EIGEN BEOORDELING VAN TOETSING VAN EEN DOSSIER AAN DE TECHNISCHE VOORWAARDEN VAN HET TOEPASSELIJK KONINKLIJK BESLUIT

Het toepasselijk koninklijk besluit is, naargelang het geval, 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*, het koninklijk besluit van 28 november 1995 *betreffende de bewijswaarde, ter zake van de sociale zekerheid der zelfstandigen, van de door de Administratie en meewerkende instellingen gebruikte informatiegegevens inzake de sociale zekerheid der zelfstandigen* of het koninklijk besluit van 15 maart 1999 *betreffende de bewijskracht, ter zake van de sociale zekerheid en het arbeidsrecht, van de door de ministeriële diensten en parastatalen van het Ministerie van Tewerkstelling en Arbeid uitgewisselde, meegedeelde, opgeslagen, bewaarde of weergegeven informatiegegevens*.

A. Wettelijk kader

https://www.ksz-bcss.fgov.be/nl (zie Wetgeving / Bewijskracht)

B. Inhoud van de eigen beoordeling - Basisvoorwaarden

De eerste focus ligt op de procedure, volgens dewelke informatiegegevens worden opgeslagen, bewaard en weergegeven op een leesbare drager.

1. de focus ligt op een procedure, niet op concrete gegevens. Anders gezegd: niet wat wordt opgeslagen, maar hoe het gebeurt.
2. de procedure moet tegelijkertijd betrekking hebben op de opslag, de bewaring en de leesbare weergave van informatiegegevens. Waar het KB spreekt van een procedure met betrekking tot één of meer van deze handelingen, heeft het Sectoraal Comité van in de beginne steeds gesteld dat deze handelingen samen in één procedure moesten voorkomen. Een procedure die enkel handelt over de opslag van gegevens, zal dus nooit voor erkenning in aanmerking komen.

Een tweede focus ligt op het feit dat de procedure en het archiveringssysteem operationeel moeten zijn. Wat beoordeeld wordt moet dus al bestaan; ontwerpen en plannen komen niet in aanmerking voor eigen beoordeling. Praktisch gevolg hiervan is dat men dient te investeren in een systeem vooraleer het ter beoordeling kan worden voorgelegd, wat een duidelijk risico inhoudt.

Tenslotte ligt de focus op de formele goedkeuring van het verslag van de eigen beoordeling door het hoogste niveau in uw organisatie.

C. Inhoud van de eigen beoordeling - Technische voorwaarden

De eigen beoordeling dient te geschieden in functie van de technische voorwaarden van het Koninklijk Besluit. De Kruispuntbank heeft deze verwerkt in 5 expliciete domeinen. Algemeen kan worden gesteld dat er een bijzondere aandacht uitgaat naar de diverse veiligheidsaspecten.

1. Het systeem omschrijft nauwkeurig de procedure.

Volledige en schematische beschrijving van alle procedures inzake:

→ de opslag en de bewaring van de informatiegegevens op elektronische informatiedrager;

→ de weergave[1], al dan niet op een voor de mens leesbare drager (bv.: scherm, papier, kopie naar andere elektronische informatiedrager), van de op elektronische drager opgeslagen informatiegegevens.

Er moet dus gedetailleerd beschreven worden welke handelingen zich in welke volgorde voltrekken vanaf het ogenblik dat de informatiegegevens worden ontvangen, tot het moment van de laatste verwerking.

Een belangrijk onderdeel van de te beschrijven procedure is het aanduiden van de personen of personeelscategorieën, bevoegd om de beschreven handelingen uit te voeren.

Sleutelwoorden: **INTEGRITEIT** en **TRACEERBAARHEID**.

Opmerking: "plaats van beelden / bestanden tijdens de workflow"
Vanaf het moment dat de beelden de 1ste keer elektronisch geregistreerd worden tot op het moment dat de elektronische gegevens weggeschreven worden op hun definitief opslagmedium (WORM functionaliteit), moet duidelijk aangegeven worden waar de (tijdelijke/tussentijdse) beelden/bestanden zich bevinden, welke software/hardware de gegevens verwerkt, en hoe de integriteit van die beelden verzekerd wordt (en wie welke toegangsrechten heeft). Dit is het cruciale punt in een dossier bewijskracht. Dus duidelijk aangeven in de workflow **waar** het beeld zich bevindt (specificaties en de beveiligingsmaatregelen beschrijven die garanderen dat de beelden niet gewijzigd kunnen worden).

