Informatieveiligheidscomité
Kamer sociale zekerheid en gezondheid

IVC/KSZG/24/456

BERAADSLAGING NR. 24/222 VAN 3 DECEMBER 2024 OVER DE MEDEDELING VAN PERSOONSGEGEVENS UIT HET NETWERK VAN DE SOCIALE ZEKERHEID DOOR EEN INSTELLING VAN SOCIALE ZEKERHEID AAN EEN ORGANISATIE, EEN ONDERNEMING OF EEN INDIVIDUELE BEROEPSBEOEFENAAR OP BASIS VAN EEN MANDAAT VERSTREKT DOOR EEN NATUURLIJKE PERSOON

Gelet op de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*, in het bijzonder artikel 15, § 1;

Gelet op de aanvraag van de betrokken instellingen van sociale zekerheid;

Gelet op het rapport van de Kruispuntbank van de Sociale Zekerheid;

Gelet op het verslag van de voorzitter.

A. ONDERWERP

1. Er doen zich diverse situaties voor waarbij een organisatie, een onderneming of een individuele beroepsbeoefenaar (hierna 'beroepshalve mandaathouders' genoemd), in het kader van een relatie met een natuurlijke persoon en mits het verkrijgen van een toestemming en het aanvaarden van een mandaat daartoe vanwege deze persoon, persoonsgegevens uit het netwerk van de sociale zekerheid over de betrokkene wil verwerken (in het kader van haar werking, haar dienstverlening, haar online platformen of toepassingen,…) en dit buiten de context van een opdracht die is voorzien in de regelgeving.

2. Het Informatieveiligheidscomité werd verzocht om enkele algemene krachtlijnen inzake de mededeling van persoonsgegevens uit het netwerk van de sociale zekerheid door instellingen van sociale zekerheid aan beroepshalve mandaathouders, op basis van een mandaat verstrekt door de betrokkene in het kader van een relatie, op te stellen.

B. BEHANDELING

<u>Bevoegdheid van het Informatieveiligheidscomité</u>

3. Het betreft een mededeling van persoonsgegevens door instellingen van sociale zekerheid aan beroepshalve mandaathouders die volgens artikel 15, § 1, van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale*

Zekerheid een beraadslaging van de kamer sociale zekerheid en gezondheid van het Informatieveiligheidscomité vergt.

Rechtmatigheid van de verwerking

4. Krachtens artikel 6 van de Verordening (EU) nr. 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 afgekort als AVG) is de verwerking van persoonsgegevens enkel rechtmatig indien en voor zover minstens één van de vermelde voorwaarden is vervuld.

5. De hogervermelde mededeling van persoonsgegevens is rechtmatig in die zin dat de betrokkene door de verstrekking van een mandaat zijn toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden en de beroepshalve mandaathouder aanvaard heeft om de voorwaarden vastgelegd in het mandaat na te leven. Er is dus op basis van het mandaat, dat juridisch kan worden gekwalificeerd als een overeenkomst tussen partijen, een rechtsbasis voor de verwerking in de zin van artikel 6, 1, eerste lid AVG.

Principes met betrekking tot de verwerking van persoonsgegevens

6. Volgens 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* moeten persoonsgegevens worden verzameld voor bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen ze vervolgens niet verder worden verwerkt op een wijze die met die doeleinden onverenigbaar is (beginsel van de doelbinding), moeten ze toereikend en ter zake dienend zijn en beperkt worden tot wat noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt (beginsel van de minimale gegevensverwerking), moeten ze worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de geldende doeleinden noodzakelijk is (beginsel van de opslagbeperking) en moeten ze zodanig worden verwerkt, met passende technische of organisatorische maatregelen, dat een passende beveiliging gewaarborgd is en dat ze onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (beginsel van de integriteit en de vertrouwelijkheid).

7. Gelet op de aard van de hem voorgelegde vraag kan het Informatieveiligheidscomité zich niet als dusdanig uitspreken over de naleving van de beginselen van doelbinding, minimale gegevensverwerking en opslagbeperking (de vraag heeft immers op een algemene wijze betrekking op de verwerking van niet-nader genoemde persoonsgegevens voor niet-nader genoemde doeleinden ten behoeve van beroepshalve mandaathouders).

8. Deze beraadslaging geldt bijgevolg uitsluitend als een algemeen kader dat steeds moet worden geëerbiedigd wanneer met een mandaat van de betrokkene zijn persoonsgegevens worden meegedeeld door instellingen van sociale zekerheid aan beroepshalve mandaathouders in het kader van een relatie maar doet voor het overige geenszins afbreuk aan de bevoegdheid van het Informatieveiligheidscomité om zich, per gevalssituatie, uit te spreken over dergelijke persoonsgegevensmededelingen.

