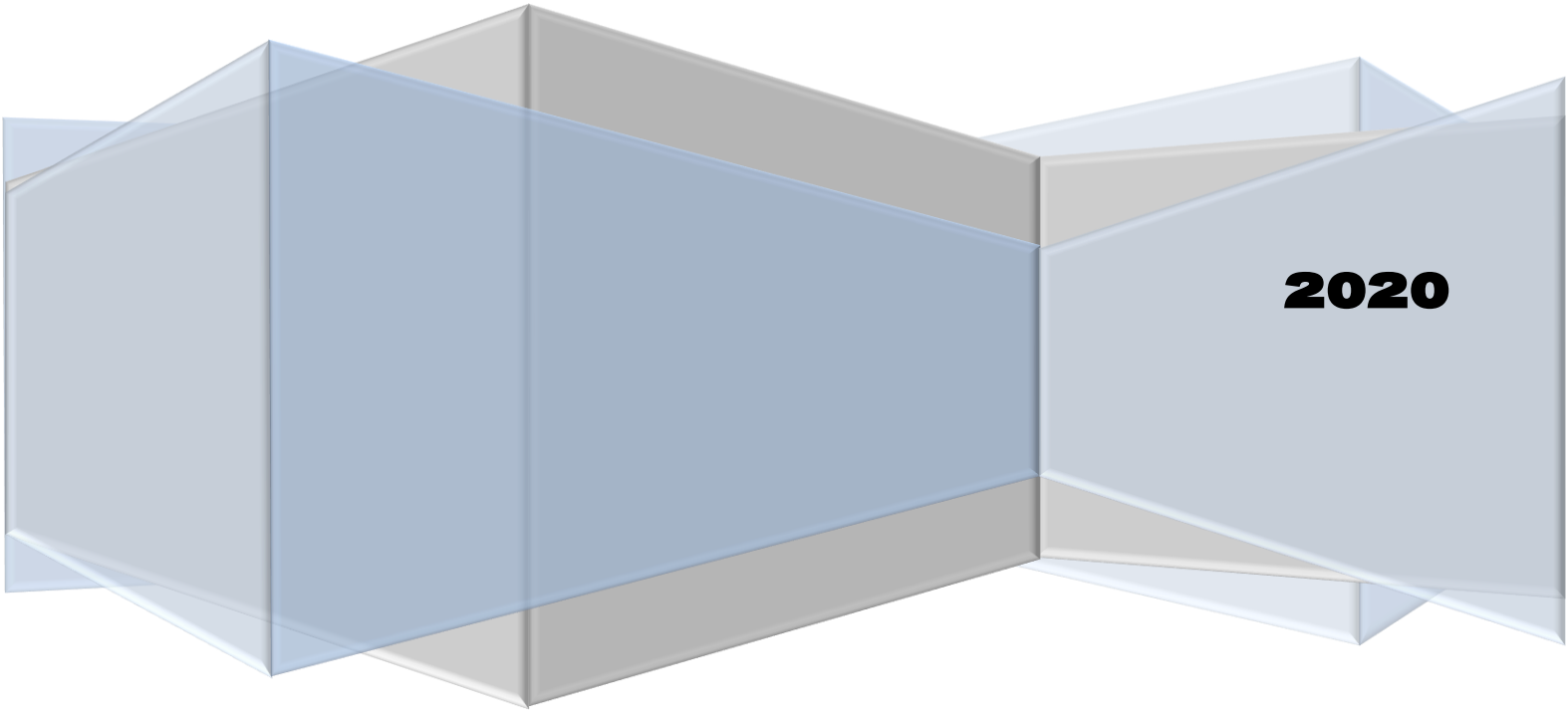
Broeders van Liefde

VADEMECUM ARCHIVERING

sector geestelijke gezondheidszorg



2020

Inhoud

1. Evolutie in doelstelling, werking en samenstelling van de werkgroep 3
2. Algemene richtlijnen m.b.t. archivering 5
   - 2.1. Bewaaromstandigheden 5
   - 2.2. Organisatie van het archief 5
   - 2.3. Digitale documenten: 6
3. Good practice voorbeeld 7
   - 3.1. Infrastructuur/beveiliging 7
   - 3.2. Organisatie/personele omkadering 7
   - 3.3. Archiefdatabase 7
4. Selectielijst GGZ 8
   - 4.1. Algemeen 8
   - 4.2. Toelichting bij de gebruikte kolommen 9
   - 4.3. Lijst gebruikte afkortingen 10
   - 4.4. De selectielijst GGZ 11

Categorie: public relations, en historisch belangrijk 11

Categorie: bestuur en beleid 12

Categorie: gebouwen, domeinen, infrastructuur 14

Categorie: personeelsbeheer 17

Categorie: welzijn en preventie 19

Subcategorie: persoonsgebonden documenten 19

Subcategorie: opvolgingsdocumenten voor intern beheer 22

Subcategorie: lijsten en registers van werknemers en activiteiten die na uitvoering van werkzaamheden moeten bewaard blijven 24

Subcategorie: rapporten en verslagen van werkzaamheden en inspecties 26

Subcategorie: verslagen, vergaderingen, … 27

Subcategorie: instructies 28

Subcategorie: documenten m.b.t. ongevallen 29

Subcategorie: documenten m.b.t. analyses, rapporten, plannen, … 30

Subcategorie: documenten m.b.t. overeenkomsten, contracten, aankoopdocumenten 31

Subcategorie: documenten m.b.t. materialen, uitrusting, gebouwen 32

Categorie: financieel-economisch, boekhouding 34

Categorie: patiënten- en bewonersadministratie, medisch secretariaat 37

Bijlage 1 Good practice voorbeeld vanuit het PC Zoete Nood Gods Lede (sinds 18/12/2017 P.C. Ariadne) 41

Bijlage 2 57

Informatieveiligheidsbeleid van de organisatie Broeders van Liefde 57
Informatieveiligheidsbeleid van de organisatie Broeders van Liefde 57
Inleiding 57
Visie 58
A. Kwaliteit 58
B. Regelgeving en ethiek 58
C. Een lerende organisatie 58
D. Realisme 59
Doelstellingen 60
A. Gegevensbeveiliging 60
B. Toegangenbeheer 65
C. Risicobeheer 65
D. Incidentenbeheer 66
E. Bewustmaking van de medewerkers 66
F. Beveiliging van de eigen elektronische infrastructuur en de eigen netwerken 66
G. Fysieke beveiliging 67
H. Beheer van afspraken met externe partijen 67
Rollen en verantwoordelijkheden 69
A. De Raad van Bestuur 69
B. De centrale stuurgroep informatieveiligheid (CSGIV) 69
C. De lokale directies 69
D. De informatieveiligheidsconsulenten (IVC's) en de data protection officer (DPO) 69
E. Lokale contactpersoon voor informatieveiligheid 70
F. De IT-diensten 70
G. De gebruikers 70
H. Beheer van archief met historische en erfgoedkundige waarde 71
Werkwijzen en middelen 71
Evaluatie 72

1. Evolutie in doelstelling, werking en samenstelling van de werkgroep

De 'werkgroep archivering' werd opgestart in juni 2010 en hernam de werkzaamheden van de CRAM (Cel Rationeel Archiefmanagement Broeders van Liefde). De opdracht van de werkgroep bestond uit het ontwikkelen van een effectief en efficiënt archiefbeleid voor het Provincialaat en de instellingen, en komen tot een archiefvademecum met richtlijnen en aanbevelingen. Het terrein van de werkgroep werd beperkt tot het 'dode' of 'statische' archief. De archivering van de digitale bestanden zat niet in de scope van de werkgroep maar zou later worden opgenomen (via stuurgroep informatica). In afwachting hiervan was het aangewezen dat directies de belangrijkste digitale documenten zouden afprinten en in het papieren archief bewaren. Ondertussen is het wel duidelijk geworden dat meer en meer documenten enkel nog digitaal aangemaakt en bewaard worden. Voor deze digitale documenten gelden wat selectie en bewaartermijnen betreft, eigenlijk dezelfde regels, termijnen en voorzorgen.

Tevens diende een marktonderzoek te gebeuren met het oog op het selecteren van een softwareleverancier voor een totaalpakket dat zowel het beheer van het papieren archief, het beheer van het digitale archief als het scannen van documenten aankon. Door de werkgroep werd eind 2010 een selectie gemaakt van mogelijke leveranciers inzake het opstellen van een centraal digitaal archief, het lokaal scannen en het lokaal softwarematig beheren van het papieren archief. Tijdens de verdere besprekingen werd echter vastgesteld dat de implementatiekost van dergelijke operatie aanzienlijk was. Zo was er niet alleen de licentiekost maar diende er ook lokaal iemand deeltijds te worden vrijgesteld om het archief 'op orde' te zetten, moest rekening worden gehouden met aanzienlijke scankosten en werd gesteld dat om een centraal digitaal archief te gebruiken er voor het archiveren van "nieuwe" archiefstukken die van oorsprong digitaal zijn hoge eisen worden gesteld aan de snelheid van de communicatielijnen. Binnen de werkgroep was er een algemeen aanvoelen dat onze organisatie nog niet klaar was om op heden al over te schakelen naar een integrale softwareoplossing.

Om een zicht te krijgen op de stand van zaken op het vlak van archivering in een aantal instellingen werden werkbezoeken gedaan in het voorjaar van 2011. Op basis van deze werkbezoeken werden volgende conclusies getrokken:

1. Er zijn grote verschillen in archiefzorg en –omgang per instelling. Zo is er in één instelling (Lede) een centraal goed georganiseerd archief, met vaste afspraken, en een ontsluiting met een eigen ontwikkelde databank.
   Daarnaast zijn er instellingen met (deels) gestructureerde archieven die niet centraal zijn georganiseerd maar doorzoekbaar zijn (zonder software). Tenslotte is er ook een instelling met weinig of geen structuur in het archief.
2. Nergens is men vragende partij voor een grootschalige scanoperatie van het (papieren en statische) archief.
3. Nergens is men vragende partij voor een 'zware' softwaretoepassing om het archief te beschrijven of te ontsluiten.
4. Overal is men vragende partij naar een vademecum met richtlijnen van wat, hoe lang en op welke manier documenten moeten worden bewaard.
5. Er wordt relatief weinig gebruik gemaakt van het archief: een aantal keer per jaar voor interne en externe opzoekingen.
6. In alle instellingen wordt aangegeven dat er weinig aandacht aan het archief wordt besteed omwille van een gebrek aan personele middelen (niet prioritaire opdracht), doch er is wel een bewustzijn van de waarde van het archief.

Op basis van deze conclusies, die nog altijd gelden, werd voorgesteld een vademecum op te stellen waarin een aantal algemene richtlijnen m.b.t. archivering zouden worden opgenomen, gevolgd door een 'good practice voorbeeld' (Lede), waarna selectielijsten met concrete richtlijnen inzake wettelijke en wenselijke bewaartermijnen voor documenten zouden worden toegevoegd.

Doorheen het afgelegde traject is de samenstelling van de werkgroep archivering regelmatig gewijzigd. Volgende personen hebben deel uitgemaakt van de werkgroep: Luc de Kezel*, Mario De Maet*, Hendrik Decroos, Michael De Geest*, Johan Jehoul, Erwin Keustermans*, Luc Querter, Michel Sinove, Nathalie Van Looy *, Carine Vanderbeken *, Etienne Verschraege * & Franky Wauters* (*maakten deel uit bij het afsluiten en opmaken van de nota in 2013).

In de loop van 2017-2018 bleek het nodig het vademecum aan te passen aan het vernieuwde informatieveiligheidsbeleid van de organisatie, en 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 (algemene verordening gegevensbescherming)" (ook gekend als **GDPR**) mee in overweging te nemen.

De vernieuwde werkgroep archivering (Geert Aerens, Luc de Kezel, Mario De Maet, Erwin Keustermans, Steven Verdonck, Etienne Verschraege) zorgde meteen voor een aantal andere aanpassingen en updates.

2. Algemene richtlijnen m.b.t. archivering

In veel organisaties komt de zorg voor het archief op de laatste plaats en worden er weinig mensen en middelen ter beschikking gesteld voor de uitbouw van een goed gestructureerd archief. Nochtans is een goed geklasseerd archief belangrijk binnen een organisatie. Zo heeft een archief vaak niet enkel een juridische en administratieve waarde doch ook een historische waarde (bronnenmateriaal voor wetenschappelijk onderzoek).

Zonder te veel in detail te vervallen willen we een aantal algemene richtlijnen meegeven die van belang zijn voor een goed uitgebouwd archief. Deze algemene (samengevatte) info werd gedeeltelijk gehaald uit terzake gespecialiseerde literatuur ('Meester over mijn schoolarchief'- Politea, 'Zakboekje archiveren' van M. Verhelst, Preventiezakboekje Kluwer,…) waar meer gedetailleerde info is te vinden. Ook op de website van het Algemeen Rijksarchief zijn verschillende brochures in Pdf-formaat ter beschikking (http://www.arch.be/content/view/634/256/lang,nl_BE)

2.1. Bewaaromstandigheden

- Temperatuur en luchtvochtigheid: er wordt een gemiddelde temperatuur vooropgesteld van 15° C met een relatieve vochtigheidsgraad van 45% (te meten via een hygrograaf). De stabiliteit van de temperatuur en luchtvochtigheid zijn van groot belang: een lokaal waar het in de winter vriest en in de zomer warm is, is derhalve niet geschikt als archief. Bij de werkbezoeken werd nochtans geregeld vastgesteld dat het archief een plaats op de zolder of in de kelder had gekregen, wat uiteraard minder geschikte plaatsen zijn.
- Overstromings- en brandgevaar: aandacht voor automatisch werkende pompen in kelders en voor branddetectoren en eventuele automatische blussystemen.
- Licht: het licht bestaat uit verschillende stralen die een negatieve invloed hebben op de bewaaromstandigheden van het archief. Het papier en de lijmstoffen ondergaan veranderingen door de ultraviolette stralen en de infraroodstralen. Derhalve is het van groot belang het licht te weren (zowel kunstmatig licht als zonlicht).
- Ongedierte , insecten en schimmels: de bewaaromstandigheden worden best dermate ingericht dat ongedierte, insecten en schimmels zo weinig mogelijk aanwezig kunnen zijn in het archief. Zo kunnen openstaande ramen toelaten dat insecten en ongedierte zich een toegang tot het archief verschaffen en is een luchtvochtigheid van boven de 70 % ideaal voor schimmelgroei. In bepaalde gevallen wordt best een beroep gedaan op professionelen om tot een ongedierte- en insectenvrij archief te komen.

2.2. Organisatie van het archief

- Inventariseren: het archief inventariseren is een niet ingewikkelde doch tijdrovende opdracht. Het opmaken van een inventaris is echter noodzakelijk om te weten welke archiefstukken precies in het bezit zijn en biedt een waarborg voor de veiligheid en volledigheid van het archief. Belangrijke stappen bij het inventariseren zijn het maken van een archiefschema (met nummering) en het ordenen en schonen (=verwijderen van overbodige documenten en van schadelijke voorwerpen zoals nietjes, paperclips, ...) van het archief. Bij het verwijderen van documenten dient de nodige aandacht te worden besteed aan de vertrouwelijkheid van de informatie (vernietigen versus bij het 'oud papier' te plaatsen).

