Informatieveiligheidscomité
Kamer sociale zekerheid en gezondheid

IVC/KSZG/23/444

BERAADSLAGING NR. 17/020 VAN 7 MAART 2017, GEWIJZIGD OP 6 JUNI 2017, OP 14 JANUARI 2020, OP 6 DECEMBER 2022, OP 7 MAART 2023 EN OP 5 DECEMBER 2023, OVER DE MEDEDELING VAN GEPSEUDONIMISEERDE PERSOONSGEGEVENS DOOR DE KRUISPUNTBANK VAN DE SOCIALE ZEKERHEID AAN DE FEDERALE OVERHEIDSDIENST SOCIALE ZEKERHEID VOOR HET UPDATEN VAN HET MICROSIMULATIEMODEL VOOR DE SOCIALE ZEKERHEID (MIMOSIS)

Gelet op de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*, in het bijzonder artikel 5 en artikel 15, § 1, eerste lid;

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 vragen van de federale overheidsdienst Sociale Zekerheid;

Gelet op de rapporten van de Kruispuntbank van de Sociale Zekerheid;

Gelet op het verslag van de heer Bart Viaene.

A. ONDERWERP VAN DE AANVRAAG

1. Het destijds bevoegde sectoraal comité van de sociale zekerheid en van de gezondheid heeft meerdere machtigingen verleend met betrekking tot de verwerking van persoonsgegevens door de federale overheidsdienst Sociale Zekerheid in het kader van de exploitatie van het microsimulatiemodel voor de sociale zekerheid (MIMOSIS – *microsimulation model for Belgian social insurance systems*), namelijk bij beraadslaging nr. 07/21 van 8 mei 2007 (meermaals gewijzigd), bij beraadslaging nr. 09/33 van 2 juni 2009 en bij beraadslaging nr. 11/22 van 1 maart 2011. De voorliggende aanvraag beoogt de verwerking van nieuwe persoonsgegevens uit het netwerk van de sociale zekerheid voor het updaten van het microsimulatiemodel voor de sociale zekerheid (omdat er ondertussen ook persoonsgegevens van *recentere jaren* en uit *meer bronnen* beschikbaar zijn).

2. Aldus zouden aangaande de betrokkenen (dat zijn ongeveer vierhonderdduizend eigenlijke steekproefpersonen alsook hun respectieve gezinsleden) de volgende persoonsgegevens (in beginsel van het jaar 2015) ter beschikking worden gesteld. De bedragen zouden telkens in klassen worden weergegeven. De datums zouden telkens met het jaar en de maand worden weergegeven.

Persoonskenmerken: het gepseudonimiseerd identificatienummer van de betrokkene, van de referentiepersoon en van het gezin, het wel/niet geselecteerd zijn bij de steekproeftrekking, het verband met het gezinshoofd, de geboortedatum, het geboorteland, het geslacht, de gemeente van de woonplaats, de eerste nationaliteit (in klassen), de huidige nationaliteit (in klassen), het gezinstype, de LIPRO-code, de burgerlijke staat, het register van inschrijving, de beroepencode (in geval van tewerkstelling bij de Europese Unie), de opleiding (niveau, vorm, net, modaliteiten) en de diplomacode.

Toestand op 1 januari 2016: het register waarin de betrokkene is opgenomen, de reden van het verblijf en het gepseudonimiseerd identificatienummer van de ouders en de grootouders.

Beroepsinkomsten en uitkeringen (voor alle kwartalen van 2013, 2014 en 2015): het brutoloon van de werknemer, het bruto belastbaar loon van de werknemer, het netto zelfstandigeninkomen, de bruto uitkering (per bevoegde instelling van sociale zekerheid), de bruto belastbare uitkering (per bevoegde instelling van sociale zekerheid), de arbeidsmarktpositie, het statuut op het vlak van de sociale zekerheid (per mogelijk statuut de aanduiding ja/neen) en de werkintensiteit op gezinsniveau (volgens twee definities).

Arbeidsongevallen: de graad van permanente/tijdelijke arbeidsongeschiktheid, de graad voor hulp van derden, het begin en het einde van de arbeidsongeschiktheid, het aantal dagen tijdelijke arbeidsongeschiktheid met volledige/gedeeltelijke afwezigheid, het verloren loon, het voorgesteld loon dat dient als basis voor de berekening van de uitkering, het bedrag voor tijdelijke arbeidsongeschiktheid met volledige/gedeeltelijke afwezigheid en de beroepscategorie op het moment van het arbeidsongeval.

