Autorité de protection des données
Gegevensbeschermingsautoriteit

Sciensano
[redacted]
Information Security Coordinator
Juliette Wytsmanstraat 14
1050 ELSENE

Uw kenmerk	Ons kenmerk	Bijlage(n)	Datum
	SA2/DOS-2020-04191		10/09/2020

Betreft: Gegevensbeschermingseffectbeoordeling (GEB) Coronalert

Geachte [redacted]

Ik heb de gegevensbeschermingseffectbeoordeling (hierna: GEB) die u op 4 september 2020 indiende bij de Gegevensbeschermingsautoriteit (hierna: de Autoriteit), in goede orde ontvangen en gelet op de urgentie van de materie overeenkomstig uw vraag bij hoogdringendheid behandeld.

De onderstaande beoordeling is gebaseerd op de informatie die u aan mijn diensten verstrekt heeft en verbindt de Autoriteit niet tot een welbepaald standpunt dat zij hier later over zou kunnen aannemen. Dit geldt in het bijzonder indien bijkomende informatie-elementen die niet ter beoordeling werden voorgelegd aan de Autoriteit, gevolgen hebben voor de rechtsgeldigheid van de verwerking.

Op basis van de tot nog toe bezorgde informatie, meen ik te mogen besluiten dat het technische ontwerp van de Belgische notificatie-app de risico's verbonden aan de verschillende verwerkingen naar best vermogen afdekt. Desalnietternin formuleer ik hieronder een aantal overkoepelende opmerkingen die hoofdzakelijk betrekking hebben op bijsturingen of verduidelijkingen van de ingediende GEB. In bijlage bij deze brief vindt u ook een aantal overige, meer factuele opmerkingen of bedenkingen met het oog op het verder verbeteren van de kwaliteit en leesbaarheid van de GEB, daarbij ook rekening houdend met uw te kennen gegeven doelstelling om deze publiek te verspreiden.

Maximale transparantie is immers niet alleen een basisprincipe in het gegevensbeschermingsrecht, maar eveneens een cruciaal element om bij te dragen aan het vertrouwen van de burgers in de Belgische notificatie-app.

1) Google & Apple Exposure Notification Network (GAEN)

De Belgische notificatie-app heeft de intentié om gebruik te maken van de API die ontwikkeld is binnen het Google & Apple Exposure Notification Network (GAEN).

De GEB vermeldt de mogelijke risico's die verbonden zijn aan deze afhankelijkheid uitsluitend in het punt R14.' Ongeautoriseerde toegang tot gegevens', maar vermeldt - voor zover die bestaat - geen sluitende maatregel om dit risico afdoend te beperken (behalve de vermelding dat Google en Apple aangeven geen vermarkting te beogen van de informatie die via deze app verkregen werd).

In een recente paper van Trinity college benoemen wetenschappers het risico dat telemetrie over het gebruik van de GAEN wordt gedeeld met Google via Google Play Services[1]. Aangezien het GAEN is geïmplementeerd binnen Google Play Services is het niet mogelijk om Google Play Services uit te schakelen indien een burger de notificatie-applicatie wenst te gebruiken. Dit risico moet veel uitvoeriger worden beschreven en heeft in het bijzonder ook een impact op het risico R07. 'Verzamelen van irrelevante gegevens'. Een uitgebreide beschrijving van de voorwaarden waarbinnen het gebruik van het Google Apple Exposure Notification Framework (GAEN) zal plaatsvinden en de manier waarop de nationale applicatie communiceert met deze Application Programming Interface (API) kunnen hiertoe bijdragen. De loutere verwijzing naar de "*Exposure Notification. Frequently Asked Questions*" van Apple en Google is onvoldoende.

Ik begrijp dat dit risico niet specifiek is voor de Belgische notificatie-app en de GEB dit risico mogelijks niet sluitend kan afdekken aangezien het inherent is aan de keuze van Google om de GAEN slechts beschikbaar te stellen binnen Google Play Services en de keuze van Apple om het GAEN te laten "indalen" in zijn besturingssysteem, iOS. Daarom is het echter van belang om dit risico zo transparant mogelijk te beschrijven en de gebruikers proactief bijkomend te informeren over de verwerking van deze bijkomende persoonsgegevens door het gebruik van Google Play Services of Apple iOS. Onduidelijkheid over de omvang van dit risico kan het vertrouwen van burgers in de Belgische notificatie-app schaden.

