

Informatieveiligheidscomité
kamer federale overheid

BERAADSLAGING NR. 22/025 VAN 5 JULI 2022 MET BETREKKING TOT DE MEDEDELING VAN PERSOONSgegevens DOOR DE FOD MOBILITEIT EN DE DIENST VREEMDELINGENZAKEN VAN DE FOD BINNENLANDSE ZAKEN AAN DE AFDELING VLAAMSE SOCIALE INSPECTIE VAN HET DEPARTEMENT WERK EN SOCIALE ECONOMIE DOOR MIDDEL VAN DE TOEPASSING MY DIGITAL INSPECTION ASSISTANT (MYDIA)

Gelet op de wet van 15 augustus 2012 *houdende oprichting en organisatie van een federale dienstenintegrator*, in het bijzonder artikel 35/1, §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 98;

Gelet op de aanvraag van het Departement Werk en Sociale Economie van de Vlaamse Overheid;

Gelet op het auditoraatsrapport van de federale overheidsdienst Beleid en Ondersteuning;

Gelet op het verslag van heer Daniel Haché.

I. ONDERWERP VAN DE AANVRAAG

1. De afdeling Vlaamse Sociale Inspectie van het departement Werk en Sociale Economie werd door de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité bij beraadslaging nr. 22/158 van 7 juni 2022 gemachtigd om databanken uit het netwerk van de sociale zekerheid te raadplegen door middel van de toepassing My Digital Inspection Assistant (MyDIA). Het betreft volgende databanken:
 - het Rijksregister en de Kruispuntbankregisters;
 - het werkgeversrepertorium;
 - de DIMONA-databank en het personeelsbestand;
 - het LIMOSA-kadaster;
 - het GOTOT-bestand;
 - het bestand van de werfmeldingen;

- de databank “aanwezigheidsregistratie” (CheckIn@Work);
 - de databank “werkloosheidsuitkeringen”;
 - de databank “multifunctionele attestaten” (openbare centra voor maatschappelijk welzijn);
 - het algemeen repertorium van de zelfstandige arbeiders;
 - de DMFA-databank;
 - de databank met persoonsgegevens inzake de arbeidsongeschiktheid.
2. De afdeling Vlaamse Sociale Inspectie van het departement Werk en Sociale Economie wil thans door de kamer federale overheid van het Informatieveiligheidscomité in de mogelijkheid worden gesteld om eveneens twee andere databanken (buiten het netwerk van de sociale zekerheid) te raadplegen door middel van de toepassing My Digital Inspection Assistant (MyDIA), mee bepaald:
 - de databank Dienst Inschrijvingen Voertuigen (federale overheidsdienst Mobiliteit en Vervoer) en
 - het platform Single Permit inzake verblijf en werkvergunning (federale overheidsdienst Binnenlandse Zaken).
 3. De toegang tot de persoonsgegevens van de databank Dienst Inschrijvingen Voertuigen van de federale overheidsdienst Mobiliteit en Vervoer betreft de identificatie van de (rechts)persoon op wiens naam een bepaald voertuig is ingeschreven: voornaam, familienaam, geboortedatum, adres, INSZ-nummer en ondernemingsnummer van de titularis van het voertuig. De opzoeking kan gebeuren aan de hand van de nummerplaat of het chassisnummer. Deze informatie moet de sociaalrechtelijke inspecteurs toelaten om een link te leggen tussen de werknemer enerzijds en de werkgever of opdrachtgever anderzijds. Deze toegang werd reeds gemachtigd bij beraadslaging nr. 20/017 van 7 juli 2020 van de kamer federale overheid van het Informatieveiligheidscomité. De huidige beraadslaging betreft dan ook de nieuwe toepassing MyDIA via dewelke de toegang wordt bekomen.
 4. De toegang tot de gegevens van het platform Single Permit inzake verblijf en werkvergunning via de toepassing MyDIA moet de sociale inspecteurs in staat stellen om de situatie van werknemers/zelfstandigen op het vlak van het verblijf op het Belgisch grondgebied en van de documenten waarover zij dienaangaande beschikken te verifiëren en bij uitbreiding of hun tewerkstelling reglementair is en alle bepalingen ter zake werden gerespecteerd. Het gegeven waartoe toegang wordt gevraagd, is beperkt tot de positieve dan wel de negatieve verblijfsbeslissing omtrent de betrokkene in kwestie. De toegang tot hetzelfde gegeven door de Rijksdienst voor sociale zekerheid, de federale overheidsdienst Werkgelegenheid, Arbeid en Sociaal overleg, de Rijksdienst voor arbeidsvoorziening en het Rijksinstituut voor sociale verzekeringen der zelfstandigen werd voor eenzelfde finaliteit, binnen de uitoefening van hun respectieve bevoegdheden uiteraard, bij beraadslaging nr. 21/019 van 6 juli 2021 van het Informatieveiligheidscomité gemachtigd.
 5. De gevraagde persoonsgegevens hebben betrekking op alle personen waarmee de sociaalrechtelijke inspecteurs geconfronteerd worden bij het vervullen van de controletaken in de strijd tegen (sociale) fraude die hun door de regelgeving zijn toevertrouwd. Ter zake kan worden verwezen naar artikel 2 van het decreet van 30 april 2004 *tot uniformisering van de toezichts-, sanctie- en strafbepalingen die zijn opgenomen in de regelgeving van de sociaalrechtelijke aangelegenheden waarvoor de Vlaamse Gemeenschap en het Vlaamse*

