworden" wordt bepaald, aangezien dit niet duidelijk uit de ontwerpen naar voren komt, en om in de definitie van "testnummer" in artikel 1, 11°, te verduidelijken wat wordt bedoeld met "correcte app".

15. Zoals gezegd is het doel van dit advies niet om de functionaliteiten van de voorgestelde applicatie te beschrijven of te becommentariëren, maar wel om met name te bepalen in hoeverre de gegevensverwerkingen die het gebruik van deze applicatie met zich meebrengt, naar behoren worden beschreven en gerechtvaardigd. De analyse van een mogelijk risico van heridentificatie van de gebruikers vormt evenmin het primaire doel van dit advies en zal daarentegen in detail en grondig geanalyseerd moeten worden in het kader van een door de auteurs uit te voeren gegevensbeschermingseffectbeoordeling (hierna "GEB"). De Autoriteit wenst evenwel een aantal opmerkingen te maken aangezien deze punten een impact hebben op het - al dan niet - indringende karakter van de applicatie en op het - al dan niet - evenredige karakter van de gegevensverwerkingen die zij met zich meebrengt:

16. De Autoriteit merkt in dit verband reeds op dat :

- de testcode op initiatief van de gebruiker opgeslagen wordt in Gegevensbank I (met de datum van staalname en de datum waarop de gebruiker besmettelijk is geworden);

- wanneer het resultaat van een test beschikbaar is in Gegevensbank I, de testcode, de datum van staalafname en de datum waarop de gebruiker besmettelijk is geworden, door Gegevensbank I meegedeeld worden aan "Gegevensbank **IV**"[8];
- na bevestiging van ontvangst van deze gegevens door Gegevensbank VI, de testcode uit Gegevensbank I wordt verwijderd, "*waardoor geen connectie meer mogelijk is tussen de gegevens in Gegevensbank I en de gegevens van de app*" volgens artikel 2, §1, 3°, a) van de ontwerpen.

a) De Autoriteit begrijpt dat het "testnummer" willekeurig door de applicatie wordt gegenereerd en vervolgens aan het testcentrum wordt verstrekt. Dit nummer wordt dan gebruikt om de beveiligde sleutels van een applicatie te matchen met het positieve resultaat van een test. De Autoriteit ziet in deze manier van werken een **tijdelijk risico van heridentificatie , aangezien de testgegevens tijdelijk niet als anonieme gegevens worden verwerkt, maar als gegevens over een persoon die geïdentificeerd wordt door middel van identificatiegegevens die opgeslagen worden in gegevensbank I.** In het kader van de GEB zal moeten worden uitgelegd waarom dit nodig is voor het functioneren van de digitale opsporingsapplicatie, maar ook hoe deze communicatie past binnen een algemene methode voor contactopsporing met enerzijds een applicatie en anderzijds een handmatige opsporing. De Autoriteit benadrukt verder dat de verwerkingsverantwoordelijke voldoende transparantie moet bieden over het feit dat, hoewel de applicatie alleen anonieme gegevens gebruikt en opslaat, **Sciensano wel degelijk persoonsgegevens gebruikt bij het gebruik van deze applicatie** wanneer een test wordt gevraagd. Hoewel Sciensano de *contacten van besmette personen* technisch gesproken niet kan identificeren, **beschikt het wel over gegevens omtrent de *gebruikers van de applicatie* en omtrent hun mogelijke besmetting**.

b) Bovendien merkt de Autoriteit op dat artikel 4, §3, 6° van de ontwerpen het volgende bepaalt: *" bij uitwisseling van gegevens van de gezondheidsinfrastructuur naar gegevensbanken I en V en naar de gegevensbank VI slechts het minimum aan gegevens mag uitgewisseld worden zodat de kans op identificatie van de betrokkene minimaal gehouden wordt* ". Deze formulering maakt niet duidelijk naar welke gegevens wordt verwezen (wat zijn de *"gegevens van de gezondheidsinfrastructuur* " waarvan noch in de ontwerpen noch elders een definitie wordt gegeven?; Wat wordt bedoeld met *"slechts het minimum aan gegevens"*?). In de ontwerpen moet gespecificeerd worden welke gegevens in dit kader worden uitgewisseld.