Van haar kant zal de Autoriteit de inschatting van dit ruimere risico van nabij opvolgen, in nauw overleg met haar Europese partners binnen het Europees Comité voor Gegevensbescherming.

2) Uitschakelen van de applicatie

De GEB moet duidelijkheid scheppen over de verschillende manieren waarop de Belgische notificatie-app (al dan niet tijdelijk) kan uitgeschakeld of verwijderd worden. Ik begrijp uit het dossier en de verstrekte toelichtingen dat het mogelijk is om de app tijdelijk uit te schakelen (waardoor minstens

[1] https://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf

binnen de app geen registratie meer plaats zou vinden). Indien dat het geval is, dient de GEB dit te verduidelijken, naast de (nu al vermelde) mogelijkheid om alle Bluetooth communicatie te onderbreken (waarbij een gebruiker ook allerlei draadloze randapparatuur niet meer zou kunnen gebruiken). De Autoriteit begrijpt dat er op dit vlak een residueel en moeilijk in te schatten risico bestaat, dat de aanbieders van mobiele besturingssoftware (resp. Android & iOS) toch verdere registraties zouden doen. In dat verband verwijs ik naar de opmerkingen in de vorige titel over het GAEN.

3) Rechtsgrond en toestemming

De Autoriteit is van mening dat de GEB in hoofdstuk D.07 'Rechtmatigheid van de verwerking' onnodige verwarring schept over de rechtsgrond van de verschillende verwerkingen. De rechtsgrond voor alle verwerkingen in het kader van de Belgische notificatie-app is de noodzaak van de vervulling van een taak van algemeen belang zoals neergelegd in artikel 6.1. e AVG[2].

Het principiële verbod tot de verwerking van gezondheidsgegevens wordt opgeheven in het kader van artikel 9.2.i AVG[3]: "*de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid [...] op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim.*"

De concrete uitwerking van deze rechtsgronden naar Belgisch recht vindt plaats door het Koninklijk besluit nr. 44 van 26 juni 2020[4], het toekomstige samenwerkingsakkoord[5] en de uitvoeringsbesluiten van de twee voornoemde instrumenten[6].

Toch alludeert de GEB in hoofdstuk D.07 'Rechtmatigheid van de verwerking' en R36. 'Bezwaar tegen verwerking van persoonsgegevens' regelmatig op de toestemming van de betrokkene als rechtsgrond of als risico beperkende maatregel, wat in tegenspraak is met het standpunt van de Autoriteit dat het vrijwillige gebruik van de Belgische notificatie-applicatie op geen enkele wijze betekent dat de toestemming in de zin van artikel 6.1.a AVG de rechtsgrond voor de verwerking zou zijn. Om elke verdere verwarring te vermijden raad ik aan om systematisch te spreken van een "instemming" (of "goedkeuring") telkens de gebruiker op vrijwillige wijze zijn akkoord geeft.

---

[2] EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING, *Richtsnoeren 04/2020 voor het gebruik van locatiegegevens en instrumenten voor contacttracering in het kader van de uitbraak van COVID-19*, §29, te raadplegen via deze link.

[3] Ibid., §33.

[4] 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, BS* 29 juni 2020.

[5] Op moment van schrijven nog niet gepubliceerd. Advies 64/2020 van de Autoriteit, 20 juli 2020, te raadplegen via deze link.

[6] Op moment van schrijven nog niet gepubliceerd. Advies 79/2020 van de Autoriteit, 7 september 2020, te raadplegen via deze link.

Anderzijds vermeldt de GEB op geen enkele plaats de noodzaak om een toestemming van de gebruiker te verkrijgen om conform artikel 129 van de *wet elektronische communicatie*[7] (WEC) toegang te verkrijgen tot de informatie die is opgeslagen in de eindapparatuur van de gebruiker, en dit ongeacht of het persoonsgegevens betreft[8]. De GEB moet bespreken hoe wordt voldaan aan artikel 129 WEC en op welke manier deze toestemming - conform de AVG - wordt verkregen.