Gewest bevoegd zijn). De aanwezigheid van een persoon op een arbeidsplaats of op een andere plaats die onder de bevoegdheid van een sociaal inspecteur valt, volstaat voor de sociaal inspecteur om persoonsgegevens van die persoon op te zoeken (er is dus geen sprake van een voorafgaande selectie).

6. De toepassing MyDIA biedt de sociaal inspecteurs ook de mogelijkheid om de persoonsgegevens die ze raadplegen in het netwerk van de sociale zekerheid te verbinden met een bepaalde controle die ze verrichten, aan de hand van de web service *FieldInspection*. De controle heeft steeds betrekking op een onderzoek dat wordt gecreëerd door een coördinerende sociaal inspecteur en waartoe andere sociaal inspecteurs toegang kunnen hebben als deelnemende actor. In het onderzoek worden de karakteristieken van de sociaal inspecteurs en van de controles opgenomen, alsook het verband tussen de sociaal inspecteurs en de controles. De sociaal inspecteurs kunnen bepaalde persoonsgegevens die zij hebben geraadpleegd in het netwerk van de sociale zekerheid tijdelijk (maximaal drie dagen) opslaan, in een beveiligde database (er worden geen persoonsgegevens opgeslagen op hun mobiel toestel). Het betreft enkel persoonsgegevens ter identificatie van de betrokken natuurlijke personen (in het bijzonder het identificatienummer van de sociale zekerheid, de naam en de voornaam), aangevuld met specifieke informatie met betrekking tot de ondernemingen (het inschrijvingsnummer, het ondernemingsnummer en de benaming) en de werven (het ondernemingsnummer van het bedrijf, de benaming van het bedrijf, het werfnummer en de postcode) en diverse indicatoren (bijvoorbeeld met betrekking tot het al dan niet bestaan van een aangifte).
7. Een minimale set van persoonsgegevens – met betrekking tot het statuut van de werknemer (voltijds of deeltijds), zijn arbeidsongeschiktheid, zijn verblijfsvergunning en arbeidvergunning als buitenlands werknemer en de identificatie van de voertuigen die op de werf aangetroffen worden – kan ook ter plaatse, door middel van MyDIA, geraadpleegd worden. Ook gestructureerde informatie over de interpretatie van de bevindingen door de sociaal inspecteurs kan tijdelijk worden opgeslagen (zoals de vaststelling van de overeenstemming van de werkgever vermeld in de DIMONA-aangifte en de DMFA-aangifte en de gecontroleerde werkgever) alsook vrije tekst ter zake, telkens met de identiteit van de betrokken sociaal inspecteur en de datum en het tijdstip van de registratie.
8. De persoonsgegevens worden uitsluitend bijgehouden indien de sociaal inspecteur vrijwillig een geïdentificeerde persoon, onderneming of werf toevoegt aan een controle. De opslag blijft voorts beperkt tot de voormelde persoonsgegevens. Er is bijgevolg geen sprake van het onverkort kopiëren van alle persoonsgegevens die in de verschillende authentieke bronnen geraadpleegd werden (er zal bijvoorbeeld bijgehouden worden dat er een DIMONA-aangifte werd verricht maar de inhoud ervan zal niet worden opgeslagen). De bedoeling van de opslag in het systeem bestaat erin de sociaal inspecteur de mogelijkheid te bieden om na te gaan of een raadpleging van de authentieke bronnen nodig is in het kader van het onderzoek. Die zal dan in voorkomend geval geschieden via de gebruikelijke kanalen.
9. Bij de beëindiging van de controle, bijvoorbeeld door de coördinerende sociaal inspecteur, zou – op een beveiligde server, niet op het mobiele toestel van de gebruiker – een tekstbestand worden gecreëerd op basis van de geregistreerde persoonsgegevens. Het zou worden

verstuurd naar de eBox¹ van de betrokken sociaal inspecteurs en daarin drie dagen worden bewaard en dan automatisch worden gewist. Aan de hand van dat (beperkt) tekstbestand (met de identiteit van de betrokken partijen en de commentaren over het onderzoek) kunnen de sociaal inspecteurs de authentieke persoonsgegevensbronnen raadplegen. De web service *FieldInspection* is dus zelf noch een authentieke persoonsgegevensbron noch een kopie van een authentieke persoonsgegevensbron. Het systeem zorgt voor de automatische verwijdering na drie dagen. De mobiele toepassing MyDIA biedt de verschillende sociaal inspecteurs dus een doeltreffend hulpmiddel bij de uitvoering van hun respectieve toezichtopdrachten. Zij kunnen hun activiteiten inzake de bestrijding van de sociale fraude op een efficiënte wijze uitvoeren door de onmiddellijke beveiligde raadpleging van persoonsgegevens in het netwerk van de sociale zekerheid en de tijdelijke beveiligde opslag ervan.