Beroepsziekten: het percentage arbeidsongeschiktheid, het type uitkering, het basisloon waarop de uitkering berekend wordt, het type periode, het begin en het einde van de betaling en het bedrag van de uitkering.

Andere arbeidsongeschiktheden: de reden van de afwezigheid, het stelsel, het aantal dagen arbeidsongeschiktheid, het begin en het einde van de arbeidsongeschiktheid, het bedrag van de uitkering, het sociaal statuut en het einde van de betrekking als grensarbeider.

Tussenkomsten van een openbaar centrum voor maatschappelijk welzijn: het bedrag, het begin en het einde van de betaling, het percentage en de omschrijving van de terugbetaling door de overheid, de toepasselijke regelgeving, de gezinscategorie, het statuut, het type, de aanvaarding van de tewerkstelling, het type tewerkstelling, de plaats van tewerkstelling, het uurrooster, het type tewerkstellingsprogramma, het type tussenkomende organisatie, het type geïndividualiseerd integratieproject, het projecttype en het activeringstype.

Invaliditeit en zwangerschapsverlof: de betalingscode, het stelsel, het aantal vergoede dagen, het bedrag van de uitkering, het begin en het einde van de betalingsperiode, het begin van de primaire arbeidsongeschiktheid, de uittredingscode per stelsel, de sociale staat per stelsel en de medische code per stelsel (de aandoening op basis waarvan de betrokkene als invalide erkend is door de Geneeskundige Raad voor Invaliditeit).

Kinderbijslag (werknemersstelsel en zelfstandigenstelsel, per kind): het begin en het einde van de betaling en de hoedanigheid van elke actor (de band tussen de actoren kan worden achterhaald aan de hand van het dossiernummer, het bevoegde kinderbijslagfonds en het bevoegde bureau).

Beroepsactiviteiten als zelfstandige (voor alle kwartalen van 2015): de beroepscode, de NACE-code, de bijdragecategorie, de hoedanigheidscode, het begin en het einde van de aansluiting en, voor de periode 2010-2015, de nettobedrijfsinkomsten (per jaar).

Beroepsactiviteiten als werknemer (per tewerkstellingslijn, voor het vierde kwartaal 2015): het gepseudonimiseerd identificatienummer van de werkgever, de sector, het nummer van het paritair comité, de werknemerscode, de (gewone/bijzondere) werknemersklasse, het werkgeverskengetal, de werkgeverscategorie, de dimensieklasse, de aard van het record (origineel/bijgeschat), de reden voor de uitsluiting, het prestatietype, het percentage deeltijdse tewerkstelling, het percentage tewerkstelling (zonder/met gelijkgestelde dagen), de hoofdprestatie, de verminderingscode, het gecumuleerd bedrag van de vermindering, het bedrag van de werkgeversbijdrage, het bedrag van de persoonlijke bijdrage, het bedrag van de bijzondere bijdrage, het aantal bezoldigde dagen (voltijds/deeltijds), het aantal bezoldigde dagen vooropzeg, het aantal bezoldigde vakantiedagen, het aantal bezoldigde gelijkgestelde dagen, de hoofdcode van de gelijkgestelde dagen, het aantal dagen per week, het aantal uren voltijdse/deeltijdse tewerkstelling, het aantal uren van de maatman, het voltijdsequivalent, het voltijdsequivalent exclusief/inclusief gelijkgestelde dagen, het aantal gepresteerde dagen/uren (specifieke prestatiecodes), de code van de bijdragevermindering, de berekeningsbasis, het basisloon, het gewoon loon, het wachtloon, het forfaitair loon, de premies, het voordeel van het gebruik van een voertuig, de vooropzeg, de verbrekingsvergoeding, het berekend dagloon, het gemiddeld dagloon, de bijdrageplichtige loonmassa, de bijdragevermindering (werkgever/werknemer), de toepasselijkheid van de Sociale Maribel, de bijdragecode, de berekeningsbasis en het bedrag van de werkgeversbijdragen voor winstparticipaties, bedrijfsvoertuigen en extralegale pensioenen en het arrondissement van de werkplaats.