[8] De Nederlandse versie bepaalt dat deze gegevens meegedeeld worden aan "Gegevensbank **VI** ", wat coherenter lijkt. In de Franse versies van de ontwerpen wordt trouwens op verschillende plaatsen (artikel 2, §1, 3°, a en c) verwezen naar Gegevensbank IV, terwijl de Nederlandse versie van de tekst systematisch verwijst naar Gegevensbank VI, wat correct lijkt. Deze fouten moeten dus in de Franse tekst worden gecorrigeerd.

c) Aangezien de toepassing interoperabel moet zijn met digitale opsporingsapplicaties die in andere landen beschikbaar worden gesteld, maar zonder dat er locatiegegevens worden verzameld, bepaalt artikel 2, §1, 4°, b): "de app verzamelt geen locatiegegevens; de gebruiker kan echter wel binnen de app vrijwillig aangeven in welk(e) land(en) hij op een bepaalde datum is geweest om te kunnen samenwerken met de contactopsporingsapplicaties van andere landen; desgevallend worden de beveiligde sleutels naar het door de gebruiker aangegeven land gestuurd". Artikel 4, §1 4° van de ontwerpen bepaalt dat de applicatie de internationale interoperabiliteit moet ondersteunen en het Bluetooth-gedeelte van de app in een zo groot aantal mogelijk landen bruikbaar moet maken en dat de gegevensbanken V en VI en daarvoor gebruikte infrastructuur de mogelijkheid moeten bieden om de beveiligde sleutels uit te wisselen met andere landen binnen de EU en dit rechtstreeks of via de EU gateway. De ontwerpen geven niet veel details over hoe de interoperabiliteit met andere landen werkt (welke gegevens worden meegedeeld, aan welke entiteiten ...). De ontwerpen zouden op dit punt moeten worden aangevuld en met name moeten specificeren wat wordt bedoeld met "contactopsporingsapplicaties van andere landen" en met "naar het land gestuurd" (behouden de ontwerpen de interoperabiliteit voor aan de applicaties van de staten of voorzien zij een interoperabiliteit met alle soorten applicaties die aangeboden worden aan alle gebruikers buiten het Belgische grondgebied?).

d) Artikel 4, §3, 1° van de ontwerpen bepaalt dat er geen locatie-informatie mag worden "gebruikt". Het is wenselijk om dit te herformuleren en te bepalen dat geen locatie-informatie mag worden "verzameld".

e) Artikel 2, §1, 1°, e) van de ontwerpen bepaalt dat elke smartphone waarop de app is geïnstalleerd, de Bluetooth bakens met de niet-gepersonaliseerde tijdelijke serienummers opslaat die door andere smartphones op een beperkte afstand worden uitgezonden (samen met de dag waarop het baken is ontvangen en de signaalsterkte). De autoriteit begrijpt dat deze beperkte afstand verwijst naar wat mogelijk is met de Bluetooth-technologie (en niet naar een beperking die door de toepassing wordt opgelegd), maar dit zou in de ontwerpen verduidelijkt moeten worden.

d. Informatie en transparantie

Artikel 5 §1 van de ontwerpen bepaalt dat de gebruikers worden geïnformeerd over de werking van de applicatie en haar interactie de Gegevensbanken I, V en VI en dat de applicatie zelf *"verwijzingen naar informatie over de functionaliteiten, de werking en de privacyverklaring*" zal bevatten. De Autoriteit is van mening dat, om een passend hoog niveau van transparantie te waarborgen, deze informatie aan de gebruiker moet worden verstrekt bij het downloaden en vóór elk gebruik van de applicatie. Dit zou in de ontwerpen opgenomen moeten worden.

e. Verwerkingsverantwoordelijke(n)

Bij het lezen van de ontwerpen is niet duidelijk welke entiteit(en) verantwoordelijk is (zijn) voor alle verwerkingen die in het kader van de werking van de digitale opsporingsapplicatie worden verricht (en voor de uitwisseling en de communicatie met de gegevensbanken). Artikel 1, 6° geeft aan dat de digitale contactopsporingsapplicatie CoronaAlert *"ter beschikking wordt gesteld door de gefedereerde entiteiten*". Deze worden echter niet aangewezen als verwerkingsverantwoordelijke of als gezamenlijke verwerkingsverantwoordelijke met Sciensano dat in het koninklijk besluit nr. 44, het ontwerp van samenwerkingsakkoord en het ontwerp van Privacy Statement van de applicatie van 4 augustus 2020 aangewezen wordt als verwerkingsverantwoordelijke voor de Gegevensbanken I tot VI.