10. Binnen het beleidsdomein Werk en Sociale Economie staat het departement Werk en Sociale Economie in voor de controle en het toezicht op de regelgeving. Daartoe is binnen de organisatie de afdeling Vlaamse Sociale Inspectie opgericht. De bij haar aangestelde sociaalrechtelijke inspecteurs gaan na of de door de regelgeving opgelegde voorwaarden om van een bepaalde regeling of een bepaald regime te genieten daadwerkelijk (nog) vervuld zijn. In het kader van deze opdracht moeten enkele persoonsgegevens geverifieerd worden. Als blijkt dat een voorwaarde niet (langer) nageleefd wordt, kan de sociaalrechtelijke inspecteur een proces-verbaal opstellen waarin hij de bevindingen, de verhoren en de vastgestelde inbreuken kan opnemen. Dit gaat gepaard met de nodige kennisgeving aan de betrokkene met het oog op de vrijwaring van zijn rechten. Het vaststellen van inbreuken zal, al naargelang het geval, aanleiding geven tot strafrechtelijke vervolging, het opleggen van een administratieve geldboete, het intrekken van een gunst of statuut of de terugvordering van uitgekeerde bedragen.
11. Het hogervermeld decreet van 30 april 2004 bevat nadere regels over de werking van de afdeling Vlaamse Sociale Inspectie. Ingevolge artikel 6, § 1, 6°, hebben de sociaalrechtelijke inspecteurs de beoordelingsbevoegdheid om processen-verbaal op te stellen, waarin alle bevindingen en verhoren en alle vastgestelde inbreuken tegen de vermelde regelgeving worden opgetekend en minstens enkele welbepaalde elementen worden opgenomen (zoals de plaats en de periode van de inbreuk, de beknopte uiteenzetting van de feiten, de identiteit van de actoren en de toepasselijke regelgeving). Ingevolge artikel 7, 2°, hebben de sociaalrechtelijke inspecteurs bij de uitoefening van hun opdrachten ruime bevoegdheden, waaronder het recht om over te gaan tot elk onderzoek, elke controle en elk verhoor van personen over relevante feiten en tot het inwinnen van alle inlichtingen die zij nodig achten

¹ In eerste instantie zou gebruik worden gemaakt van de professionele eBox vermits die strikt persoonlijk is en enkel toegankelijk is voor de houder, in tegenstelling tot de eBox ondernemingen. Later zou eventueel wel de eBox ondernemingen worden gebruikt, voor zover die op een unieke wijze gecompartmenteerd kan worden ten behoeve van de sociaal inspecteurs. De professionele eBox is de elektronische brievenbus voor professionals die wordt aangeboden op het portaal van de sociale zekerheid onder de rubriek “ambtenaren en andere professionelen” en is geïntegreerd in de *Federal Authentication Service* (FAS), waarbij de toegang wordt geregeld door de verantwoordelijke voor het toegangsbeheer van de organisatie, die de gebruikers onder een professionele hoedanigheid in het *User and Access Management* (UAM) inbrengt. Wanneer een nieuw document gepost wordt in de professionele eBox ontvangt de inspecteur een notificatie in zijn professionele mailbox.

om zich ervan te vergewissen dat de bepalingen van de regelgeving waarop zij toezicht uitoefenen werkelijk wordt nageleefd

