Informatieveiligheidscomité
verenigde kamers
(kamer sociale zekerheid/kamer federale overheid)[1]

BERAADSLAGING NR. 23/003 VAN 7 MAART 2023 MET BETREKKING TOT DE TERBESCHIKKINGSTELLING VAN DE ISI+KAART EN DE EU DIGITALE COVID CERTIFICATEN AAN DE BETROKKENE VIA DE DIGITALE PORTEFEUILLE

Gelet op de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid, in het bijzonder artikel 15, § 2, eerste lid;

Gelet op de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform, in het bijzonder artikel 11, eerste lid;

Gelet op de wet van 13 december 2006 houdende diverse bepalingen betreffende gezondheid, in het bijzonder artikel 42;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, in het bijzonder artikels 111 en 114;

Gelet op de wet van 5 september 2018 *tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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*, in het bijzonder de artikelen 97 en 98;

Gelet op de aanvraag betreffende de ontsluiting van de ISI+kaart en de EU Digitale COVID Certificaten via de digitale portefeuille;

Gelet op het gezamenlijk auditoraatsrapport van Kruispuntbank van de Sociale Zekerheid en de federale overheidsdienst Beleid en Ondersteuning;

Gelet op het verslag van de heer B. VIAENE en de heer D. HACHÉ.

I. ONDERWERP

1. In opdracht van de federale overheid ontwikkelt de federale overheidsdienst Beleid en Ondersteuning de digitale portefeuille[2]. De digitale portefeuille is een toepassing (app) voor

[1] Deze beraadslaging geldt enkel als een beraadslaging van de **verenigde kamers** (kamer sociale zekerheid en kamer federale overheid) voor de mededeling van persoonsgegevens door de verzekeringsinstellingen (via de KSZ) aan de federale overheidsdienst Beleid en Ondersteuning (als federale dienstenintegrator) met het oog op de ter beschikking stelling aan de rechthebbende in de digitale portefeuille. De in de beraadslaging vermelde mededeling van persoonsgegevens betreffende de EU Digitale COVID Certificaten voor de terbeschikkingstelling aan de rechthebbende behoort tot de bevoegdheid van de **kamer sociale zekerheid en gezondheid** van het Informatieveiligheidscomité.

[2] In deze beraadslaging wordt de mobiele toepassing 'de digitale portefeuille' genoemd, naar analogie met het voorstel voor een Verordening van het Europees Parlement en de Raad *tot wijziging van Verordening (EU) nr.*

mobiele toestellen, zowel voor het besturingssysteem iOS als Android, die de burger toelaat zijn identiteit op mobiele wijze te bewijzen, berichten, attesten en documenten op te vragen en/of te ontvangen, en te bewaren.

2. Met de digitale portefeuille bereidt België zich voor op de toekomstige Europese verplichting dat iedere lidstaat een dergelijke digitale portefeuille moet aanbieden[3]. Het is thans voorzien dat eens de verordening tot wijziging van de eIDAS-verordening hieromtrent is goedgekeurd, de lidstaten de digitale portefeuille binnen een bepaalde termijn, waarschijnlijk 12 maanden, dienen te implementeren.

3. De functionaliteiten van de Belgische digitale portefeuille worden door de federale overheidsdienst Beleid en Ondersteuning in verschillende fasen ontwikkeld. **Op termijn** zal de digitale portefeuille volgende functionaliteiten kunnen bevatten[4]:

- Mobiele identiteit: in de digitale portefeuille worden de nodige componenten opgeslagen om de digitale identiteit van de betrokkene te kunnen bewijzen.

- eSign: de mogelijkheid voor de burger om via het ondertekeningscertificaat van zijn digitale identiteitskaart zijn elektronisch handtekening te plaatsen

- **eBox-berichten** via My eBox: in de digitale portefeuille kan de betrokkene zijn eBox berichten en documenten zien, van zodra hij daartoe de toestemming heeft gegeven. Hij krijgt een melding wanneer er een nieuw bericht of document wordt verzonden.

- **eLoket**: de betrokkene kan via toepassingen van aangesloten instanties officiële attesten, vergunningen, afschriften of uittreksels evenals het digitaal rijbewijs opvragen en bewaren.

- **eSafe**: de ontvangen documenten kunnen lokaal en beveiligd worden opgeslagen.

- **MyData**: de betrokkene kan de informatie die via MyData ter beschikking wordt gesteld via de digitale portefeuille ontsluiten. Via MyData zal de burger toegang hebben tot de gegevens die de deelnemende overheidsinstellingen over hem of haar beschikken.

- **Scanfunctie**: de QR-codes die deel uitmaken van documenten opgenomen in de digitale portefeuille van de ene persoon kunnen via deze functionaliteit van de digitale portefeuille van een andere persoon worden gescand. Voor zover de codes aan de vast te leggen criteria voldoen (bv. valabele elektronische handtekening, formaat QR-code, …), zal de juistheid ervan kunnen worden bevestigd. Zo zal bijvoorbeeld, op termijn, de juistheid van de QR-code van een digitaal rijbewijs kunnen worden nagegaan.

