

**Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid
Afdeling « Sociale Zekerheid »**

SCSZ/10/021

**ADVIES NR 10/03 VAN 2 FEBRUARI 2010 BETREFFENDE DE AANVRAAG VAN
DE RIJKSDIENST VOOR JAARLIJKSE VAKANTIE (RJV) VOOR HET
VERKRIJGEN VAN EEN MINISTERIËLE ERKENNING VOOR EEN
ELEKTRONISCH ARCHIVERINGSSYSTEEM IN TOEPASSING VAN HET
KONINKLIJK BESLUIT VAN 22 MAART 1993 BETREFFENDE DE
BEWIJSKRACHT**

Gelet op de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid, inzonderheid op artikel 15, tweede lid;

Gelet op de aanvraag van de Rijksdienst voor Jaarlijkse Vakantie (RJV) van 7 december 2009;

Gelet op het auditoraatsrapport van de Kruispuntbank van 27 januari 2010;

Gelet op het verslag van de heer Yves Roger.

A. CONTEXT EN ONDERWERP VAN DE AANVRAAG

- 1.1.** De Rijksdienst voor Jaarlijkse Vakantie (*RJV*) heeft op 7 december 2009 een erkenningsaanvraag ingediend bij het Sectoraal Comité van de Sociale Zekerheid.

Deze aanvraag heeft het verkrijgen van een ministeriële erkenning voor haar procedures in het kader van de toepassing van het koninklijk besluit van 22 maart 1993 betreffende de bewijskracht, ter zake van de sociale zekerheid, van de door instellingen van sociale zekerheid opgeslagen, bewaarde of weergegeven informatiegegevens tot doel.

B. BEHANDELING VAN DE AANVRAAG

2. De evaluatie van de procedures die werden ingediend voor het verkrijgen van de ministeriële erkenning is opgesplitst volgens de technische voorwaarden van artikel 3 van het koninklijk besluit van 22 maart 1993.

Deze voorwaarden werden punt voor punt besproken in het dossier van de **RJV**.

Het auditoraatsrapport is het resultaat van een samenwerking met de verantwoordelijken en de interne en externe technici van de betrokken instelling.

Deze samenwerking omvatte verschillende stappen, namelijk:

- ✓ de overmaking door de instelling van een eerste versie van zijn dossier aan de informatieveiligheidsdienst van de Kruispuntbank van de Sociale Zekerheid (7 augustus 2009);
- ✓ het opstellen door de veiligheidsdienst van de Kruispuntbank van een reeks vragen over verschillende aspecten van de geïmplementeerde procedure;
- ✓ een werkvergadering op 28 oktober 2009 besteed aan een kritische analyse van het dossier;
- ✓ er werden tevens e-mails uitgewisseld met het oog op een kritische analyse van het dossier en om een aantal details te preciseren;
- ✓ het opstellen door de **RJV** van een dossier ten behoeve van het Sectoraal Comité van de Sociale Zekerheid (officiële versie: 7 december 2009);
- ✓ een bezoek (audit) van de Informatieveiligheidsdienst van de Kruispuntbank aan de site van de **RJV** waar een demonstratie en een vragenronde met de betrokken actoren plaatsvonden (12 januari 2010).

In bijlage bij dit rapport vindt u een document met daarin de antwoorden van de **RJV** op de opmerkingen die gemaakt werden door de dienst Informatieveiligheid van de Kruispuntbank.

Het voorstel omschrijft nauwkeurig de procedure.

- 2.1. De **RJV** heeft een voorstel ingediend ter erkenning van de bewijskracht voor de binnenkomende documenten die via haar documentbeheersysteem Uruk worden gescand, bewaard en verwerkt.

Uruk beheert de dossiers van de dienst Diverse Schuldeisers. Het systeem zorgt voor het elektronische beheer van de documenten (scannen, indexeren, archiveren, consulteren) in combinatie met een workflowsysteem, dat de routing van de documenten en de automatisering van welbepaalde taken beheert. De doelstelling van dit voorstel van de **RJV** is het bekomen van de bewijskracht voor de informatiegegevens, met het oog op de toepassing van de sociale zekerheid, die via het documentbeheersysteem Uruk worden opgeslagen, bewaard en weergegeven.

In het voorgestelde dossier worden de mechanismen, de controles en de tussenkomende partijen nauwkeurig omschreven.

De aangewende technologie waarborgt een getrouwe, duurzame en volledige weergave van de informatie.

2.2. Het door de **RJV** toegelichte dossier heeft ons ertoe aangezet na te gaan of de beschreven oplossing inzake elektronisch documentenbeheer de bepalingen van § 2 van artikel 3 van het koninklijk besluit van 22 maart 1993 wel naleeft.