12. De aanvrager merkt op dat een onmiddellijke (correcte en eenduidige) identificatie op het terrein een belangrijke meerwaarde biedt, zoals bij het controleren van personen die illegaal op het grondgebied verblijven, het opsporen van schijnarbeiders en schijnzelfstandigen die proberen illegaal een verblijfsvergunning of een sociale uitkering te krijgen en het nagaan of ondervraagde personen een uitkering ontvangen. Wanneer een inspecteur op het terrein een persoon ondervraagt, zal hij die trachten te identificeren in MyDIA en zal hij de gegevens raadplegen om na te gaan of er geen sprake is van een anomalie. Als hij per vergissing de gegevens raadpleegt van een persoon die niet de ondervraagde persoon is, past hij zijn zoekcriteria aan en worden er geen gegevens bewaard, terwijl in de veiligheidsloggings wordt opgeslagen dat de inspecteur de gegevens van die persoon heeft geraadpleegd. Als de persoon in regel is, bewaart de inspecteur de business-ID en de technische ID alsook een aantal flags om aan te duiden dat de persoon op het terrein geïdentificeerd werd en verschijnt de persoon in de samenvatting. Indien de persoon niet in regel is, slaat de inspecteur dezelfde gegevens in MyDIA op maar gaat hij ook over tot het opstellen van een proces-verbaal en het invullen van een papieren formulier met het oog op het vervolg van het onderzoek. Wanneer de inspecteur de controle afsluit (hij heeft hiervoor 24 uur de tijd, daarna wordt de controle automatisch afgesloten), worden de gegevens naar de eBox verstuurd en zijn ze beschikbaar door middel van de web service *FieldInspection*. Het betreft steeds uitsluitend business-identificatiegegevens en technische identificatiegegevens en een aantal indicatoren maar geen businessgegevens van de geraadpleegde diensten.
13. Terug op kantoor kan de inspecteur de lijst met geïdentificeerde personen op het terrein opvragen met enkele flags om aan te duiden wat de verdere te ondernemen stappen zijn. Hij heeft drie dagen de tijd om deze gegevens op te vragen, waarna zijn werk verloren zal gaan. De gegevens worden fysiek verwijderd, zowel uit de eBox als uit *FieldInspection*. Ze worden niet gearchiveerd vermits het de bedoeling is dat ze bij het ophalen opgeslagen worden in de businessstoepassingen van de inspecteur. Die businessstoepassingen zijn de authentieke bron van het resultaat van de controle. Indien er dan verdere opzoeken nodig zijn, zal de inspecteur voor de raadpleging van de authentieke bronnen gebruik moeten maken van DOLSIS (of een andere dienst). MyDIA is hiervoor geen optie.
14. MyDIA is een toepassing die tot doel heeft het terreinwerk (de controleacties op de plaatsen waar werknemers of zelfstandigen actief zijn, in sectoren waar de kans op het aantreffen van inbreuken hoog is) van de sociaalrechtelijke inspecteurs te ondersteunen. Deze controles zijn vaak intensief en tijdrovend en vragen een grote mate van voorbereiding en coördinatie van de deelnemers. De controleacties op het terrein zijn meestal gemeenschappelijke acties en vergen een multidisciplinaire aanpak, wat betekent dat afhankelijk van de omvang van de controle en de vermoede problematieken meerdere inspectiediensten deelnemen. MyDIA biedt deze verschillende inspectiediensten een transversaal instrument dat multidisciplinaire samenwerking ondersteunt en de aanpak van de controles op het terrein efficiënter maakt. Daarenboven wordt ook de kwaliteit van de uitwisselingen verbeterd omdat alle deelnemers hetzelfde zicht hebben op de informatie. Langs deze weg wordt ook een gemeenschappelijke interpretatie van de verkregen zoekresultaten bereikt, aangezien elkeen toegang tot dezelfde informatie krijgt en die op een uniforme manier wordt voorgesteld.

15. Het departement Werk en Sociale Economie vraagt om een beraadslaging van onbepaalde duur. De opdrachten van de afdeling Vlaamse Sociale Inspectie, op basis van het decreet van 30 april 2004 *tot uniformisering van de toezichts-, sanctie- en strafbepalingen die zijn opgenomen in de regelgeving van de sociaalrechtelijke aangelegenheden waarvoor de Vlaamse Gemeenschap en het Vlaamse Gewest bevoegd zijn*), zijn immers niet beperkt in de tijd.
16. De persoonsgegevens worden enkel tijdelijk bijgehouden, als de sociaalrechtelijke inspecteur vrijwillig een persoon, onderneming of werf toevoegt aan een controle. De opslag gebeurt niet op het mobiel toestel en blijft beperkt tot de voormelde gegevens. Bij de beëindiging van de controle wordt op basis van de geregistreerde gegevens een tekstbestand gecreëerd op een beveiligde server (niet op het mobiele toestel van de gebruiker). Het wordt verstuurd naar de eBox van de betrokken sociaalrechtelijke inspecteurs en daarin drie dagen bewaard en dan automatisch gewist. Met dat tekstbestand (met de identiteit van de betrokken partijen en de commentaren over het dossier) kan worden overgegaan tot het raadplegen van de authentieke persoonsgegevensbronnen. De web service *FieldInspection* is geenszins een authentieke bron of een kopie van een authentieke bron. Het systeem zorgt steeds voor de automatische verwijdering van het rapport uit de tijdelijke database *FieldInspection* (na 24 uren) en uit de eBox (na 72 uren). Het tijdelijk elektronisch bewaren van de gegevens vormt een veilig alternatief voor het beheren van papieren dossiers.
15. De persoonsgegevens zijn uitsluitend toegankelijk voor de daartoe aangeduide medewerkers van de afdeling Vlaamse Sociale Inspectie (de personeelsleden die belast zijn met de controle en de handhaving van de regelgeving). Derden hebben in geen geval toegang tot de persoonsgegevens.
16. Het departement Werk en Sociale Economie wil met het oog op het verwezenlijken van zijn opdrachten een permanente toegang tot enkele persoonsgegevens uit het netwerk van de sociale zekerheid. De verschillende controles gebeuren immers steeds in de loop van het gehele jaar.