4. De digitale portefeuille is dus een generiek platform dat het mogelijk maakt dienstverlening vanuit de publieke sector op een standaard manier aan te bieden aan burgers op mobiele toestellen. Het platform bestaat uit een mobiele applicatie, onder de controle van de betrokkene, en datacentercomponenten, onder het beheer van de federale overheidsdienst beleid en ondersteuning. De installatie en het gebruik van de functionaliteiten van de digitale

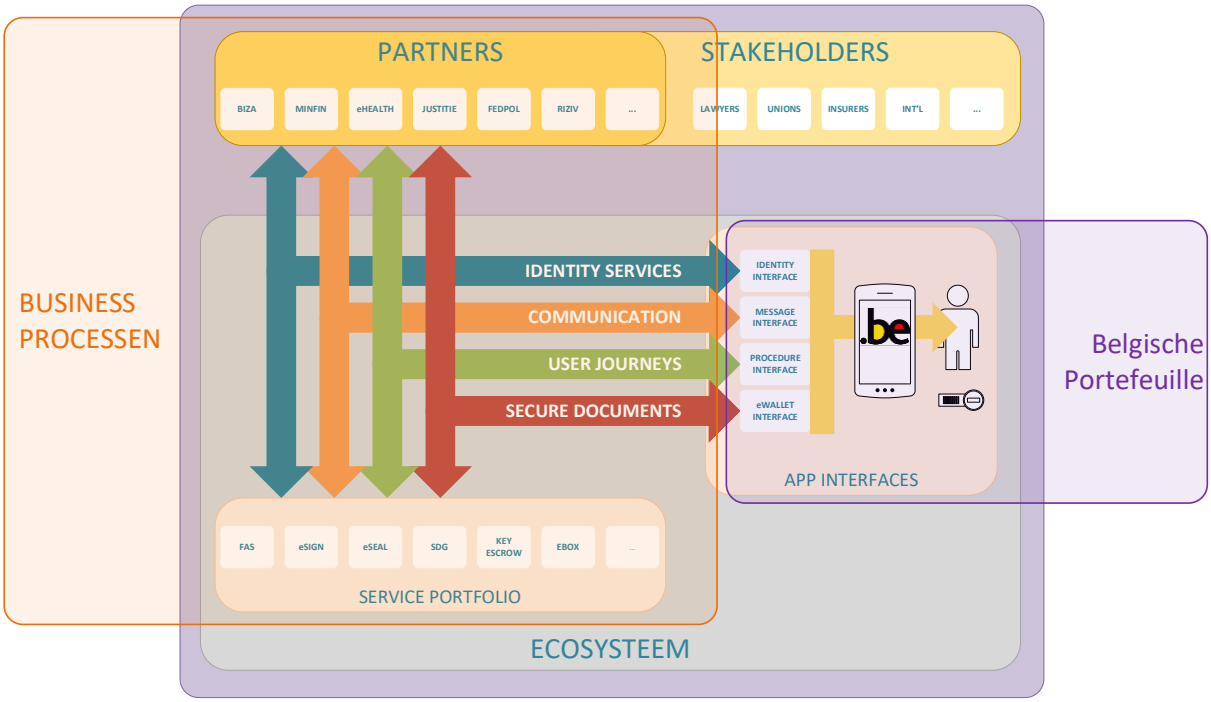
---

910/2014 betreffende een Europees kader voor een digitale identiteit. De benaming van de mobiele toepassing kan nog wijzigen.

[3] Voorstel voor een Verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit, https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52021PC0281 .

[4] De concrete modaliteiten en benamingen van de toekomstige functionaliteiten, evenals de benaming van de digitale portefeuille kunnen nog wijzigen.

portefeuille is vrijwillig. De betrokkene dient akkoord te gaan met de gebruiksvoorwaarden en de privacyverklaring die hem of haar zullen worden voorgelegd naar aanleiding van de installatie en activatie.

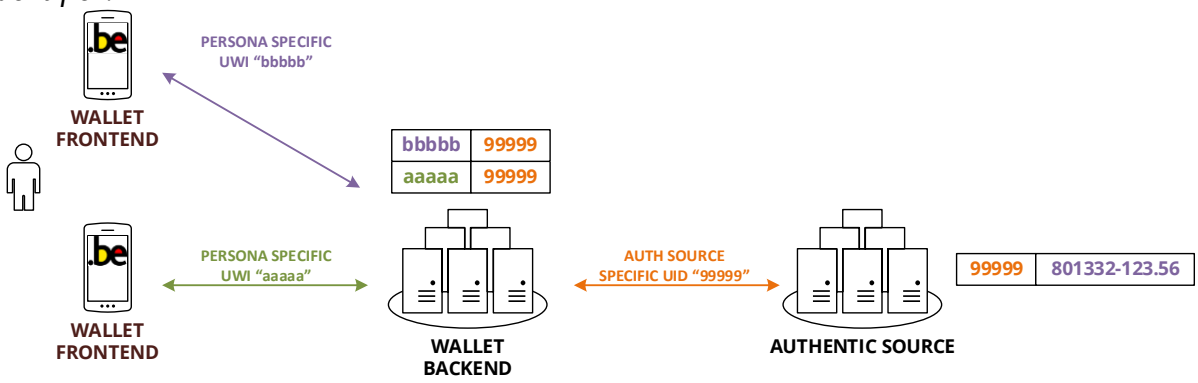


5. Er wordt gewerkt in een privacy-by-design logica vanuit de volgende basisprincipes, die gelden voor alle functies van de digitale portefeuille:

- De datacentercomponenten van de digitale portefeuille bevatten enkel technische referenties om het ecosysteem te doen werken. Afgezien van gepseudonimiseerde identificatienummers, worden er geen persoonsgegevens van de gebruiker in de datacentercomponenten opgeslagen en er is geen cross-referentie mogelijk.
- De mobiele applicatie spreekt niet rechtstreeks de authentieke bronnen aan. Gegevensuitwisseling gebeurt via de datacentercomponenten van de digitale portefeuille op een beveiligde manier.
- Gegevens die bestemd zijn voor de mobiele applicatie kunnen versleuteld worden bij de bron (dus buiten de digitale portefeuille), waarna de garantie geboden wordt dat deze enkel door de juiste applicatie instance[5], op het juiste toestel, en door de juiste gebruiker gelezen kunnen worden.
- Gegevens die in de digitale portefeuille bewaard worden, kunnen op de telefoon versleuteld opgeslagen worden op dezelfde manier.

[5] De 'instance' is een geïnstalleerde applicatie. Op Android is er de mogelijkheid om meerdere gebruikers op 1 toestel aan te maken. Als er op een toestel 2 gebruikers zijn die elk de applicatie geïnstalleerd hebben, dan wordt het als 2 instances beschouwd.

6. Om de digitale portefeuille te activeren, dient deze gelinkt te worden aan een reële persoon. Tijdens de activatie genereert de digitale portefeuille random geheimen[6] en *identifiers*. Deze worden vervolgens bij een bron gelinkt aan een reële persoon op basis van een neutrale *identifier*.



De digitale portefeuille hoeft niet te beschikken over de persoonsattributen die de authentieke bron beheert om het ecosysteem te doen werken (in het voorbeeld: 801332-123.56).

De *identifier* die gebruikt wordt om een gebruiker van de digitale portefeuille te identificeren bij de authentieke bron[7] is intern en kan louter voor dat doel en enkel tussen deze partijen gebruikt worden (in het voorbeeld: 99999).

De *identifier* die gebruikt wordt om de actieve applicaties en toestellen te onderscheiden waarover een gebruiker beschikt, is enkel beschikbaar voor de applicatie en datacentercomponenten van de digitale portefeuille (in het voorbeeld: aaaaa en bbbbb).

Voor elke combinatie van actieve gebruiker, applicatie, toestel en bron wordt een andere set geheimen gegenereerd. De *identifiers* aaaaa en bbbbb zijn dus uniek per gebruiker, geïnstalleerde applicatie, gebruikt toestel en de bron waarmee de gebruiker geactiveerd is.

De *identifiers* die gebruikt worden per bron (99999) zijn uniek per bron. Bronnen kunnen deze gegevens niet gebruiken om gebruikers te detecteren die gekend zijn op beide.

7. De digitale portefeuille biedt een aantal basisdiensten die partners in staat stelt gegevens en diensten aan te bieden aan de gebruiker. Deze gegevens en diensten blijven te allen tijde onder de controle van de betrokken dienst en/of de eindgebruiker.

- De digitale portefeuille kan gebruikt worden om de gebruiker te authentiseren en/of identificeren (als digitale sleutel), maar enkel de authentieke bron (i.e. het Rijksregister) beschikt over de persoonsgegevens die nodig zijn om de link te maken naar een natuurlijk persoon. De authentieke bron kan deze ontsluiten via het *Federal Authentication System* (FAS) of rechtstreeks aan de partij die gegevens wil ontsluiten via de digitale portefeuille.[8]

---

[6] Meer bepaald asymmetrische sleutelparen.

[7] In principe kan elke authentieke bron een identifier aan een gebruiker toekennen. In het kader van de activatie van de digitale portefeuille en de creatie van de digitale sleutel, betreft het Rijksregister.

[8] Op termijn zal de digitale portefeuille eveneens de componenten van de digitale elektronische identiteitskaart, uit te geven door de FOD Binnenlandse Zaken, bevatten waarmee de burger zich ten aanzien van derden kan identificeren en authentificeren (door middel van het authenticatiecertificaat van de digitale eID) en documenten kan ondertekenen (door middel van het handtekeningscertificaat van de digitale eID). In afwachting van die digitale

- Gegevens kunnen end-2-end beveiligd worden. In dit geval kan de partij die de gegevens wil ontsluiten via de digitale portefeuille deze gegevens versleutelen op basis van encryptiesleutels die door de digitale portefeuille op het toestel gegenereerd werden. Enkel de juiste gebruiker kan vervolgens op het juiste toestel met de correctie instantie van de digitale portefeuille deze gegevens weer decrypteren.