Beroepsactiviteiten als werknemer (voor elk jaar van 2006-2015): de werknemersklasse, de bijdragecode, de reden voor de uitsluiting, het aantal uren deeltijdse tewerkstelling, het aantal gelijkgestelde dagen/uren, het aantal vergoede dagen/uren, het aantal bezoldigde dagen voltijdse/deeltijdse tewerkstelling, het percentage tewerkstelling (zonder/met gelijkgestelde dagen), het voltijdsequivalent exclusief/inclusief gelijkgestelde dagen, de bezoldigingen op jaarbasis, de bezoldigingen op kwartaalbasis (volgens diverse berekeningswijzen) en het gemiddeld dagloon.

Beroepsactiviteiten als werknemer (voor alle kwartalen van 2015): de toepasselijke tewerkstellingsmaatregel, de tewerkstelling in het stelsel van de dienstencheques en de belangrijkste activiteitensector van de werkgever.

Werkloosheid: het werkloosheidsstatuut (voor elk jaar van 2006-2015), de reden (in geval van loopbaanonderbreking/tijdskrediet), het bedrag van de dagvergoeding die aan de werkloze toegekend wordt, het aantal dagen waarvoor een werkloosheidsuitkering wordt ontvangen, het bedrag van de werkloosheidsuitkering ontvangen tijdens het jaar, de werkloosheidsduur, het aantal uren gewerkt in het kader van een plaatselijk werkgelegenheidsagentschap gedurende het jaar en de vergoedingscategorie van de werkloze.

Pensioenen: de code alleenstaande, de code gezinslast, de code echtgenoot ten laste, het aantal kinderen ten laste, het aantal andere personen ten laste, de begindatum van het pensioen, de begindatum van het huidig recht, het type pensioenrecht en het brutobedrag van het pensioen.

Statuut van persoon met een handicap (voor alle kwartalen van 2015): het type record, de toepasselijke regelgeving, het begin en het einde van de medische procedure tot erkenning van de handicap, de erkenning van de handicap (50% onderste ledematen, volledige blindheid, amputatie van de bovenste ledematen, verlamming van de bovenste ledematen), het percentage van de ongeschiktheid van het kind, het aantal punten dat het kind scoort op het vlak van de gevolgen van de aandoening (in totaal en voor elk van de drie pijlers afzonderlijk: lichamelijke of geestelijke ongeschiktheid, activiteit en participatie, familiale omgeving), het aantal punten dat het kind scoort op het vlak van de vermindering van de zelfredzaamheid, de erkenning van de vermindering van het verdienvermogen, het aantal punten dat de volwassene scoort voor de vermindering van de zelfredzaamheid (in totaal en voor elk van de zes criteria afzonderlijk: verplaatsingsmogelijkheden, voedsel nuttigen of bereiden, persoonlijke hygiëne en zichzelf kleden, woning onderhouden en huishoudelijk werk verrichten, leven zonder toezicht, communicatie en sociaal contact), de overlijdensdatum van de betrokkene, het theoretisch bedrag voor de betalingsperiode, het werkelijk bedrag betaald gedurende de betalingsperiode, de statistische classificatie, het begin en het einde van de betalingsperiode, het totaal gesimuleerd maandbedrag, het gesimuleerd maandbedrag van de integratietegemoetkoming, de maand ten opzichte van dewelke geïndexeerd moet worden, het begin en het einde van het recht, de datum van de beslissing tot eventuele herziening van het recht, de gewijzigde datum van de beslissing, het gecodeerd identificatienummer van de partner van de rechthebbende, het begin en het einde van het partnerschap en de aanduiding van de integratietegemoetkoming, de inkomensvervangende tegemoetkoming of de tegemoetkoming voor hulp aan bejaarden.

Loopbaan (SIGEDIS, 1954-2015, per loopbaancode): de loopbaancode, het loopbaanjaar, de jaarbezoldiging, het aantal gepresteerde dagen, het aantal gelijkgestelde dagen, het aantal uren per week van de maatman, het aantal uren gepresteerd als deeltijdse arbeider, het aantal gelijkgestelde uren, de periode van arbeidsongeschiktheid (begindatum en einddatum), het percentage arbeidsongeschiktheid, het recht op de inkomensgarantieuitkering, de aanduiding dat de inkomensgarantieuitkering wordt toegekend per maand van het jaar, de startdatum van het behoud van rechten, de start en het einde van de deeltijdse periode (met

inkomensgarantieuitkering), het type onderwerping, de bevoegde instelling van sociale zekerheid en de toekenningscode.