→ "**waar**" – hiervoor komt het volgende in aanmerking: op welk fysiek opslagmedium en in welk formaat, welk (file)systeem / OS / DB, toegankelijk voor welke applicaties en welke users (admins, normale gebruikers, …) … .

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

Weergave = opslag op elektronische informatiedrager + weergave van de opgeslagen informatie op een al dan niet voor de mens leesbare drager

Voor dit domein moeten minstens de volgende aspecten verplicht beoordeeld worden in deze volgorde:

- **A.** de beschrijving van de geïnstalleerde hardware- en softwareconfiguratie (met toevoeging schematische voorstelling);
- **B.** de duurzaamheid van het gebruikte opslagmedium (bijv. WORM, …)
- **C.** het circuit van verwerking en scanning van de betrokken dragers;
- **D.** het automatische en manuele controlepunt volgens de fases van het proces;
- **E.** de overmaking van de elektronische documenten in het document management systeem;
- **F.** de formaten van de bestanden en de overeenstemming ervan met de archiveringsstandaarden die de duurzaamheid van de geregistreerde gegevens garandeert;
- **G.** het beheer van de incidenten, de fouten en de mechanismen van eventuele overname of verwerping van de informatie;

[1] Onder 'weergave' verstaat men de weergave, al dan niet op een voor de mens visueel leesbare drager, van de op elektronische drager opgeslagen informatie. Het kopiëren van de informatie naar een andere elektronische gegevensdrager valt dus ook onder de noemer 'weergave'. Een echte *visualisatie* is dus niet nodig.

H. de instructies voor de aanwending van de oplossing;
I. 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, … ;
J. het voorzien van onderhoudscontracten m.b.t. de geïnstalleerde soft- en hardware;
K. de beschikbaarheidscijfers voor wat de hardware en de software betreft (failure & repair)
L. de aanwezigheid van bijstand voor gebruikers
M. de aanwezigheid van back-up apparatuur (voor de volledige infrastructuur)
N. de maatregelen/controles die waarborgen dat er aan de opgeslagen informatiegegevens geen wijzigingen worden aangebracht;
O. de maatregelen met betrekking tot de archivering en de consultatie op afstand (bijvoorbeeld garantie tegen wijziging tijdens gegevensoverdracht)
P. de controle van de kwaliteit en van de kwantiteit.

3. De informatie wordt systematisch (= gemakkelijk op te zoeken) en zonder weglatingen geregistreerd.

Samen met de informatiegegevens dienen er indexgegevens te worden opgeslagen die toelaten om het gegeven in de massa te kunnen situeren en om het gebruik van de informatie te reconstrueren. Er dient tevens beschreven te worden welke de procedure is voor het uitvoeren van kwaliteits- en kwantiteitscontroles bij het opslaan van informatiegegevens.

Voor dit domein moeten minstens de volgende aspecten verplicht beoordeeld worden in deze volgorde:

A. hoe verloopt de indexering van de elektronisch opgeslagen documenten;
B. de maatregelen om te voorkomen dat ingescande en geïndexeerde documenten worden gewijzigd/verwijderd of meermaals worden opgeslagen
C. de uitvoering van een kwaliteits- en kwantiteitscontrole bij het inscannen van documenten (eventueel herscannen, quid recto verso documenten)
D. de wijze van indexatie van ingescande documenten waardoor het opzoeken van opgeslagen beelden eenvoudig is
E. de voorziening van nodige schikkingen teneinde de toekenning van verkeerde indexgegevens te voorkomen
F. de mogelijkheid tot wedersamenstelling van de indexgegevens bij verlies ervan
G. de beperking van de toegang tot de indexgegevens en de bescherming tegen wijzigingen en verwijderingen
H. medium waar de indexgegevens opgeslagen worden
I. de onmiddellijke melding van problemen die optreden tijdens de scanning van documenten
J. de procedure om geconstateerde problemen op te lossen

Een demonstratie moet toelaten om deze verschillende componenten te kunnen controleren.

