Informatieveiligheidscomité
Kamer sociale zekerheid en gezondheid

IVC/KSZG/19/050

BERAADSLAGING NR. 19/032 VAN 5 FEBRUARI 2019 OVER HET GEBRUIK VAN PERSOONSGEGEVENS UIT HET NETWERK VAN DE SOCIALE ZEKERHEID DOOR DE KREDIETINSTELLINGEN EN DE AANBIEDERS VAN FINANCIËLE PRODUCTEN EN DIENSTEN (EN HUN RESPECTIEVE KANTOREN EN FILIALEN) TEN BEHOEVE VAN DE BETROKKEN (BESTAANDE EN PROSPECTIEVE) KLANTEN

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 wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, in het bijzonder artikel 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 95/46/EG*, in het bijzonder artikel 97;

Gelet op de aanvraag van de vereniging zonder winstoogmerk SIGEDIS;

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

Gelet op het verslag van de heer Bart Viaene.

A. ONDERWERP

1. Bij beraadslaging nr. 19/004 van 15 januari 2019 besliste de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité, naar aanleiding van een vraag van de vereniging zonder winstoogmerk SIGEDIS, dat de verwerking van persoonsgegevens uit het netwerk van de sociale zekerheid door de betrokkene zelf, door middel van toepassingen die door een derde partij worden aangeboden, steeds moet geschieden volgens de bepalingen van die beraadslaging, die geldt als een algemeen kader dat steeds moet worden geëerbiedigd maar geen afbreuk doet aan de bevoegdheid van het informatieveiligheidscomité om zich, geval per geval, over dergelijke verwerkingen van persoonsgegevens uit te spreken. Dat betekent dat elke organisatie (desgevallend een groep van organisaties) die een toepassing ontwikkelt om de burger de mogelijkheid te bieden om zijn persoonsgegevens te raadplegen in een bepaalde bron van het netwerk van de sociale zekerheid, al dan niet samen met

persoonsgegevens uit andere bronnen en al dan niet met bijkomende dienstverlening, daartoe vooraf een beraadslaging van het informatieveiligheidscomité moet bekomen.

2. Deze beraadslaging heeft betrekking op het gebruik van persoonsgegevens uit het netwerk van de sociale zekerheid (in het bijzonder persoonsgegevens van de vereniging zonder winstoogmerk SIGEDIS) door de kredietinstellingen met vergunning door de Nationale Bank van België (zie *https://www.nbb.be/nl/financieel-toezicht/prudentieel-toezicht/toezichtsdomeinen/kredietinstellingen/lijsten-4*), de aanbieders van diverse financiële producten en diensten met vergunning door de Nationale Bank van België of de FSMA (zie *https://www.fsma.be/nl/welke-dienstverleners-mogen-u-financiele-producten-en-diensten-aanbieden* en *https://www.fsma.be/nl/content/bank-en-beleggingsdiensten*), en hun respectieve kantoren en filialen. Zij willen overgaan tot het verwerken van persoonsgegevens van bestaande klanten en prospectieve klanten, die daartoe hun toestemming moeten geven, met het oog op het aanvullen van de gegevens die ze zelf reeds ter consultatie aanbieden, het verstrekken van financieel advies en het formuleren van passende commerciële voorstellen (het betreft personen die al een contractuele relatie met de dienstenaanbieder hebben of gebruik willen maken van een vrijblijvend, eventueel precontractueel aanbod van de dienstenaanbieder). Het initiatief gaat uit van de betrokkene zelf: hij kiest autonoom de dienstenaanbieder en beslist vervolgens om al dan niet gebruik te maken van de voorgestelde diensten die met de verwerking van de persoonsgegevens uit het netwerk van de sociale zekerheid samenhangen.

