CBPL
Commissie voor de bescherming van de persoonlijke levenssfeer

KSZ-BCSS

Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid
Afdeling "Sociale Zekerheid"

SCSZ/12/089

AANBEVELING NR. 12/01 VAN 8 MEI 2012 MET BETREKKING TOT DE WEBTOEPASSING DOLSIS

Gelet op de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*, inzonderheid op artikel 46, § 1;

Gelet op het auditoraatsrapport van de Kruispuntbank van de Sociale Zekerheid van 25 april 2012;

Gelet op het verslag van de Voorzitter.

A. ONDERWERP

1. In het kader van diverse controles en fraudeonderzoeken hebben de gemeenschappen en gewesten behoefte aan middelen om vanuit het netwerk van de sociale zekerheid op een beveiligde, efficiënte en uniforme manier een elektronische mededeling van persoonsgegevens te kunnen verkrijgen.

2. De federale inspectiediensten van de sociale zekerheid gebruiken hiervoor de GENESIS-toepassing, een webtoepassing die rechtstreeks de persoonsgegevens gaat raadplegen bij de Rijksdienst voor Sociale Zekerheid of de Rijksdienst voor Sociale Zekerheid van de Provinciale en Plaatselijke Overheidsdiensten (zie beraadslaging nr. 04/44 van 7 december 2004). Andere inspectiediensten en administratieve diensten kunnen hier niet meer op aansluiten vermits de uitwisseling van persoonsgegevens via GENESIS niet met tussenkomst van de Kruispuntbank van de Sociale Zekerheid gebeurt.

3. Om aan de hogervermelde behoeften tegemoet te komen, werd de nieuwe webtoepassing DOLSIS ontwikkeld, die gebaseerd is op GENESIS en een optimalisering van de strijd tegen fraude en een harmonisering van de werkingsmiddelen van de betrokken inspectiediensten beoogt.

4. De DOLSIS-doelgroep bestaat uit een beperkt aantal overheidsdiensten die bepaalde persoonsgegevens uit het netwerk van de sociale zekerheid willen opvragen en die, gelet op het beperkt aantal bevragingen, niet in een eigen ontwikkeling kunnen voorzien voor de integratie en de raadpleging via de standaardstromen en webservices.

5. In het DOLSIS-project is de huidige basisbehoefte het identificeren van een werknemer en een werkgever en het online zicht krijgen op de actuele tewerkstellingspersoonsgegevens. Voor de identificatie van natuurlijke personen zal de toepassing verwijzen naar het Rijksregister van de natuurlijke personen en/of naar de (subsidiaire en complementaire) Kruispuntbankregisters. Voor de tewerkstelling gaat het om persoonsgegevens van de Rijksdienst voor Sociale Zekerheid en de Rijksdienst voor Sociale Zekerheid van de Provinciale en Plaatselijke Overheidsdiensten, meer bepaald persoonsgegevens uit het personeelsbestand van de werkgevers, het werkgeversrepertorium, het LIMOSA-kadaster en de DMFA-persoonsgegevensbank.

6. Er zijn twee types gebruikers van DOLSIS: enerzijds de inspectiediensten en anderzijds de administratieve diensten (met uitzondering van het ondersteunend administratief personeel dat werkt in opdracht van de inspectiediensten).

   De gebruikers die persoonsgegevens opzoeken aan de hand van de identiteit van de werkgever en de identiteit van de werknemer (typisch voor de inspectiediensten) kunnen zowel opvragingen aangaande natuurlijke personen (via de naam en/of het identificatienummer van de sociale zekerheid) als opvragingen aangaande rechtspersonen (via de benaming en/of het ondernemingsnummer) verrichten. In de DOLSIS-webtoepassing kunnen ze uitgaande van een werknemer van de ene werkgever naar de andere werkgever navigeren. Voor de natuurlijke personen die het voorwerp van een raadpleging uitmaken, is geen voorafgaande integratie in het verwijzingsrepertorium van de Kruispuntbank van de Sociale Zekerheid noodzakelijk.