De Autoriteit wijst er in dit verband op dat het Europees Comité voor gegevensbescherming in zijn richtsnoeren[9] heeft benadrukt dat de verwerkingsverantwoordelijke van elke digitale opsporingsapplicatie duidelijk moet worden aangegeven en dat, indien bij de inzet van contactopsporingsapplicaties verschillende actoren betrokken, hun taken en verantwoordelijkheden van meet af aan duidelijk moeten worden vastgesteld en aan de gebruikers moeten worden uitgelegd. De Autoriteit is van oordeel dat uit de ontwerpen niet duidelijk blijkt welke entiteit verantwoordelijk is voor het geheel van de verwerkingen van persoonsgegevens in het kader van de werking van de digitale opsporingsapplicatie. De ontwerpen moeten op dit punt aangepast en aangevuld worden. Dit is van fundamenteel belang aangezien de verwerkingsverantwoordelijke aan een reeks verplichtingen moet voldoen, met name op het gebied van verwerking, transparantie, inwilligen van verzoeken om uitoefening van rechten, enz. en aansprakelijk is voor iedere schending van de regels en beginselen inzake gegevensbescherming.

f. Bewaarduur

Artikel 4, §3, 5° van de ontwerpen bepaalt: "het systeem uitgeschakeld kan worden en alle opgeslagen informatie verwijderd kan worden ten laatste vijf dagen na de publicatie van het koninklijk besluit dat het einde van de toestand van de coronavirus COVID-19 epidemie afkondigt". Het verdient ook aanbeveling om te vermelden of en wanneer het feit dat een persoon de applicatie heeft geïnstalleerd (en/of gede-installeerd) opgeslagen of afgeleid wordt en, in voorkomend geval, wanneer deze informatie wordt verwijderd.

[9] Richtsnoeren 4/2020 voor het gebruik van locatiegegevens en instrumenten voor contacttracering in het kader van de uitbraak van COVID-19

Voorts neemt de Autoriteit er nota van dat de ontwerpen systematisch in de verwijdering van de gegevens uit de gegevensbanken en de applicatie voorzien na een in de ontwerpen vastgestelde periode[10].

g. Publicatie van de GEB en van de broncode

De Autoriteit neemt er nota van dat door de verwerkingsverantwoordelijke(n) een GEB zal worden uitgevoerd en dat deze zal worden gepubliceerd op de website www.coronalert.be, zoals bepaald in artikel 5, § 1, tweede lid, van de ontwerpen. Deze GEB moet absoluut worden uitgevoerd voordat de applicatie beschikbaar wordt gesteld. De Autoriteit nodigt de auteurs uit om in de ontwerpen te vermelden dat het advies van de Autoriteit over deze GEB eveneens zal worden gepubliceerd, zoals reeds werd aanbevolen in advies nr. 43/2020. De Autoriteit wijst erop dat artikel 36 van de AVG bepaalt dat de verwerkingsverantwoordelijke de toezichthoudende autoriteit moet raadplegen voorafgaand aan de verwerking, wanneer uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken.