- Gegevens die opgeslagen worden op het mobiele toestel worden versleuteld opgeslagen, waarna enkel de juiste gebruiker op het juiste toestel met de correctie instantie van de digitale portefeuille deze gegevens weer kan inkijken.

8. **De huidige beraadslaging beoogt uitsluitend en specifiek de terbeschikkingstelling van de ISI+ kaart en van de EU Digitale COVID Certificaten (vaccinatie, test en herstel)** door de betrokken verantwoordelijke instellingen via de digitale portefeuille aan de rechthebbenden. Deze documenten zullen door de betrokkenen via een toepassing in de digitale portefeuille kunnen worden opgevraagd. Ze worden vervolgens via de federale dienstenintegrator bij de betreffende authentieke bronnen opgehaald en overgemaakt aan de digitale portefeuille van de betrokkene. Zowel wat de ISI+kaart als de EU Digitale COVID Certificaten betreft, gaat het om de terbeschikkingstelling aan de betrokkenen zelf of, in geval van minderjarigen, hun ouders of wettelijk vertegenwoordigers.

9. **Wat ISI+kaart betreft:** Volwassenen en kinderen vanaf 12 jaar kunnen zich bij een apotheker, een arts of een ziekenhuis aanmelden met hun elektronische identiteitskaart of eID. Met de eID kan de zorgverlener de online databank van het ziekenfonds raadplegen. Zo beschikken de zorgverleners altijd over de meest recente gegevens en kan men nagaan of de betrokkene recht heeft op een terugbetaling van het ziekenfonds. Wie geen eID kan krijgen, ontvangt een **ISI+-kaart**. De ISI+-kaart kan worden gebruikt bij de apotheker, bij de dokter of in het ziekenhuis, net zoals een eID. De ISI+-kaart is geen identiteitskaart: ze kan enkel gebruikt worden om zich te identificeren bij zorgverleners en bij de verzekeringsinstelling.

10. De ISI+-kaart wordt uitgereikt door de verzekeringsinstellingen, conform de bepalingen van de wet van 29 januari 2014 *houdende bepalingen inzake de sociale identiteitskaart en de ISI+-kaart* en het uitvoeringsbesluit van 26 februari 2014. De Kruispuntbank van de sociale zekerheid beheert het centrale bestand van de ISI+-kaarten. Het centrale bestand van de ISI+-kaarten beoogt de uitreiking, de vernieuwing, de vervanging en de aanwending van de ISI+-kaarten op een beveiligde wijze en bevat de daartoe noodzakelijke informatie.

11. **Wat de EU Digitale COVID Certificaten betreft:** Sinds de COVID-pandemie dienen burgers - afhankelijk van de toepasselijke regels - hun status wat vaccinatie, test of herstel betreft, te kunnen bewijzen door middel van certificaten. Door middel van een samenwerkingsakkoord tussen de federale en regionale overheden[9] werden er afspraken gemaakt omtrent het opmaken, afgeven, verifiëren van het digitaal EU-COVID-certificaat.

---

elektronische identiteitskaart, zal de burger een digitale sleutel aanmaken waarmee hij zich online kan authentificeren bij de instanties die aangesloten zijn op het Federal Authentication System (FAS) van de FOD BOSA.

[9] Het samenwerkingsakkoord van 14 juli 2021, herhaaldelijk gewijzigd, tussen de Federale Staat, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Gemeenschappelijke Gemeenschapscommissie, het Waalse Gewest en de Franse Gemeenschapscommissie betreffende de verwerking van gegevens met betrekking tot het digitaal EU-COVID-certificaat, het COVID Safe Ticket, het PLF en de verwerking van persoonsgegevens van in het buitenland wonende of verblijvende werknemers en zelfstandigen die activiteiten uitvoeren in België en het Uitvoerend samenwerkingsakkoord van 15 oktober 2021.

De digitale EU COVID certificaten worden aangemaakt via een applicatie op een mobiel toestel (de COVIDSafe-applicatie) of via de websites van bepaalde overheidsinstanties.

12. Overeenkomstig artikel 6, § 2, van het samenwerkingsakkoord van 14 juli 2021, gewijzigd op 28 oktober 2021, werd het agentschap Digitaal Vlaanderen op vraag van het e-Health-platform, ermee belast de operationele diensten te leveren voor de ontwikkeling van de COVIDSafe-applicatie evenals de COVIDScan-applicatie (aan de hand waarvan de respectieve certificaten digitaal leesbaar zijn), waarbij het agentschap Digitaal Vlaanderen optreedt als onderaannemer en verwerker. Het agentschap Digitaal Vlaanderen beslist noch over welke toepassing ter beschikking wordt gesteld aan de burger, noch over de modaliteiten en het tijdstip van de de-activering van de COVIDSafe- en COVIDScan-applicatie. Het agentschap Digitaal Vlaanderen handelt enkel *op instructies van het e-Health-platform*.