- Personele omkadering: het verdient aanbeveling iemand verantwoordelijk te stellen voor de organisatie en ontsluiting van het archief. Deze persoon is het centrale aanspreekpunt binnen de instelling: hij zorgt, in overleg met de persoon of dienst die documenten aanlevert, voor een plaats in de archiefruimte waar het document wordt geklasseerd en staat ook in voor de registratie van de verschillende acties die worden ondernomen m.b.t de documenten (opslag, ontlening, terugbrenging, vernietiging).
- Softwareondersteuning: de opgemaakte inventaris van de aanwezige stukken en documenten wordt best ingebracht in een database met uitgebreide zoekmogelijkheden. Dit kan een gerust een eigen ontwikkelde toepassing zijn.

2.3. Digitale documenten:

- Belangrijke digitale tekstbestanden worden bij voorkeur ook afgedrukt, of anders opgeslagen als pdf-A-bestanden. Dit formaat biedt op lange termijn de beste garanties voor leesbaarheid en integriteit (onveranderlijkheid).

3. Good practice voorbeeld

Tijdens de werkbezoeken viel op dat het archief van Lede in vergelijking met andere instellingen goed is uitgebouwd en georganiseerd. Vandaar dat we dit archief als een 'good practice voorbeeld' willen voorstellen. De volledige beschrijving van de organisatie van het archief in Lede is weergegeven in het document als bijlage en kan inspiratie bieden voor de uitbouw of reorganisatie van het archief (zie bijlage 1).

Het centraal archief in Lede werd opgestart in 1999. Het samenvoegen van de verschillende dossiers in een centraal archief vergde de nodige tijd en energie.

De belangrijkste vaststellingen bij het bezoek van dit archief kunnen als volgt worden samengevat:

3.1. Infrastructuur/beveiliging

De oppervlakte van het lokaal bedraagt ong. 300 m² en is goed onderhouden. Er wordt gebruik gemaakt van rekken en van een hangsysteem. Het lokaal is voorzien van branddetectie maar er is geen automatisch blussysteem aanwezig. Verder is er geen klimaatregeling voorzien maar wordt verluchting voorzien via ramen. Het lokaal is afgesloten en slechts enkele personen hebben toegang tot het archief waarbij wordt gewerkt met een getrapt systeem van sleutels: hoe vertrouwelijker de documenten hoe meer 'afgesloten' deze zijn. Tenslotte kan worden vermeld dat er geen gebruik wordt gemaakt van speciale verpakkingen (bv. geen zuurvrije dozen).

3.2. Organisatie/personele omkadering

Het beheer van het archief berust bij het medisch secretariaat (en gedeeltelijk bij het directiesecretariaat) met ondersteuning door een steward, zodat kan worden gesteld dat er een centraal beheer is. Documenten die klaar zijn om gearchiveerd te worden, worden in samenspraak met het medisch secretariaat door de betrokken afdeling naar het archief gebracht. Het uitlenen van documenten en hangmappen gebeurt eveneens via het medisch secretariaat. De afspraken m.b.t het archiveren zijn opgenomen in het procedureboek.
Het aantal VTE dat wordt ingezet voor het beheer van het centraal archief wordt ingeschat op +/- 0,2 VTE (8-tal uren per week).
Jaarlijks worden lijsten of rapporten gemaakt van de 'vervallen stukken zonder historische waarde' en vooraleer deze te vernietigen wordt aan de onderscheiden diensten een expliciete goedkeuring gevraagd.

3.3. Archiefdatabase

Samen met de opstart van het archief werd een database op maat gemaakt (eigen ontwikkelde toepassing in MS Access). Via de archiefdatabase krijgt elk document en elke hangmap bij archivering automatisch een recordnummer toegewezen, kunnen documenten worden opgezocht aan de hand van de ingegeven data via de zoekfunctie (met meerdere mogelijkheden om een document terug te vinden) en kunnen lijsten worden getrokken van welke documenten wanneer en aan wie werden uitgeleend (bij elke uitlening worden deze gegevens steeds ingebracht in de database). Bij de jaarlijkse opruiming van het archief wordt gebruik gemaakt van de database (lijst met items die mogen worden verwijderd). Bij verwijdering uit het archief wordt het recordnummer uit de database gehaald.

4. Selectielijst GGZ

4.1. Algemeen

Zoals hiervoor reeds aangehaald was één van de besluiten van de werkbezoeken dat alle bezochte instellingen vragende partij zijn naar een vademecum met richtlijnen inzake de bewaartermijnen van documenten. Bij de praktische uitwerking van dit vademecum werd vastgesteld dat de verscheidenheid van bestaande documenten in instellingen en voorzieningen dermate groot was dat het niet haalbaar noch zinvol was om bewaartermijnen voor te stellen voor al deze documenten.

In overleg met de Raad van Bestuur werd besloten om een middenweg te zoeken tussen een minimalistische en maximale benadering. Hierbij zouden enkel richtlijnen worden verschaft rond de documenten waarvoor een wettelijke bewaringstermijn is vooropgesteld (i.e. de eerder door de juridische dienst verspreide documenten en de door de dienst preventie geïnventariseerde documenten) alsook over de 20-25 belangrijkste documenten uit de door de instellingen ingestuurde documenten. Aldus werd een selectielijst opgemaakt met enerzijds de belangrijkste documenttypes zoals doorgegeven door de instellingen en anderzijds de documenttypes waarvoor een wettelijke bewaartermijn is vooropgesteld.

Een veel ruimere lijst met documenttypes werd in november 2012 ter beschikking gesteld door het 'Algemeen Rijksarchief'. Het Rijksarchief werd regelmatig geconfronteerd met vragen over bewaartermijnen van documenten en besloot daarom een selectielijst voor ziekenhuisarchieven op te stellen. Deze ruime selectielijst (83 blz.) is online raadpleegbaar (www.arch.be > advies over archiefbeheer > selectielijsten > (boven)lokale instellingen > ziekenhuizen).

De wettelijke bewaartermijnen van de documenten in ons vademecum werden hierbij nog eens afgetoetst aan de wettelijke bewaartermijnen zoals vermeld in de selectielijst van het 'Algemeen Rijksarchief'. De wenselijke bewaartermijnen wijken af. De werkgroep heeft getracht om bij de bepaling van de wenselijke bewaartermijn rekening te houden met elementen als 'historisch waardevol' maar ook met de werkdruk die het bv. jaarlijks schonen of verwijderen van dossiers uit het archief meebrengt. Zo wordt bv. in de selectielijst van het Rijksarchief voorgesteld om personeelsdossiers te bewaren tot 75 jaar na het geboortejaar van het personeelslid, wat impliceert dat elk jaar moet worden nagegaan welke ex-personeelsleden 75 jaar zijn geworden om vervolgens hun dossier te verwijderen. Binnen onze selectielijst is voorgesteld personeelsdossiers tot 10 jaar na uitdiensttreding te bewaren.

Tijdens de verdere uitwerking zag de werkgroep een duidelijke meerwaarde in het leggen van een link binnen het vademecum met het op te maken veiligheidsplan en de lokale risicoanalyse die in elke instelling zou moeten gebeuren. De sector GGZ werd stilaan en nadien geconfronteerd met het verplicht opmaken van een informatieveiligheidsplan en –beleid maar zowel vanuit Europese, federale en Gemeenschapsoverheid kwamen er ook voor de andere sectoren steeds strengere eisen inzake privacy en bewaring van informatie. Hiertoe werden bij elk te bespreken document naast de bestaande kolommen over bewaartermijn, verantwoordelijke voor bewaring enz., vier kolommen toegevoegd m.n. een classificatie van de aard van het document volgens de graad van vertrouwelijkheid ('openbaar' , 'intern', 'vertrouwelijk' of 'geheim'), volgens de vereiste beveiliging ('geen beperking op toegankelijkheid', 'enkelvoudig afgesloten', 'dubbel of meervoudig afgesloten'), een kolom met aanduiding van wie gemachtigd is om toegang tot de informatie in kwestie te verstrekken en een kolom met aanduiding wie inzagerecht heeft ('iedereen', 'intern breed', 'beperkt', 'geheim'). Op die manier zou het vademecum ook een houvast kunnen zijn voor de lokale risicoanalyse.

De classificatie van de aard van het document volgens de graad van vertrouwelijkheid was gebaseerd op het document 'Aanduiding van vertrouwelijkheid van informatie' dat ontwikkeld was binnen onze organisatie in het kader van het op te maken informatieveiligheidsplan.

In de loop van 2017-2018 werd een vernieuwd informatieveiligheidsbeleid ontwikkeld in de organisatie Broeders van Liefde (zie Bijlage 2). Dit noopte tot aanpassingen in de kolommen 5 en 8.

4.2. Toelichting bij de gebruikte kolommen

1. Naam en beschrijving van het document: de naamgeving is gebaseerd op de door de instellingen ingestuurde documenttypes en eigen ervaringen en inzichten. Een aantal documenttypes werden waar mogelijk samengevoegd.
2. Bewaartermijn: wettelijk en wenselijk: de vooropgestelde bewaartermijnen zijn minimale termijnen. Om evidente redenen kan het van belang zijn om bepaalde documenten langer te bewaren (bv. documenten die als bewijsstuk nuttig kunnen zijn bij betwistingen die ontstaan zijn voor het einde van de vooropgestelde bewaartermijn).
3. Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn: waar van toepassing wordt verwezen naar het wettelijk kader op basis waarvan de bewaartermijn is bepaald.
4. Verantwoordelijke voor de bewaring: instelling, personeelslid, externe organisatie: in de meeste gevallen zal dit de directie zijn met mogelijkheid van delegatie. Voor een aantal documenten is wettelijk bepaald wie verantwoordelijk is voor de bewaring.
5. Classificatie volgens de graad van vertrouwelijkheid en gevoeligheid. Hiervoor verwezen we aanvankelijk naar het document 'Aanduiding van vertrouwelijkheid van informatie' dat als bijlage was opgenomen. Volgende classificatieniveaus werden onderscheiden: openbaar, intern, vertrouwelijk en geheim. Dit wordt nu (2017-2018) vervangen door 2 x 3 subcategorieën conform de nieuwe classificatie van het informatieveiligheidsbeleid:
   P 1: Gewone persoonsgegevens
   P 2: Gevoelige persoonsgegevens
   P 3: Bijzonder gevoelige persoonsgegevens
   B 1: Publieke bedrijfsgegevens
   B 2: Interne bedrijfsgegevens
   B 3: Vertrouwelijke bedrijfsgegevens
6. Classificatie volgens de vereiste beveiliging: hier wordt verwezen naar de fysieke toegankelijkheid waarbij volgend onderscheid wordt gemaakt: A= geen beperking op de toegankelijkheid, B= enkelvoudig afgesloten archiefruimte en C= dubbel of meervoudig afgesloten (bv. een afgesloten kast in een afgesloten archiefruimte).
7. Gemachtigd om toegang/inzage te geven: in veel gevallen zal dit de directie (of delegatie) zijn tenzij andere personen op basis van een wetgevend of reglementair kader gemachtigd zijn om dit te doen.
8. Inzagerecht voor wie?: deze classificatie hangt uiteraard nauw samen met de (aangepaste) classificatie inzake de graad van vertrouwelijkheid en gevoeligheid. Volgende drie categorieën worden onderscheiden: iedereen of openbaar, intern (personeelsleden van de instelling), beperkt (met aanduiding van bevoegden).

4.3. Lijst gebruikte afkortingen

ARA	Algemeen Rijksarchief
ARAB	Algemeen Reglement voor de Arbeidsbescherming
AREI	Algemeen Reglement op de Elektrische Installaties
AVG	Algemene Verordening Gegevensbescherming
Bijlage AAV	Bijlage Algemene Aannemingsvoorwaarden (bij KB 26.09.1996)
BW	Burgerlijk Wetboek
CBM's	Collectieve Beschermingsmiddelen
CBPL	Commissie voor de Bescherming van de Persoonlijke Levenssfeer
CPBW	Comité voor Preventie en Bescherming op het Werk
CVGW	Comité Veiligheid en Gezondheid op het Werk
DIMONA	Déclaration Immédiate - Onmiddellijke aangifte
DMFA	Déclaration Multifonctionelle - Multifunctionele aangifte
EDPBW	Externe Dienst voor Preventie en Bescherming op het Werk
EDTC	Externe Dienst voor Technische Controle (Keurder)
EPD	Elektronisch Patiëntendossier
GPP	Globaal Preventieplan
GDPR	General Data Protection Regulation
JAP	Jaaractieplan
KB	Koninklijk Besluit
MB	Ministerieel Besluit
NVT	Niet Van Toepassing
OGGW	Ongewenst en Grensoverschrijdend Gedrag op het Werk
PBM's:	Persoonlijke Beschermingsmiddelen
PBW	Preventie en Bescherming op het Werk
RIZIV	Rijksinstituut voor Ziekte en Invaliditeitsverzekering
RSZ	Rijksdienst voor Sociale Zekerheid

4.4. De selectielijst GGZ

Categorie: public relations, en historisch belangrijk

1. Naam en beschrijving van het document	2. Bewaartermijn: wettelijk en wenselijk	3. Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn	4. Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie	5. Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)	6. Classificatie volgens vereiste beveiliging (3 graden)	7. Gemachtigd om toegang/inzage te geven	8. Inzagerecht voor wie? (3 graden)
Jaarverslag of jaarboek en activiteitenverslag	Wettelijke termijn: geen Gewenst: permanent	-	Instelling (Directie, met mogelijkheid om te delegeren naar… (bv. plaatselijke archiefverantwoordelijke)	B1	**A**	Niet van toepassing = NVT	Openbaar
Publicatie, geschiedenis(boek), jubileumboek, historisch overzicht, kroniek,…	Wettelijke termijn: geen Gewenst: permanent	-	Instelling (Directie, met mogelijkheid van delegatie)	B1	**A**	NVT	Openbaar
Tijdschrift van de instelling Eventueel ook het personeelstijdschrift	Wettelijke termijn: geen Gewenst: permanent	-	Instelling (Directie, met mogelijkheid van delegatie)	B2	**A**	NVT	Openbaar
Foto's en afbeeldingen, film- en geluidsopnamen (ook postkaarten-reeksen, opnamen van evenementen.	Wettelijke termijn: geen Gewenst: permanent	-	Instelling (Directie, met mogelijkheid van delegatie)	B2	B	Directie, met mogelijkheid van delegatie	Openbaar, maar indien herkenbare personen afgebeeld: na gemotiveerd verzoek
Promotiemateriaal (brochures, folders…)	Wettelijke termijn: geen Gewenst: permanent (enkele exemplaren, géén voorraad!)	-	Instelling (Directie, met mogelijkheid van delegatie)	B1	A	NVT	Openbaar