   Een tweede type van gebruikers zoekt uitsluitend persoonsgegevens op aan de hand van de identiteit van de natuurlijke persoon (typisch voor de administratieve diensten). Hier is een voorafgaande integratie van het dossier in het verwijzingsrepertorium van de Kruispuntbank van de Sociale Zekerheid noodzakelijk. Op basis van de naam en/of het identificatienummer van de sociale zekerheid kan de gebruiker de specifieke tewerkstellingspersoonsgegevens en de identificatiepersoonsgegevens van de bijbehorende werkgever raadplegen. Dit type gebruiker kan niet op basis van de identiteit van de werkgever alle werknemers opvragen of verder vrij navigeren. De raadpleging blijft beperkt tot de nuttige persoonsgegevens van de betrokken natuurlijke persoon.

B. VEILIGHEIDSMAATREGELEN

7. Voor de (online) toegang worden twee middelen ter beschikking gesteld van de verschillende diensten.

   Enerzijds de *DOLSIS-webtoepassing*, voor de dienst zonder eigen ontwikkeling waarbij persoonsgegevens uit het netwerk van de sociale zekerheid geraadpleegd worden.

Anderzijds de *DOLSIS-webservice*, die wordt opgeroepen door de DOLSIS-webtoepassing. De webservice staat ook ter beschikking van eindgebruikers die een eigen datapresentatie maken en wordt dan geïntegreerd in een eigen toepassing.

8. Deze mededelingen van persoonsgegevens zullen gebeuren met 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.*

De Kruispuntbank van de Sociale Zekerheid coördineert de vragen aan de verschillende authentieke bronnen van persoonsgegevens. Elk betrokken lid van het netwerk van de sociale zekerheid zorgt voor de coördinatie van zijn persoonsgegevensbronnen.

Het verkregen antwoord wordt door de Kruispuntbank van de Sociale Zekerheid verwerkt en gefilterd in functie van de bestemmeling van de persoonsgegevens (bepaalde bestemmelingen mogen bijvoorbeeld niet over alle beschikbare DMFA-persoonsgegevens beschikken) volgens de specifieke machtigingen van de afdeling sociale zekerheid van het sectoraal comité van de sociale zekerheid en van de gezondheid.

9. De DOLSIS-webtoepassing bevindt zich op de portaalsite van de sociale zekerheid, in het gedeelte bestemd voor de professionals. Voor het geïntegreerde beheer van gebruikers en toegangen (identificatie, authenticatie en autorisatie) wordt gebruik gemaakt van basisdiensten zoals uitgewerkt voor het portaal van sociale zekerheid met het systeem van "*user and access management*" (UAM) voor professionals. De gebruiker dient zich eenduidig te authentiseren door middel van het authenticatiecertificaat op zijn elektronische identiteitskaart (hij logt met zijn elektronische identiteitskaart in op het portaal). Na een geslaagde authenticatie en een positieve controle van de autorisaties via het UAM-systeem van het portaal van de sociale zekerheid, roept de DOLSIS-webtoepassing de achterliggende DOLSIS-webservice op.

De beveiliging op transportniveau gebeurt door het gebruik van HTTPS via "*two-way SSL*" (zowel cliënt- als serverauthenticatie).

Indien de betrokken entiteit een eigen webtoepassing wenst te gebruiken om de DOLSIS-webservice op te roepen, dienen minimaal dezelfde veiligheidsmaatregelen gerespecteerd te worden als voor de DOLSIS-webtoepassing: sterke authenticatie van de gebruiker (door middel van de elektronische identiteitskaart), beveiligde verbinding met de DOLSIS-webservice ("*two-way SSL*"), verificatie van de autorisatie via het UAM en verzekeren van loggings (zie verder).

De documentatie voor de evaluatie van de veiligheid van de zelf ontwikkelde webtoepassing dient steeds ter inzage beschikbaar te zijn voor de afdeling sociale zekerheid van het sectoraal comité van de sociale zekerheid en van de gezondheid.

10. Bij de betrokken entiteit dient een informatieveiligheidsconsulent aangeduid te worden. Deze informatieveiligheidsconsulent staat, met het oog op de veiligheid van de persoonsgegevens die door zijn opdrachtgever worden verwerkt en met het oog op de

bescherming van de persoonlijke levenssfeer van de personen op wie deze persoonsgegevens betrekking hebben, in voor het verstrekken van deskundige adviezen aan de persoon belast met het dagelijks bestuur en voor het uitvoeren van opdrachten die door deze laatste worden toevertrouwd. Hij heeft een adviserende, stimulerende, documenterende en controlerende opdracht inzake informatieveiligheid.