II. BEHANDELING VAN DE AANVRAAG

A. ONTVANKELIJKHEID EN BEVOEGDHEID VAN HET COMITE

17. Krachtens artikel 35/1, §1, eerste lid, van de wet van 15 augustus 2012 *houdende oprichting en organisatie van een federale dienstenintegrator* vergt de mededeling van persoonsgegevens door overheidsdiensten en openbare instellingen van de federale overheid aan instellingen van sociale zekerheid bedoeld in artikel 2, eerste lid, 2^o, a), van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de 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.

18. Het Informatieveiligheidscomité stelt vast dat er geen protocol werd afgesloten en dat het Departement Werk en Sociale Economie een aanvraag tot toelating heeft ingediend. Het Informatieveiligheidscomité acht zich dan ook bevoegd om zich uit te spreken.

B. TEN GRONDE

B.1. VERANTWOORDINGSPLICHT

19. Overeenkomstig artikel 5.2 van de *Verordening 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 gegevens* (de Algemene Verordening Gegevensbescherming, hierna ‘AVG’) zijn de FOD Mobiliteit en de FOD Binnenlandse Zaken (als verzendende instantie) en het Departement Werk en Sociale Economie (als ontvangende instantie) voor de hen aanbelangende verwerkingen als verwerkingsverantwoordelijken verantwoordelijk voor het naleven van de beginselen vermeld in artikel 5.1 de AVG² en moeten ze in staat zijn dit aan te tonen.
20. 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

² 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 ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid”).

21. Overeenkomstig artikel 5.1 a) AVG moeten persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig is. Dit houdt onder meer in dat de verwerking een basis moet vinden in één van de rechtmatigheidsgronden vermeld in artikel 6 AVG.
22. Het Informatieveiligheidscomité stelt vast dat de beoogde mededeling van persoonsgegevens noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust (art. 6.1 c) AVG). Het decreet van 30 april 2004 *tot uniformisering van de toezichts-, sanctie- en strafbepalingen die zijn opgenomen in de regelgeving van de sociaalrechtelijke aangelegenheden waarvoor de Vlaamse Gemeenschap en het Vlaamse Gewest bevoegd zijn* regelt de bevoegdheden van de sociaalrechtelijk inspecteurs van de afdeling Vlaamse Sociale Inspectie van het Departement Werk en Sociale Economie. Zij kunnen processen-verbaal opstellen, waarin alle bevindingen en verhoren en alle vastgestelde inbreuken tegen de vermelde regelgeving worden opgetekend, en hebben bij de uitoefening van hun opdrachten ruime bevoegdheden, zoals het recht om over te gaan tot onderzoeken, controles en verhoren van personen over relevante feiten en het inwinnen van de inlichtingen die zij nodig achten om na te gaan dat de regelgeving waarop zij toezicht uitoefenen effectief wordt nageleefd. De sociaalrechtelijke inspecteurs zijn belast met de controle en het toezicht op de federale wetten en uitvoeringsbesluiten en de decreten van de Vlaamse Raad en uitvoeringsbesluiten, opgesomd in artikels 2 en 3 van voormeld decreet. Specifiek wat de toegang tot de single permit databank van de dienst Vreemdelingenzaken betreft, stelt het Informatieveiligheidscomité vast dat voormeld decreet van 30 april 2004 in art. 2, §1, 57°, de bevoegdheden bepaalt van de sociaalrechtelijke inspecteurs die belast zijn met de controle en het toezicht op de wet van 30 april 1999 betreffende de tewerkstelling van buitenlandse werknemers.

