Informatieveiligheidscomité
Kamer sociale zekerheid en gezondheid

IVC/KSZG/19/004

BERAADSLAGING NR. 19/004 VAN 15 JANUARI 2019 OVER HET GEBRUIK VAN PERSOONSGEGEVENS UIT HET NETWERK VAN DE SOCIALE ZEKERHEID DOOR DE BETROKKENE ZELF DOOR MIDDEL VAN EEN TOEPASSING VAN EEN DERDE PRIVATE PARTIJ

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. De vereniging zonder winstoogmerk SIGEDIS stelt vast dat personen het recht hebben om te weten welke persoonsgegevens zij over hen bijhoudt en biedt hun aldus een beter inzicht in hun professionele en financiële situatie aan de hand van de beveiligde online toepassingen *mycareer.be* en *mypension.be*. Zij is echter van oordeel dat personen niet verplicht kunnen worden om hun recht op informatie uitsluitend uit te oefenen via de door de overheid gekozen en ontwikkelde toepassingen. Volgens het principe van de *data portability*, geregeld door 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*, hebben personen overigens het recht om hun persoonsgegevens onder bepaalde voorwaarden te laten overdragen aan een partner van hun keuze.

2. Diverse derden blijken momenteel bezig met de ontwikkeling van toepassingen die de burger (veelal, maar niet uitsluitend, de klant of de potentiële klant) de mogelijkheid geven om zijn gegevens te raadplegen in een bepaalde bron, al dan niet samen met gegevens uit andere bronnen en al dan niet met bijkomende dienstverlening, die niet noodzakelijk van publieke aard is, zoals verstrekking van financieel advies of portefeuillebeheer. De gebruikssituaties kunnen volgens SIGEDIS zeer verscheiden zijn. Te denken valt aan de volgende gevallen (niet-limitatieve opsomming).

- een persoon wil de stand van zaken van de opbouw van zijn aanvullend pensioen toegevoegd zien aan het globaal overzicht van zijn financiële portefeuille dat de bank hem aanbiedt;

- een persoon wil gebruik maken van een simulator voor loopbaanoptimalisatie zonder zelf zijn loopbaangegevens te moeten ingeven of ze per mail of op papier aan een medewerker van de dienstenaanbieder te moeten bezorgen;

- een persoon wil een financieel product aankopen en zijn bank moet daartoe, onder meer op basis van de reserves van zijn aanvullend pensioen, een beleggersprofiel opstellen en regelmatig actualiseren, in functie van de evolutie van de financiële toestand;

- een persoon wil een op maat gemaakte analyse van zijn financiële situatie die rekening houdt met zijn reële pensioenopbouw in de eerste en de tweede pijler en met zijn reëel fiscaal of sociaal inkomen en dus moeten zijn gegevens eenmalig opgeladen worden;

- een persoon wil regelmatig, in functie van de periodieke wijziging van zijn financiële situatie, een update van zijn financiële analyse zodat hem beleggingsopties kunnen geboden worden wanneer die door de gewijzigde situatie alsnog interessant worden;

- een persoon wil het overzicht van zijn loopbaan kunnen raadplegen in de vertrouwde toepassing van zijn eigen middenveldorganisatie, eerder dan in de toepassing van de sociale zekerheid (mycareer.be);

- een persoon wil het Europees platform Find Your Pension gebruiken om een globaal overzicht te hebben van de pensioenaanspraken die hij inmiddels heeft opgebouwd in de verschillende landen waar hij gewerkt heeft, waaronder België.

3. Naargelang de situatie kan de toepassing van de derde de visualisatie van de eigen gegevens van de betrokkene dus combineren met een specifieke verwerking (zoals bij een simulatie). In elk van de situaties kan de betrokkene, zoals hij dat ook kan met de overheidstoepassingen, besluiten om zijn gegevens lokaal, in de toepassing van de derde of op het apparaat dat hij gebruikt om de toepassing te gebruiken, al dan niet op te slaan. Voorts kan het gaan om een eenmalig gebruik van de gegevens (visualisatie, simulatie,…) maar er kan ook een langdurige relatie bestaan tussen de betrokkene en de (toepassing van) de derde (zoals in een relatie tussen bank en klant). In dat laatste geval kan het zelfs voorkomen dat de toepassing regelmatig de gegevens actualiseert, ook op momenten dat de betrokkene zelf niet ingelogd is, om het aanbod van begeleidende diensten te actualiseren en de betrokkene te informeren over het feit dat zich nieuwe mogelijkheden aandienen.

4. SIGEDIS wil het mogelijk maken dat de burger zijn eigen gegevens op een veilige wijze raadpleegt of laat verwerken in toepassingen van door hemzelf gekozen private dienstenaanbieders, zonder dat de integriteit van zijn persoonlijke levenssfeer in het gedrang komt. Zij verzoekt het informatieveiligheidscomité bijgevolg – niet enkel voor zichzelf maar ook voor alle andere instellingen van sociale zekerheid – om de beginselen vast te stellen die gelden bij het overmaken van gegevens van een sociaal verzekerde die te raadplegen zijn aan de hand van een door een instelling van sociale zekerheid ontwikkelde toepassing of het voorwerp van het inzagerecht uitmaken aan een derde partij die toepassingen of diensten aanbiedt aan diezelfde sociaal verzekerde. Onverminderd de toepassing van artikel 15, § 1, van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid* zouden die beginselen moeten worden gerespecteerd telkens vanuit het netwerk van de sociale zekerheid gegevens van een sociaal verzekerde worden meegedeeld aan een derde partij die aan de betrokkene toepassingen of diensten aanbiedt.