9. In tegenstelling tot de uitwisselingen van persoonsgegevens tussen actoren van het netwerk van de sociale zekerheid, die gebaseerd zijn op door de overheid gekende relaties tussen de sociaal verzekerde en de instellingen van sociale zekerheid, die zijn vastgelegd in het verwijzingsrepertorium van de Kruispuntbank van de Sociale Zekerheid, zijn de relaties tussen de betrokkene en de beroepshalve mandaathouders niet gekend bij de overheid. Er is geen sprake van een verwijzingsrepertorium dat weergeeft dat een persoon klant is van een bepaalde bank, verzekeraar, makelaar, middenveldorganisatie,… Bovendien kunnen de relaties eenmalig of van zeer korte duur zijn (bijvoorbeeld indien een simulatie of offerte aangevraagd wordt door een prospectieve klant en die vervolgens niet resulteert in een langdurige relatie).

10. De enige die kan bevestigen dat een dergelijke relatie bestaat, is de betrokkene zelf. In het kader van de transparantie moet de betrokkene ook een zicht hebben op het gebruik dat beroepshalve mandaathouders van zijn persoonsgegevens maken. Er wordt voorzien in een eenvoudig middel waarmee de betrokkene een mandaat verstrekt aan een beroepshalve mandaathouder waarmee de betrokkene een relatie heeft voor het bekomen van zijn persoonsgegevens. De betrokkene kan op elk moment raadplegen welke actieve mandaten er geregistreerd zijn en deze desgewenst beëindigen.

11. Essentieel is dat de mededeling van persoonsgegevens wel degelijk gebeurt met een mandaat, verstrekt door de betrokkene en in het kader van een relatie. De mededeling met gebruik van een mandaat is te onderscheiden van de mededeling van persoonsgegevens die noodzakelijk zijn voor de uitvoering van wettelijk opgedragen taken.

12. De mededeling van persoonsgegevens in het kader van een relatie gebeurt met een gestandaardiseerd mandaat verstrekt door de betrokkene. De draagwijdte van elk (type) mandaat dat kan verstrekt worden, moet door het Informatieveiligheidscomité worden goedgekeurd, met een aparte beraadslaging waarin minstens vastgelegd wordt voor welke doeleinden de persoonsgegevens worden uitgewisseld, welke persoonsgegevens er worden uitgewisseld, hoelang de persoonsgegevens worden bijgehouden en hoelang een mandaat uiterlijk kan gelden, en daarenboven wordt gepreciseerd welke veiligheidsmaatregelen moeten worden genomen bij de verwerking van de gegevens. Het IVC zal zich bij de beraadslaging desgewenst baseren op een gegevensbeschermingseffectbeoordeling die wordt opgesteld door de instantie die het IVC verzoekt om een beraadslaging.

13. Het verstrekken van een mandaat gebeurt middels een geïnformeerde toestemming van de betrokkene. Dit houdt in dat de betrokkene bij het verlenen van het mandaat door het systeem – in eenvoudige taal – wordt geïnformeerd over de volgende aspecten: de draagwijdte van het mandaat, de identiteit van de beroepshalve mandaathouder die het mandaat ontvangt, de toepassing van een authenticatieniveau 400 of hoger binnen de *Federal Authentication Service* bij het verstrekken van het mandaat, de mogelijkheid om het mandaat in te trekken en het feit dat het verstrekken of intrekken van een mandaat wordt geregistreerd.

14. Vooraleer een mededeling van persoonsgegevens uit het netwerk van de sociale zekerheid door instellingen van sociale zekerheid aan een beroepshalve mandaathouder kan plaatsvinden, moet het mandaat worden gecontroleerd. Hiertoe zal de Kruispuntbank van de Sociale Zekerheid een verificatiesysteem ter beschikking stellen (zij is voor deze toepassing de verwerkingsverantwoordelijke).

15. Verwerking van persoonsgegevens waaruit ras, etnische afkomst, politieke opvatting, religieuze of levensbeschouwelijke overtuiging, lidmaatschap van een vakbond, seksueel gedrag of seksuele gerichtheid blijken, zijn verboden. Om die reden moet er bij de mededeling van persoonsgegevens aan derden steeds over gewaakt worden dat van een betrokkene geen bijzondere (gevoelige) persoonsgegevens aan de instelling van sociale zekerheid worden meegedeeld in de aanvraag (zonder dat dit afbreuk doet aan de controle inzake het bestaan van de relatie en het verstrekken van het mandaat). Bij wijze van voorbeeld kan worden verwezen naar het geval waarin een persoon die aangesloten is bij een ziekenfonds aan dat ziekenfonds een mandaat heeft verstrekt: het Nationaal Intermutualistisch College (de organisatie die optreedt als beheerder van het secundair netwerk van de ziekenfondsen) zal tussenkomen bij de verwerking van persoonsgegevens en waarborgen dat de bevoegde instelling van sociale zekerheid (de verstrekker van de gevraagde persoonsgegevens) de identiteit van het ziekenfonds niet kan achterhalen.