B.3. DOELBINDING

23. Artikel 5.1 b) AVG laat de verwerking van persoonsgegevens slechts toe voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (principe van doelbinding).
24. Het project MyDIA kadert in de verschillende acties die de voorbije jaren reeds werden ondernomen voor de verbetering van de transversale samenwerking tussen de sociale inspecties en de strijd tegen de sociale fraude. Met de mobiele toepassing beschikken de betrokken sociaalrechtelijk inspecteurs tijdens het uitvoeren van hun opdrachten op het terrein over een tool waarmee ze de meest recente persoonsgegevens snel, gemakkelijk en veilig online kunnen raadplegen, de personen zonder officiële identiteitsdocumenten kunnen identificeren zonder daartoe een beroep te moeten doen op de politiediensten en de voorbereiding en de nabespreking kunnen vereenvoudigen. Ze kunnen aldus tijd winnen bij het uitvoeren van controles, het opsporen van anomalieën en het verschaffen van feedback aan de bevoegde organisaties. Ze kunnen tevens op een vlotte wijze inlichtingen over de werven en de daar aanwezige werknemers opzoeken, zoals het type werknemer beschikbaar in DIMONA en LIMOSA, de effectieve aanwezigheidsregistratie in CheckIn@Work, de ketting van onderaannemers en de positie van een onderneming in die ketting. Ze kunnen voorts de verschillende verplichtingen van de partijen op een werf (werknemers, werkgevers, zelfstandigen, werfcoördinatoren,...) controleren om tijd te winnen. Ze kunnen ook nagaan of de verschillende meldingen met betrekking tot de werf werden verricht. Wat de uitzendkrachten betreft, is de gebruiker verantwoordelijk voor de gezondheid en de veiligheid van de werknemer en kan de sociaalrechtelijk inspecteur die gebruiker snel identificeren met behulp van MyDIA.

25. Rekening houdend met de uitdrukkelijk decretale opdrachten van sociaalrechtelijke inspecteurs, acht het Informatieveiligheidscomité deze doeleinden welbepaald, uitdrukkelijk omschreven en gerechtvaardigd.

B.4. PROPORTIONALITEIT

B.4.1. Minimale gegevensverwerking

26. Artikel 5.1 c) AVG stelt dat persoonsgegevens ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt, moeten zijn (“minimale gegevensverwerking”).
27. De persoonsgegevens uit de databank MOVIBIS van de FOD Mobiliteit moeten de sociaalrechtelijke inspecteurs in staat stellen de werkgever van de werknemers die het voorwerp uitmaken van aan controle, te identificeren voor zover dit niet mogelijk is op grond van andere middelen. Zoals bepaald in beraadslaging nr. 20/017 van 7 juli 2020 van de kamer federale overheid van het Informatieveiligheidscomité moet de mededeling van persoonsgegevens uit de databank MOVIBIS van de FOD Mobiliteit dan ook beperkt te blijven tot de identificatie van de (rechts)persoon op wiens naam een bepaald voertuig dat wordt aangetroffen in het kader van een controle, is ingeschreven: voornaam, familienaam, geboortedatum, adres, INSZ-nummer³ en ondernemingsnummer van de titularis van het voertuig. De opzoeking kan gebeuren aan de hand van de nummerplaat of het chassisnummer.
28. Het Informatieveiligheidscomité stelt verder vast dat de mededeling van de beoogde gegevens door de Dienst Vreemdelingenzaken van de FOD Binnenlandse Zaken beperkt blijft tot de positieve dan wel de negatieve verblijfsbeslissing omtrent de betrokkene in kwestie. Een rechtstreekse toegang tot deze gegevens is voor de sociaalrechtelijke inspecteurs noodzakelijk om het toezicht uit te kunnen oefenen op de toepassing van de wettelijke en reglementaire bepalingen inzake het verblijf en de tewerkstelling van buitenlandse werknemers en de uitoefening van zelfstandige beroepsactiviteiten door vreemdelingen
29. Enkel de sociaalrechtelijk inspecteurs van de afdeling Vlaamse Sociale Inspectie (de personeelsleden belast met de controle en de handhaving van de regelgeving) hebben toegang tot de hogervermelde databanken.

B.4.2. Opslagbeperking

30. Aangaande de bewaringstermijn herinnert het Comité er aan dat persoonsgegevens niet langer mogen worden bewaard in een vorm die het mogelijk maakt de betrokkenen te

³ Het Identificatienummer van de sociale zekerheid bestaat uit ofwel het Rijksregisternummer ofwel het identificatienummer toegekend door de Kruispuntbank van de Sociale Zekerheid. Het gebruik van het Rijksregisternummer is niet vrij en vereist een machtiging. Het Departement Werk en Sociale Economie is gemachtigd om het Rijksregisternummer te gebruiken op grond van Koninklijk besluit van 29 juni 1993 *tot regeling van de toegang tot de informatiegegevens en van het gebruik van het identificatienummer van het Rijksregister van de natuurlijke personen in hoofde van de administratie Werkgelegenheid van het Ministerie van de Vlaamse Gemeenschap voor het vervullen van taken met betrekking tot de programma's voor wedertewerkstelling.*

identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is.