B. BEHANDELING VAN DE AANVRAAG

Bevoedheid van het informatieveiligheidscomité

3. Krachtens artikel 5, § 1, van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid* verzamelt de Kruispuntbank van de Sociale Zekerheid persoonsgegevens bij de instellingen van sociale zekerheid, slaat ze op, voegt ze samen en deelt ze mee aan de personen die ze nodig hebben voor het verrichten van onderzoeken die nuttig zijn voor de kennis, de conceptie en het beheer van de sociale bescherming.

4. Het betreft voorts een mededeling van persoonsgegevens die krachtens artikel 15, § 1, van de wet van 15 januari 1990 een beraadslaging van de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité vereist.

Rechtmatigheid van de verwerking

5. Overeenkomstig 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* is de verwerking van persoonsgegevens uitsluitend rechtmatig indien en voor zover minstens één van de vermelde voorwaarden is vervuld.

6. De mededeling van de vermelde gepseudonimiseerde persoonsgegevens aan de federale overheidsdienst Sociale Zekerheid is rechtmatig vermits ze, in de zin van artikel 6, 1, eerste lid, c), noodzakelijk is om te voldoen aan een door de regelgeving opgelegde verplichting die op de verwerkingsverantwoordelijke rust, ingevolge artikel 2, § 1, 4° en 5°, van het koninklijk besluit van 23 mei 2001 *houdende oprichting van de federale overheidsdienst Sociale Zekerheid*.

Principes met betrekking tot de verwerking van persoonsgegevens

7. 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 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 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).

Doelbinding

8. De federale overheidsdienst Sociale Zekerheid wil het microsimulatiemodel voor de sociale zekerheid – met persoonsgegevens van recentere jaren en uit meer bronnen – gebruiken voor beleidsondersteunend onderzoek. Het betreft een gerechtvaardigd doeleinde. Het destijds bevoegde sectoraal comité van de sociale zekerheid en van de gezondheid stelde dit eerder reeds vast (zie hoger).

9. De hogervermelde gepseudonimiseerde persoonsgegevens uit het netwerk van de sociale zekerheid zouden door de federale overheidsdienst Sociale Zekerheid onder meer worden aangewend voor het verwezenlijken van beleidsvoorbereidend onderzoek met betrekking tot de cumulatie van arbeidsinkomsten en uitkeringen en de automatische toekenning van sociale rechten.

Minimale gegevensverwerking

10. De kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité stelt vast dat de mededeling betrekking heeft op een heel groot aantal persoonsgegevens. Zij is echter van oordeel dat die persoonsgegevens, niettegenstaande hun zeer omvangrijk aantal, op zich niet van die aard zijn dat ze tot een heridentificatie van de betrokkene kunnen leiden, behoudens in het – nooit volledig uit te sluiten – geval van voorkennis in hoofde van de onderzoekers (het betreft dan een indirecte contextuele heridentificatie). De eigenlijke persoonskenmerken worden daartoe beperkt en doorgaans in klassen aan de onderzoekers meegedeeld. Aan elke betrokkene wordt voorts een betekenisloos volgnummer toegekend.

11. De persoonsgegevens worden door de Kruispuntbank van de Sociale Zekerheid op een individueel niveau meegedeeld. De federale overheidsdienst Sociale Zekerheid moet immers de algemene impact van beleidsbeslissingen kunnen bepalen door die beleidsbeslissingen toe te passen op een steekproef van concrete gevallen die representatief is voor de Belgische bevolking. Een mededeling van anonieme gegevens kan niet volstaan.

Opslagbeperking

12. De federale overheidsdienst Sociale Zekerheid mag de meegedeelde gepseudonimiseerde persoonsgegevens bewaren zolang hun verwerking noodzakelijk is in het kader van voormelde exploitatie en maximaal tot 31 maart 2024. Daarna dienen zij, behalve in geval van een nieuwe beraadslaging vanwege het informatieveiligheidscomité, te worden vernietigd.

Integriteit en vertrouwelijkheid

13. Het microsimulatiemodel en de persoonsgegevens zijn momenteel op door de federale overheidsdienst Sociale Zekerheid beveiligde *stand alone* computers geïnstalleerd met het oog op de exploitatie ervan. Derden kunnen deze persoonsgegevens als verwerker van de federale overheidsdienst Sociale Zekerheid gebruiken voor exploitatiedoeleinden, maar enkel op dezelfde binnen de federale overheidsdienst Sociale Zekerheid geïnstalleerde beveiligde computers.