Categorie: bestuur en beleid

1. Naam en beschrijving van het document	2. Bewaartermijn: wettelijk en wenselijk	3. Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn	4. Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie	5. Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)	6. Classificatie volgens vereiste beveiliging (3 graden)	7. Gemachtigd om toegang/inzage te geven	8. Inzagerecht voor wie? (3 graden)
Beleidsnota , beleidsplan, beleidsverklaring, beleidsvisie	Wettelijke termijn: geen Gewenst: permanent	-	Instelling (Directie, met mogelijkheid van delegatie)	B2	**B**	Directie	Intern
Verslagen of notulen van plaatselijk directie - (comité)vergaderingen	Wettelijke termijn: geen Gewenst: permanent	-	Instelling (Directie, met mogelijkheid van delegatie)	B3	**C**	Directie	Beperkt (directie, en door deze aangeduide functies als directiesecretariaat…
Erkenningsdossier	Wettelijke termijn: 30 jaar Gewenst: het huidige en het vorige dossier, maar minstens 30 jaar	Gecoördineerde ZHW, titel III, hfst. III: ”Erkenning van ziekenhuizen en ziekenhuisdiensten”	Instelling (Directie, met mogelijkheid van delegatie)	B3	**B**	Directie	Beperkt (directie, en door deze aangeduide functies als directiesecretariaat…
Erkenningsbesluit	Wettelijke termijn: geen Gewenst: permanent	-	Instelling (Directie, met mogelijkheid van delegatie)	B1	**B**	Directie	Openbaar
Auditverslagen (extern)	Wettelijke termijn: geen Gewenst: het huidige en het vorige	-	Instelling (Directie, met mogelijkheid van delegatie)	B2	**B**	Directie	Beperkt
Auditverslagen (intern)	Wettelijke termijn: geen Gewenst: het huidige en het vorige		Instelling (Directie, met mogelijkheid van delegatie)	B3	**C**	Directie	Beperkt (directie)
Plaatselijke missie en/of opdrachtverklaring, ook identiteitsverklaring (indien niet opgenomen in jaarverslagen)	Wettelijke termijn: geen Gewenst: permanent	-	Instelling (Directie, met mogelijkheid van delegatie)	B1	**A**	NVT	Openbaar

Zorgstrategisch plan (= 5 jaarlijks strategisch toekomstplan, voor overheid)	Wettelijke termijn: geen Gewenst: permanent	-	Instelling (Directie, met mogelijkheid van delegatie)	B2	**B**	Directie	Openbaar
Ondernemingsraad (verslagen, agenda, documenten)	Wettelijk: onbepaald, volgens huishoudelijk reglement van de O.R. Gewenst: 10 jaar	-	Instelling (Directie, met mogelijkheid van delegatie)	B3	**B**	Directie	Beperkt (leden ondernemingsraad)
Huishoudelijk reglement van de ondernemingsraad	Wettelijk: onbepaald, volgens huishoudelijk reglement van de O.R. Gewenst: actualiseren bij installatie ondernemingsraad, lopend exemplaar bewaren	-	Instelling (Directie, met mogelijkheid van delegatie)	B3	**B**	Directie	Beperkt (leden ondernemingsraad)

Categorie: gebouwen, domeinen, infrastructuur

1. Naam en beschrijving van het document	2. Bewaartermijn: wettelijk en wenselijk	3. Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn	4. Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie	5. Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)	6. Classificatie volgens vereiste beveiliging (3 graden)	7. Gemachtigd om toegang/inzage te geven	8. Inzagerecht voor wie? (3 graden)
Masterplannen indien lokaal aanwezig)	Wettelijke termijn: geen Gewenst: permanent	-	Instelling (Directie, met mogelijkheid van delegatie)	B2	**B**	Directie	Openbaar
Bouwvergunning (indien lokaal aanwezig)	Wettelijke termijn: geen Gewenst: permanent	-	Instelling (Directie, met mogelijkheid van delegatie)	B2	**B**	Directie	Openbaar
Bouwaanvraag	Wettelijke termijn: geen Gewenst: permanent	-	Instelling (Directie, met mogelijkheid van delegatie)	B2	**B**	Directie	Openbaar
Bouwdossiers:	Wettelijk: geen Gewenst: Bouwdossier: de plannen, het lastenboek, de meetstaat, het post-interventiedossier, de as-built-dossiers, de sonderingsverslagen, bodemonderzoeken,… worden bijgehouden zolang het gebouw bestaat. De documenten van oplevering, werfvergaderingen en andere teksten: 10 jaar + 1 jaar.	-	Instelling (Directie, met mogelijkheid van delegatie)	B3	**B**	Directie	Beperkt (directie, en Dienst Gebouwen
Plannen en plattegronden van gebouwen, installaties, netwerkplannen, alarminstallaties, nutsvoorzieningen… (indien lokaal aanwezig!)	Wettelijk: geen Gewenst: permanent	-	Instelling (Directie, met mogelijkheid van delegatie)	B3	**B**	Directie	Beperkt (directie, en deze aangeduide functies en/of diensten)

Milieuvergunning (indien lokaal aanwezig)	Wettelijk: minstens zolang ze geldig is Wenselijk: zolang geldig	-	Instelling: Directie, met mogelijkheid van delegatie)	B1	**B**	Directie	Openbaar
Dossier openbare aanbestedingen (overheidsopdracht) (Lokaal) Vóór 1 juli 2013 Voor deze datum moest alleen een openbare aanbesteding gebeuren in geval van gesubsidieerde werkzaamheden. Concreet zijn dat de meeste bouwprojecten en verbouwingen, maar zeker niet allemaal. Leveringen en diensten vielen hier nooit onder.	Wettelijk: A. Gunningsdossier (bestek, alle offertes, verslagen, briefwisseling, … m.b.t. publicatie, selectie en gunning van de opdracht: → 5 jaar bewaren (=verjaringstermijn voor buitencontractuele aansprakelijkheid) B. Contractuele documenten tijdens de uitvoering (bestek, offerte opdrachtnemer, PV's, verslagen, …) vanaf PV van definitieve oplevering: → 10 j. bewaren bij werkzaamheden met 10-jarige aansprakelijkheid van architect/aannemer → 2 j. bewaren bij (kleinere) werkzaamheden zonder 10-jarige aansprakelijkheid van architect/aannemer → 2 jaar bewaren bij Leveringen en Diensten: dit kan ook betrekking hebben op leveringen en diensten buiten deze rubriek (dus buiten gebouwen, domeinen, infrastructuur) Wenselijk: idem, we volgen hierin telkens de wettelijke bepalingen	Art. 2262bis, §1 van BW Wet 24.12.1993, Bijlage AAV bij KB 26.09.1996, art 18	Instelling: directie, met mogelijkheid van delegatie	B3	**B**	Directie	Beperkt: directie en door deze aangeduide diensten en/of functies

Dossier openbare aanbestedingen (overheidsopdracht) (Lokaal) Vanaf 1 juli 2013 Hier valt het onderscheid gesubsidieerd / niet-gesubsidieerd weg. Alle werkzaamheden, en ook leveringen en diensten vallen voortaan onder 'overheidsopdrachten', en moeten openbaar gebeuren (met toenemende eisen volgens grootte van het te spenderen bedrag…)	Wettelijk A. Gunningsdossier (bestek, alle offertes, verslagen, briefwisseling, … m.b.t. publicatie, selectie en gunning van de opdracht: → 10 jaar bewaren B. Contractuele documenten (bestek, offerte opdrachtnemer, PV's, verslagen, …) →10 jaar bewaren na voorlopige oplevering bij werken met 10-jarige aansprakelijkheid van Architect/aannemer → 30 maanden bewaren na betekening van PV van voorlopige oplevering bij kleinere werken, leveringen en diensten. Voor feiten en omstandigheden die zich voordoen tijdens de waarborgperiode bedraagt de bewaartermijn dertig maanden na het verstrijken van de waarborgperiode Wenselijk: idem, we volgen hierin telkens de wettelijke bepalingen	Onderhevig aan de nieuwe wetgeving van 2016 en latere wijzigingen en bijhorende KB's (in uitvoering vanaf 30 juni 2017) Art. 164 §2 van de Wet Overheidsopdrachten van 17 juni 2016 Art 84 §2 van het KB Uitvoering van 13 januari 2013 Art. 73 van het KB Uitvoering van 13 januari 2013	Instelling: directie, met mogelijkheid van delegatie	B3	**B**	Directie	Beperkt: directie en door deze aangeduide diensten en/of functies

Categorie: personeelsbeheer

1. Naam en beschrijving van het document	2. Bewaartermijn: wettelijk en wenselijk	3. Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn	4. Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie	5. Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)	6. Classificatie volgens vereiste beveiliging (3 graden)	7. Gemachtigd om toegang/inzage te geven	8. Inzagerecht voor wie? (3 graden)
Personeelsregister: algemeen voor de instelling, papier of elektronisch ('stamboek') = centrale inschrijving van de personeelsleden	Wettelijk: 5 jaar (concreet: 5 jaar te tellen vanaf inschrijving laatste verplichte vermelding) Gewenst: permanent.	Art. 25 KB van 08.08.80 m.b.t. soc.doc.	Instelling: Directie, met mogelijkheid van delegatie	P2	**C**	Directie	Beperkt (Directie, personeelsdienst)
DIMONA-aangiften bij de RSZ (vanaf 2001) d.i. een melding telkens er een werknemer in dienst komt of uit dienst gaat	Wettelijk: 6 maanden De DIMONA-aangifte moet volgens RA maar 6 maanden bewaard worden in de instelling Gewenst: 3 jaar	Dimona-reglementering	Instelling: Directie, met mogelijkheid van delegatie	P2	**B**	Directie	Beperkt (Directie, personeelsdienst)
Speciaal personeelsregister – papier of elektronisch - (register per plaats van tewerkstelling, campus of huis dus, officieel 'per vestigingseenheids-nummer'	Wettelijk: 5 jaar (concreet 5 jaar te tellen vanaf inschrijving laatste verplichte vermelding. Bij stopzetting mag het weg. Gewenst: 5 jaar na laatste verplichte vermelding. Bij stopzetting mag het weg.	Art. 25 KB van 08.08.80 m.b.t. soc.doc.	Instelling: Directie, met mogelijkheid van delegatie	P2	C	Directie	Beperkt (directie, personeelsdienst)
Personeelsdossier (kan meerdere andere documenten bevatten, te beginnen met arbeidsovereenkomst…). Bevat ook het gebeurlijke dossier 'arbeidsongevallen werknemer'	Wettelijk: 5 jaar Wenselijk: 10 jaar	-	Instelling: Directie, met mogelijkheid van delegatie	P3	**C**	Directie	Beperkt (Directie, personeeldienst, betrokken personeelslid)
Individuele rekening personeelslid	Wettelijk: 5 jaar Gewenst: 5 jaar	Art. 25 KB van 08.08.80 m.b.t. soc.doc.	Instelling: Directie, met mogelijkheid van delegatie	P2	**C**	Directie	Beperkt: personeelsdienst, betrokken werknemer)

Overeenkomst tewerkstelling studenten	Wettelijk: 5 jaar Gewenst: 5 jaar	Art.2 en 25 van KB van 08.08.80 m.b.t. soc.doc.	Instelling: Directie, met mogelijkheid van delegatie	P2	**C**	Directie	Beperkt (personeelsdienst en betrokkene)
Beroepsinlevingsovereen-komst (dit zijn dossiers of stukken inzake stagiairs)	Wettelijk: 5 jaar Gewenst: 5 jaar	Art. 2 en 25 KB van 08.08.80 m.b.t. soc.doc. én de programmawet van 2 augustus 2002, art. 104-105	Instelling: Directie, met mogelijkheid van delegatie	P2	**C**	Directie	Beperkt (personeelsdienst en betrokkene)
Aanwezigheidslijsten, prikklokgegevens en controlelijsten.	Wettelijk: onbepaald Wenselijk: 3 jaar (Toezicht sociale wetten kan tot 3 jaar terug gaan), bij glijdende uurroosters: verplichting van 1 jaar	-	Instelling: Directie, met mogelijkheid van delegatie	P2	**B**	Directie	Beperkt: Directie, personeelsdienst
Register afwijking op de deeltijdse uurroosters (indien prikklokgegevens niet voorkomen) (deeltijdse uurrooster zelf staat overigens in het arbeidsreglement)	Wettelijk: 5 jaar vanaf de maand na het kwartaal van de laatste vermelding Wenselijk: 5 jaar	Art. 167 Programmawet van 22.12.1989	Instelling: Directie, met mogelijkheid van delegatie)	P2	**B**	Directie	Beperkt (directie, personeelsdienst en betrokkene
Bekendmaking variabele uurroosters	Wettelijk: 3 jaar na toepassing van het variabele uurrooster Wenselijk: 3 jaar	Art. 159 Programmawet van 22.12.1989	Instelling: Directie, met mogelijkheid van delegatie)	P2	**B**	Directie	Beperkt (directie, personeelsdienst en betrokkene
Gewerkte uurroosters (effectief)	Wettelijk: geen Gewenst: 3 jaar	-	Instelling: Directie, met mogelijkheid van delegatie)	P2	**B**	Directie	Beperkt (directie, personeelsdienst en betrokkene)
Ziektebriefjes	Wettelijk niet bepaald Gewenst: 5 jaar	-	Instelling: Directie, met mogelijkheid van delegatie)	P3	**C**	Directie	Beperkt (directie, personeelsdienst, externe medische dienst, personeelsdienst)
Andere afwezigheidsattesten: omstandigheidsverlof, syndicaal verlof…	Wettelijk niet bepaald Gewenst: 5 jaar	-	Instelling: Directie, met mogelijkheid van delegatie)	P3	**C**	Directie	Beperkt (directie, personeelsdienst)
Arbeidsreglement + bijlagen	Permanent actualiseren, Lopend exemplaar bewaren	Wet 08/04/1965	Werkgever	B2	**B**	Directie	Intern

Categorie: welzijn en preventie

Subcategorie: persoonsgebonden documenten

1. Naam en beschrijving van het document	2. Bewaartermijn: wettelijk en wenselijk	3. Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn	4. Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie	5. Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)	6. Classificatie volgens vereiste beveiliging (3 graden)	7. Gemachtigd om toegang/inzage te geven	8. Inzagerecht voor wie? (3 graden)
Formulier gezondheidsbeoordeling met aanbevelingen	Wettelijk: Zolang werknemer in de onderneming (voorziening) is tewerkgesteld (kan in personeelsdossier gestoken worden) Gewenst: idem	CODEX WELZIJN, BOEK I, titel 4, art.46	Werkgever (directie dus)	P3	**C**	Directie	Beperkt: (directie, betrokken werknemer, preventieadviseur-arbeidsarts
Formulier gezondheidsbeoordeling zonder aanbevelingen	Wettelijk: Maximum 3 jaar (praktisch gezien: na einde 3de jaar kan men systematisch elk jaar deze formulieren wegnemen en vernietigen) Gewenst: idem	CODEX WELZIJN, BOEK I, titel 4, art.46	Werkgever (directie dus)	P3	**C**	Directie	Beperkt: (directie, betrokken werknemer, preventieadviseur-arbeidsarts
Getuigschrift EHBO-verleners	Wettelijk: Zolang taak uitgevoerd wordt Gewenst: idem	CODEX WELZIJN, BOEK I, titel 5, artikel 8 en 9	Werkgever (directie dus) en werknemer	P2	**B**	Interne preventieadviseur	Intern
Gezondheidsdossier, te verdelen over							
Blootstelling- en ontsmettingstabel per individuele werknemer blootgesteld aan ioniserende straling	Wettelijk: 40 jaar, moet opgenomen worden in GEZONDHEIDSDOSSIER werknemer, inclusief de aangifte Wenselijk: 40 jaar	CODEX WELZIJN, BOEK V, titel 5, artikel 26	Dienst belast met medisch toezicht: extern: EDPBW	P3	**C**	Extern: preventieadviseur-arbeidsarts	Beperkt, via preventieadviseur en arbeidsarts