Hij vervult tevens de functie van aangestelde voor de gegevensbescherming, bedoeld in artikel 17bis van de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*.

Hij staat in voor het uitvoeren van het informatieveiligheidsbeleid van zijn opdrachtgever. Daartoe kan hij in voorkomend geval een beroep doen op het document "*referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens*" van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer.

11. De betrokken entiteit dient tevens rekening te houden met de minimale veiligheidsnormen zoals bepaald door het Algemeen Coördinatiecomité van de Kruispuntbank van de Sociale Zekerheid en goedgekeurd door het sectoraal comité van de sociale zekerheid en van de gezondheid.

12. Uit de door de aanvrager meegedeelde stukken dient te blijken dat de betrokken entiteit over een informatieveiligheidsbeleid beschikt en dat dit ook praktisch op het terrein geïmplementeerd wordt. Er dient voldoende aandacht besteed te worden aan de wijze van sensibilisering omtrent de veiligheidsproblematiek en aan de nodige opleidingen met betrekking tot de informatieveiligheid.

13. Inzake identificatie- en authenticatieprocedure dient uit het meegedeelde dossier te blijken welke soort infrastructuur aangewend wordt. Daarbij dient ook onder andere een onderscheid te worden gemaakt tussen het werkstation (zowel vaste pc als laptop) met directe (fysieke) verbinding met het interne netwerk van de betrokken entiteit en de laptop zonder directe verbinding (connectie via VPN) voor de toegang tot de persoonsgegevensbanken uit het netwerk van de sociale zekerheid.

14. Telewerk (de mogelijkheid om zich vanop afstand te verbinden met het interne netwerk van de betrokken entiteit, veelal waar de toezichtsopdracht uitgevoerd wordt) en het gebruik van een laptop zijn twee essentiële factoren in de werkwijze van inspectiediensten. Ook kunnen administratieve diensten telewerk als werkwijze aan hun personeel aanbieden.

15. De werkgroep Informatieveiligheid van het Algemeen Coördinatiecomité van de Kruispuntbank van de Sociale Zekerheid heeft in het kader van de ontwikkeling van een gemeenschappelijk informatieveiligheidsbeleid een aantal veiligheidspolicy's opgesteld en goedgekeurd met betrekking tot de volgende belangrijke domeinen: "Veiligheidsbeleid voor de laptops", "Beleid voor de beveiliging van werkstations" en "Beleid voor toegang op afstand – Technisch beleid voor de klantinstellingen en de eindgebruikers".

16. Het sectoraal comité van de sociale zekerheid en van de gezondheid wijst op de noodzaak om, wanneer gebruik wordt gemaakt van een werkstation (zowel vaste pc als laptop) dat al

dan niet verbonden is met het netwerk van de Kruispuntbank van de Sociale Zekerheid, de regels die door de werkgroep Informatieveiligheid werden geformuleerd in de policy "Beleid voor de beveiliging van werkstations" toe te passen.

17. Het sectoraal comité van de sociale zekerheid en van de gezondheid wijst tevens op de noodzaak voor de betrokken entiteit om bij het gebruik van een laptop, al dan niet verbonden met het netwerk van de Kruispuntbank van de Sociale Zekerheid, de regels geformuleerd door de werkgroep Informatieveiligheid toe te passen, waaronder de volgende:

- de portable en zijn randapparatuur, die aan de gebruiker ter beschikking worden gesteld in het kader van zijn beroepsactiviteiten, zijn en blijven eigendom van de betrokken instelling;

- wanneer hij de instelling verlaat of van functie verandert, moet de gebruiker de portable en zijn randapparatuur die hem ter beschikking werden gesteld terugbezorgen;