14. MIMOSIS is dus momenteel enkel toegankelijk door middel van beveiligde *stand alone* computers. Een systeem van *remote access*, op beveiligde infrastructuur, zal die werkwijze echter vervangen. De federale overheidsdienst Sociale Zekerheid wil de beide werkwijzen (beveiligde *stand alone* computers en *remote access*) echter tot het einde van de verwerking van de persoonsgegevens – op 31 maart 2024 – naast elkaar laten bestaan waarbij de stand alone PCs fungeren als backup voor het systeem van remote access.

15. Zowel de fysieke beveiliging als de logische beveiliging van de remote access en van de voormelde *stand alone* computers moet zodanig georganiseerd worden dat inbreuken tegen de regelgeving met betrekking tot de bescherming van de persoonlijke levenssfeer maximaal afgewend worden. De federale overheidsdienst Sociale Zekerheid moet de *stand alone* computers daarenboven onverkort gebruiken volgens de geldende beleidslijnen van de Kruispuntbank van de Sociale Zekerheid met betrekking tot de beveiliging van computers.

16. Het informatieveiligheidscomité stelt vast dat een vijftal medewerkers van de federale overheidsdienst Sociale Zekerheid aan de hand van de remote access en van een beveiligde computer toegang hebben tot de gepseudonimiseerde persoonsgegevens. De gespeudonimiseerde gegevens worden opgeslagen op een externe drager die geëncrypteerd is. De computer is niet verbonden met het internet. De betrokken medewerkers moeten zich steeds houden aan de "*richtsnoeren voor het beschermen van gegevens verwerkt op PC*" van de afdeling Informatieveiligheid van de Kruispuntbank van de Sociale Zekerheid (zie bijlage).

17. Bij het (tijdelijk) gebruik van de *stand alone* computers worden alleszins steeds de volgende maatregelen toegepast:

- de gepseudonimiseerde persoonsgegevens worden uitsluitend bewaard op een beveiligd *remote access* systeem en op twee externe harde schijven als back-up optie;
- de externe dragers zijn volledig geëncrypteerd ("*Full Disk Encryption*") met Bitlocker of VeraCrypt en bij het instellen van een paswoord worden de volgende regels gehanteerd:
    - het paswoord is minstens twintig tekens lang en het bevat minstens één kleine letter, één hoofdletter, één cijfer en één speciaal teken;
    - het paswoord wordt op geen enkele manier bewaard op de *stand alone* computer en het wordt bij elk gebruik handmatig ingegeven;
- het transport van de externe drager wordt tot een minimum beperkt en de externe drager wordt nooit samen in dezelfde draagtas opgeborgen met de *stand alone* computer die de mogelijkheid geeft om de gepseudonimiseerde persoonsgegevens te lezen.

18. Voorts worden de volgende maatregelen getroffen:

- de veiligheid van de *stand alone* computers zelf wordt gegarandeerd:
  - er is geen netwerk/internet-verbinding wanneer de computer toegang tot de externe drager heeft;
  - er is op de harde schijf geen sprake van temp files die afgeleid zijn van de beschermde informatie;
- inzake de externe dragers:
  - er wordt een *chain of custody* voorzien (men weet steeds op welk moment wie de schijf in zijn bezit heeft) wanneer een externe drager de gebouwen verlaat;
  - wanneer de schijf niet gebruikt wordt, wordt deze veilig opgeborgen zodat deze enkel kan bekomen worden door de personen aan wie toegang gemachtigd is
  - de persoonsgegevens op de drager (of de drager zelf) worden vernietigd wanneer deze niet langer gebruikt worden.

19. Bij de verwerking van de persoonsgegevens in het kader van de exploitatie van het microsimulatiemodel voor de sociale zekerheid moet rekening worden 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*.

20. Aldus moet de federale overheidsdienst Sociale Zekerheid onder meer artikel 28 van de voormelde Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (over de verhouding tussen de verantwoordelijke voor de verwerking en zijn verwerker) naleven.

21. De federale overheidsdienst Sociale Zekerheid moet er zich contractueel toe verbinden alle mogelijke middelen te zullen inzetten om te vermijden dat de identiteit van de personen op wie de meegedeelde gepseudonimiseerde persoonsgegevens betrekking hebben, zou worden achterhaald.