3. De gevraagde verwerking heeft betrekking op persoonsgegevens die de burger zelf al kan raadplegen in het onderdeel “mijn aanvullend pensioen” van mypension.be. Het gaat, per bestaande combinatie van pensioeninstelling, inrichter en pensioenplan, om de aanvullende pensioenrekening met daarop de laatst gekende verworven reserve, de verworven prestatie, de verwachte prestatie, met telkens de bijhorende berekenings- en evaluatiedatums, het financieringsniveau, de eventuele overlijdensdekkingen en de eventuele gebeurtenissen die de voormelde waarden beïnvloeden (zoals een gedeeltelijke uitbetaling).

Globale inlichtingen over alle aanvullende pensioenen van de betrokkene (aangesloten als werknemer en/of zelfstandige): de evaluatiedatum (het jaar waarop de inlichtingen betrekking hebben), de totale reserve (het bedrag dat inmiddels gespaard werd voor alle aanvullende pensioenen samen), de totale maandelijkse indicatieve rente (het pensioenbedrag dat de totale reserve bij benadering zou opleveren voor de aangeslotene), de totale overlijdensdekking (het bedrag dat de begunstigden zouden ontvangen bij overlijden van de aangeslotene), de totale aanvullende verzekering tegen het risico op een ongeval (de aanduiding dat de begunstigden al dan niet een bijkomende tegemoetkoming ontvangen bij het overlijden van de aangeslotene door een ongeval) en de totale bijkomende wezenrente (de aanduiding dat de kinderen al dan niet een bijkomende wezenrente ontvangen bij het overlijden van de aangeslotene).

Onderscheid tussen werknemers en zelfstandigen: de totale pensioenreserve als werknemer, de totale pensioenreserve als zelfstandige, de totale overlijdensdekking als werknemer, de totale overlijdensdekking als zelfstandige, de totale aanvullende verzekering tegen het risico op een ongeval als werknemer, de totale aanvullende verzekering tegen het risico op een ongeval als zelfstandige, de totale bijkomende wezenrente als werknemer en de totale bijkomende wezenrente als zelfstandige.

Inlichtingen over het extern pensioenplan (beheerd door een extern pensioenorgaan): het ondernemingsnummer en de sociale benaming van de inrichter, het ondernemingsnummer en de sociale benaming van de pensioeninstelling (een pensioenfonds of een verzekeraar), het type pensioenplan, de status van de aansluiting ("actief" of "slapend"), de pensioenreserve (op het niveau van het pensioenplan), de aard en de datum van de specifieke gebeurtenis die die zich tijdens het evaluatiejaar heeft voorgedaan en de aansluitingsdatum.

Inlichtingen over de pensioenrekening: de pensioenreserve op het niveau van de rekening, de overlijdensdekking op het niveau van de rekening, de minimumgarantie op het niveau van de rekening (het bedrag dat ten opzichte van de aangeslotene wordt gewaarborgd bij diens pensionering of uitstap), het actueel financieringsniveau op het niveau van de rekening (de bekostigingsdraagkracht van de pensioeninstelling) en de verwachte prestatie op het niveau van de rekening.

Inlichtingen over de pensioenrekening – dekking van het type "leven": het type van dekking, de oorsprong van de bijdragen (werknemersbijdragen, werkgeversbijdragen, persoonlijke bijdragen of bijdragen van de vennootschap), de formule voor de berekening van de reserves, de basis voor de kapitalisatie van de reserves bij de verzekeraar, de basis voor de kapitalisatie van de reserves bij het pensioenfonds, de verworven reserves, de minimumgarantie, het actueel financieringsniveau, de verworven prestatie en de verwachte prestatie.

Inlichtingen over de pensioenrekening – dekking van het type "overlijden": het type van dekking (de aanduiding dat het luik van de pensioenrekening betrekking heeft op een dekking in geval van overlijden van de aangeslotene vóór diens pensioen), de overlijdensdekking (het bedrag dat de begunstigden zouden ontvangen bij overlijden van de aangeslotene), de aanduiding van de aanvullende verzekering tegen het risico op een ongeval en de aanduiding van de bijkomende wezenrente.