31. De persoonsgegevens worden uitsluitend en tijdelijk in de database *FieldInspection* bijgehouden indien de sociaalrechtelijk inspecteur vrijwillig een geïdentificeerde persoon, onderneming of werf toevoegt aan een controle. De opslag gebeurt niet op het toestel en blijft voorts beperkt tot de voormelde persoonsgegevens. Er is bijgevolg geen sprake van het onverkort kopiëren van alle persoonsgegevens die in de verschillende authentieke bronnen werden geraadpleegd. Bij de beëindiging van de controle wordt op basis van de geregistreerde persoonsgegevens op een beveiligde server een tekstbestand gecreëerd. Het wordt verstuurd naar de eBox van de betrokken sociaal inspecteurs en daarin drie dagen bewaard en dan automatisch gewist. Aan de hand van dat (beperkt) tekstbestand (met de identiteit van de betrokken partijen en de commentaren over het onderzoek) kunnen de sociaalrechtelijk inspecteurs overgaan tot het raadplegen van de authentieke persoonsgegevensbronnen. Het systeem zorgt voor de automatische verwijdering na 72 uren van het rapport uit de eBox en na 24 uren uit de tijdelijke database *FieldInspection*.

B.5. BEVEILIGING

32. 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”).
33. Het Informatieveiligheidscomité beoordeelt de veiligheid van het systeem tot raadpleging van de persoonsgegevensbanken uit het netwerk van de sociale zekerheid met mogelijkheid tot tijdelijke opslag van een beperkte set van geraadpleegde persoonsgegevens. Het heeft dat bovendien eerder reeds gedaan in zijn beraadslaging 20/126 van 31 juli 2020, gewijzigd op 7 december 2021, over de raadpleging van diverse persoonsgegevensbanken door diverse (federale) sociale inspectiediensten door middel van de toepassing MyDIA. Met die toepassing kunnen de sociaalrechtelijk inspecteurs de geraadpleegde persoonsgegevens linken aan een controle waarvan ze deelnemende actor zijn en die hoogstens drie dagen opslaan, samen met informatie over de interpretatie van hun bevindingen. Bij de beëindiging van de controle wordt op basis van de geregistreerde persoonsgegevens een beperkt tekstbestand gecreëerd en verstuurd naar de eBox van de bevoegde inspecteurs, waarin het drie dagen wordt bewaard en dan automatisch wordt gewist. Derden zouden geenszins toegang hebben tot de aldus verwerkte persoonsgegevens. Het tijdelijk bewaren van de persoonsgegevens beoogt de vervanging van het huidige papieren dossier (onderzoek) door een veiliger elektronisch dossier (onderzoek).
34. De communicatie tussen de server en de toepassing op het mobiele toestel wordt beveiligd door middel van encryptie. De gebruiker van de toepassing wordt door de server geïdentificeerd met een authenticatiemiddel equivalent aan niveau 450 zoals bepaald door de *Federal Authentication Service* (FAS). De sessie is beperkt in de tijd en de gebruiker meldt zich op regelmatige tijdstippen opnieuw aan.

35. De toegang tot de toepassing en de informatie die door de toepassing op het mobiele toestel beschikbaar is, wordt beveiligd door een *Mobile Device Management* (MDM) of een equivalent systeem dat valt onder de controle van de organisatie onder wiens bevoegdheid de inspectiediensten opereren. Hierbij worden minstens de volgende veiligheidsmaatregelen afgedwongen.

- de toepassing MyDIA en de geassocieerde bewaarde informatie worden gescheiden van de niet-professionele toepassingen op het mobiele toestel door middel van encryptie (containerization⁴);
- de toegang tot de container wordt beperkt tot de beoogde gebruiker door middel van een voldoende complex paswoord of door middel van biometrische informatie van de gebruiker;
- de organisatie heeft de mogelijkheid om minstens de containers op het mobiele toestel te wissen in geval van verlies of diefstal of wanneer het niet langer wenselijk is de informatie en de toegang ter beschikking te stellen van de gebruiker (remote wiping);
- vóór de toepassing wordt opgestart en toegang tot informatie wordt verleend, wordt een nazicht van het *Operating Systeem* (OS) van het mobiele toestel doorgevoerd. Indien er aanwijzingen zijn dat dit OS niet langer als veilig geldt, wordt de toegang tot informatie geweigerd en worden de bewaarde gegevens gewist;
- er is sprake van een verificatie inzake het gebruik van een beveiligingssoftware die het toestel beschermt tegen virussen en de kans op hacking beperkt;
- er wordt een controle inzake "jailbreaking"⁵ van het toestel gerealiseerd.

Deze verplichting rust op de verwerkingsverantwoordelijke en het komt eveneens iedere gebruiker toe om de nodige voorzorgsmaatregelen te nemen bij het gebruik van de toepassing.