Gezondheidsdossier van werknemer blootgesteld aan biologisch agens met mogelijke effecten op lange termijn	Wettelijk: tot 30 jaar na vertrek van werknemer, dan overdragen aan de Algemene Directie Humanisering van de Arbeid	CODEX WELZIJN, BOEK VII, titel 1, artikel 49	Dienst belast met medisch toezicht: extern (EDPBW)	P3	**C**	Extern: preventieadviseur-arbeidsarts	Beperkt, via preventieadviseur-arbeidsarts
Gezondheidsdossier van werknemer blootgesteld aan kankerverwekkend of mutageen agens. Bijvoorbeeld: dossiers van personeelsleden blootgesteld aan asbest	Tot 40 jaar na vertrek van werknemer, dan overdragen aan de Algemene Directie Humanisering van de Arbeid Ten minste 40 jaar na het einde van blootstelling, dan overdragen aan de Algemene Directie Humanisering van de Arbeid *Van de in deze dossiers opgenomen inentingskaarten dienen slechts de laatste drie bewaard te worden; van de 'formulieren voor de gezondheidsbeoordeling', deze van de drie laatste jaren alsook alle formulieren waarop aanbevelingen vermeld staan*	CODEX WELZIJN, BOEK VI, titel 2, artikel 15	Dienst belast met medisch toezicht: extern (EDPBW)	P3	**C**	Extern: preventieadviseur-arbeidsarts	Beperkt, via preventieadviseur-arbeidsarts

Gezondheidsdossier voor alle werknemers onderworpen aan medisch onderzoek; bevat ook fiche medisch onderzoek van werknemer, en drie recentste inentingsfiches	Wettelijk: tot 15 jaar na vertrek van werknemer Gewenst: idem Wettelijk: tijdens de duur van de tewerkstelling voor de fiche 'medisch onderzoek en drie laatste inentingsfiches Gewenst: idem	CODEX WELZIJN, BOEK I, titel 4, artikel 89	Dienst belast met medisch toezicht: extern (EDPBW)	P3	**C**	Extern: preventieadviseur-arbeidsarts	Beperkt, via preventieadviseur-arbeidsarts
Formele psychosociale interventies zoals bij geweld, pesterijen en ongewenst seksueel gedrag op het werk	Wettelijk: twintig jaar vanaf datum van indiening van het verzoek Gewenst: idem	CODEX WELZIJN, BOEK I, titel 3, artikel 32	Preventieadviseur psychosociale aspecten: extern	P3	**C**	preventieadviseur psychosociale aspecten	Beperkt (preventieadviseur-arbeidsarts)
Informele psychosociale interventies zoals bij geweld, pesterijen en ongewenst seksueel gedrag op het werk	Tot einde tewerkstelling Gewenst: idem	CODEX WELZIJN, BOEK I, titel 3, artikel 31	Intern: bij de vertrouwenspersoon Extern: bij de preventieadviseur-psychosociale aspecten	P3	**C**	Interne vertrouwenspersoon en preventieadviseur psychosociale aspecten	Beperkt (Interne vertrouwenspersoon, en preventieadviseur psychosociale aspecten)
Opleidingsattesten, brevetten, bekwaamheidsattesten	Wettelijk: Zolang personen in dienst zijn Gewenst: idem	ARAB, AREI en Codex Welzijn	Werkgever (Directie met mogelijkheid van delegatie) en werknemer	P2	**B**	Directie	Beperkt (directie, personeelsdienst, betrokken werknemer)
Werkboekje voor werknemers werkzaam in hyperbare omgeving inclusief procedure	Wettelijk: 1 jaar na tewerkstelling Gewenst: idem	Codex Welzijn, BOEK V, titel 4, artikel 10	Werkgever	P2	**B**	Directie	Beperkt (directie, personeelsdienst, betrokken werknemer) interne preventieadviseur, preventieadviseur-arbeidsarts
Stagedocument met specifieke voorgeschreven informatie	Wettelijk: 1 jaar na tewerkstelling Gewenst: idem	CODEX WELZIJN, BOEK X, titel 4, artikel 5	Werkgever-stagegever	P2	**B**	Directie	Beperkt (directie, personeelsdienst, betrokken werknemer)

Werkpostfiche stagiair, waarop ook individuele gegevens van stagiair	Wettelijk: 1 jaar na tewerkstelling Gewenst: idem	CODEX WELZIJN, BOEK X, titel 4 , artikel 5	Werkgever-stagegever	P2	**B**	Directie	Beperkt (directie, personeelsdienst, betrokken werknemer)
Werkpostfiche uitzendkracht waarop ook individuele gegevens van uitzendkracht	1 jaar na tewerkstelling Gewenst: idem	CODEX WELZIJN, BOEK X, titel 4	Werkgever-inlener en uitzendonderneming	P2	**B**	Directie	Beperkt (directie, personeelsdienst, betrokken werknemer)

Subcategorie: opvolgingsdocumenten voor intern beheer

1. **Naam en beschrijving van het document**	**2.** **Bewaartermijn: wettelijk en wenselijk**	**3.** **Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn**	**4.** **Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie**	**5.** **Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)**	**6.** **Classificatie volgens vereiste beveiliging (3 graden)**	**7.** **Gemachtigd om toegang/inzage te geven**	**8.** **Inzagerecht voor wie? (3 graden)**
Asbestdossier: - Beheersprogramma	Wettelijk: Permanente actualisering, en permanente bewaring Gewenst: idem	CODEX WELZIJN, Boek VI, titel 3	Werkgever: Directie met mogelijkheid van delegatie	B2	**B**	Directie	Intern
- Meetgegevens van asbest	Wettelijk: 40 jaar, dan vernietigen Gewenst: idem	CODEX WELZIJN, Boek VI, titel 3	Werkgever: Directie	B2	**B**	Directie	Intern
- Inventaris van het asbest	Wettelijk: Levensduur gebouw/installatie Gewenst: idem	CODEX WELZIJNBoek VI, titel 3	Werkgever: directie	B2	**B**	Directie	Intern
- Werfplan, werfregister… bij werkzaamheden met asbest	Wettelijk: Duur van werkzaamheden Gewenst: idem		Werkgever: Directie	B2	**B**	Directie	Beperkt: facilitaire dienst, directie, betrokken werknemers, interne preventieadviseur, en preventieadviseur-arbeidsarts

Document waarin hiërarchische lijn uitvoering van onthaal van beginnende werknemer bevestigt	Wettelijk: 3 jaar Gewenst: idem	CODEX WELZIJN, Boek I, titel 2	Interne preventieadviseur	B2	I **B**	Interne preventieadviseur	Intern
Kennisgeving aan overheid van werkzaamheden: hyperbare omgeving, bepaalde chemische en biologische agentia, asbest,…	Wettelijk: 2 jaar na beëindiging werkzaamheden Gewenst: idem	Meerdere	Werkgever: Directie met mogelijkheid van delegatie	B2	**B**	Directie	Intern
Dossiers inzake de kennisgeving van het gebruik van biologische agentia	Wettelijk: 30 jaar Wenselijk: 30 jaar	CODEX, Boek VII, titel 1	Werkgever: Directie met mogelijkheid van delegatie	B2	**B**	Directie	Intern
Naamlijsten van gezondheidstoezicht (kwartaallijsten)	Wettelijk: Permanente actualisering, dan nog 5 jaar Wenselijk: idem	CODEX WELZIJN, Boek I, titel 4	Werkgever: Directie	P2	**B**	Directie	Beperkt (Interne preventieadviseur, preventieadviseur-arbeidsarts, directie)
Lijst van uitzendkrachten werkzaam in onderneming	Permanente actualisering	CODEX WELZIJN, Boek X, titel 2	Werkgever: Directie met mogelijkheid van delegatie	P2	**B**	Directie	Beperkt
Naamlijst van personen blootgesteld aan chemische stoffen	Permanente actualisering	CODEX WELZIJN, Boek VI, titel 1	Werkgever: Directie met mogelijkheid van delegatie	P2	**B**	Directie	Beperkt (Interne preventieadviseur, preventieadviseur-arbeidsarts, directie)
Register voor rechtstreekse participatie van werknemers, waar geen Comité PBW of syndicale afvaardiging is	Wenselijk: 5 jaar Wettelijk: idem	CODEX WELZIJN, Boek II, titel 8	interne preventieadviseur	P2	**B**	Directie en interne preventieadviseur	Beperkt

Risicoanalyses m.b.t. welzijn en preventie	Geen bewaartermijn, maar permanente actualisering	Administratieve taken van Interne preventieadviseur	Interne preventieadviseur	B3	**C**	Directie en interne preventieadviseur	Beperkt (directie, interne preventieadviseur)
Werkpostfiches voor uitzendarbeid opgemaakt voor functie of werkpost	Geen bewaartermijn, maar permanente actualisering (jaarlijks nakijken)	CODEX WELZIJN, Boek X, titel 2 en 3	Werkgever-inlener (dus directie)	B2	**B**	Directie	Intern
Werkpostfiches voor stagiairs opgemaakt voor functie of werkpost	Geen bewaartermijn, maar permanente actualisering (jaarlijks nakijken)	CODEX WELZIJN Boek X, titel 2 en 3	Werkgever-stagegever (dus directie)	B2	**B**	Directie	Intern
Opleidingsprogramma voor medewerkers en hiërarchische lijn	Duur van tewerkstelling, in personeelsdossier bewaren	CODEX WELZIJN, Boek I, titel 2, art.18	Werkgever: directie	P2	**C**	Directie	Beperkt (directie, betrokken werknemer)

Subcategorie: lijsten en registers van werknemers en activiteiten die na uitvoering van werkzaamheden moeten bewaard blijven

1. Naam en beschrijving van het document	**2. Bewaartermijn: wettelijk en wenselijk**	**3. Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn**	**4. Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie**	**5. Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)**	**6. Classificatie volgens vereiste beveiliging (3 graden)**	**7. Gemachtigd om toegang/inzage te geven**	**8. Inzagerecht voor wie? (3 graden)**
Lijst werknemers blootgesteld aan biologische agentia	Wettelijk: 10 jaar Gewenst: idem	CODEX WELZIJN, Boek VII, titel 1, art. 11	Dienst belast met medisch toezicht: externe dienst EDPBW	P3	**C**	'Dienst belast met medisch toezicht'	Beperkt (directie, Interne preventieadviseur, preventieadviseur-arbeidsarts)
Lijst werknemers blootgesteld aan biologische agentia die kunnen resulteren in bepaalde infecties	Wettelijk: 30 jaar Gewenst: idem	CODEX WELZIJN, Boek VII, titel 1, art.11	Dienst belast met medisch toezicht: externe dienst EDPBW	P3	**C**	'Dienst belast met medisch toezicht'	Beperkt: Directie, interne preventieadviseur, preventieadviseur-arbeidsarts
Register eerste hulp	Wettelijk: 3 jaar Gewenst: idem	Codex Welzijn, Boek I, titel 5	Werkgever	P3	**C**	Hulpverlener	Beperkt

Register van werknemers die blootgesteld werden aan asbest	Wettelijk: 40 jaar na het einde van de blootstelling Gewenst: idem	CODEX WELZIJN, Boek VI, titel 3, artikel 30	Werkgever: Directie met mogelijkheid van delegatie	P3	**C**	Directie	Beperkt: directie, interne preventieadviseur, preventieadviseur-arbeidsarts
Register (jaarlijks opgesteld, en naamloos) met klachten i.v.m. pesten en geweld, seksueel grensoverschrijdend gedrag op werk (ook door contact met anderen dan eigen werknemers of uitzendkrachten: bv. klanten, leveranciers, werkzoekenden, publiek)	Wettelijk: 5 jaar na verklaring klacht Gewenst: idem	CODEX WELZIJN, Boek I, titel 3, art.3	Werkgever: Directie met mogelijkheid van delegatie	P3	**C**	Interne preventieadviseur en vertrouwenspersoon	Beperkt: vertrouwenspersoon; bij ontstentenis hiervan: interne preventieadviseur
Register aanslagmateriaal (aanslagmateriaal: kettingen, lengen, haken, katrollen e.d.)	Wettelijk: Permanente actualisering Gewenst: idem	ARAB, art. 269	Werkgever: Directie met mogelijkheid van delegatie	B2	**B**	Directie	Intern
Register begassing	Wettelijk: 3 jaar Gewenst: idem	KB 14.1.92, art. 38	Werkgever	B2	**B**	Directie	Intern
Register werkzaamheden in hyperbare omgeving (omgeving onder druk)	Wettelijk: 20 jaar na werkzaamheden Gewenst: idem	CODEX WELZIJN, Boek V, titel 4	Werkgever, op de werf: dus de Directie. 'Op de werf': zolang de werkzaamheden duren.	B2	**B**	Directie	Intern

Subcategorie: rapporten en verslagen van werkzaamheden en inspecties

1. Naam en beschrijving van het document	2. Bewaartermijn: wettelijk en wenselijk	3. Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn	4. Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie	5. Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)	6. Classificatie volgens vereiste beveiliging (3 graden)	7. Gemachtigd om toegang/inzage te geven	8. Inzagerecht voor wie? (3 graden)
Bestralingspaspoort voor werknemers blootgesteld aan ioniserende straling	Wettelijk: 1 jaar na overmaken rapport aan overheid Gewenst: idem	CODEX WELZIJN, Boek V, titel 5	Exploitant van installatie: kan dit bij ons de werkgever zijn, en dus de directie	P3	**C**	Directie	Beperkt: directie, betrokken werknemers, interne preventieadviseur en preventieadviseur-arbeidsarts
Interventieverslagen van EDPBW	Wettelijk: 5 jaar Gewenst: idem	CODEX WELZIJN, Boek II, titel 3	Interne preventieadviseur	P3	**C**	Directie en interne preventieadviseur	Beperkt: directie, interne preventieadviseur
Keuringsverslag arbeidsmiddelen die tijdens gebruiksduur risico's inhouden	Wettelijk: 1 jaar na volgend verslag Gewenst: idem	CODEX WELZIJN, Boek IV, titel 2	interne preventieadviseur	B2	**B**	Directie en interne preventieadviseur	Intern
Verslag nazicht materiaal branddetectie, verwarmingsinstallatie	Wettelijk: 1 jaar na volgend verslag Gewenst: idem	Boek III, titel 3, artikel 31	Werkgever	B2	**B**	Directie en interne preventieadviseur	Intern
Verslag (jaarlijkse) rondgang CPBW met hiërarchische lijn en preventieadviseur(s)	Wettelijk: 5 jaar Gewenst: idem	CODEX WELZIJN, Boek II, titel 7	interne preventieadviseur	B2	**B**	Directie en interne preventieadviseur	Intern
Verslagen van EDTC (=Externe Dienst voor Technische Controle of Keurder) inclusief de inventaris van de toestellen en machines die moeten gecontroleerd worden door EDTC	Wettelijk: 1 jaar na volgend verslag Gewenst: idem	ARAB, AREI en Codex Welzijn	Werkgever: Directie met mogelijkheid van delegatie	B2	**B**	Directie	Intern

Buitenlands verslag van keuring hefwerktuigen en toebehoren	Wettelijk: Totale gebruiksduur Gewenst: idem	ARAB, art. 281 quater	Werkgever	B2	**B**	Directie	Intern
Indienststellingsverslag installaties en machines	Wettelijk: Tot einde gebruik Gewenst: idem	ARAB en Codex Welzijn	Werkgever	B2	**B**	Directie en interne preventieadviseur	Intern
Indienststellingsverslag arbeidsmiddelen en PBM (Persoonlijke Beschermingsmiddelen)	Wettelijk: Volledige gebruiksduur Gewenst: idem	CODEX WELZIJN, Boek IX, titel 2	Werkgever (dus: Directie met mogelijkheid van delegatie)	B2	**B**	Directie	Intern