Inlichtingen over het intern pensioenplan (niet beheerd door een extern pensioenorgaan): het ondernemingsnummer en de sociale benaming van de inrichter, het type pensioenplan, de datum van de geldigheid van het pensioenplan, de datum van de inwerkingtreding van het pensioenplan, de pensioenbelofte (de aanduiding dat al dan niet een pensioen in het kader van een intern pensioenplan is beloofd) en de beloofde overlijdensdekking (de aanduiding dat al dan niet een overlijdensdekking in het kader van een intern pensioenplan is beloofd).

4. Het raadplegen en verwerken van deze persoonsgegevens is aan een dubbele voorwaarde onderworpen.

Enerzijds moet er een afspraak zijn hierover tussen de betrokkene en de kredietinstellingen en de aanbieders van financiële producten en diensten (alsook hun kantoren en filialen). De afspraak regelt enkel de relatie tussen die beide partijen en bepaalt onder andere de finaliteit en de duurtijd van de verwerking. Bij het raadplegen en bijwerken van de persoonsgegevens controleren de kredietinstellingen en de aanbieders van financiële producten en diensten (alsook hun kantoren en filialen) steeds of de toestemming van de (bestaande en prospectieve) klanten wel degelijk nog van toepassing is. Die toestemming is geldig voor de

met de betrokkene afgesproken periode of tot aan de uitdrukkelijke intrekking ervan door de betrokkene (in dat geval vervalt meteen de toegang tot de gevraagde persoonsgegevens).

Anderzijds is er relatie Sigedis-Burger-Gegevensverwerker. Deze relatie is niet contractueel van aard en wordt eerst en vooral geregeld door de machtiging nr. 19/004 van 15 januari 2019 (waarvan deze machtigingsaanvraag de precisering is). Die machtiging bepaalt dat de gegevensmededeling door Sigedis geoorloofd is indien en voor zolang aan de eerste voorwaarde (het bestaan van een relatie tussen de burger en de instelling of aanbieder) voldaan is, en indien de burger het bestaan van die relatie heeft bevestigd (volgens de modaliteiten bepaald in dit document). Om veiligheidsredenen heeft de toegang tot de gegevens die hieruit resulteert een maximale geldigheidsduur van twee jaar.

De aanvrager merkt verder op dat de persoonsgegevens over de aanvullende pensioenen – behalve door de toepassingen van de instellingen en aanbieders - enkel zouden worden verwerkt door de financiële adviseurs (voor het verstrekken van financieel advies aan de betrokkenen) en door de medewerkers van de centrale diensten (voor het ondersteunen van de commerciële activiteiten van de organisatie).

B. BEHANDELING

5. Het betreft een mededeling van persoonsgegevens door een instelling van sociale zekerheid (de vereniging zonder winstoogmerk SIGEDIS) aan derden (de kredietinstellingen, de aanbieders van financiële producten en diensten en hun kantoren en filialen), 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.

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 opslagbeperking) en moeten ze met passende technische of organisatorische maatregelen zodanig worden verwerkt 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 integriteit en vertrouwelijkheid).

<u>doelbinding</u>

7. De mededeling beoogt een gerechtvaardigd doeleinde, namelijk het verstrekken van financieel advies en het formuleren van passende commerciële voorstellen aan bestaande klanten en prospectieve klanten, voor zover die daartoe vooraf hun toestemming hebben gegeven. Het informatieveiligheidscomité stelt vast dat de kredietinstellingen en de aanbieders van financiële producten en diensten (evenals hun kantoren en filialen) – mits toestemming van de betrokkenen – gebruik willen maken van welbepaalde persoonsgegevens uit het netwerk van de sociale zekerheid om hun diensten op een efficiënte wijze te kunnen aanbieden. De verwerking van persoonsgegevens geschiedt bijgevolg steeds in het kader van een vastgestelde relatie tussen de betrokkene en de bestemmeling.