II. ONDERZOEK VAN DE AANVRAAG

A. ONTVANKELIJKHEID EN BEVOEGDHEID VAN HET COMITE

13. Overeenkomstig artikel 15, §2 van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid* vereist **elke mededeling van sociale gegevens van persoonlijke aard door de Kruispuntbank van de sociale zekerheid of een instelling van sociale zekerheid** bedoeld in artikel 2, eerste lid, 2°, a), aan een andere federale overheidsdienst, programmatorische overheidsdienst of federale instelling van openbaar nut dan een instelling van sociale zekerheid, een voorafgaande beraadslaging van **de verenigde kamers** van het informatieveiligheidscomité voor zover de verwerkingsverantwoordelijken van de meedelende instantie, de ontvangende instantie en de Kruispuntbank van de sociale zekerheid in uitvoering van artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, niet tot een akkoord komen over de mededeling of minstens één van die verwerkingsverantwoordelijken om een beraadslaging verzoekt en de andere verwerkingsverantwoordelijken daarvan in kennis heeft gesteld. In vermelde gevallen wordt de aanvraag ambtshalve gezamenlijk ingediend door betrokken verwerkingsverantwoordelijken.

14. Wat de mededeling van de gegevens van **de ISI+kaart** betreft, is er sprake van de mededeling van persoonsgegevens door de verzekeringsinstellingen en de Kruispuntbank van de Sociale Zekerheid aan de federale dienstenintegrator (FOD BOSA) teneinde de ISI+kaart ter beschikking te stellen aan de rechthebbende, meer bepaald de betrokkene zelf of, ingeval van minderjarigen, aan de ouders of de wettelijk vertegenwoordigers. De verenigde kamers van het Informatieveiligheidscomité achten zich dan ook bevoegd om zich hierover uit te spreken.

15. Overeenkomstig artikel 11 van de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform vereist elke mededeling van persoonsgegevens door of aan het eHealth-platform een principiële machtiging van **de kamer sociale zekerheid en gezondheid** van het Informatieveiligheidscomité.

16. Bovendien is de kamer sociale zekerheid en gezondheid overeenkomstig artikel 42 van de wet van 13 december 2006 *houdende diverse bepalingen betreffende gezondheid* bevoegd voor het verlenen van een principiële machtiging met betrekking tot elke mededeling van persoonsgegevens die de gezondheid betreffen, behoudens de in voormelde wet voorziene uitzonderingen.

17. Overeenkomstig art. 6, § 2, van het Samenwerkingsakkoord van 14 juli 2021, gewijzigd op 28 oktober 2021, verwerkt het agentschap Digitaal Vlaanderen als onderaannemer en verwerker *op vraag van en op instructie van* het eHealth-platform de persoonsgegevens in het kader van de operationele diensten voor de ontwikkeling van de COVIDSafe-applicatie en de COVIDScan-applicatie (aan de hand waarvan de respectieve certificaten digitaal leesbaar zijn). De mededeling van de gegevens betreffende de EU Digitale COVID Certificaten via de COVIDSafe-applicatie aan de federale dienstenintegrator betreft een mededeling *op vraag van en op instructie van* het eHealth-platform. De kamer sociale zekerheid en gezondheid van het Informatieveiligheidscomité acht zich dan ook bevoegd om zich hierover uit te spreken. Het Informatieveiligheidscomité wijst er volledigheidshalve op dat het zich niet uitspreekt over de samenstelling van de certificaten of het gebruik van de certificaten. In het kader van deze beraadslaging betreft het uitsluitend wijze waarop de EU Digitale COVID Certificaten ter beschikking kunnen worden gesteld aan de betrokkene of, indien het een minderjarige betreft, aan de ouders of wettelijk vertegenwoordigers.

B. TEN GRONDE

B.1. VERANTWOORDINGSPLICHT

18. Overeenkomstig artikel 5.2 van de Algemene Verordening Gegevensbescherming[10] (hierna 'AVG' genoemd) zijn de verzekeringsinstellingen, de Kruispuntbank van de Sociale Zekerheid en het eHealth-platform (meedelende instanties) en FOD BOSA (ontvangende instantie in de hoedanigheid van federale dienstenintegrator en aanbieder van de digitale portefeuille) als verwerkingsverantwoordelijken verantwoordelijk voor het naleven van de beginselen vermeld in artikel 5.1 de AVG[11] en moeten ze in staat zijn dit aan te tonen.

---

[10] 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.

[11] Persoonsgegevens moeten:

a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is („rechtmatigheid, behoorlijkheid en transparantie");
b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd („doelbinding");
c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking");
d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren („juistheid");
e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen („opslagbeperking");
f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen

19. De verwerkingsverantwoordelijke dient overeenkomstig de AVG aan een aantal verplichtingen te voldoen. In voorliggende beraadslaging worden de belangrijkste verplichtingen overlopen. Het Informatieveiligheidscomité wijst er in dit kader op dat de verwerkingsverantwoordelijke een register van verwerkingsactiviteiten dient bij te houden overeenkomstig de bepalingen van art. 30 AVG.