Subcategorie: verslagen, vergaderingen, …

1. **Naam en beschrijving van het document**	**2.** **Bewaartermijn: wettelijk en wenselijk**	**3.** **Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn**	**4.** **Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie**	**5.** **Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)**	**6.** **Classificatie volgens vereiste beveiliging (3 graden)**	**7.** **Gemachtigd om toegang/inzage te geven**	**8.** **Inzagerecht voor wie? (3 graden)**
Administratieve en andere documenten: uitnodigingen, samenstelling, adviezen, notulen met bijlagen van het CPBW en voorgangers (CVGW) (vergaderingen, rondgang, …) Ook register waarin werknemers voorstellen, opmerkingen en advies kunnen optekenen	Wettelijk: Vastgelegd in huishoudelijk reglement van het CBPW en diens voorgangers Gewenst: minimum 10 jaar	CODEX WELZIJN Boek II, titel 7, artikel 31.10°	Interne preventieadviseur	B2	**B**	Directie - interne preventieadviseur	Intern

Huishoudelijk reglement CPBW	Wettelijk: Bij elke nieuwe samenstelling (lees sociale verkiezing) van een CPBW moet er een nieuw huishoudelijk reglement worden opgesteld of een herbevestiging zijn van het bestaande Gewenst:: actualiseren bij installatie CPBW, lopend exemplaar bewaren	Codex Welzijn, Boek II, titel 7, artikel 31.10°	Interne preventieadviseur	B2	**B**	Directie – interne preventieadviseur	Beperkt (leden CPBW)
Jaarverslag Interne preventieadviseur	Wettelijk: 10 jaar Gewenst: idem	CODEX WELZIJN, Boek II, titel 1	Interne preventieadviseur	B2	**B**	Directie - Interne preventieadviseur	Intern
Maandverslag Interne preventieadviseur (bevat ook voorstellen en adviezen van de interne preventieadviseur)	Wettelijk: 3 jaar na werkjaar Gewenst: 5 jaar	CODEX WELZIJN, Boek II, titel 1	Interne preventieadviseur	B2	**B**	Directie - Interne preventieadviseur	Beperkt (interne preventieadviseur, en directie)

Subcategorie: instructies

1. Naam en beschrijving van het document	**2. Bewaartermijn: wettelijk en wenselijk**	**3. Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn**	**4. Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie**	**5. Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)**	**6. Classificatie volgens vereiste beveiliging (3 graden)**	**7. Gemachtigd om toegang/inzage te geven**	**8. Inzagerecht voor wie? (3 graden)**
Gebruiksaanwijzingen, handleidingen voor arbeidsmiddelen, PBM's, CBM's, procedures,…	Wettelijk: Duur van werkzaamheden Gewenst: idem	CODEX WELZIJN, Boek IV, titel 2 CODEX WELZIJN, Boek IX, titel 1 en 2	Werkgever (Directie met mogelijkheid van delegatie)	B2	**A**	Hiërarchische lijn en interne preventieadviseur	Intern
Instructienota voor werken met kankerverwekkende en mutagene stoffen	Wettelijk 1 jaar na werkzaamheden Gewenst: idem	CODEX WELZIJN, Boek VI, titel 2, art. 5	Werkgever (Directie met mogelijkheid van delegatie)	B2	**A**	Hiërarchische lijn en interne preventieadviseur	Intern

Instructienota voor montage, afbraak, ombouw en gebruik van steiger, berekeningsnota	Wettelijk: Totale gebruiksduur Gewenst: idem	CODEX WELZIJN, Boek IV, titel 5	Werkgever (Directie met mogelijkheid van delegatie)	B2	**A**	Hiërarchische lijn en interne preventieadviseur	Intern
Instructies voor gebruik biologische agentia en maatregelen bij ongeval	Wettelijk 1 jaar na werkzaamheden Gewenst: idem	CODEX WELZIJN, Boek VII, titel 1	Werkgever (Directie met mogelijkheid van delegatie)	B2	**A**	Hiërarchische lijn en interne preventieadviseur	Intern
Instructies werking, gebruik, inspectie, onderhoud collectieve beschermingsmiddelen	Wettelijk: Totale gebruiksduur Gewenst: idem	CODEX WELZIJN, Boek IX, titel 1	Interne preventieadviseur	B2	**A**	Directie en interne preventieadviseur	Intern

Subcategorie: documenten m.b.t. ongevallen

1. **Naam en beschrijving van het document**	**2.** **Bewaartermijn: wettelijk en wenselijk**	**3.** **Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn**	**4.** **Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie**	**5.** **Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)**	**6.** **Classificatie volgens vereiste beveiliging (3 graden)**	**7.** **Gemachtigd om toegang/inzage te geven**	**8.** **Inzagerecht voor wie? (3 graden)**
Aangifteformulier arbeidsongeval aan verzekeraar (voorbeeld: prikaccident)	Wettelijk: 3 jaar na definitieve afsluiting door verzekeraar Gewenst: 10 jaar	Wet 10.4.71, art. 62 K.B. 24/02/2005 (BS 14/03/2005) i.v.m. arbeidsongevallen(aangifte), art. 1.	Personeelsdienst (dus: Directie met mogelijkheid van delegatie)	P3	**C**	Directie	Beperkt: directie, personeelsdienst, betrokken werknemer, Interne preventieadviseur, preventieadviseur-arbeidsarts
Arbeidsongevallensteekkaart	Wettelijk: 10 jaar Gewenst: idem	CODEX WELZIJN, Boek I, titel 6, art.12 K.B. 24/02/2005 (BS 14/03/2005) i.v.m. arbeidsongevallen(aangifte) art. 1.	Interne preventieadviseur	P3	**C**	Directie en Interne preventieadviseur	Beperkt (directie, personeelsdienst, betrokken werknemer, interne preventieadviseur)
Omstandig verslag van ernstig ongeval	Wettelijk: 10 jaar Gewenst: 30 jaar	CODEX WELZIJN, Boek I, titel 6	Interne preventieadviseur	P3	**C**	Directie en Interne preventieadviseur	Beperkt: directie, betrokken werknemer, Interne preventieadviseur

Subcategorie: documenten m.b.t. analyses, rapporten, plannen, …

1. Naam en beschrijving van het document	2. Bewaartermijn: wettelijk en wenselijk	3. Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn	4. Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie	5. Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)	6. Classificatie volgens vereiste beveiliging (3 graden)	7. Gemachtigd om toegang/inzage te geven	8. Inzagerecht voor wie? (3 graden)
Adviezen interne preventieadviseur, preventieadviseur-arbeidsarts	Wettelijk: 5 jaar Gewenst: idem	ARAB en Codex Welzijn, talrijke artikelen	interne preventieadviseur	B2	**B**	Directie en interne preventieadviseur	Intern
Gegevens van monstername van chemische agentia, en verslag van metingen van chemische agentia	Wettelijk: 5 jaar Gewenst: idem	CODEX WELZIJN, Boek VI, titel 1, art.56	interne preventieadviseur	B2	**B**	Directie en interne preventieadviseur	Intern
Globaal preventieplan - GPP	Wettelijk: Permanent actualiseren Gewenst: 10 jaar	CODEX WELZIJN, Boek I, titel 2, art.8	Werkgever (dus Directie met mogelijkheid van delegatie)	B2	**A**	Directie	Intern
Jaaractieplan – JAP	Wettelijk: 5 jaar Gewenst: 10 jaar	CODEX WELZIJN, Boek I, titel 2,a rt.9	Werkgever (dus Directie met mogelijkheid van delegatie)	B2	**A**	Directie	Intern
Intern noodplan (overkoepelt evacuatieplan, bevat of is gelijk aan: calamiteitenplan, rampenplan, ontruimingsplan…). Omvat ook verslagen van brand- en evacuatieoefeningen.	Wettelijk: Permanent actualiseren Gewenst: idem	CODEX WELZIJN, Boek I, titel 2, art. 23 tot 26 CODEX WELZIJN, Boek VI, titel 1, art. 21 tot 26	Werkgever	B2	**A**	Directie	Intern
Meetresultaten i.v.m. bestrijding van hinder	Wettelijk: 3 jaar na volgend resultaat Gewenst: idem	ARAB, art. 148*decies*	Interne preventieadviseur	B2	**A**	Directie en interne preventieadviseur	Intern
Meetresultaten geluid	Wettelijk: 5 jaar Gewenst: idem	CODEX WELZIJN, Boek V, titel 2	interne preventieadviseur	B2	**A**	Directie en interne preventieadviseur	Intern

Meetresultaten trillingen	Wettelijk: 5 jaar Gewenst: idem	CODEX WELZIJN, Boek V, titel 3	interne preventieadviseur	B2	**A**	Directie en interne preventieadviseur	Intern
Veiligheids- en gezondheidsplan, coördinatiedagboek op tijdelijke of mobiele bouwplaatsen	Wettelijk: 10 jaar na beëindiging van werken Gewenst: idem	KB van 25/01/2001 (BS 07/02/2001) tijdelijke en mobiele bouwplaatsen, art. 26 e.v.	Veiligheidscoördinator en interne preventieadviseur	B2	**B**	Directie + Interne preventieadviseur + Veiligheidscoördinator	Intern

Subcategorie: documenten m.b.t. overeenkomsten, contracten, aankoopdocumenten

1. **Naam en beschrijving van het document**	**2.** **Bewaartermijn: wettelijk en wenselijk**	**3.** **Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn**	**4.** **Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie**	**5.** **Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)**	**6.** **Classificatie volgens vereiste beveiliging (3 graden)**	**7.** **Gemachtigd om toegang/inzage te geven**	**8.** **Inzagerecht voor wie? (3 graden)**
Aannemingscontracten, overeenkomst voor uitzendarbeid met uitzendbureau met bepalingen i.v.m. onthaal	Wettelijk: 5 jaar na uitvoering contract Gewenst: idem	Welzijnswet 04/08/1996, H.IV en XI*bis*	Werkgever (dus: Directie met mogelijkheid van delegatie)	P3?	**C**	Directie	Beperkt: Directie, interne preventieadviseur, personeelsdienst
Aanstelling veiligheidscoördinator tijdelijke of mobiele bouwplaatsen	Wettelijk: 10 jaar na afloop werken Gewenst: idem	KB van 25/01/2001 (BS 07/02/2001) tijdelijke en mobiele bouwplaatsen, art. 26 e.v.	Directie	B2	**B**	Directie	Beperkt (Directie, interne preventieadviseur, veiligheidscoördinator)
Identificatiedocument van de werkgever waarbij interne en externe dienst aangeven wie wat doet op vlak van de 7 preventiedomeinen	Wettelijk: Permanent actualiseren Gewenst: idem	Codex Welzijn, Boek II, titel 1, art.7	Werkgever	B2	**B**	Directie en interne preventieadviseur	Intern
Minimumprestatieduur m.b.t. interne preventieadviseur met advies van de CPBW	Wettelijk: Permanent actualiseren Gewenst: idem	Codex Welzijn, Boek II, titel 1, art.16	Werkgever	B2	**B**	Directie en interne preventieadviseur	Intern

Overeenkomst met EDPBW, EDTC	Wettelijk: 3 jaar na jaarlijkse herziening Gewenst: idem		Werkgever (dus: Directie met mogelijkheid van delegatie)	B2	**B**	Directie	Beperkt (directie, interne preventieadviseur, CBPW)
Werkvergunningen en vuurvergunningen voor brandgevaarlijke werkzaamheden	Wettelijk: tot einde werkzaamheden en eindinspectie Gewenst: idem	KB over werken met derden – wet van 04/08/1996	Werkgever	B2	**A**	Directie en interne preventieadviseur	Intern

Subcategorie: documenten m.b.t. materialen, uitrusting, gebouwen

1. **Naam en beschrijving van het document**	**2.** **Bewaartermijn: wettelijk en wenselijk**	**3.** **Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn**	**4.** **Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie**	**5.** **Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)**	**6.** **Classificatie volgens vereiste beveiliging (3 graden)**	**7.** **Gemachtigd om toegang/inzage te geven**	**8.** **Inzagerecht voor wie? (3 graden)**
Bestelbon, CE-verklaring van overeenstemming en leveranciersattesten van arbeidsmiddelen en PBM's en CBM's	Wettelijk: Volledige gebruiksduur Gewenst: idem	CODEX WELZIJN Boek IV, titel 2 CODEX WELZIJN, Boek IX, titel 2	Werkgever (dus: Directie met mogelijkheid van delegatie)	B2	**B**	Directie	Intern
Bewijs brandgedrag bouwmaterialen	Wettelijk: Volledige gebruiksduur Gewenst: idem	ARAB, art. 52.2 CODEX WELZIJN, Boek IV, titel 2	Werkgever (dus: Directie met mogelijkheid van delegatie)	B2	**B**	Directie	Intern
Postinterventiedossier bij nieuwbouw of renovaties	Wettelijk: Volledig levensduur van het gebouw Gewenst: idem	CODEX WELZIJN, KB van 25/01/2001 (BS 07/02/2001) tijdelijke en mobiele bouwplaatsen	Eigenaar (dus: Directie met mogelijkheid van delegatie)	B2	**B**	Directie	Intern
Veiligheidsinformatieblad gevaarlijke stoffen en preparaten – VIB (inclusief de lijst van de GSP (Gebruikte Stoffen en Preparaten))	Wettelijk: Zolang product in bedrijf aanwezig is Gewenst: idem	Codex Welzijn, Boek VI, titel 1, art.29,4°	Werkgever	B2	**B**	Directie	Intern

Explosieveiligheids-documenten (EVD)	Wettelijk: permanent actualiseren Gewenst: tot opmaak nieuwe versie	CODEX WELZIJN, Boek III, titel 4	Werkgever	B3	**C**	Directie en interne preventieadviseur	Beperkt: directie, interne preventieadviseur en CPBW

Categorie: financieel-economisch, boekhouding

1. Naam en beschrijving van het document	2. Bewaartermijn: wettelijk en wenselijk	3. Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn	4. Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie	5. Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)	6. Classificatie volgens vereiste beveiliging (3 graden)	7. Gemachtigd om toegang/inzage te geven	8. Inzagerecht voor wie? (3 graden)
Jaarrekening van de instelling	Wettelijk: 30 jaar te tellen vanaf het jaar na de afsluiting Gewenst: permanent	Wet van 17.07.1975 op de boekhouding + art. 17 gecoördineerde tekst vzw-wet van 27 juni 1921	Directie met mogelijkheid van delegatie	B2	**B**	Directie	Openbaar
Herzieningsdossier (vroeger: 'Budget financiële middelen', of nog: ligdagprijsdossier) (Verzorgingsinstellingen)	Wettelijk: - Gewenst: permanent		Directie met mogelijkheid van delegatie	B3	**B**	Directie	Beperkt (Directie en boekhouding)
Bewijsstukken statistische gegevens (m.b.t. opnamen, anciënniteit, en andere. Worden elektronisch via Finhosta doorgestuurd)	5 jaar Wenselijk: 5 jaar	Art. 6 K.B. van 14.12.87 m.b.t. de jaarrekeningen van de ziekenhuizen	Directie met mogelijkheid van delegatie	B2	**B**	Directie	Beperkt (directie en boekhouding)
Belastingsstukken	Wettelijk: tot 7 jaar na het verstrijken van het belastbaar tijdperk Wenselijk: 7 jaar	Art. 221 Wetboek der inkomstenbelastingen	Directie met mogelijkheid van delegatie	B2	**B**	Directie	Beperkt (directie en boekhouding)
Documenten m.b.t. beheer van patiëntengelden	Wettelijk: 7 jaar Wenselijk: 7 jaar	Wet van 17/07/1975	Directie met mogelijkheid van delegatie	P3	**C**	Directie	Beperkt (Directie, Boekhouding, Audit, betrokkene en zijn/haar gemachtigde, …