22. De federale overheidsdienst Sociale Zekerheid moet met derden die als zijn verwerker optreden en de persoonsgegevens gebruiken een overeenkomst sluiten waarbij die derden zich ertoe verbinden de persoonsgegevens te zullen verwerken overeenkomstig de bepalingen van de hogervermelde regelgeving. Hierbij dient bij de uitvoering van beleidssimulaties in het bijzonder aandacht te worden besteed aan de omschrijving van de precieze finaliteit.

23. De resultaten van de verwerking mogen niet worden bekendgemaakt in een vorm die de identificatie van de betrokken persoon mogelijk maakt. De persoonsgegevens mogen voorts niet verder worden meegedeeld aan derden behalve indien het informatieveiligheidscomité daartoe uitdrukkelijk zijn goedkeuring verleent.

Gelet op het voorgaande besluit

de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité

dat de mededeling van de hogervermelde persoonsgegevens door de Kruispuntbank van de Sociale Zekerheid aan de federale overheidsdienst Sociale Zekerheid, met het oog op het actualiseren van het microsimulatiemodel voor de sociale zekerheid, zoals in deze beraadslaging beschreven, is toegestaan mits er wordt voldaan aan de vastgestelde maatregelen ter waarborging van de gegevensbescherming.

Bart VIAENE
Voorzitter

Bijlage: richtsnoeren voor het beschermen van gegevens verwerkt op PC

Context

Bij de verwerking van gegevens moeten de veiligheidsmaatregelen ervoor zorgen dat de vertrouwelijkheid van de verwerkte gegevens maximaal gegarandeerd wordt. Hoewel PC's meestal een basisbescherming hebben, blijft het aangeraden om de gegevens extra te beschermen zodat de kans op gegevenslekken verder geminimaliseerd wordt. Dit document heeft tot doel de relevante maatregelen voor de bescherming van de PC's op te sommen samen met extra maatregelen om de gegevens te beschermen. Het standpunt waarvan uitgegaan wordt, is dat de gegevens op een speciaal daartoe bestemde PC worden verwerkt. Deze PC wordt "*stand alone* PC" genoemd.

Bescherming van de PC

De PC dient voorzien te zijn van basismaatregelen om deze te beschermen. Deze maatregelen omvatten onder andere:

- een regelmatige patching van het *Operating System* en de gebruikte toepassingen – wanneer de PC voornamelijk offline wordt gebruikt, moet die geüpdatet worden voordat er een *Mass Storage Device* (MSD) of een andere mobiele geheugendrager wordt aangebracht of wanneer er een netwerkverbinding met drives wordt gemaakt;
- een toegangscontrole, zodat enkel de personen die toegang tot de PC nodig hebben deze toegang effectief kunnen bekomen – het wachtwoord dient voldoende complexiteit te bevatten;
- een antimalware die actief en up-to-date is – wanneer de PC voornamelijk offline wordt gebruikt, moet die geüpdatet worden voordat er een *Mass Storage Device* (MSD) of een andere mobiele geheugendrager wordt aangebracht of wanneer er een netwerkverbinding met drives wordt gemaakt;
- een versleuteling van de gegevens op de interne gegevensdragers (HD, SSD,…);
- een in *lock-mode* gaan van de PC wanneer deze gedurende een bepaalde tijd niet gebruikt wordt;
- een niet aanvaarden van externe connecties – enkel sessies opgezet vanuit de PC zijn toegestaan.

Bijkomend dienen volgende maatregelen voorzien te worden voor de *stand alone* PC.

- aanduiden van een verantwoordelijke voor het toegangsbeheer

    - Deze persoon zal verantwoordelijk zijn voor het toestaan van de toegang tot de informatie op de PC, het waken over de veilige configuratie van de PC en voor het verwijderen van de toegang wanneer deze niet langer noodzakelijk is voor het project of wanneer de medewerker niet langer binnen het project actief is.
    - Deze verantwoordelijke kan hiervoor een beroep doen op IT- departementen maar zal steeds het overzicht van de toegekende toegangen houden.

    - De verantwoordelijke voor het toegangsbeheer zal waken over een gepaste vernietiging van de informatie wanneer deze niet langer noodzakelijk is.