De Autoriteit stelt vast dat - in overeenstemming met een aanbeveling die zij heeft gedaan - in artikel 5, § 2, van de ontwerpen wordt bepaald dat de broncode van de app en van de programma's voor het beheer van de Gegevensbank V en de Gegevensbank VI worden publiek gemaakt, maar om de nodige transparantie te waarborgen, verdient het aanbeveling om in de ontwerpen te specificeren waar en hoe deze informatie wordt of zal worden gepubliceerd. De Autoriteit werd ervan in kennis gesteld dat er reeds een referentiebroncode van de applicatie zou zijn gepubliceerd. De Autoriteit dringt er evenwel op aan dat de *volledige* broncode van de applicatie, zoals aangeboden in de app stores, ten minste één week vóór de terbeschikkingstelling van de applicatie aan het publiek wordt gepubliceerd.

h. Andere opmerkingen

a) De Autoriteit is verbaasd in de beschrijving van de werking van de digitale opsporingsapplicatie niets te vinden over de door Apple en Google ontwikkelde Exposure Notifications API ("application programming interface"). Aangezien de werking van de applicatie op deze API steunt, lijkt het gepast om dit in de ontwerpen te specificeren en aan te geven of deze twee entiteiten al dan niet toegang zullen hebben tot een deel van de gegevens die bij gebruik van de applicatie worden gebruikt of gegenereerd. De Autoriteit wijst ook op de verplichtingen van de verwerkingsverantwoordelijke bij een doorgifte van gegevens buiten het EAS en/of het gebruik van verwerkers:

[10] De bewaartermijnen worden gespecificeerd in artikel 2, §1, 1°, f; artikel 2, §1, 3°, a; artikel 2, §1, 3°, c; artikel 2, §1, 3°, d; artikel 2, §1, 3°, e; artikel 2, §1, 4°, c; artikel 2, §1, 4°, e van de ontwerpen.

- enerzijds in geval van doorgifte van gegevens buiten het EAS (d.w.z. in wezende naleving van Hoofdstuk V van de AVG die voorschrijft dat een dergelijke doorgifte gebaseerd moet zijn op één van de in dat hoofdstuk beschreven mechanismen, zoals een adequaatheidsbesluit of één van de vastgestelde passende waarborgen of afwijkingen en dit, rekening houdend met recente ontwikkelingen in verband met de ongeldigverklaring van het "Privacy shield") en/of;
- anderzijds, indien een beroep wordt gedaan op verwerkers (keuze van verwerkers die voldoende garanties bieden voor de uitvoering van passende technische en organisatorische maatregelen, sluiting van een contract of andere rechtshandeling die de verwerker bindt en waarin het doel, de duur, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, alsmede de verplichtingen en rechten van de verwerkingsverantwoordelijke zijn vastgelegd, overeenkomstig de artikelen 28 en 29 van de AVG)

b) Artikel 4, §4, van de ontwerpen bepaalt: *" de integratie met gezondheidsinfrastructuur voorziet in minimale overhead bij het aanvragen van een test*". De Autoriteit interpreteert dit als een rechtvaardiging voor het centraliseren bij Sciensano van de in Gegevensbank VI opgenomen gegevens. De Autoriteit verwijst naar haar eerdere opmerkingen over de risico's die deze centralisatie met zich meebrengt (zie met name punt C van haar advies 034 van 28 april 2020), zoals het risico dat deze instantie toegang heeft tot informatie over het feit dat een geïdentificeerde persoon de applicatie al dan niet gebruikt, en dringt er in ieder geval op aan dat de nodige maatregelen worden genomen om mogelijke kruisingen tussen de verschillende gegevensbanken die in het bezit zijn van of toegankelijk zijn voor deze (of andere) instanties te voorkomen, met name door ten aanzien van de verschillende gegevensbanken een strikt toegangsbeleid te hanteren om te beletten dat dezelfde personen toegang hebben tot gegevensbanken in het kader van contactopsporing via digitale applicaties en tot andere gegevensbanken. Bovendien zullen deze scheiding en de goede werking van de wismechanismen gecontroleerd moeten worden tijdens audits.

c) In artikel 6, tweede lid, van de ontwerpen wordt, in overeenstemming met onze vorige aanbeveling, bepaald dat de applicatie het voorwerp zal uitmaken van een informatieveiligheidsaudit. Het verdient aanbeveling om hieraan toe te voegen dat deze audit uitgevoerd zal worden door een onafhankelijke derde. Deze onafhankelijke audit en de mechanismen voor de bescherming van het verkeer door middel van fictieve sleutels zullen helpen om de risico's voor de gebruikers van de applicatie te beperken.