Boekhouding: - (wettelijke) boeken: centraal boek, hulpdagboeken, dagboeken (zoals een kasboek), ontvangstbewijsboekjes, inventarisboek - Verantwoordingstukken, zoals facturen, creditnota's, kassatickets, offertes en bestekken, gegevens uit de analytische boekhouding, bankrekeninguittreksels… BTW-wetgeving eist ook documenten waarnaar verwezen wordt op de factuur zoals bestelbon, leveringsbon… . - Tabel van de bedrijfsmiddelen	Wettelijk: 10 jaar (concreet: 10 jaar vanaf 1 januari van het jaar na de afsluiting) Wettelijk: 10 jaar, of 15 jaar (de normale bewaartermijn van 10 jaar wordt verlengd tot 15 jaar voor documenten die betrekking hebben op de oprichting of de verkrijging van een gebouw dat als bedrijfsmiddel dient, of van de verkrijging van zakelijke rechten op een dergelijk gebouw, , dit omwille van de herzieningstermijn van 15 jaar voor de BTW). Facturen m.b.t. investeringen (bv. machines en gebouwen) moeten worden bewaard tot 10 jaar na het laatste jaar waarin afgeschreven werd. Wettelijk: deze moeten worden bewaard gedurende 10 jaar vanaf het verstrijken van het herzieningstijdvak.	Art. 78 Ziekenhuiswet (ZHW) & Art. 6 en 9 §2 van de wet van 17.07.75 op de boekhouding en jaarrekeningen + art. 17 gecoördineerde tekst vzw-wet van 27 juni 1921 Art. 9, § 1, K.B. nr. 3, en artikel 11, § 4, K.B. nr. 3. (K.B. van welke datum, welk K.B.?)	Directie met mogelijkheid van delegatie	B2	**B**	Directie	Beperkt (Directie en boekhouding)

	Het uitgangspunt van het herzieningstijdvak is normaal de eerste januari van het jaar waarin het recht op aftrek ontstaat (art. 9, § 1, K.B. nr. 3). Wanneer het uitgangspunt van het herzieningstijdvak echter de eerste januari is van het jaar waarin het bedrijfsmiddel in gebruik werd genomen, en dit tijdstip valt later dan het uitgangspunt van de bewaringstermijn zoals vastgesteld in het vorige lid, dan begint de bewaringstermijn te lopen op de eerste januari van het jaar waarin dat bedrijfsmiddel in gebruik werd genomen (artikel 11, § 4, K.B. nr. 3).						
- Interne stukken (stukken die niet nodig zijn als bewijs tegenover derden)	3 jaar						
- Digitale bestanden die de boekhouding bevatten	Wettelijk: zoals de papieren boekhouding, maar de leesbaarheid moet gegarandeerd blijven (dus oude software moet indien nodig lang genoeg bewaard blijven)						

Categorie: patiënten- en bewonersadministratie, medisch secretariaat

Algemene opmerking m.b.t. inzagerecht (laatste kolom): onderzoekers (wetenschappelijk, historisch, statistisch) kunnen onder voorwaarden (vnl. eerbiedigen privacy), meestal na een termijn van 30 jaar, een aantal documenten raadplegen, en dit overigens na toelating. Het zou anders ook geen zin hebben deze documenten permanent bij te houden (voorbeeld: tot op heden bewaarde registers en dossiers van de 19de en 20ste eeuw). De Commissie voor de Bescherming van de Persoonlijke Levenssfeer laat overigens ook toe dergelijke archieven te bewaren met het oog op onderzoek. Huidige Belgische wetgeving en ook GDPR laten expliciet toe om dergelijke documenten te bewaren met oog op later onderzoek (historisch, wetenschappelijk, statistisch).

1. Naam en beschrijving van het document	2. Bewaartermijn: wettelijk en wenselijk	3. Verwijzing in geval van wettelijke of gereglementeerde bewaartermijn	4. Verantwoordelijk voor de bewaring: instelling, personeelslid, externe organisatie	5. Graad van vertrouwelijkheid en gevoeligheid (2 x 3 subcategorieën)	6. Classificatie volgens vereiste beveiliging (3 graden)	7. Gemachtigd om toegang/inzage te geven	8. Inzagerecht voor wie? (3 graden)
Oude patiënten- en bewonersregisters (19de eeuw, 20ste eeuw, in gebruik tot de jaren 1980) Eigenlijk kunnen er twee reeksen van registers voorkomen: de stamboeken (‘régistres matricules’) en de medische registers	Wettelijk: onbepaald Gewenst: permanent	-	Instelling: Directie, of bij delegatie	P3	**C**	Directie en/of hoofdarts indien ouder dan 30 jaar (afsluitdatum)	Beperkt
Patiënten- en bewonersdossiers (Medisch)	Wettelijk: 30 jaar. Ook de Code van de Geneeskundige plichtenleer geeft 30 jaar na afsluiting dossier (laatste wijziging) Gewenst: permanent	KB van 3 mei 1999 houdende bepaling van de algemene minimumvoorwaarden waaraan het medische dossier, bedoeld in artikel 15 van de wet op de ziekenhuizen, gecoördineerd op 7 augustus 1987 moet voldoen (BS 30.07.1999) In de wet op de ziekenhuizen en andere instellingen … van 10 juli 2008 is dit opgenomen in artikel 20 (BS 07/11/2008)	Directie, met mogelijkheid van delegatie	P3	**C**	Hoofdarts	Beperkt

Patiënten- en bewonersdossier (administratief)	Wettelijk: onbepaald Gewenst: permanent	-	Instelling: Directie, met mogelijkheid te delegeren	P3	**C**	Directie	Beperkt
Verpleegkundige dossiers - Kan deel uitmaken van het medische dossier	Wettelijk: 30 jaar Gewenst: gezien het geïntegreerd wordt in het medische dossier: ook permanent Zit thans (EPD) samen met medisch dossier.	Art. 15 Ziekenhuiswet geeft dus 30 jaar	Instelling: Directie, met mogelijkheid van delegatie	P3	**C**	Hoofdarts	Beperkt
Dossiers van andere diensten per patiënt of bewoner: therapeutische diensten, sociale dienst, …: bij afsluiten bij voorkeur samenvoegen in het unieke dossier per patiënt/bewoner	Wettelijk: - geen, maar in geval van samenvoeging met het medische dossier: 30 jaar Gewenst: 30 jaar, maar in geval van samenvoeging met het medische dossier: permanent	-	Instelling: Directie, met mogelijkheid van delegatie	P3	**C**	In geval van samenvoeging of consolidatie in één dossier: hoofdarts	Beperkt
Afzonderingsregister (-registratie) (bestond al in de 19de eeuw)	Wettelijk: onbepaald, maar de Code van de Geneeskundige plichtenleer geeft 30 jaar Gewenst: permanent	-	Instelling: Directie, met mogelijkheid van delegatie	P3	**C**	Hoofdarts	Beperkt
Register van de gedwongen opnamen (vanaf 1991 verplicht).	Wettelijk: onbepaald, maar de Code van de Geneeskundige plichtenleer geeft 30 jaar Gewenst: permanent	-	Instelling: Directie, met mogelijkheid van delegatie	P3	**C**	Hoofdarts	Beperkt

Protocollen van radiografieën en labo-onderzoeken, andere documenten, verslagen, tracés en grafieken	Wettelijk: 2 jaar Gewenst: zie de algemene opmerking m.b.t. afsluiten en schonen van patiënten/bewonersdossiers: alleen relevante documenten permanent in het dossier laten indien men al beslist deze in het dossier op te nemen	Art. 1 §8 van bijlage bij K.B. van 14.09.84 betreffende de nomenclatuur van geneeskundige verstrekkingen	Instelling: Directie, met mogelijkheid van delegatie	P3	**C**	Hoofdarts	Beperkt
Lijst artsen van wachtdienst	Wettelijk: 2 jaar Gewenst: niet langer dan 2 jaar	Art. 25 §3 K.B. van 14.09.84	Instelling: Directie, met mogelijkheid van delegatie	P1	**B**	Directie	Intern
Voorschriften: voor analyses inzake klinische biologie	Wettelijk : 3 jaar Gewenst: 3 jaar	Art. 24 §12 punt 6 K.B. van 14.09.84	Instelling: Directie, met mogelijkheid van delegatie	P3	**C**	Hoofdarts	Beperkt
Voorschriften: voor geneesmiddelen	Wettelijk :10 jaar Gewenst: 10 jaar	Art. 34 K.B.31.05.1885	Instelling: Directie, met mogelijkheid van delegatie	P3	**C**	Hoofdarts	Beperkt
Voorschriften: voor radiologie	Wettelijk: 2 jaar Gewenst: 2 jaar	Art. 17 §12, 5° K.B. 14.09.1984	Instelling: Directie, met mogelijkheid van delegatie	P3	**C**	Hoofdarts	Beperkt
Register van analysen van de grondstoffen door de ziekenhuisapotheker	Wettelijk: 10 jaar Gewenst: 10 jaar	Art. 6 K.B. 20.10.1994	Instelling: Directie, met mogelijkheid van delegatie	B2	**B**	Ziekenhuisapotheker	Beperkt: ziekenhuisapotheker
Verklaring van opneming Aanvraag om verlenging ziekenhuisverpleging Kennisgeving einde ziekenhuisverpleging	Wettelijk: 3 jaar vanaf het ogenblik van de vergoeding van de prestatie Gewenst: 3 jaar	Omzendbrief RIZIV van 27.03.1987	Instelling: Directie, met mogelijkheid van delegatie	P3	**C**	Directie	Beperkt
Verzamelgetuigschrift voor verstrekte hulp (facturatie ambulanten)	Wettelijk: 7 jaar Wenselijk: 7 jaar	MB van 31.03.2009	Instelling: Directie, met mogelijkheid van delegatie	P3	**C**	Directie	Beperkt

Uittreksel verpleegnota (patiëntenfacturen)	Wettelijk: 7 jaar Wenselijk: 7 jaar	MB van 31.03.2009	Instelling: Directie, met mogelijkheid van delegatie	P3	**C**	Directie	Beperkt
Individuele kostennota (mutualiteitsfactuur)	Wettelijk: 7 jaar Wenselijk: 7 jaar	MB van 31.03.2009	Instelling: Directie, met mogelijkheid van delegatie	P3	**C**	Directie	Beperkt

Bijlage 1

Good practice voorbeeld vanuit het PC Zoete Nood Gods Lede (sinds 18/12/2017 P.C. Ariadne)

PSYCHIATRISCH CENTRUM
ZOETE NOOD GODS

WERKING VAN HET ARCHIEF

Inge Vandendriessche

Administratief directeur

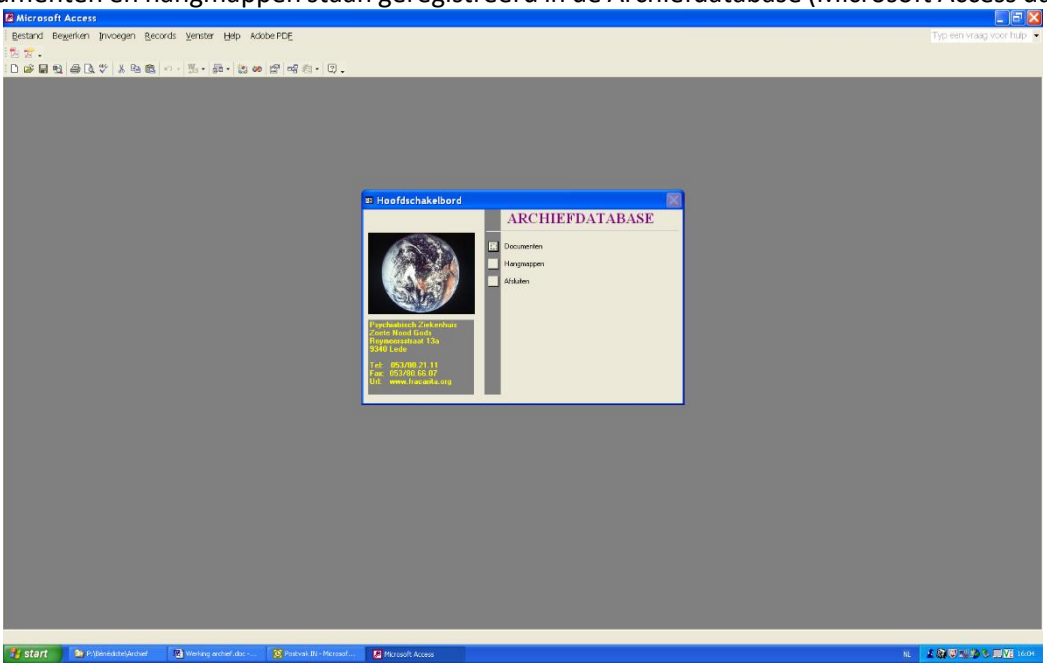
26 augustus 2013

1. Inleiding

Het archief kan grosso modo opgesplitst worden in

a) Documenten (archiefdozen, mappen, …).
b) Hangmappen (volgens het systeem van Jalema).

Alle documenten en hangmappen staan geregistreerd in de Archiefdatabase (Microsoft Access database).



<u>Archiveren</u> (= input in database en klasseren)
Het medisch secretariaat staat in voor de archivering van de hangmappen met als code '**DOP**' (verpleegkundige en (para)medische dossiers) en '**SOD**' (sociale dossiers). De steward staat in voor de etikettering van de hangmappen met als code '**ARG**' (oude arbeidsgeneeskundige dossiers – nieuwe dossiers worden elektronisch bijgehouden) en '**PED**' (personeelsdossiers). De administratieve dossiers en alle andere documenten (met uitzondering van deze van de directie), die geen code in de database hebben toegewezen, worden eveneens geklasseerd door de steward. Het directiesecretariaat archiveert de documenten van de directie en de loonsadministratie staat in voor de archivering van de personeelsdossiers.

De afdelingen kunnen voor de documenten die klaar zijn om gearchiveerd te worden, een beroep doen op de stewards. Zij staan in voor archivering: een gepaste locatie wordt uitgezocht, de data worden in de Archiefdatabase ingebracht en de documenten worden voorzien van een etiket.

Bij opname van een patiënt of bewoner maakt het medisch secretariaat het medische en sociale dossier op. Enkel het medische en sociale dossier worden in de archiefdatabase genummerd. Het psychologische dossier, dat een onderdeel is van het medische dossier, en het administratieve dossier worden niet apart gearchiveerd (cfr. Regas). Het aanmaken van een dossier houdt in dat de data ingegeven worden en vervolgens afgedrukt worden op een etiket dat aangebracht wordt op de bruine hangmap. De mappen gaan vervolgens naar de betrokken diensten. Bij ontslag van de patiënt of bewoner gaat het dossier naar het archief.