- behoudens expliciete toestemming van de persoon die belast is met het dagelijks beheer van de opdrachtgever en mits naleving van de bijkomende voorwaarden uit de policy "Beleid voor toegang op afstand – Technisch beleid voor de klantinstellingen en de eindgebruikers", mag enkel de aangeduide gebruiker de ter beschikking gestelde portable en randapparatuur gebruiken, zelfs indien geen gebruik wordt gemaakt van een netwerkverbinding;

- het is de gebruiker verboden om andere randapparatuur dan deze die samen met de portable geleverd werd aan te sluiten zonder de uitdrukkelijke toestemming van de bevoegde dienst;

- het ter beschikking stellen van een portable aan een gebruiker betekent niet dat hij meer toegangsrechten ontvangt dan hem toegekend werden in het raam van het gebruik van een vaste pc. Dit geldt zowel voor de toegang tot de toepassingen als voor het gebruik van e-mail en internet of iedere andere functionaliteit. Er kunnen evenwel maatregelen getroffen worden om de toegangsrechten te wijzigen;

- om de veiligheid van het hem toevertrouwde materiaal te waarborgen, dient de gebruiker te handelen als een goede huisvader en alles in het werk te stellen om het materiaal en de informaticagegevens veilig te stellen. In de policy worden hieromtrent strikte regels vastgesteld;

- de gebruiker moet onder meer vermijden om zijn portable onbewaakt achter te laten. Het is aanbevolen om deze achter slot te bewaren in een kast of een bureau. Wanneer hij het lokaal waarin zijn portable actief is tijdelijk verlaat, moet de gebruiker zijn portable vergrendelen of de beveiligde screensaver activeren alvorens hij het lokaal verlaat;

- bij verlies of diefstal moet de gebruiker onmiddellijk de bevoegde dienst van zijn opdrachtgever verwittigen en de richtlijnen opvolgen;

- behoudens tegenbericht van de persoon belast met het dagelijks bestuur staat enkel de bevoegde dienst in voor de installatie of het onderhoud van een software op de draagbare pc of voor de configuratie ervan;

- de regels inzake definiëring, frequentie van de wijzigingen en wijze van opslag van de authenticatiemiddelen (bijvoorbeeld paswoord) moeten strikt toegepast worden;

- de gevoelige persoonsgegevens moeten opgeslagen worden in het netwerk ofwel moeten de regels bepaald in de policy "Beleid voor toegang op afstand – Technisch beleid voor de klantinstellingen en de eindgebruikers" worden nageleefd. In ieder geval moet de bewaring van gevoelige persoonsgegevens op de portable vermeden worden en moeten ze zo snel mogelijk opgeslagen worden in het netwerk;

- gevoelige persoonsgegevens mogen enkel versleuteld op de draagbare pc en zijn randapparatuur worden bewaard. Als de randapparatuur (bijvoorbeeld de USB-sleutel) geen versleutelde opslag toelaat, is het registreren van vertrouwelijke persoonsgegevens op deze apparatuur expliciet verboden;

- de portable-persoonsgegevens worden opgeslagen (back-up) volgens de strategie die door de opdrachtgever vastgesteld werd inzake het gebruik van vaste pc's. Enkel de netwerkgegevens worden automatisch opgeslagen. Bijzondere aandacht moet worden besteed aan de back-up van de lokale schijf.

18. Met betrekking tot het gebruik van een vaste pc in een gebouw van de opdrachtgever, mag de betrokken entiteit in geen geval afwijken van de toepasselijke regels en dient hij zich te houden aan het beleid dat vastgesteld werd in de minimale veiligheidsnormen van het netwerk van de Kruispuntbank van de Sociale Zekerheid, die in het hoofdstuk "Logische toegangsbeveiliging" onder meer stellen dat elke instantie aangesloten op het netwerk van de Kruispuntbank van de Sociale Zekerheid de toegang tot de persoonsgegevens nodig voor het uitvoeren van haar opdrachten moet beveiligen door middel van een identificatie-, authenticatie- en autorisatiesysteem.