d) Het ontwerp bepaalt niet welk bericht verstuurd zal worden wanneer de applicatie een "risicocontact" detecteert. In dit verband wordt verwezen naar overweging 30 van advies nr. 34/2020 en de Autoriteit wijst erop dat deze berichten volledig in overeenstemming moeten blijven met het hierboven uiteengezette doel en dat de keuzevrijheid van de gebruikers van de opsporingsapplicaties gehandhaafd moet blijven, zodat er geen onnodige druk op hen uitgeoefend mag worden.

e) De Autoriteit begrijpt dat het ontwerp voor advies aan de Raad van State zal worden voorgelegd, aan wie zij de taak overlaat om zich uit te spreken over de vraag of een ontwerp van koninklijk 'uitvoeringsbesluit' de uitvoering van een koninklijk besluit kan pareren, over de vraag of de Koning gemachtigd is om het koninklijk besluit houdende uitvoering van het koninklijk besluit nr. 44 goed te keuren (de wet van 27 maart 2020 die machtiging verleent aan de Koning om maatregelen te nemen in de strijd tegen de verspreiding van het coronavirus COVID-19) en over de vraag of de wetgeving verbeterd moet worden.

OM DEZE REDENEN,

De Autoriteit benadrukt dat de auteurs van de ontwerpen:

- Met regelmatige tussenpozen moeten herevalueren in hoeverre een manuele en digitale opsporing nodig is om na te gaan of de inmenging in het recht op de eerbiediging van de persoonlijke levenssfeer nodig blijft in het licht van de gezondheidscontext;
- De doeleinden van de verwerking moeten opnemen in de ontwerpen of moeten verwijzen naar artikel 14, § 1, van koninklijk besluit nr. 44 en van het ontwerp van samenwerkingsakkoord;
- Moeten verduidelijken waarom het risico van heridentificatie ten gevolge van de communicatie tussen Gegevensbank I en Gegevensbank VI noodzakelijk is voor de werking van de digitale opsporingsapplicatie, maar ook hoe deze communicatie past binnen een algemene methode voor contactopsporing met enerzijds een applicatie en anderzijds een handmatige opsporing;
- In de ontwerpen moeten opnemen welke gegevens worden uitgewisseld bij de uitwisseling van de gegevens van de gezondheidsinfrastructuur met de Gegevensbanken I en V en met Gegevensbank VI;
- De ontwerpen moeten aanvullen betreffende de werking van de interoperabiliteit met de digitale opsporingsapplicaties van andere landen;
- Artikel 4, §3, 1° van de ontwerpen moeten herformuleren en moeten bepalen dat er geen locatie-informatie mag worden "verzameld".
- Moeten bepalen dat de informatie over de functionaliteiten, de werking en de privacyverklaring aan de gebruiker moet worden verstrekt bij het downloaden en vóór elk gebruik van de applicatie;
- De entiteit(en) moeten aanwijzen die verantwoordelijk is (zijn) voor de verwerking van de gegevens die in het kader van de werking van de digitale toepassing zal plaatsvinden en specificeren welke entiteit(en) verantwoordelijk is (zijn) voor de keuze van de applicatie;
- Moeten aangeven of en wanneer het feit dat een persoon de applicatie heeft geïnstalleerd (en/of gede-installeerd) opgeslagen of afgeleid wordt en, in voorkomend geval, wanneer deze informatie verwijderd zal worden;

- De publicatie moeten verplicht stellen van het advies van de Autoriteit over de GEB die uitgevoerd moet worden voordat de digitale opsporingsapplicatie beschikbaar wordt gesteld;
- Moeten de plaats specificeren waar de hele broncode van de digitale opsporingsapplicatie wordt gepubliceerd;
- Moeten de rol verduidelijken van de Exposure Notifications API in de werking van de digitale opsporingsapplicatie;
- Moeten bepalen dat de informatieveiligheidsaudit van de applicatie uitgevoerd zal worden door een onafhankelijke derde;

(get.) Alexandra Jaspar
Directeur van het Kenniscentrum