B. BEHANDELING

5. Het betreft een mededeling van persoonsgegevens door instellingen van sociale zekerheid (waaronder SIGEDIS) aan derden (private dienstenaanbieders), 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).

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 niet-nader genoemde dienstenaanbieders).

Deze beraadslaging geldt bijgevolg uitsluitend als een algemeen kader dat steeds moet worden geëerbiedigd wanneer gegevens uit het netwerk van de sociale zekerheid worden

meegedeeld aan een derde partij die aan de betrokkene toepassingen of diensten aanbiedt maar doet voor het overige geenszins afbreuk aan de bevoegdheid van het informatieveiligheidscomité om zich, geval per geval, uit te spreken over dergelijke gegevensmededelingen. Per groep van gelijkaardige organisaties die hetzelfde doel nastreven, moet het informatieveiligheidscomité dus afzonderlijk beoordelen welke gegevens zij in dat algemeen kader (volgens de geldende spelregels) mogen verwerken.

8. Essentieel is dat, ongeacht de instantie die de toepassing aanbiedt en ongeacht het ruimer dienstenkader dat aangeboden wordt, de raadpleging wel degelijk gebeurt op initiatief van de betrokkene. Bij de verwerking van de persoonsgegevens gebeurt elke handeling op initiatief van de persoon in kwestie en met zijn toestemming (bijvoorbeeld aan de hand van een pop up met bewijs van het aanklikken door de burger na een voldoende sterke authenticatie). De derde partij spreekt expliciet met de betrokkene af wat de draagwijdte van de tussenkomst is en stelt de betrokkene in kennis van zijn mogelijke interventies. De betrokkene heeft de volledige vrijheid om al dan niet in te stemmen en kan zijn instemming ook intrekken of wijzigen. De derde partij bewaart alle nodige bewijzen van de toestemming van de betrokkene en houdt ze ter inzage van de authentieke bronnen van de gegevens.

Het weze overigens opgemerkt dat de verwerking van persoonsgegevens in dat algemeen kader zijn rechtmatigheid niet put uit de toestemming van de betrokkene maar uit deze beraadslaging van het informatieveiligheidscomité, die volgens artikel 46, § 2, van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid* een algemene bindende draagwijdte heeft tussen partijen en jegens derden en niet in strijd mag zijn met hogere rechtsnormen.

9. Elke toepassing van een derde partij 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 niveau 400 of hoger binnen de Federal Authentication Service), zoals die reeds gelden voor de overheidstoepassingen *mycareer.be* en *mypension.be*.

10. 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.

11. In tegenstelling tot bij 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 burger en de derde partij in de hogervermelde situaties 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). De enige die kan bevestigen dat een dergelijke relatie bestaat, is de burger zelf. In het kader van de transparantie moet de burger ook een zicht hebben op het gebruik dat derde partijen van zijn gegevens maken. Daarom moet de burger eerst een waarschuwing krijgen op het door hemzelf geregistreerde mailadres (bijvoorbeeld in zijn eBox) over het feit dat een toepassing gebruik maakt van een toegang tot zijn gegevens. Dit is ondertussen een gangbare praktijk in tal van beveiligde private toepassingen, zoals LinkedIn, Facebook en Google-account. Op die manier kan de burger meteen reageren indien de toegang hem verdacht lijkt en niet overeenstemt met de relaties die hij heeft met derde partijen. Verder wordt voorzien in een eenvoudig middel waarmee de burger te kennen kan geven dat er tussen hem en de derde een relatie bestaat, via de technologie van *Open Authorization*. Hij kan ook op elk moment raadplegen welke actieve relaties er bestaan en deze desgewenst beëindigen, bijvoorbeeld als reactie op de eerder vermelde waarschuwing die hij per mail ontvangt.

12. De derde partij die gebruik wil maken van de hiervoor bedoelde mogelijkheden, zal vóór een eerste uitwisseling van gegevens uitdrukkelijk en schriftelijk de gebruiksvoorwaarden aanvaarden. Vermits elke gegevensaanbieder bijkomende restricties kan opleggen, is een document per gegevensset en per gegevensaanbieder aangewezen.

13. De derde 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 gegevens in kwestie zijn.

14. 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 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 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, 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 gegevens uit het netwerk van de sociale zekerheid worden meegedeeld aan een derde partij die aan de betrokkene toepassingen of diensten aanbiedt maar doet op geen enkele wijze afbreuk aan de bevoegdheid van het informatieveiligheidscomité om zich, geval per geval, uit te spreken over dergelijke gegevensmededelingen.

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.