19. De afdeling sociale zekerheid van het sectoraal comité van de sociale zekerheid en van de gezondheid vestigt bovendien de aandacht op de noodzaak voor de betrokken entiteit om bij het gebruik van een laptop vanop een externe locatie (indien er dus geen directe fysieke verbinding met het netwerk mogelijk is) de door de werkgroep Informatieveiligheid geformuleerd regels toe te passen, waaronder de volgende:

Beleid op het niveau van het systeem

- het gebruik van het VPN-protocol is verplicht bij iedere verbinding met het lokale netwerk van de betrokken entiteit die dient voor de raadpleging van de betrokken persoonsgegevensbanken;

- het gebruikte VPN-systeem moet ten minste aan de veiligheidsvereisten voldoen zoals beschreven in de door de werkgroep Informatieveiligheid opgestelde policy "Beleid voor toegang op afstand – Technisch beleid voor de klantinstellingen en de eindgebruikers";

- de dienst die verantwoordelijk is voor het beheer van de pc's dient het initiatief te nemen voor een regelmatige controle van de portables teneinde de naleving van de configuratie te controleren, met inbegrip van de configuratie van de veiligheidssoftware. In geval van niet-naleving dient de hiërarchie van de gebruiker of de dienst die bevoegd is voor het beheer van de pc's verslag uit te brengen bij de veiligheidsdienst van de opdrachtgever over de eventuele schade voor laatstgenoemde.

Beleid voor de eindgebruikers

- er is de verplichting om de verschillende authenticatieniveaus in acht te nemen zoals vastgesteld in de veiligheidspolicy "Beleid voor toegang op afstand – Technisch beleid voor de klantinstellingen en de eindgebruikers";

- er is eveneens de verplichting om de aanbeveling inzake persoonsgegevensbescherming op te volgen;

- de configuratie van de portable moet verplicht de verschillende veiligheidstools omvatten die vereist zijn in de veiligheidspolicy "Beleid voor toegang op afstand – Technisch beleid voor de klantinstellingen en de eindgebruikers" en dient onverkort de regels na te komen die inzake installatie, configuratie, controle van de softwareversie en gebruik van deze tools vastgesteld werden;

- de regels inzake gebruik van de randapparatuur moeten nageleefd worden;

- de betrokken entiteit dient ervoor te zorgen dat de betrokken inspecteurs en administratieve medewerkers een gepaste opleiding over het gebruik van hun portable kunnen volgen, waarin de veiligheidsrisico's uitgelegd worden.

20. Uit het ingediende dossier dient te kunnen worden afgeleid dat de situatie bij de betrokken entiteit in overeenstemming lijkt met de vereisten inzake het gebruik van een vaste pc of een portable die al dan niet aangesloten is op het netwerk van de Kruispuntbank van de Sociale Zekerheid.

21. Voor de betrokken entiteit wordt de aandacht gevestigd op de noodzaak om het sectoraal comité in te lichten en documentatie te verschaffen in geval van evolutie naar nieuwe technieken of nieuwe toegangswijzen tot de persoonsgegevensbanken uit het netwerk van

de sociale zekerheid in het raam van de werkzaamheden van hun inspectiediensten en/of administratieve diensten.

22. De DOLSIS-webtoepassing houdt loggings bij met per mededeling een aanduiding van wie wanneer over wie welke persoonsgegevens heeft verkregen voor welke doeleinden.

Deze loggings zijn toegankelijk via de portaaltoepassing IRIS. De toegang tot deze loggings vereist een sterke authenticatie door middel van de elektronische identiteitskaart.

In geval van gebruik van een zelf ontwikkelde webtoepassing dient de betrokken entiteit te voorzien in een gelijkwaardig systeem van loggings.

23. Deze loggings zullen minstens gedurende tien jaar worden bewaard met het oog op het behandelen van eventuele klachten of het opsporen van eventuele onregelmatigheden met betrekking tot de verwerking van de persoonsgegevens.

De loggings zelf dienen te worden beveiligd aan de hand van maatregelen die de vertrouwelijkheid, de integriteit en de beschikbaarheid garanderen.

Ze worden aan het sectoraal comité van de sociale zekerheid en van de gezondheid en aan de Kruispuntbank van de Sociale Zekerheid overgemaakt indien zij daarom verzoeken.