8. De raadpleging van de persoonsgegevens moet onverkort gebeuren op initiatief van de betrokkene zelf en, wat de relatie met de instelling of aanbieder betreft, met diens toestemming, enerzijds, en, wat Sigedis betreft, na diens bevestiging van het bestaan van die relatie (zie verder), anderzijds. De kredietinstellingen en de aanbieders van financiële producten en diensten (en hun kantoren en filialen) spreken expliciet met de betrokkene de draagwijdte van hun tussenkomst af en stellen hem in kennis van hun mogelijke interventies. Zij bewaren de bewijzen van de toestemming van de betrokkene en houden die in voorkomend geval ter inzage van de vereniging zonder winstoogmerk SIGEDIS, de Kruispuntbank van de Sociale Zekerheid en het informatieveiligheidscomité. Zij verwerken de meegedeelde gegevens enkel voor het verstrekken van financieel advies en het formuleren van passende commerciële voorstellen aan de individuele betrokkene. Indien de individuele betrokkene aangeeft niet in te gaan op de commerciële voorstellen, mogen de meegedeelde gegevens op basis van deze beraadslaging niet verder worden verwerkt.

minimale gegevensverwerking

9. De persoonsgegevens zijn, uitgaande van dat doeleinde, relevant en niet overmatig. Ze blijven beperkt tot inlichtingen over de aanvullende pensioenrekeningen van de betrokkene, met vermelding van de laatst gekende verworven reserve, de verworven prestatie, de verwachte prestatie, de bijhorende berekenings- en evaluatiedatums, het financieringsniveau en de eventuele overlijdensdekkingen en pertinente gebeurtenissen.

10. Die persoonsgegevens moeten de gemachtigde organisaties in staat stellen om aan hun bestaande en prospectieve klanten correcte informatie te verschaffen over hun aanvullende pensioenen en om gepaste financiële voorstellen te formuleren op basis van correcte en volledige informatie over hun financiële situatie, steeds binnen de lijnen van de toestemming die zij hebben verleend.

opslagbeperking

11. De kredietinstellingen, de aanbieders van financiële producten en diensten en hun kantoren en filialen bewaren de persoonsgegevens in voorkomend geval niet langer dan nodig voor de geldende doeleinden. Als de persoonsgegevens niet langer dienstig zijn voor het verstrekken van financieel advies en het formuleren van passende commerciële voorstellen moeten ze worden vernietigd.

12. De persoonsgegevens over de aanvullende pensioenen, geraadpleegd met, wat de instellingen en aanbieders betreft, de toestemming van de betrokkene, en na, wat Sigedis betreft, de bevestiging door de betrokkene van die relatie met de instelling of aanbieder, worden in geen geval bijgehouden na het verstrijken van de geldigheid van die toestemming (ofwel door het aflopen van afgesproken termijn, ofwel door het intrekken van de toestemming door de betrokkene zelf).

Indien persoonsgegevens worden verwerkt van prospectieve klanten, waarbij uiteindelijk geen contractuele relatie met de dienstenaanbieder tot stand komt, mogen de persoonsgegevens evenwel maximaal één maand na het precontractueel aanbod van de dienstenaanbieder worden verwerkt.

integriteit en vertrouwelijkheid

13. De door de partijen gebruikte toepassing moet voldoen aan dezelfde veiligheidsstandaarden als deze die gelden voor gelijkaardige toepassingen van de overheid. Inzake beveiligde login moet het veiligheidsniveau van de toepassing voldoen aan de hoogste eisen op het vlak van authenticatie (dat wil zeggen niveau 400 of hoger binnen de Federal Authentication Service), zoals die reeds gelden voor de overheidstoepassingen *mycareer.be* en *mypension.be*. De uitwisseling van de persoonsgegevens uit het netwerk van de sociale zekerheid moet voorts beveiligd en gestructureerd geschieden, tussen servers met de nodige certificaten, zoals dat gebeurt binnen de sociale zekerheid.