4) Risico's die de GEB onvoldoende of niet bespreekt

De GEB bespreekt een aantal risico's niet of onvoldoende zoals bijvoorbeeld:

- het risico op de re-identificatie van besmette personen (en een daaruit voortvloeiend risico op stigmatisering) door gebruikers van de Belgische notificatie-app met weinig of slechts een beperkt aantal regelmatige contacten. Eventuele (sensibiliserende) maatregelen om dit risico op te vangen ontbreken.

- het risico verbonden aan het gebruik van de Belgische notificatie-app door zwakke groepen van gebruikers zoals minderjarigen, anderstaligen en ouderen. Voor minderjarigen bespreekt R24 'Verwerking gegevens minderjarigen' uitsluitend het risico om geen toestemming van de ouders te hebben verkregen. Eerst en vooral is dit risico niet van toepassing aangezien artikel 8 AVG slechts geldt in zoverre de toestemming in de zin van artikel 6.1.a AVG de rechtsgrond voor de verwerking is, *quod non* (zie in dit verband punt 3). Het eigenlijk risico bestaat erin dat kinderen (en bij uitbreiding andere zwakke groepen) recht hebben op specifieke bescherming, aangezien zij zich minder bewust zijn van de betrokken risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking van persoonsgegevens[9]. Nochtans vermeldt de GEB bijv. in het kader van D.08. 'Naleving van het recht op informatie' geen enkel risico, noch maatregelen om minderjarigen zo goed mogelijk te informeren op een aangepaste wijze (bijv. een aangepaste privacyverklaring of een specifieke informatiecampagne). De GEB bevat overigens geen enkele indicatie hoe zou worden toegezien op de naleving van concrete leeftijdsgrens voor het gebruik van de app.

- Het risico op vals positieve resultaten voor zorgverstrekkers die de Belgische notificatie-app gebruiken (zij komen immers in contact met veel risicopatiënten, maar dragen beschermende kledij).

- De GEB bespreekt niet systematisch op welke manier de naleving van alle rechten van de betrokkenen wordt gegarandeerd (de rechten op toegang, verwijdering en beperking van de verwerking worden niet duidelijk besproken). De GEB vermeldt wel dat op grond van artikel

---

[7] Wet van 13 juni 2005 *betreffende de elektronische communicatie, BS* 20 juni 2005.

[8] Voor de duidelijkheid: de rechtsgrond voor de verwerking van persoonsgegevens onder de AVG en de noodzaak om een toestemming te verkrijgen conform artikel 129 WEC staan los van elkaar. Het zijn twee cumulatieve vereisten.

[9] Overweging 38 AVG.

11 van de AVG Sciensano niet kan worden verplicht om aanvullende gegevens te verwerken om de gebruiker te identificeren met als enig doel het naleven van de rechten van de betrokkene op grond van de AVG. Bijkomende toelichting is nodig om te verifiëren of artikel 11 AVG al dan niet van toepassing is. Bovendien breng ik in herinnering dat in tegenstelling tot bijvoorbeeld de Franse notificatie-app[10], in de huidige stand van de wetgeving, er geen wetsbepaling voor handen lijkt te zijn die krachtens artikel 23 AVG toelaat de rechten van de betrokkenen te beperken.

5) Risico's die de GEB niet juist inschat of onvoldoende afdekt

De GEB dekt enkele risico's onvoldoende af of levert onvoldoende informatie aan om te beoordelen of de genomen maatregelen adequaat zijn, zoals bijvoorbeeld:

- R09. 'Volledigheid en juistheid van gegevens' identificeert meerdere risico's met betrekking tot mogelijke vals positieve resultaten. Een goede opvolging van dit risico naar aanleiding van de geplande test, is noodzakelijk om dit risico verder in kaart te brengen en zo goed mogelijk weer te geven hoe vaak een onterechte, tijdelijke quarantaine daadwerkelijk wordt opgelegd. De GEB vermeldt dat hier een graad van maatschappelijke aanvaarding voor nodig zal zijn, maar geeft niet aan op welke manier hier proactief een draagvlak voor gebouwd wordt. Gebruikers moeten eerst en vooral goed geïnformeerd worden over dit risico.