24. Het sectoraal comité van de sociale zekerheid en van de gezondheid benadrukt de rol van de informatieveiligheidsconsulent van de betrokken entiteit, die erover moet waken dat de technische middelen die ter beschikking worden gesteld van de inspecteurs en/of de administratieve diensten in overeenstemming zijn met enerzijds de veiligheidspolicy's die door de werkgroep Informatieveiligheid van het Algemeen Coördinatiecomité van de Kruispuntbank van de Sociale Zekerheid uitgewerkt werden en anderzijds het specifieke informatieveiligheidsbeleid van de betrokken entiteit.

25. De informatieveiligheidsconsulent van de betrokken entiteit zal daarom toezien op de strikte toepassing van het informatieveiligheidsbeleid betreffende het gebruik van een portable, telewerk (toegang op afstand), het gebruik van e-mail en internet, het gebruik van authenticatiemiddelen en de activering, bewaring en archivering van de loggings die garant staan voor de traceerbaarheid van de toegangen.

26. Bovendien zal de informatieveiligheidsconsulent, indien dit nog niet gebeurd is, instaan voor de organisatie van een procedure waardoor hij geïnformeerd wordt over:

- de correcte toepassing van de maatregelen die aan het sectoraal comité van de sociale zekerheid en van de gezondheid meegedeeld worden in geval van langdurige afwezigheid of vertrek van een inspecteur;

- de inventaris en de toestand van het computerpark en het bijhorende materiaal dat aan de inspecteurs en het ondersteunende administratief personeel ter beschikking wordt gesteld;

- de incidenten die eigen zijn aan het gebruik van de portables en het bijhorende materiaal;

- het correcte gebruik, binnen de betrokken inspectiedienst, van de verleende machtigingen in functie van de reële behoeften van iedere inspecteur.

C. CONTROLEPROCEDURE

27. Een logging waarborgt de integriteit van de gebruikers van het netwerk van de Kruispuntbank van de Sociale Zekerheid. Het is daarom belangrijk om steeds de begrippen "wie", "wat" en "wanneer" te kunnen rechtvaardigen en om, in de context van de inspecteurs, deze informatie te kunnen toetsen aan de opdrachtverslagen.

Om het sectoraal comité een rechtmatig gebruik van de verleende machtigingen te garanderen in het kader van de raadplegingen door inspectiediensten waarvoor geen voorafgaande integratie in het verwijzingsrepertorium van de Kruispuntbank van de Sociale Zekerheid noodzakelijk is, wordt naar analogie met de federale sociale inspectiediensten (zie beraadslaging nr. 04/32 van 5 oktober 2004) een specifieke controleprocedure voor de betrokken inspectiediensten ingevoerd, waarbij twee welomschreven contexten beoogd worden.

28. *In het kader van een automatische procedure van opvolging van de opdrachtverslagen en de naleving van de finaliteits- en proportionaliteitsprincipes.*

De controles betreffen de raadplegingen in de persoonsgegevensbanken die gespreid doorheen de tijd worden uitgevoerd ofwel door de inspecteurs van de betrokken inspectiedienst (vanop verschillende locaties) ofwel door het ondersteunende administratief personeel van de inspecteurs op vraag van deze laatste (op het bureau in het gebouw van de betrokken entiteit en tijdens de kantooruren of via telewerk).

Op basis van een betekenisvol percentage behandelde dossiers zal de integriteit van de aanpak door de inspecteur worden gecontroleerd. Hiervoor zal de betrokken inspectiedienst, in het kader van een procedure die in overleg met haar informatieveiligheidsconsulent georganiseerd wordt, vragen om, in functie van de gebruikte werkwijze, uit de logbestanden de loggegevens te halen met betrekking tot een welbepaald aantal significante dossiers van de inspecteur in kwestie. Hij zal daarna het verkregen resultaat toetsen aan de verschillende opdrachtverslagen en de rechtmatigheid van de raadplegingen controleren ten aanzien van de door het sectoraal comité verleende machtigingen. Onder "significante dossiers" wordt verstaan: dossiers die verschillende periodes van het jaar bestrijken, verschillende dossiers die aan verschillende inspecteurs toevertrouwd werden en dossiers die representatief zijn voor de verleende machtigingen, de geraadpleegde persoonsgegevens en de opdrachten van de dienst.