B.2. RECHTMATIGHEID

20. Overeenkomstig art. 5, §1, a), AVG moeten persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig is. Dit houdt in dat de beoogde verwerking een basis moet vinden in één van de rechtmatigheidsgronden vermeld in artikel 6 AVG of, wat de verwerking van gezondheidsgegevens betreft, in één van de uitzonderingen vermeld in artikel 9 AVG.

21. Het aanmaken en uitreiken van de ISI+-kaart wordt geregeld bij wet van 29 januari 2014 *houdende bepalingen inzake de sociale identiteitskaart en de ISI+-kaart* en het uitvoeringsbesluit van 26 februari 2014. Hierin wordt bepaald dat de verzekeringsinstellingen de ISI+-kaart uitreiken en dat de Kruispuntbank van de Sociale Zekerheid het centrale bestand van de ISI+-kaarten beheert, dat de uitreiking, de vernieuwing, de vervanging en de aanwending van de ISI+-kaarten op een beveiligde wijze beoogt.

22. Wat de rol van de Federale Overheidsdienst Beleid en Ondersteuning betreft, voorziet artikel 2, eerste lid, 33°, van het koninklijk besluit van 22 februari 2017 de Federale Overheidsdienst Beleid en Ondersteuning uitdrukkelijk in de opdracht tot "*het ontwikkelen en beheren van digitale diensten en platformen met het oog op digitale interactie met burgers en ondernemingen en tussen administraties*". De rol van de Federale Overheidsdienst Beleid en Ondersteuning als federale dienstenintegrator wordt dan weer geregeld bij wet van 15 augustus 2012 *houdende oprichting en organisatie van een federale dienstenintegrator,* meer bepaal de artikelen 4, 5 en volgenden. Gelet op het voorgaande is de verwerking van persoonsgegevens in het kader van de ter beschikking stelling van de ISI+-kaart via de digitale portefeuille aan de betrokkene zelf of, indien het een minderjarige betreft, aan zijn ouders of wettelijke vertegenwoordigers, noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijken rust (art. 6.1 c) AVG).

23. Het aanmaken en uitreiken van de EU Digitale COVID Certificaten wordt geregeld door het Samenwerkingsakkoord van 14 juli 2021, gewijzigd op 28 oktober 2021, op grond waarvan de COVIDSafe-app werd ontwikkeld door het Agentschap Digitaal Vlaanderen op instructie van het eHealth-platform. Het Samenwerkingsakkoord stelt uitdrukkelijk dat het agentschap Digitaal Vlaanderen op vraag van het eHealth-platform, ermee belast is om de operationele diensten te leveren voor de ontwikkeling van de COVIDSafe-applicatie en de COVIDScan-applicatie (aan de hand waarvan de respectieve certificaten digitaal leesbaar zijn), waarbij het agentschap Digitaal Vlaanderen optreedt als onderaannemer en verwerker. Op grond van het Samenwerkingsakkoord is het eHealth-platform bijgevolg bevoegd om de noodzakelijke instructies te verlenen voor de ontwikkeling van de COVIDSafe-applicatie, waaronder de wijze van terbeschikkingstelling van de EU Digitale COVID Certificaten aan de betrokkene zelf of, ingeval van een minderjarige, aan de ouders of wettelijke vertegenwoordiger moet

---

ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid").

worden begrepen. Gelet op het feit dat het de verwerking van gezondheidsgegevens betreft, kan worden vastgesteld dat de verwerking voldoet aan één van de voorwaarden waaronder het verbod op de verwerking van dergelijke gegevens overeenkomstig artikel 9.2 AVG. De verwerking is immers noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid, 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. Terzake dient dus verwezen te worden naar het Samenwerkingsakkoord van 14 juli 2021, gewijzigd op 28 oktober 2021.

B.2. DOELBINDING

24. Artikel 5.1 b) AVG laat de verwerking van persoonsgegevens slechts toe voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (principe van doelbinding).

25. Het Informatieveiligheidscomité stelt vast dat de mededelingen doeleinden beogen die wel degelijk welbepaald en uitdrukkelijk omschreven zijn, namelijk de terbeschikkingstelling van de ISI+-kaart en de EU Digitale COVID Certificaten aan de betrokkene zelf of, ingeval van minderjarige, aan de ouders of wettelijk vertegenwoordigers via de digitale portefeuille.

26. Gelet op de wettelijk voorziene opdrachten van de verschillende betrokken instanties, zoals hoger beschreven, acht het Informatieveiligheidscomité de doeleinden eveneens gerechtvaardigd.

B.3. MINIMALE GEGEVENSVERWERKING EN OPSLAGBEPERKING

27. Artikel 5.1 c) AVG stelt dat persoonsgegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ("minimale gegevensverwerking").