- minimalisatie van de toepassingen

    - Enkel de toepassingen noodzakelijk voor het project waarvoor de informatie verwerkt wordt, zijn toegestaan. Zo zal in het bijzonder vermeden worden dat programma's waarmee informatie kan gekopieerd of getransfereerd worden aanwezig zijn op het toestel.

- minimalisatie van de toegangen

    - Toegang naar het internet dient uitgeschakeld te worden. Updates van antimalware, operating systemen en software dient gepusht te worden vanuit een beschermd netwerk.
    - Toegang voor MSD dient uitgeschakeld te worden. Een uitzondering is mogelijk wanneer beveiligde data gekopieerd dienen te worden, waarna deze functionaliteit wordt uitgeschakeld.
    - De gebruikers hebben minimale rechten die toestaan om de opdracht uit te voeren. Verhoogde toegangsrechten worden enkel toegekend aan de verantwoordelijke voor het toegangsbeheer die deze rechten kan delegeren aan de IT-afdeling.
    - De IT-afdeling kan enkel toegang hebben tot de PC na expliciete toestemming van de gebruikers of de verantwoordelijke voor het toegangsbeheer. Deze toestemming wordt technisch bekomen indien deze via het beschermde netwerk gebeurt en kan enkel onder voorwaarde dat geen toegang tot de informatie wordt bekomen. Alternatief kan de toegang voor de IT-administrator beperkt worden tot een fysieke toegang onder toezicht van de gebruiker of de verantwoordelijke voor het toegangsbeheer.

- bijkomende bescherming van de gevoelige gegevens

    - De PC wordt zo ingericht dat de gevoelige informatie als een apart (en bijkomend) geëncrypteerd volume op de interne harde schijf beschikbaar wordt gesteld.
    - De toegang tot dit volume wordt geregeld met een wachtwoord van voldoende complexiteit en een tweede factor. Deze tweede factor kan gebaseerd zijn op een externe sleutel maar kan ook gebruik maken van een *key file* op de harde schijf van de PC. De externe sleutel of de informatie over de *key file* wordt enkel meegedeeld aan de personen die toegang nodig hebben tot de informatie.
    - De ontsluiting van dit geëncrypteerd volume mag niet gebeuren wanneer er andere toegangen genomen zijn tot de PC. Zo zal er op dat moment geen toegang zijn tot het internet en zal er ook geen toegang verleend worden aan systeembeheerders.
    - Het geëncrypteerd volume wordt afgekoppeld wanneer de PC wordt afgesloten of wanneer de gebruiker uitlogt van de PC.

  - Er wordt geen back-up voorzien van het geëncrypteerde volume.
  - Wanneer de informatie niet langer noodzakelijk is, wordt het geëncrypteerde volume verwijderd van de schijf op zo een manier dat dit niet kan gerecupereerd worden.

- fysieke beveiliging van de PC

  - De PC wordt enkel gebruikt op plaatsen waar dit veilig kan gebeuren.
  - Wanneer het lokaal waar de PC gebruikt wordt voor meer personen dan de gebruiker toegankelijk is, dan wordt de PC verankerd middels een slot.
  - Het zicht op het scherm wordt zodanig beperkt dat enkel de gebruiker de gegevens kan consulteren.
  - De PC mag nooit onbewaakt gelaten worden. Indien de PC niet wordt gebruikt, dan wordt deze beveiligd bewaard.
  - Transport van deze PC wordt zo veel als mogelijk vermeden. Indien dit toch noodzakelijk zou zijn, dan waakt de gebruiker erover dat alle sessies afgesloten zijn (*log-out*) en dat de PC uitgeschakeld werd (*shut-down*).

- aanbrengen van de informatie

  - De informatie wordt behandeld met het concept van "*Chain of Custody*". Dit houdt in dat op elk moment geweten is wie beschikking heeft over de informatie.
  - De informatie wordt in geëncrypteerde vorm ter beschikking gesteld aan de verantwoordelijke voor het toegangsbeheer.
  - De verantwoordelijke voor het toegangsbeheer controleert de veiligheidsmaatregelen op de PC en zorgt ervoor dat deze informatie op het geëncrypteerde volume wordt gekopieerd. Hierbij wordt ervoor gezorgd dat er geen tijdelijke files met gegevens onbeschermd op de PC worden aangemaakt. Er wordt geen informatie opgeslagen in tijdelijke files buiten het geëncrypteerde volume.