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

Voor dit domein moeten minstens de volgende aspecten verplicht beoordeeld worden in deze volgorde:

A. de infrastructuur (o.a. servers, databank en file storage) is redundant uitgevoerd en over twee van elkaar gelegen sites verspreid, waardoor de continuïteit van de dienstverlening en de reconstructie in geval van een belangrijk incident worden

gewaarborgd; de gearchiveerde documenten worden bewaard in een WORM-architectuur die over beide sites is opgesplitst [OF afdoende maatregelen werden genomen om de continuïteit van de dienstverlening en de reconstructie ingeval van een belangrijk incident te kunnen waarborgen (o.a. redundante SAN-infrastructuur)];

B. met betrekking tot het back-up/restore systeem 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-up/restore systeem van de instelling opgenomen;

C. afdoende disaster recovery maatregelen werden genomen en uitgetest;

D. 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;

E. voor de fysieke toegangscontrole wordt gebruik gemaakt van een centraal beheerd badgesysteem;

F. de periode van retentie en bewaring van de dragers is vastgelegd;

G. 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);

H. de aansluiting op het informatiesysteem is mogelijk via afdoende beveiligde werkposten binnen de instelling en via een beveiligde toegang op afstand (VPN) in het kader van telewerk en de toegang wordt enkel verleend via de standaard IT security policy van uw instelling;

I. 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 van uw instelling release management proces. De procedures en voorbeelden van documentatie m.b.t. release management waren ter inzage beschikbaar tijdens de audit van de Kruispuntbank van Sociale Zekerheid;

J. als instelling van het [primaire/secundaire] netwerk rond de Kruispuntbank van de Sociale Zekerheid leeft uw instelling de minimale veiligheidsnormen na.

5. De bewaring van de volgende gegevens m.b.t. de verwerking van de informatie: de 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 plaats en de datum van de verrichting, de eventuele storingen die zijn vastgesteld tijdens de verwerking.

Verwerking = opslag op elektronische informatiedrager + weergave van de opgeslagen informatie op een al dan niet voor de mens leesbare drager

Voor dit domein moeten beide aspecten (opslag en weergave) expliciet in het dossier vermelden in welke mate en op welke wijze het geïnstalleerde systeem tegemoetkomt aan de criteria. De bedoeling van het bijhouden van loggegevens is te allen tijde te kunnen achterhalen wie wat gedaan heeft en welke problemen er zich hebben voorgedaan. Er dient beschreven te zijn op welke verrichtingen de loggegevens betrekking hebben, hoe deze gegevens opgeslagen en bewaard worden en hoe de weergave van deze gegevens gebeurt. M.b.t. de creatie en het bijhouden van loggegevens is het belangrijk om de volgende regels te kunnen aantonen:

a. de loggegevens dienen even lang te worden bijgehouden als de informatie waarop ze betrekking hebben (ongeacht het gebruikte opslagmedium);

b. de loggegevens dienen relatief snel beschikbaar te zijn en ze moeten toelaten om op een gemakkelijke en gebruiksvriendelijke manier gegevens snel te kunnen opzoeken.
c. de logische en de fysische toegang tot loggegevens dient tot bevoegde personen te worden beperkt;
d. de loggegevens mogen niet kunnen gewijzigd worden;
e. de logbestanden worden mee in de standaard back-up/restore procedures van de instelling geïntegreerd.

D. Eigen beoordeling – praktische opzet

De stappen in de beoordeling van uw eigen dossier zullen zijn:

1) Bespreking van het voorlopig verslag van de eigen beoordeling volgens de 5 domeinen (met documentatie in bijlage) met de verantwoordelijke medewerkers en directie;
2) Voorleggen van het finaal verslag van de eigen beoordeling ter goedkeuring aan de administrateur-generaal van uw instelling die deze dan formeel goedkeurt via handtekening;

Het is een goede praktijk om het finaal goedgekeurde verslag van de eigen beoordeling ook ter informatie mee te delen aan het directiecomité van uw instelling zodanig dat alle betrokkenen op de hoogte zijn.

Belangrijke opmerking: het is nog steeds mogelijk dat de KSZ onafhankelijke controles uitvoert op uw eigen beoordeling.

E. Referenties

- ISO/TR 13028:2010, Information and documentation - Implementation guidelines for digitization of records http://www.iso.org/iso/catalogue_detail.htm?csnumber=52391
- MoReq2 (Model Requirements for the management of electronic records. Update and extension, 2008); http://www.moreq2.eu
- ISO 15489
  - Information and documentation — Records management — Part 1: General ISO 15489-1, 2016-04-15 http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62542
  - Information and documentation — Records management — Part 2: Guidelines ISO 15489-1, 2001-09-15 http://www.iso.org/iso/catalogue_detail?csnumber=35845
- ISO/TR 15801:2009, Document management -- Information stored electronically -- Recommendations for trustworthiness and reliability (142 CHF) http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=50499
- ISO/FDIS 14641- Electronic archiving -- Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation; http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=54911
- DoD 5015.2 v3, Electronic Records Management Software Applications Design Criteria (April 25, 2007)

- ISO/IEC 27002:2013, Information technology -- Security techniques -- Code of practice for information security management http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54533

EINDE VAN DIT DOCUMENT