Hiertoe hebben we bijzondere aandacht besteed aan de volgende aspecten:

- ✓ de componenten van de technische oplossingen (technische architectuur en software);
- ✓ het circuit van verwerking en scanning van de betrokken dragers;
- ✓ het automatische en manuele controlepunt volgens de fases van het proces;
- ✓ de overmaking van de elektronische documenten in het document management systeem (Uruk);
- ✓ de formaten van de bestanden en de overeenstemming ervan met de archiveringsstandaarden die de duurzaamheid van de geregistreerde gegevens garandeert (TIFF);
- ✓ het beheer van de incidenten, de fouten en de mechanismen van eventuele overname of verwerping van de informatie;
- ✓ de instructies voor de aanwending van de oplossing;
- ✓ afhandeling van het scanproces: de behandeling van een blanco bladzijde tijdens de scanning, de behandeling van documenten waarvan het formaat groter of kleiner is dan A4, ... ;
- ✓ het voorzien van onderhoudscontracten m.b.t. de geïnstalleerde soft- en hardware;
- ✓ de aanwezigheid van een interne supportafdeling;
- ✓ de maatregelen/controles die waarborgen dat er aan de opgeslagen informatiegegevens geen wijzigingen worden aangebracht;
- ✓ de controle van de kwaliteit en van de kwantiteit.

De informatie wordt systematisch geregistreerd.

2.3. In het dossier van de **RJV** worden de procedures beschreven met betrekking tot:

- ✓ de indexering van de documenten;
- ✓ de onmogelijkheid om gescande documenten te wijzigen of te verliezen of ze meermaals te registreren;
- ✓ de wijze van registratie en het geldigheidsmechanisme van de indexen;
- ✓ het opnieuw samenstellen van de indexen;
- ✓ de toegangsbeperking tot de indexen;
- ✓ de uitvoering van kwaliteits- en kwantiteitscontrole bij het inscannen van documenten.

Tijdens de demonstratie hebben we deze verschillende aspecten kunnen controleren.

De verwerkte informatie wordt op een zorgvuldige manier bewaard, systematisch gerangschikt en beschermd tegen elke vervalsing.

2.4. De **RJV** heeft onder meer de volgende maatregelen geïmplementeerd:

- ✓ de infrastructuur (o.a. servers, databank en file storage) is voldoende redundant uitgevoerd, waardoor de continuïteit van de dienstverlening en de reconstructie in geval van een belangrijk incident worden gewaarborgd;
- ✓ de gearchiveerde documenten worden bewaard in een repository (redundante opslagmedia); dagelijks worden de documenten in deze repository weggeschreven op LTO WORM tapes. Deze set van WORM tapes blijft permanent beschikbaar in de computerzaal van de **RJV**. Daarnaast wordt er nog op een externe site een extra kopie van de ingescande documenten op WORM tape bewaard;
- ✓ met betrekking tot het back-upstelsel zijn er duidelijke uitvoeringsregels volgens een vooraf bepaalde planning en rotaties van dragers in functie van de planning voorzien; deze procedures zijn in het globale back-upstelsel van de instelling opgenomen (back-up op tapes en archivering op WORM tapes verloopt via een gecentraliseerde backup, archive en recovery software);
- ✓ afdoende disaster recovery maatregelen werden genomen en uitgetest;
- ✓ afdoende maatregelen werden getroffen m.b.t. fysieke beveiliging van gebouw, apparatuur en back-ups tegen natuurlijke risico's zoals brand, wateroverlast, acclimatisatie- en elektriciteitsproblemen;
- ✓ voor de fysieke toegangscontrole wordt gebruik gemaakt van een centraal beheerd badgesysteem;
- ✓ de periode van retentie en bewaring van de dragers is vastgelegd;
- ✓ de logische toegangsbeveiliging berust op verschillende methodes naargelang het beoogde informatiesysteem en de aan de gebruikers toevertrouwde activiteiten; de toegangsrechten worden bepaald door middel van RBAC (role based access control);
- ✓ de aansluiting op het informatiesysteem is mogelijk via afdoende beveiligde werkposten binnen de instelling en via een beveiligde toegang op afstand (VPN oplossing van het extranet van sociale zekerheid);
- ✓ de betrokken toepassingen en software worden onderhouden d.m.v. een patchbeleid dat mogelijke zwakheden in de geïmplementeerde oplossing dicht. Testen, acceptatie en release van nieuwe versies van een component van de oplossing lopen in overeenstemming met het standaard **RJV** release management proces;
- ✓ als instelling van het primaire netwerk rond de Kruispuntbank van de Sociale Zekerheid leeft de **RJV** de minimale veiligheidsnormen na.

Bewaren van de volgende gegevens met betrekking tot de verwerking van de informatie: identiteit van de verantwoordelijke voor de verwerking evenals van diegene die ze heeft uitgevoerd, de aard en het onderwerp van de informatie waarop de verwerking betrekking heeft, de datum en de plaats van de verwerking, de eventuele storingsen die zijn vastgesteld tijdens de verwerking.

2.5. De **RJV** heeft zijn systeem uitgerust met:

- ✓ diverse automatische loggings- en opvolgingsbetanden waardoor de gebeurtenissen van de verschillende componenten in ieder stadium van het proces kunnen worden bewaard; de toegang tot deze informatie gebeurt volgens een beveiligd proces; de loggings worden mee in de standaard back-upprocedures van de instelling geïntegreerd.

Om deze redenen, verleent

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

een gunstig advies. Het door de **RJV** ingediende dossier blijkt te voldoen aan de technische voorwaarden van artikel 3 van het koninklijk besluit van 22 maart 1993.

Yves ROGER
Voorzitter

De zetel van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid is gevestigd in de kantoren van de Kruispuntbank van de Sociale Zekerheid, op volgend adres : Sint-Pieterssteenweg 375 – 1040 Brussel (tel. 32-2-741 83 11)