29. *In het raam van een incident of een klacht.*

Alle klachten of incidenten dienen het voorwerp uit te maken van een specifieke controle. Onder incident wordt verstaan: iedere belangrijke gebeurtenis in de activiteit van een inspecteur, zoals het niet meedelen van zijn opdrachtverslagen, het verlies of de diefstal of het niet langer gebruiken van zijn portable of van ieder gevoelig materiaal dat hem in het kader van zijn functie toevertrouwd werd.

Verschillende scenario's zijn mogelijk:

- op basis van het identificatienummer van de inspecteur of van een ondersteunend administratief personeelslid de loggegevens analyseren met betrekking tot een periode van inactiviteit (vakantie of ziekte). Behoudens afwijking of rechtvaardiging zou het resultaat nihil moeten zijn;

- op basis van het identificatienummer van de inspecteur of van een ondersteunend administratief personeelslid de loggegevens analyseren met betrekking tot de week voorafgaand aan en volgend op de verdwijning van zijn pc of toegangstoken en het resultaat vergelijken met de opdrachtverslagen. In geval van een klacht dient de inhoud van de loggings vergeleken te worden met de elementen die door de aanklager geleverd worden en met de opdrachtverslagen.

30. Jaarlijks en uiterlijk tegen 28 februari (iedere vertraging in de indiening van het jaarlijks verslag dient het voorwerp uit te maken van een advies en een schriftelijk verzoek om afwijking bij het sectoraal comité), deelt de betrokken inspectiedienst aan het sectoraal comité, per brief ondertekend door de leidende ambtenaar, een beknopt verslag mee waarin de volgende informatie gegeven wordt.

31. *Algemeen.*

Aan de afdeling sociale zekerheid van het sectoraal comité van de sociale zekerheid en van de gezondheid dient een boordtabel te worden bezorgd waarin volgende vermeldingen worden opgenomen:

- het aantal medewerkers van de betrokken inspectiedienst waarop de verleende machtiging van toepassing is;

- het personeelsverloop (aantal indiensttredingen en uitdiensttredingen) in de dienst gedurende het afgelopen jaar;

- het aantal gerealiseerde toegangen mee te delen door de informaticadienst die belast is met het bijhouden van de loggings;

- het aantal opzoekingen in de loggings betreffende de opvolging van de dossiers en de naleving van de finaliteits- en proportionaliteitsregels;

- het aantal incidenten en klachten en de opzoekingen in de betrokken loggings.

32. *Verslag over de toegangscontroles.*

In een vrij formaat zal de betrokken inspectiedienst het sectoraal comité van de sociale zekerheid en van de gezondheid informeren over het resultaat van de toetsing van de verschillende opzoekingen in de loggings aan de opdrachtverslagen. In een afzonderlijk hoofdstuk worden de gerealiseerde onderzoeken in het kader van klachten of incidenten en de verkregen resultaten beschreven, alsook de eventuele getroffen sancties.

In zijn conclusie zal de betrokken inspectiedienst het sectoraal comité inlichten over de eventuele maatregelen die getroffen werden om de controle binnen de dienst te verbeteren.

Het verslag zal ook voor iedere betrokken persoonsgegevensbank het gebruikspercentage aanduiden (hoeveel procent van alle raadplegingen van de persoonsgegevensbanken die onder de machtiging vallen vertegenwoordigt de raadpleging van een bepaalde persoonsgegevensbank).

Om deze redenen, beslist

de afdeling sociale zekerheid van het sectoraal comité van de sociale zekerheid en van de gezondheid

dat elke instantie die via DOLSIS toegang wenst te krijgen tot persoonsgegevens van het netwerk van de sociale zekerheid een aparte machtigingsaanvraag moet indienen bij het sectoraal comité van de sociale zekerheid en van de gezondheid, waarin de lijst van persoonsgegevens en het doeleinde uitdrukkelijk worden vermeld

en

dat een machtiging slechts kan worden verleend op voorwaarde dat de hogervermelde veiligheidsmaatregelen worden gerespecteerd en op voorwaarde dat de betrokken instantie gemachtigd is om toegang te hebben tot het Rijksregister van de natuurlijke personen en om gebruik te maken van het identificatienummer van het Rijksregister van de natuurlijke personen.

Yves ROGER
Voorzitter