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

SCSZ/13/266

ADVIES NR 13/104 VAN 3 DECEMBER 2013 BETREFFENDE DE AANVRAAG VAN PARTENA KINDERBIJSLAGFONDS VOOR HET VERKRIJGEN VAN EEN MINISTERIËLE ERKENNING VAN HET ELEKTRONISCH ARCHIVERINGSSYSTEEM IN TOEPASSING VAN HET KONINKLIJK BESLUIT VAN 22 MAART 1993 BETREFFENDE DE BEWIJSKRACHT VAN DE DOOR DE INSTELLINGEN VAN SOCIALE ZEKERHEID OPGESLAGEN, BEWAARDE OF WEERGEGEVEN INFORMATIEGEGEVENS

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 PARTENA Kinderbijslagfonds van 20 september 2013;

Gelet op het auditoraatsrapport van de Kruispuntbank van 26 november 2013;

Gelet op het verslag van de heer Yves Roger.

A. CONTEXT EN ONDERWERP VAN DE AANVRAAG

1.1. PARTENA Kinderbijslagfonds (kortweg PARTENA) heeft op 20 september 2013 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 PARTENA.

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

Het voorgelegde dossier en het bijhorend auditoraatsrapport hebben betrekking op de digitaliseringsprocedures van de in- en uitgaande documentenstroom. Het gaat om alle gedigitaliseerde papieren documenten die gebruikt worden in het proces voor het beheer van de dossiers inzake kinderbijslag van aangesloten rechthebbenden.

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

Het voorstel omschrijft nauwkeurig de procedure.

2.1. Het door PARTENA ingediend dossier bevat een beschrijving van de geïmplementeerde procedures voor de registratie en het zorgvuldig bewaren van de informatiegegevens aan de hand van de oplossing PARTENA GED (Gestion Electronique des Documents)**,** en de weergave ervan op een leesbare drager.

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 PARTENA 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;
- ✓ de formaten van de bestanden en de overeenstemming ervan met de archiveringsstandaarden die de duurzaamheid van de geregistreerde gegevens garandeert;
- ✓ 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 PARTENA 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. PARTENA heeft onder meer de volgende maatregelen geïmplementeerd:

- ✓ de infrastructuur (o.a. servers, databank en storage) is redundant uitgevoerd en over twee sites verspreid, waardoor de continuïteit van de dienstverlening en de reconstructie in geval van een belangrijk incident worden gewaarborgd;
- ✓ met betrekking tot het back-upsysteem 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-upsysteem van de instelling opgenomen;
- ✓ 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 logische toegangsbeveiliging berust op methodes waarbij 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) en de toegang wordt enkel verleend via de standaard IT security policy van PARTENA;

- ✓ 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 PARTENA release management proces;
- ✓ als instelling van het secundaire netwerk rond de Kruispuntbank van de Sociale Zekerheid dient PARTENA de minimale veiligheidsnormen na te leven.

Tijdens het plaatsbezoek was alle nodige documentatie (disaster recovery plannen, architectuur, handleidingen, security policies, …) ter inzage beschikbaar.

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 storingen die zijn vastgesteld tijdens de verwerking.

2.5. PARTENA 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.

3. *Aanbevelingen m.b.t. informatieveiligheid.*

- ✓ Op databankniveau (SQL Server) dienen de audit mogelijkheden voor de administrators te worden benut.
- ✓ Het gebruikte VPN-systeem moet ten minste aan de veiligheidsvereisten voldoen zoals beschreven in de door de werkgroep Informatieveiligheid1 opgestelde policy “Beleid voor toegang op afstand tot het interne netwerk". Belangrijke elementen hierbij zijn o.a. :
  - o authenticatie op meerdere niveaus (machine/eindgebruiker) en sterke authenticatie (2-factor authenticatie) van de eindgebruiker;
  - o vooraleer eindapparatuur (workstation) toegang krijgt tot het interne bedrijfsnetwerk, zal het VPN-systeem minimum nagaan of de goede versies antivirus software en virusdefinitie bestanden geïnstalleerd zijn.
- ✓ Het aantal gebruikers met administrator rechten op de workstations (laptop / vast pc) dient tot een minimum beperkt te worden. Gebruikersaccounts met speciale rechten mogen enkel gebruikt worden voor het uitvoeren van specifieke taken die speciale rechten. Dit wil dus zeggen dat de dagdagelijkse taken uitgevoerd worden met een account met beperkte rechten.

[1] Opgericht in de schoot van het Algemeen Coördinatiecomité van de Kruispuntbank van de Sociale Zekerheid.

Om deze redenen, verleent

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

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

Yves ROGER
Voorzitter