28. De mededeling betreft uitsluitend enerzijds de gegevens van de ISI+-kaart zoals beschreven in wet van 29 januari 2014 *houdende bepalingen inzake de sociale identiteitskaart en de ISI+-kaart* en het uitvoeringsbesluit van 26 februari 2014, en anderzijds de EU Digitale COVID Certificaten zoals beschreven in het Samenwerkingsakkoord van 14 juli 2021, gewijzigd op 28 oktober 2021.

29. De identificatie van de betrokkene in het kader van de mededeling door de betrokken partijen via de federale dienstenintegrator tot ontsluiting van de ISIS+-kaart en de EU Digitale COVID Certificaten aan de betrokkene of, ingeval van een minderjarige, aan de ouders of de wettelijk vertegenwoordiger via de digitale portefeuille, verloopt aan de hand van het identificatienummer van de sociale zekerheid, hetgeen bestaat uit ofwel het Rijksregisternummer ofwel het identificatienummer toegekend door de Kruispuntbank van de Sociale Zekerheid (het zogenaamde bisregisternummer). Het gebruik van het Rijksregisternummer is evenwel niet vrij en vereist een uitdrukkelijke machtiging. Terzake stelt het Informatieveiligheidscomité vast de federale dienstenintegrator effectief gemachtigd is om het Rijksregisternummer te gebruiken zoals voorzien in artikel art. 5, § 1 van de wet van 15 augustus 2012 *houdende oprichting en organisatie van een federale dienstenintegrator*.

30. Voor de ontsluiting van deze specifieke gegevens (ISI+-kaart en de EU Digitale COVID Certificaten) in de digitale portefeuille van de betrokkene of, in geval van een minderjarige, de ouders of de wettelijk vertegenwoordiger, zal de federale overheidsdienst Beleid en

Ondersteuning eveneens het Rijksregisternummer (meer bepaald een gepseudonimiseerde vorm van het Rijksregisternummer, cfr. randnummer 6) van de betrokkene en, in geval van een minderjarige, van de ouders of de wettelijk vertegenwoordiger verwerken. Overeenkomstig artikel 15, §3, van de wet van 15 januari 1990 *houdende oprichting en organisatie van een kruispuntbank van de sociale zekerheid* en overeenkomstig art. 35/1, §2, van de wet van 15 augustus 2012 *houdende oprichting en organisatie van een federale dienstenintegrator* zijn respectievelijk de kamer sociale zekerheid en gezondheid en de kamer federale overheid bevoegd om een beraadslaging te verlenen voor het gebruik van het identificatienummer van het Rijksregister van de natuurlijke personen door de betrokken instanties indien dat noodzakelijk is in het kader van de beoogde mededeling. Beide kamers verlenen dan ook een beraadslaging aan de federale overheidsdienst Beleid en Ondersteuning om het Rijksregisternummer voor het doeleinde zoals beschreven in deze beraadslaging te gebruiken. De bewaartermijn van de gepseudonimiseerde gegevens door de FOD BOSA is beperkt tot hetgeen noodzakelijk is, meer bepaald de duurtijd van de activatie van de toepassing door de betrokken persoon. Bovendien acht het Informatieveiligheidscomité het noodzakelijk dat de FOD BOSA voorziet in een *life cycle management* van de accounts teneinde te verzekeren dat de nodige acties worden genomen in geval van het overlijden van de gebruiker.

31. Aangaande de bewaringstermijn wijst het Informatieveiligheidscomité er op dat persoonsgegevens niet langer mogen worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt, noodzakelijk is.

32. Het Informatieveiligheidscomité neemt akte van het feit dat de federale dienstenintegrator de gegevens betreffende de ISI+-kaart en de EU Digitale COVID Certificaten slechts bewaart voor de duurtijd die noodzakelijk is voor de doorgifte aan de digitale portefeuille van de betrokkene zelf of, in geval van een minderjarige, de ouders of de wettelijk vertegenwoordiger. De opslag van de ontvangen documenten en attesten in de digitale portefeuille worden uitsluitend bepaald door de houder van de digitale portefeuille, inclusief de bewaartermijn van de betreffende gegevens.

B.4. VEILIGHEID

33. Persoonsgegevens moeten door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid").[12]

34. Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, moet de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de Algemene verordening gegevensbescherming wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

---

[12] Art. 5.1 f) AVG.

35. Het Informatieveiligheidscomité neemt akte van het feit dat de Federale Overheidsdienst Beleid en Ondersteuning zowel een functionaris voor gegevensbescherming als een informatieveiligheidsconsulent (CISO) heeft aangeduid.

36. Het Informatieveiligheidscomité neemt akte van het feit dat bij de ontwikkeling van de digitale portefeuille het principe van privacy by design werd toegepast.