14. De partijen treffen organisatorische maatregelen waardoor de persoonsgegevens enkel kunnen worden verwerkt door de toepassing, de financiële adviseurs (voor het verstrekken van financieel advies aan de betrokkenen) en de medewerkers van de centrale diensten (voor het ondersteunen van de commerciële activiteiten van de organisatie) die daartoe speciaal zijn aangeduid en er zich toe verbonden hebben om de veiligheid en de vertrouwelijkheid van de informatie te waarborgen. Ze houden een permanent geactualiseerde lijst van die personen ter beschikking.

15. De partijen implementeren een systeem waarbij de betrokkene (bestaande klant of prospectieve klant) eerst via de technologie van *Open Authorization*, te kennen geeft dat er tussen hem en de derde een relatie bestaat. Hier kan hij ook de actieve relaties raadplegen en desgewenst beëindigen. Bovendien krijgt hij op het door hem geregistreerde mailadres een waarschuwing over het gebruik van een toegang tot zijn persoonsgegevens door de toepassing. Dat stelt hem in staat te reageren als de toegang hem verdacht lijkt en niet overeenstemt met de relaties die hij met derde partijen heeft.

16. Om de naleving van het voorgaande te waarborgen, doen de partijen een beroep op een functionaris voor gegevensbescherming, zoals bedoeld in 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*. Ze delen zijn identiteit mee aan het informatieveiligheidscomité.

17. Kredietinstellingen en aanbieders van financiële producten en diensten (en hun kantoren en filialen) die zich willen beroepen op deze beraadslaging, moeten er zich vooraf uitdrukkelijk ten opzichte van het informatieveiligheidscomité toe verbinden om te waarborgen dat de verwerkingen van de persoonsgegevens van de vereniging zonder winstoogmerk SIGEDIS door de medewerkers die daartoe om functionele redenen gemachtigd zijn conform zijn aan de voorwaarden die worden vermeld in deze beraadslaging (in het bijzonder deze bedoeld in de punten 13-16) en in de beraadslaging nr. 19/004 van 15 januari 2019 (in het bijzonder deze bedoeld in de punten 8-13).

18. Ze delen daarbij de identiteit van hun functionaris voor gegevensbescherming mee en voegen een ingevulde evaluatievragenlijst toe met betrekking tot de referentiemaatregelen inzake de informatieveiligheid die van toepassing zijn op elke verwerking van persoonsgegevens. Die vragenlijst wordt waarheidsgetrouw ingevuld en moet de mogelijkheid bieden om het informatieveiligheidsbeleid te beoordelen.

19. Deze beraadslaging treedt pas in werking ten opzichte van een geïnteresseerde kredietinstelling of aanbieder van financiële producten en diensten (en de respectieve kantoren en filialen) voor zover de organisatie daarvan uitdrukkelijk door het informatieveiligheidscomité in kennis wordt gesteld.

20. Ten slotte wordt bij de verwerking van de persoonsgegevens rekening gehouden met de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid* en elke andere regelgevende bepaling 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 verwerking van persoonsgegevens uit het netwerk van de sociale zekerheid door de kredietinstellingen, de aanbieders van diverse financiële producten en diensten en hun respectieve kantoren en filialen voor het verstrekken van financieel advies en het formuleren van passende commerciële voorstellen aan bestaande klanten en prospectieve klanten, zoals in deze beraadslaging beschreven, toegestaan is mits wordt voldaan aan de vastgestelde maatregelen ter waarborging van de gegevensbescherming, in het bijzonder de maatregelen op het vlak van doelbinding, minimale gegevensverwerking, opslagbeperking en informatieveiligheid, alsook aan de maatregelen bedoeld in de beraadslaging nr. 19/004 van 15 januari 2019.

Elke concrete kredietinstelling of aanbieder van financiële producten en diensten die zich wil beroepen op deze beraadslaging, moet er zich vooraf uitdrukkelijk ten opzichte van het informatieveiligheidscomité toe verbinden om te waarborgen dat de verwerkingen van de persoonsgegevens in overeenstemming zijn met de voorwaarden die worden vermeld in deze beraadslaging en in de beraadslaging nr. 19/004 van 15 januari 2019.

Bart VIAENE

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.