36. De organisatie richt de nodige processen in om de veiligheid inzake het gebruik van de toepassing mee te ondersteunen. Zij zorgt voor de ontwikkeling of aanpassing van de *Acceptable Use Policy* met betrekking tot het gebruik van mobiele toestellen, met minstens aandacht voor de paswoordbeveiliging door de gebruiker, de installatie van een antivirusprogramma, het gebruik van WIFI-netwerken en publieke laadpunten, het afschakelen van de mogelijkheid tot toegang tot het toestel middels *Mass Storage Device* (MSD), het jailbreaken of rooten van het toestel, de encryptie van het toestel, het updaten van de OS en de software, het installeren van toepassingen en het toekennen van toegangsrechten aan deze toepassingen. Zij regelt voldoende awareness programma's, die de risico's met betrekking tot het gebruik van mobiele toestellen onder de aandacht van de gebruikers brengen, alsook een incident management proces, dat rekening houdt met het verlies van mobiele toestellen en voorziet in het wissen van de gegevens van de toepassing en het stoppen van de toegang tot de toepassing en de authentieke bronnen. Ze voorziet dat processen met betrekking tot veranderingen in het personeelsbestand ook rekening houden met het toekennen en schrappen van toegangen van gebruikers via het mobiele toestel en met het wissen van de informatie. De organisatie voorziet ook regelmatig een DPIA voor deze toepassing en neemt gepaste maatregelen met betrekking tot nieuwe risico's. De nodige

⁴ Het opdelen van onderdelen van een applicatie in afzonderlijke blokken, i.e. containers.

⁵ Het 'kraken' van het besturingssysteem.

maatregelen moeten worden getroffen zodat de data die worden verzameld in de MyDIA toepassing niet kunnen worden gekopieerd en verzonden via een andere, private toepassing op het toestel van de gebruiker.

37. De uitwisseling van persoonsgegevens geschiedt in beginsel met de tussenkomst van de Kruispuntbank van de Sociale Zekerheid, overeenkomstig artikel 14 van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*.
38. Voor de toegang tot het Rijksregister en de Kruispuntbankregisters, de DIMONA-databank, de DMFA-databank, de *UnemploymentData*, de *LivingWages*, het Algemeen Repertorium van de Zelfstandige Arbeiders (ARZA), de persoonsgegevens over de arbeidsongeschiktheid en de persoonsgegevens van de Dienst Inschrijvingen Voertuigen gaat het om een fysieke tussenkomst, waarbij de Kruispuntbank van de Sociale Zekerheid haar klassieke rol vervult.
39. Voor de toegang tot het werkgeversrepertorium, de LIMOSA-databank, het GOTOT-bestand, het bestand van de werfmeldingen, de databank “aanwezigheidsregistratie” (CheckIn@Work) en het platform Single Permit gaat het om een niet-fysieke tussenkomst, zonder dat daarbij afbreuk wordt gedaan aan de opdrachten die de organisatie doorgaans vervult bij mededelingen van persoonsgegevens. Ze komt in dit geval op een specifieke (technische) wijze tussen. Per instantie die gebruik maakt van de MyDIA-toepassing dwingt ze gepaste regels inzake toegangsbeheer en toegangsmachtigingen af. Ze staat daarenboven in voor het loggen van alle ingaande en uitgaande mededelingen van persoonsgegevens.
40. Voor zover het departement Werk en Sociale Economie voor de realisatie van dit project een beroep doet op een verwerker, wordt de relatie tussen de beide partijen onverkort geregeld overeenkomstig de bepalingen van artikel 28 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*.
41. Alle medewerkers van de afdeling Vlaamse Sociale Inspectie zijn gehouden aan een vertrouwelijkheidsplicht. Ingevolge artikel 8, § 1, van het decreet van 30 april 2004 *tot uniformisering van de toezichts-, sanctie- en strafbepalingen die zijn opgenomen in de regelgeving van de sociaalrechtelijke aangelegenheden waarvoor de Vlaamse Gemeenschap en het Vlaamse Gewest bevoegd zijn* nemen de sociaalrechtelijke inspecteurs de nodige maatregelen om het vertrouwelijk karakter te respecteren van de gegevens waarvan ze kennis hebben gekregen in de uitoefening van hun opdracht en kunnen zij deze gegevens uitsluitend aanwenden voor de uitoefening van hun toezichts- en controleopdrachten.
42. Het departement Werk en Sociale Economie heeft een functionaris voor gegevensbescherming aangeduid met toepassing van artikel 28 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*.

43. Bij de verwerking van de persoonsgegevens houden de partijen rekening met de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid* en elke andere 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 federale overheid van het informatieveiligheidscomité

dat de raadpleging van de databank MOBIVIS van de FOD Mobiliteit en het Single Permit platform van de Dienst Vreemdelingenzaken van de FOD Binnenlandse Zaken door de afdeling Vlaamse Sociale Inspectie van het Departement Werk en Sociale Economie door middel van de toepassing My Digital Inspection Assistant (MyDIA), zoals in deze beraadslaging beschreven, is toegestaan 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.

Daniel HACHE
Voorzitter

De zetel van de kamer federale overheid van het Informatieveiligheidscomité is gevestigd in de kantoren van de FOD
Beleid en Ondersteuning, op volgend adres: Simon Bolivarlaan 30, 1000 Brussel.