- R10. 'Accuraatheid en actueelheid (sic) van gegevens' is als risico volgens de GEB niet van toepassing, terwijl R09. 'Volledigheid en juistheid van gegevens' een beschrijving geeft van het risico met betrekking tot vals positieve resultaten. Dit lijkt tegenstrijdig en is niet duidelijk. Bovendien moet er een zeer goede motivering gegeven worden die kan rechtvaardigen dat nergens in de ketting van verwerkingen een procedure kan geïmplementeerd worden om de accuraatheid van de persoonsgegevens op regelmatige basis te verifiëren (R09 vermeldt nochtans dat er op macroniveau wel een kwaliteitscontrole plaatsvindt bij Sciensano).

- R12. 'Verwijderen van gegevens'. De GEB zou hier moeten specifiëren binnen welke termijn de persoonsgegevens van een gebruiker worden gewist die de Belgische notificatie-app des-installeert.

- R14. 'Ongeautoriseerde toegang tot gegevens' en R15. 'Pseudonimisatie van gegevens' worden apart besproken terwijl het in essentie gaat over hetzelfde risico. Deze risico's lijken onvoldoende hoog ingeschat. Voor het centrale platform verwijst de GEB naar de veiligheids-maatregelen van de verwerker (Amazon Web Services en SoftwareOne), terwijl uit het dossier echter blijkt dat deze nog niet geïmplementeerd zijn.

[10] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041936881&categorieLien=id

6) Beschrijving van de veiligheidsmaatregelen

Sectie V van de GEB behandelt het thema informatieveiligheid, maar is onvoldoende specifiek en maakt niet duidelijk welke veiligheidsmaatregelen daadwerkelijk geïmplementeerd zullen worden. De GEB vermeldt immers slechts dat de "*AWS public cloud een scala aan veiligheidscontroles om gegevens te beschermen tegen ongeoorloofde toegang, wijziging of verwijdering [aanbiedt]*" en geeft een lijst van de beveiligingsdiensten die men voor de Belgische notificatie-app "*plant*" te gebruiken.

Een eenvoudige verwijzing naar het documentatieportaal van AWS *Overview of Security Processes* whitepaper volstaat dus niet. Het moet duidelijk zijn welke specifieke maatregelen worden getroffen om tegemoet te komen aan de hoge risico's die gepaard gaan met de verwerking in kwestie. Dit is des te meer waar gelet op de keuze voor een publieke cloud die – in tegenstelling tot het advies van de Veiligheid van de Staat[11] - niet in België gehost wordt. Alle veiligheidskenmerken en maatregelen moet in detail beschreven worden.

In dit verband dring ik ook aan om bij een nieuwe versie van de GEB ook de verwerkersovereenkomst in de zin van artikel 28 AVG te bezorgen samen met de gedetailleerde beschrijving van de definitieve veiligheidsmaatregelen die de verwerkers, zoals Amazon Web Services en SoftwareOne, krachtens deze verwerkingsovereenkomst moeten respecteren.

Inzake de controle op informatieveiligheid is het ook noodzakelijk om de frequentie van de veiligheids-audits te bepalen en de resultaten van deze veiligheidsaudits te bezorgen aan de Autoriteit. Zo bepaalt R18. 'Testen van beveiligingsmaatregelen' dat een regelmatige test cruciaal is voor het platform, zonder evenwel de frequentie en de aard van de tests te bepalen die zullen volgen op de penetration test die plaatsvindt voor de release van de Belgische notificatie-app. Tot slot is ook een specifieke externe, onafhankelijke en regelmatige audit noodzakelijk om de evoluties van een aantal in dit advies besproken risico's verder in kaart te brengen (in het bijzonder m.b.t. punten 1) en 2) van dit advies).