Uitlenen (= input in database en uithalen)
Het uitlenen van hangmappen (DOP en SOD) gebeurt via het medisch secretariaat. Het uitlenen van documenten gebeurt via de steward. Uitzondering hierop zijn de hangmappen ARG en PED, alsook de mappen/documenten voor de directie. Deze worden ofwel door het directiesecretariaat ofwel door de medewerkers van de loonsadministratie opgehaald.

2. Documenten (aanduidingen in het blauw)

Dit onderdeel is opgesplitst volgens de verschillende afdelingen/diensten. Elke categorie beschikt over één of meerdere rekken/kasten in het archief, telkens aangeduid met een letter. Op de rekken zelf zijn ook nog eens schapnummers aangebracht, zodat elk gearchiveerd stuk vrij snel kan teruggevonden worden. Deze gegevens staan geregistreerd in de Archiefdatabase.

document overzicht categorie		
categorie	**omschrijving**	**rekletter**
APO	Apotheek	I - J
ARG	Arbeidsgeneeskundige Dienst	V
BHD	Boekhouding	C - D
DIA	Directiearchief	F - V
DIE	Diensten	H-R
DOP	Dossiers Patiënten	B
FAC	Facturatie	M
FAD	Facilitaire Dienst	W
HIS	Historisch archief	S
IWG	Inwendige Geneeskunde	U
MDK	Middenkader	E
MES	Medisch Secretariaat	J - L
MPG	Minimale Psychiatrische Gegevens	G
NEU	Neurologie	X
PED	Personeelsdienst	T
PTF	Patiëntenadministratie	O - Q
SOD	Sociale Dienst	A - N - O

Archiefdatabase/Documenten/Opzoeken en uitlenen documenten/
Opzoeken/Overzicht categorieën documenten

Categorie APO: Apotheek:
Voorschriften, attesten, bestelbons, facturatie, teruggaves, …

Categorie BHD: Boekhouding:
Facturen leveranciers, erelonen, magazijnbons, verantwoordingsstukken, rappels, facturen en creditnota's, …

Categorie DIA: Directiearchief:
Jaarverslagen, verslagen raad van bestuur, verslagen directiecomité, notulen ondernemingsraad, dienstnota's, …

Categorie DIE: Diensten:
Afzonderingsboeken, dagboeken, cognitieve screeningtests, …
Op deze rekken staan documenten van verschillende afdelingen of diensten gerangschikt: verpleegafdelingen, pastorale dienst, assistent in de psychologie, beschut wonen, SAVA (activeringscentrum), … Deze afdelingen/personen zijn eerder beperkt wat het aantal archiveringsstukken betreft. Om archiveringsruimte uit te sparen, wijzen we hier geen volledig rek toe.

Categorie FAC: Facturatie:
RIZIV-facturatie, facturatie ziekenhuis, facturatie PVT, …

Het gaat hier enkel om de facturatie in het kader van het verblijf van patiënten en bewoners. Het gaat enkel om documenten van de patiëntenadministratie. Hier is enige overlapping met categorie PTF.

Categorie FAD: Facilitaire dienst:
Alle documenten i.v.m. bouw- en verbouwingswerken, plannen, verslagen van bouwcomités, …

Categorie HIS: Historisch archief:
Opnameboeken, brieven, … die dateren van tientallen jaren terug. Het betreft 'historische' stukken.

Categorie IWG: Inwendige geneeskunde:
Alle medische dossiers van de internist die jarenlang in onze instelling actief was.

Categorie MDK: Middenkader:
Tevredenheidsonderzoeken, verslagen afdelingshoofdenvergaderingen, …

Categorie MES: Medisch Secretariaat:
Dossiers overleden patiënten, opname- en ontslagbrieven, aanvragen medische beeldvorming, …

Categorie MPG: Minimale Psychiatrische Gegevens:
De minimale psychiatrische gegevens van ziekenhuis en PVT.
Deze dienst behoort toe aan de patiëntenadministratie.

Categorie NEU: Neurologie:
Alle medische dossiers van de neuroloog die jarenlang in onze instelling actief was.

Categorie PED: Personeelsdienst:
Verlofbriefjes, uurroosters, bedrijfsvoorheffing, sociale verkiezingen, …
Deze categorie vinden we ook terug bij het onderdeel 'hangmappen'.

Categorie PTF: Patiëntenadministratie:
Administratieve dossiers overleden patiënten, facturatie ziekenhuis, facturatie PVT, …
Hier is enige overlapping met categorie FAC.

Categorie SOD: Sociale dienst:
Sociale dossiers overleden patiënten, patiëntengelden, rekeninguittreksels, …
Deze categorie vinden we ook terug bij het onderdeel 'hangmappen'.

Alle documenten worden bewaard volgens de officieel geldende afspraken.

3. Hangmappen

Dit onderdeel is opgesplitst volgens de verschillende afdelingen/diensten. Elke categorie beschikt over één of meerdere hangrekken, telkens aangeduid met een rekletter. We gebruiken hiervoor Jalema: archivering volgens geboortemaand en geboortedag. Al deze gegevens registreren we in de Archiefdatabase.

hangmap overzicht categorie		
categorie	**omschrijving**	**rekletter**
DOP	Dossiers Patiënten	B
ARG	Arbeidsgeneeskunde	T
PED	Personeel	T
SOD	Sociale Dienst	A

Archiefdatabase/Hangmappen/Hangmappen opzoeken en uitlenen/
Opzoeken/Overzicht categorieën hangmappen

Categorie DOP: Dossiers patiënten:
Medische dossiers van ontslagen patiënten en bewoners.
Sinds een paar jaren bevindt zich in het archief bovenop dit rek nog een apart rek met alle administratieve dossiers van ontslagen patiënten. De archivering van deze administratieve dossiers is gestart in 2004.

Categorie ARG: Arbeidsgeneeskunde:
Arbeidsgeneeskundige dossiers van ex-werknemers (gebeurt nu digitaal).

Categorie PED: Personeelsdienst:
Personeelsdossiers van ex-werknemers.
Deze categorie vinden we ook terug bij het onderdeel ‘documenten’.

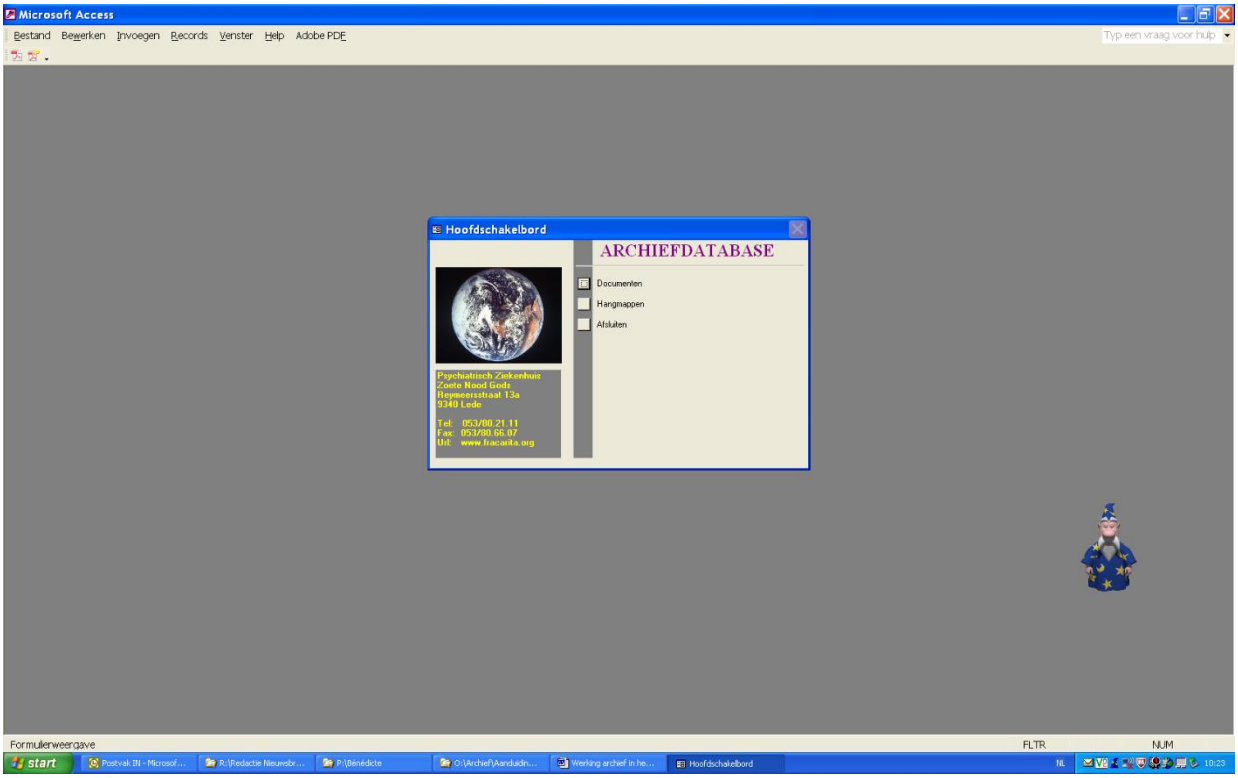
Categorie SOD: Sociale dienst:
Sociale dossiers van ontslagen patiënten en bewoners.
Deze categorie vinden we ook terug bij het onderdeel ‘documenten’.

Alle hangmappen worden bewaard volgens de officieel geldende afspraken.

4. Archiefdatabase

Samen met de opstart van het archief is een database op maat ontwikkeld. Ook hier maken we de opsplitsing in ‘documenten’ en ‘hangmappen’.

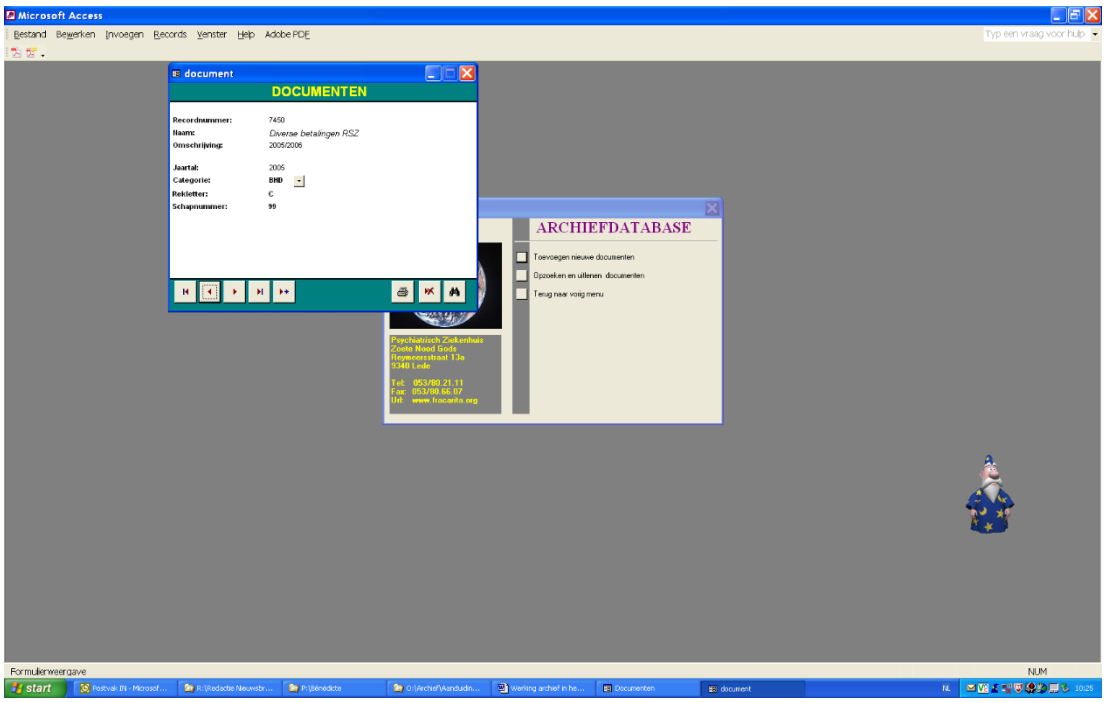
4.1. Documenten



Elk document krijgt bij archivering automatisch een recordnummer toegewezen.
De andere velden zijn

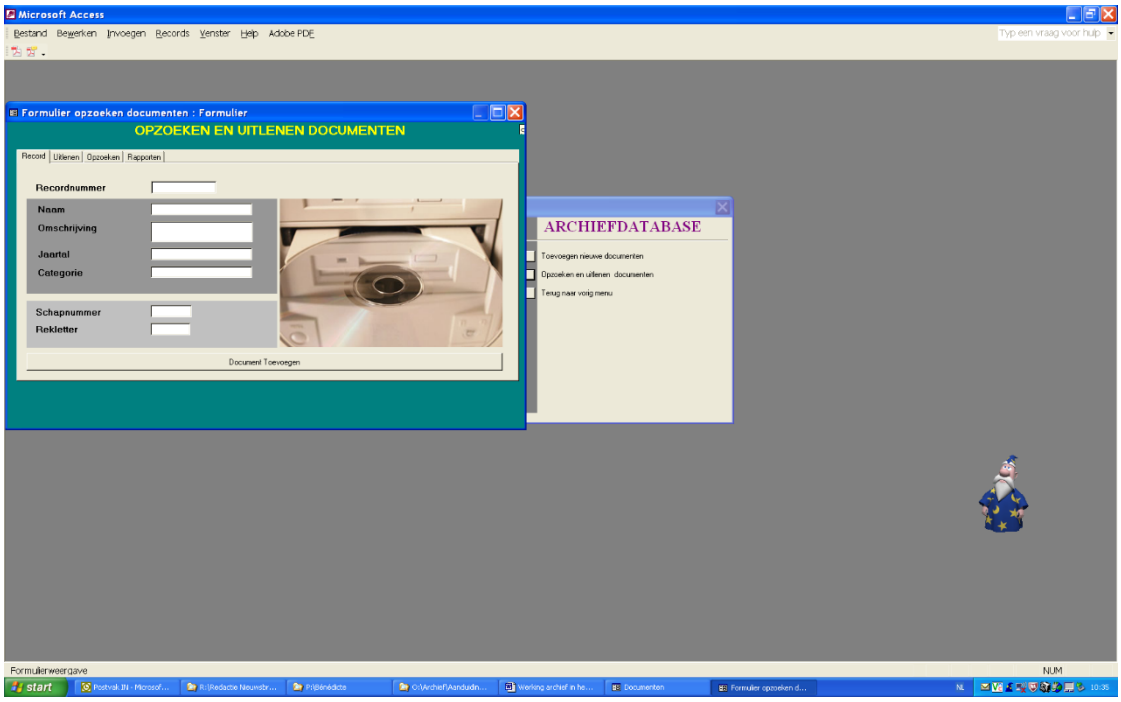
a) Naam
b) Omschrijving
c) Jaartal
d) Categorie
e) Rekletter
f) Schapnummer

De archivaris geeft deze informatie in.