- De datacentercomponenten van de digitale portefeuille bevatten enkel technische referenties om het ecosysteem te doen werken. Afgezien van gepseudonimiseerde identificatienummers, worden er geen persoonsgegevens van de gebruiker in de datacentercomponenten opgeslagen en er is geen cross-referentie mogelijk.
- De mobiele applicatie spreekt niet rechtstreeks de authentieke bronnen aan. Gegevensuitwisseling gebeurt via de datacentercomponenten van de digitale portefeuille op een beveiligde manier.
- Gegevens die bestemd zijn voor de mobiele applicatie kunnen versleuteld worden bij de bron (dus buiten de digitale portefeuille), waarna de garantie geboden wordt dat deze enkel door de juiste applicatie instance[13], op het juiste toestel, en door de juiste gebruiker gelezen kunnen worden.
- Gegevens die op in de digitale portefeuille bewaard worden, kunnen op de telefoon versleuteld opgeslagen worden op dezelfde manier.
- De digitale portefeuille hoeft niet te beschikken over de persoonsattributen die de authentieke bron beheert om het ecosysteem te doen werken. De datacentercomponenten van de digitale portefeuille beschikken in principe uitsluitend over een gepseudonimiseerd identificatienummer.
- De digitale portefeuille kan gebruikt worden om de gebruiker te authentiseren en/of identificeren, maar enkel de authentieke bron beschikt over de persoonsgegevens die nodig zijn om de link te maken naar een natuurlijk persoon. De authentieke bron kan deze ontsluiten via het *Federal Authentication System* (FAS) of rechtstreeks aan de partij die gegevens wil ontsluiten via de digitale portefeuille.
- Gegevens kunnen end-2-end beveiligd worden. In dit geval kan de partij die de gegevens wil ontsluiten via de digitale portefeuille deze gegevens versleutelen op basis van encryptiesleutels die door de digitale portefeuille op het toestel gegenereerd werden. Enkel de juiste gebruiker kan vervolgens op het juiste toestel met de correctie instantie van de digitale portefeuille deze gegevens weer decrypteren.
- Gegevens die opgeslagen worden op het mobiele toestel worden versleuteld opgeslagen, waarna enkel de juiste gebruiker op het juiste toestel met de correctie instantie van de digitale portefeuille deze gegevens weer kan inkijken.

37. Het Informatieveiligheidscomité neemt akte van het feit dat de Federale Overheidsdienst Beleid en Ondersteuning in uitvoering van artikel 35 AVG een gegevensbeschermingseffectbeoordeling uitvoert. Gelet op de noodzaak van deze gegevensbeschermingseffectbeoordeling oordeelt het Informatieveiligheidscomité dat deze

[13] De ‘instance’ is een geïnstalleerde applicatie. Op Android is er de mogelijkheid om meerdere gebruikers op 1 toestel aan te maken. Als er op een toestel 2 gebruikers zijn die elk de applicatie geïnstalleerd hebben, dan wordt het als 2 instances beschouwd.

beraadslaging alleszins slechts onder voorbehoud van de uitvoering ervan kan worden verleend. Indien uit deze beoordeling zou blijken dat bijkomende maatregelen moeten worden getroffen, dienen de betrokken partijen op eigen initiatief een aanvraag tot wijziging van onderhavige beraadslaging in. De mededeling van persoonsgegevens mag in voorkomend geval niet plaatsvinden totdat de vereiste toelating van het Informatieveiligheidscomité is bekomen. Indien uit de gegevensbeschermingseffectbeoordeling zou blijken dat er een hoog residuair risico is, dient de aanvrager de beoogde gegevensverwerking voor te leggen aan de Gegevensbeschermingsautoriteit, overeenkomst art. 36.1 AVG.

Om deze redenen, besluiten

de verenigde kamers van het Informatieveiligheidscomité en de kamer sociale zekerheid en gezondheid, elk met betrekking tot de mededeling die tot hun respectieve bevoegdheden behoort,

dat de mededeling van persoonsgegevens betreffende de ISI+kaart en de EU Digitale COVID Certificaten aan de betrokkene of, ingeval van een minderjarige, de ouders of de wettelijk vertegenwoordigers via de digitale portefeuille zoals aangeboden door de Federale Overheidsdienst Beleid en Ondersteuning, zoals in deze beraadslaging beschreven, is toegestaan mits wordt voldaan aan de vastgestelde maatregelen ter waarborging van de bescherming van de persoonlijke levenssfeer, meer bepaald de bescherming van de persoonsgegevens, en in het bijzonder de maatregelen op het vlak van doelbinding, minimale gegevensverwerking, opslagbeperking en informatieveiligheid.

Het Informatieveiligheidscomité neemt akte van het feit dat een gegevensbeschermingseffectbeoordeling betreffende de digitale portefeuille zal worden uitgevoerd door de Federale Overheidsdienst Beleid en Ondersteuning. Het zal een kopie ter informatie meedelen aan het Informatieveiligheidscomité. Als uit die beoordeling zou blijken dat bijkomende maatregelen moeten worden getroffen om de rechten en vrijheden van de betrokkenen te vrijwaren, dan zijn de partijen ertoe gehouden om de gewijzigde modaliteiten van de gegevensverwerking ter beraadslaging aan het Comité voor te leggen.

B. VIAENE
Kamer sociale zekerheid en gezondheid

D. HACHÉ
Kamer federale overheid