7) Materiële rechtzettingen

De ingediende versie van de GEB bevat heel wat vormelijke onvolkomenheden en materiële fouten. In de bijlage vindt u hiervan een uitgebreider overzicht. Voor de leesbaarheid en het goede begrip van de GEB door de betrokkenen is het nodig om de kwaliteit en toegankelijkheid van de GEB nog verder te verbeteren.

In dat opzicht merk ik op dat de GEB ook een aantal begrippen definieert in haar inleidende bepalingen. Sommige definities parafraseren op onvolledige of zelfs foutieve wijze de wettelijke

---

[11] https://www.vsse.be/sites/default/files/parlement_28042020_nl_0.pdf

definities van de rechtstreeks van toepassing zijnde Algemene Verordening Gegevensbescherming (AVG). Het komt de toegankelijkheid van de GEB niet ten goede om begrippen die in de AVG worden gedefinieerd in de GEB anders te omschrijven. Uiteraard kan de wettelijke definitie in de context van de GEB wel verder praktisch worden toelicht. Een revisie van het ontwerp is bovendien ook nodig om te verzekeren dat de GEB de gedefinieerde begrippen consequent blijft gebruiken doorheen de tekst, wat nu niet steeds het geval is.

Tot slot merk ik op dat sommige maatregelen niet altijd beantwoorden aan het omschreven risico en vice versa. Dit lijkt deels toe te schrijven aan de vaststelling dat de weerhouden risico-categorieën niet altijd voldoende zijn afgestemd op de specifieke risico's van de Belgische notificatie-app. Het verdient aanbeveling om bepaalde risico-categorieën te herformuleren zodat zij nog beter aansluiten op de specifieke risico's van de concrete notificatie-app.

8) Bijkomende informatie

Om in het kader van de GEB een sluitende beoordeling te maken over de risico's die verbonden zijn aan de verwerking, is het noodzakelijk om bijkomende informatie-elementen op te nemen in de GEB. Momenteel ontbreekt het in de GEB aan:

- een gedetailleerde beschrijving van de verwerkingen in het kader van de federatieve gateway die ter beschikking wordt gesteld door de Europese Commissie op basis van het uitvoeringsbesluit (EU) 2020/1023[12]. In het bijzonder is het nodig om te verduidelijken hoe de betrokkene zijn rechten kan uitoefenen ten aanzien van de verschillende verwerkingsverantwoordelijken in meerdere lidstaten.

- een visuele weergave van de informatie-elementen en schermen die aan de gebruiker van de app worden getoond bij het doorlopen van de verschillende gebruiksfasen, alsook de precieze inhoud van de berichten die de gebruiker ontvangt. Deze informatie is nodig om te beoordelen of de implementatie van de app alle risico's inzake transparantie en informatie goed aanpakt.

[12] Uitvoeringsbesluit (EU) 2020/1023 van de commissie van 15 juli *2020 tot wijziging van Uitvoeringsbesluit (EU) 2019/1765 wat betreft de grensoverschrijdende uitwisseling van gegevens tussen nationale mobiele applicaties voor het traceren en waarschuwen van contacten met het oog op de bestrijding van de COVID-19-pandemie.*

Conclusie

Ik nodig u uit om de GEB aan te passen, in lijn te brengen met de hierboven vermelde opmerkingen en de bijkomende informatie te verstrekken die de Autoriteit in staat moet stellen om conform artikel 36 AVG te beslissen of de verwerking in het kader van de Belgische notificatie-app al dan niet doorgang kan vinden[13]. Dit advies verhindert u echter niet om het lopende test- en ontwikkelingstraject (inclusief de ruime test met werkelijke gebruikers en gegevens) van de Belgische notificatie-app verder te zetten.

Tot slot verzoek ik om minstens na respectievelijk drie, zes en negen maanden te rekenen vanaf het voorliggende advies, een geüpdatete versie van de GEB in te dienen die de risico's opnieuw evalueert op grond van de intussen verkregen informatie, inzichten en ervaringen.

Hoogachtend

[redacted]

Voorzitter

[13] En dit voordat de Belgische notificatie-app officieel gelanceerd wordt in het hele land.