16. Omwille van deze vereiste kan de Kruispuntbank van de Sociale Zekerheid die bijzondere (gevoelige) informatie zelf niet opnemen in haar verificatiesysteem en zijn de instellingen van sociale zekerheid die – als beheersinstelling van een secundair netwerk van de sociale zekerheid – reeds over die informatie beschikken ertoe gehouden de nodige controles te verrichten. Die organisaties zijn de respectieve verwerkingsverantwoordelijken voor wat betreft de toepassing van hun verificatiesysteem.

17. Elk verificatiesysteem moet de hogervermelde functionaliteiten (zie de randnummers 12, 13 en 14) regelen. Het verificatiesysteem geeft toelating voor de mededeling van persoonsgegevens middels een token verstrekt aan de gebruiker of de toepassing van beroepshalve mandaathouder. Voor zover dat nodig is, wordt in de token de identiteit van de aanvrager gepseudonimiseerd. In de token wordt steeds informatie over het verificatiesysteem vermeld zodat de echtheid ervan kan gecontroleerd worden door de instelling van sociale zekerheid die de informatie verstrekt.

18. Om redenen van transparantie ontwikkelt de Kruispuntbank van de Sociale Zekerheid een systeem dat de burger een overzicht van alle actieve mandaten biedt. Hiervoor zal de organisatie zich beroepen op de verschillende verificatiesystemen, evenwel zonder dat daarom de informatie van de verificatiesystemen zelf aan haar wordt doorgegeven. Het overzicht van de actieve mandaten betreft de mandaten die, overeenkomstig de beraadslagingen van het Informatieveiligheidscomité, zijn verleend en elektronisch zijn opgeladen in het systeem, ongeacht de wijze waarop ze zijn verleend.

19. Elke toepassing van een beroepshalve mandaathouder die gebruik maakt van persoonsgegevens uit het netwerk van de sociale zekerheid en deze persoonsgegevens vervolgens, al dan niet verder verwerkt, aan de betrokkene ter beschikking stelt, moet voldoen aan dezelfde veiligheidsstandaarden als deze die gelden voor gelijkaardige toepassingen van de overheid. Inzake beveiligde login moet het veiligheidsniveau van de toepassing van de derde partij voldoen aan de hoogste eisen op het vlak van authenticatie (dat wil zeggen equivalent aan niveau 400 of hoger binnen de *Federal Authentication Service* wanneer de betrokkene die gegevens consulteert), zoals die reeds gelden voor de overheidstoepassingen *mycareer.be* en *mypension.be*.

20. De mededeling van persoonsgegevens door instellingen van sociale zekerheid moet geschieden met eerbiediging van de door het Algemeen Coördinatiecomité van de Kruispuntbank van de Sociale Zekerheid vastgestelde informatieveiligheidsnormen van

het netwerk van de sociale zekerheid (de zogenaamde "minimale veiligheidsnormen") en de verdere verwerking door de beroepshalve mandaathouder moet gebeuren met gelijkwaardige veiligheidswaarborgen.

21. De mededeling moet worden gelogd met een taakverdeling die het mogelijk maakt om de gehele ketting van de mededeling te reconstrueren. Dit beginsel houdt onder meer in dat de betrokken instanties bij de elektronische dienstverlening duidelijke afspraken maken over de volgende aspecten.

- wie welke authenticaties, verificaties en controles verricht aan de hand van welke middelen en daarvoor verantwoordelijk en aansprakelijk is;
- hoe tussen de betrokken instanties de resultaten van de verrichte authenticaties, verificaties en controles op een veilige wijze elektronisch worden uitgewisseld;
- wie welke loggings bijhoudt;
- hoe ervoor wordt gezorgd dat bij onderzoek – hetzij op eigen initiatief van de derde instantie, hetzij door een controle-orgaan naar aanleiding van een klacht of een vraag van de betrokkene – een volledige *tracing* ("*wie, wat, waar, wanneer, waarom?*") kan geschieden ("*welke persoon heeft welke dienst/transactie met betrekking tot welke persoon op welk ogenblik, via welk kanaal en voor welk doeleinde gebruikt?*").

22. Die afspraken mogen niet leiden tot het onnodig bekendmaken van bijzondere (gevoelige) informatie zoals bedoeld in artikel 9 van 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* bij een instelling van de sociale zekerheid, zoals bv. het lidmaatschap van een vakbond.

23. De organisatie of onderneming die als beroepshalve mandaathouder gebruik wil maken van de hiervoor bedoelde mogelijkheden via het aanroepen vanuit een toepassing van een API (Application Programming Interface) zal vóór een eerste mededeling van persoonsgegevens uitdrukkelijk en schriftelijk de algemene gebruiksvoorwaarden die zijn opgesomd in de *Circle of Trust* (COT) en de specifiek voor een bepaalde gevalssituatie en persoonsgegevensset geldende gebruiksvoorwaarden (zoals onder meer bepaald in de specifieke beraadslaging van het Informatieveiligheidscomité) moeten aanvaarden. Met de implementatie van een dergelijke COT verbindt de organisatie of onderneming er zich toe om zelf de nodige maatregelen te treffen opdat het netwerk van de sociale zekerheid er te allen tijde op kan vertrouwen dat alleen rechtmatige gebruikers toegang tot de beschikbare persoonsgegevens hebben. Dan moet dat aspect niet meer worden afgedwongen in de toepassingen van de actoren van de sociale zekerheid. Die gaan dan enkel na of de organisatie als dusdanig wel degelijk gemachtigd is om persoonsgegevens te verwerken in het voormeld kader. De organisatie moet er dan zelf voor zorgen dat de persoonsgegevens in haar eigen schoot enkel op een rechtmatige wijze gebruikt worden.

24. Wanneer een beroepshalve mandaathouder enkel de webtoepassing ter beschikking gesteld door de bevoegde instelling van sociale zekerheid wenst te gebruiken, dient de CoT niet ondertekend te worden. De individuele gebruiker dient zich te authentiseren met een authenticatiemiddel van authenticatieniveau 400 of hoger binnen de *Federal Authentication Service*. Bovendien moet de individuele gebruiker gekend zijn in het systeem van gebruikersbeheer van organisaties, ondernemingen en beroepsbeoefenaars

en aangeven in die rol op te treden. De beroepshalve mandaathouder aanvaardt, in het geval van een organisatie of een onderneming via de individuele gebruiker die voor rekening van de onderneming of organisatie optreedt, voorafgaand aan het gebruik van de toepassing de algemene gebruiksvoorwaarden en de specifiek voor een bepaalde gevalssituatie en persoonsgegevensset geldende gebruiksvoorwaarden (zoals onder meer bepaald in de specifieke beraadslaging van het Informatieveiligheidscomité). Via die aanvaarding wordt de beroepshalve mandaathouder verantwoordelijk voor de correcte uitvoering van het mandaat en de correcte verwerking van de persoonsgegevens van de betrokkene.

25. De beroepshalve mandaathouder houdt zich ter beschikking voor een eventuele audit door de functionaris voor gegevensbescherming van de instellingen van sociale zekerheid die de authentieke bron van de persoonsgegevens in kwestie zijn alsook door de bevoegde toezichthoudende autoriteit.

26. De beroepshalve mandaathouder zal, bij de dienstverlening aan een betrokkene, handelen vanuit het belang van de betrokkene. Dit houdt in dat beroepshalve mandaathouder nooit om een mandaat zal verzoeken of zichzelf een mandaat zal verstrekken indien dat niet noodzakelijk is voor de afgesproken dienstverlening.

27. Bij de verwerking van de persoonsgegevens wordt rekening gehouden met de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid* en elke andere regelgeving tot bescherming van de persoonlijke levenssfeer, in het bijzonder 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* en de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*.

Om deze redenen, besluit

de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité

dat de mededeling van persoonsgegevens door instellingen van sociale zekerheid aan een beroepshalve mandaathouder met mandaat van de betrokkene, zoals beschreven in deze beraadslaging, steeds moet geschieden volgens de bepalingen van deze beraadslaging.

Deze beraadslaging geldt als een algemeen kader dat steeds moet worden geëerbiedigd wanneer persoonsgegevens uit het netwerk van sociale zekerheid door instellingen van sociale zekerheid met een mandaat van de betrokkene worden meegedeeld aan een beroepshalve mandaathouder in het kader van een relatie, maar doet op geen enkele wijze afbreuk aan de bevoegdheid van het Informatieveiligheidscomité om zich, geval per geval, uit te spreken over dergelijke persoonsgegevensmededelingen.

De beraadslaging nr. 19/004 van 15 januari 2019 van de kamer sociale zekerheid en gezondheid van het Informatieveiligheidscomité wordt opgeheven.

Deze beraadslaging treedt in werking op 18 december 2024.

Michel DENEYER
Voorzitter

De zetel van de kamer sociale zekerheid en gezondheid van het Informatieveiligheidscomité is gevestigd in de kantoren van de Kruispuntbank van de Sociale Zekerheid, op het volgende adres: Willebroekkaai 38, 1000 Brussel.