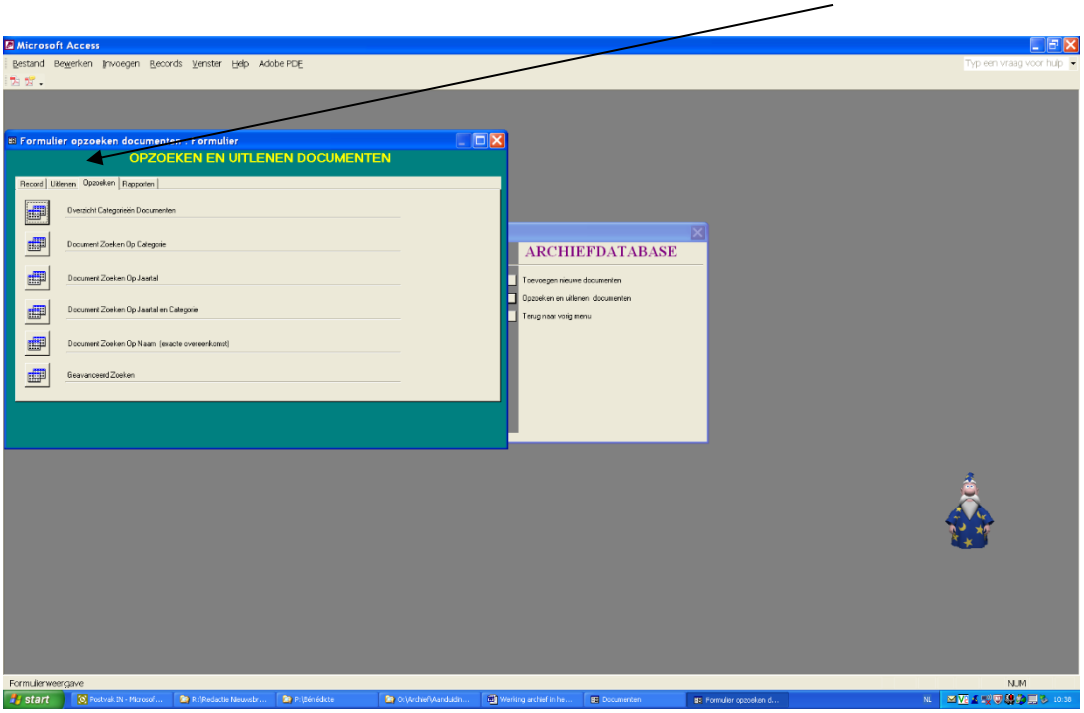


Het spreekt voor zich dat hoe nauwkeuriger deze data ingegeven worden, hoe gemakkelijker het voor de archivaris of betrokken medewerker wordt om het gezochte document terug te vinden. Bij aanlevering van stukken die klaar zijn voor archivering worden deze data duidelijk op de archiefdoos of map vermeld. Het is niet de taak van de archivaris zelf om uit te zoeken over welke documenten het precies gaat. De betrokken afdelingen of diensten hebben er alle belang bij hun te archiveren stukken duidelijk te benoemen. Na het ingeven in de database wordt een etiket met de gegevens, zoals aangeduid in bovenvermeld voorbeeld, afgedrukt en op een duidelijk zichtbare plaats op de map of archiefdoos aangebracht.

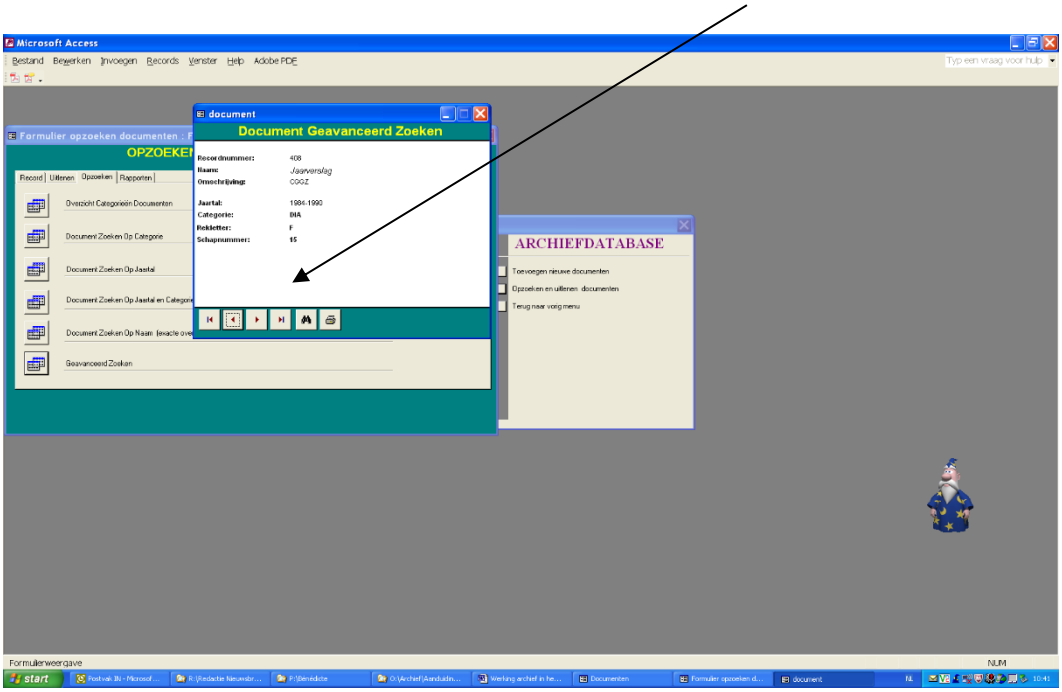
Gearchiveerde documenten zijn terug te vinden, via ‘opzoeken en uitlenen documenten’.



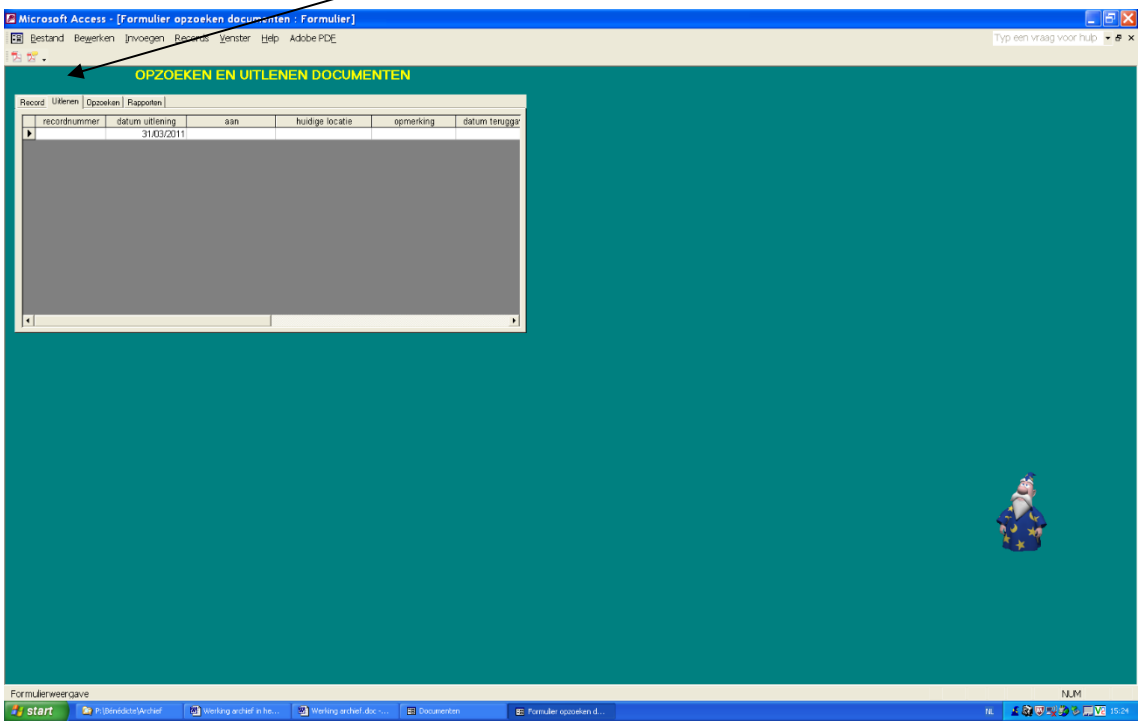
Er zijn meerdere mogelijkheden om een document terug te vinden. Indien je het recordnummer weet, kan je meteen via het hiervoor afgebeelde scherm de nodige gegevens terugvinden. In de meeste gevallen echter weet de archivaris enkel de naam van de betrokken dienst, de omschrijving van het gezochte stuk en het jaartal. In dat geval kan je het tabblad “opzoeken” gebruiken.



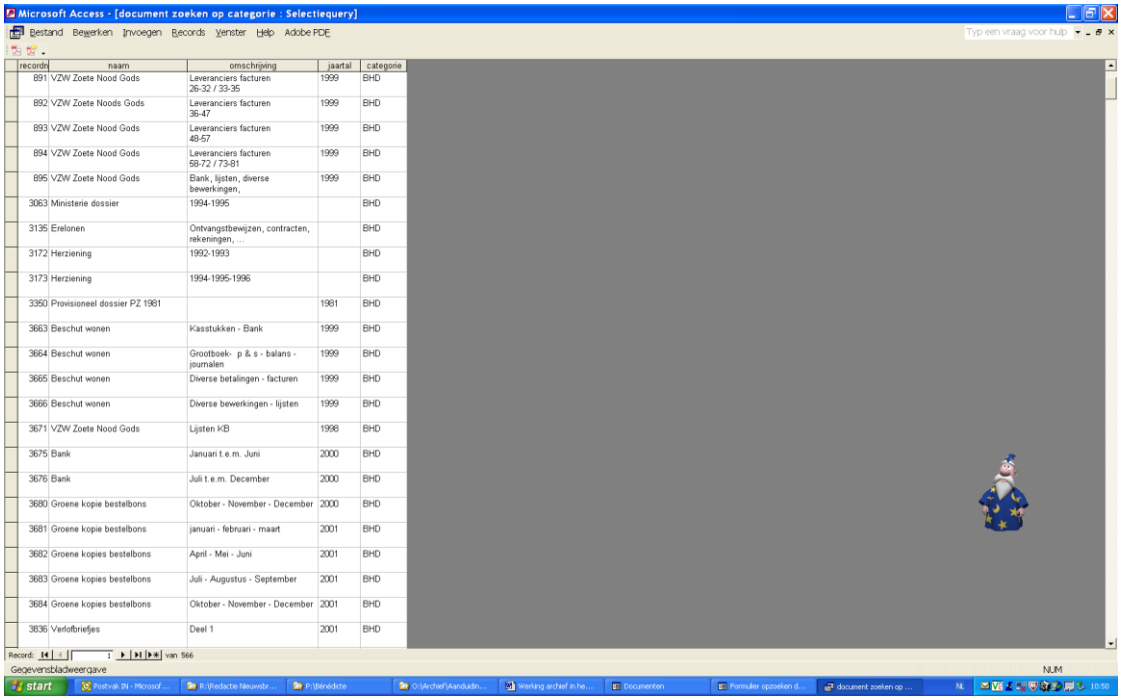
Opzoeken kan via de categorie (= betrokken dienst), het jaartal of de naam. Bij het opzoeken via de naam kan je ofwel zoeken via ‘document zoeken op naam (exacte overeenkomst)’ of ‘geavanceerd zoeken’. Het nadeel bij ‘document zoeken op naam’ is dat je de exacte naam moet weten, wat vaak niet het geval is. Bij het ingeven van woorden die tot de naam behoren, geeft de database geen resultaten weer. Bij ‘geavanceerd zoeken’ kan je via de velden ‘naam’ en ‘omschrijving’ de lokatie van het gezochte document terugvinden. Het volstaat om met de cursor in één van deze twee velden te gaan staan en via de knop een gedeelte van de naam of de volledige naam in te geven.



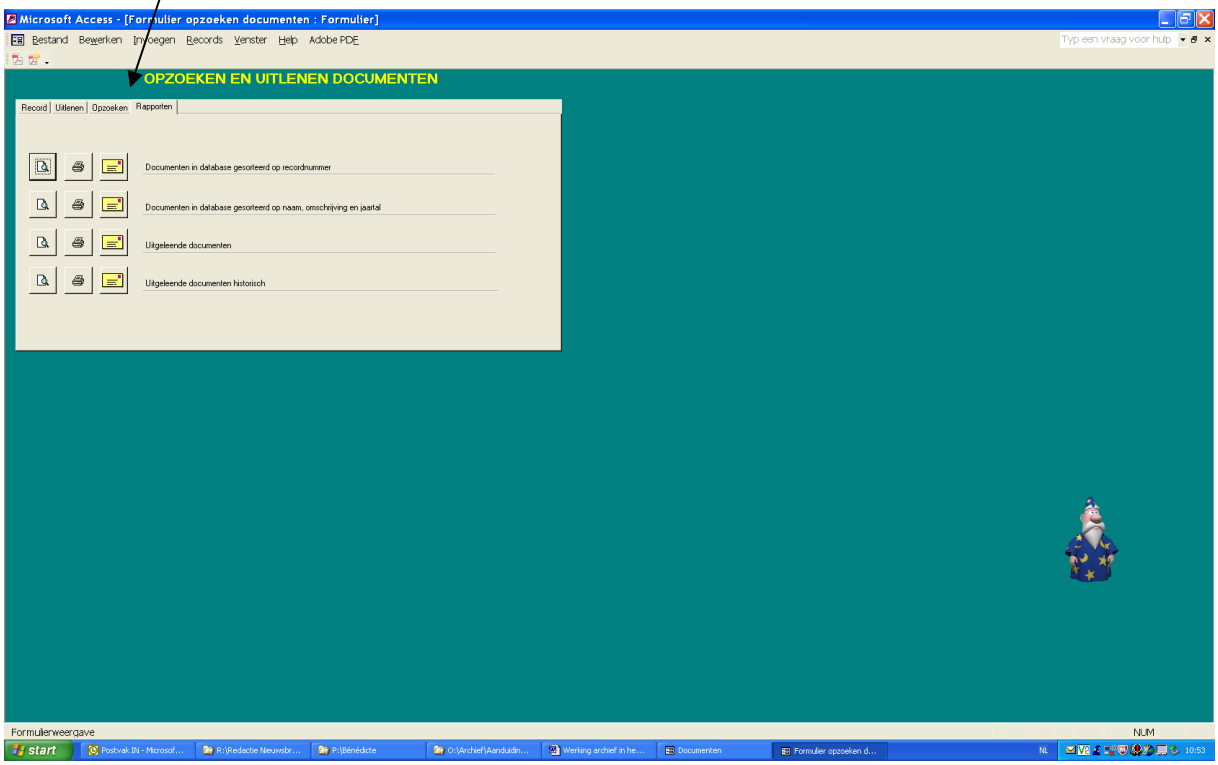
Bij het uitlenen van een document , noteert de verantwoordelijke wanneer en aan wie dit document is uitgeleend. Deze data kunnen bij het tweede tabblad ‘uitlenen’ ingevoerd worden. De archivaris heeft er alle belang bij dit zo nauwkeurig mogelijk bij te houden.



Bij de jaarlijkse opruiming van het archief wordt gebruik gemaakt van ‘document zoeken op categorie’. Bij ingave van de categorie krijg je meteen een overzicht van alle gearchiveerde stukken van de betrokken dienst. Dit overzicht wordt vervolgens afgedrukt, de documenten/mappen die mogen verwijderd worden, worden aangeduid met fluo en overhandigd aan de betrokken dienst voor een laatste controle zodat geen onnodige stukken worden verwijderd. Bij verwijdering uit het archief wordt ook het recordnummer uit de archiefdatabase gehaald.



Het tabblad ‘rapporten’ maakt het mogelijk om allerlei overzichten, zoals bijvoorbeeld een overzicht van alle uitgeleende documenten, te maken.



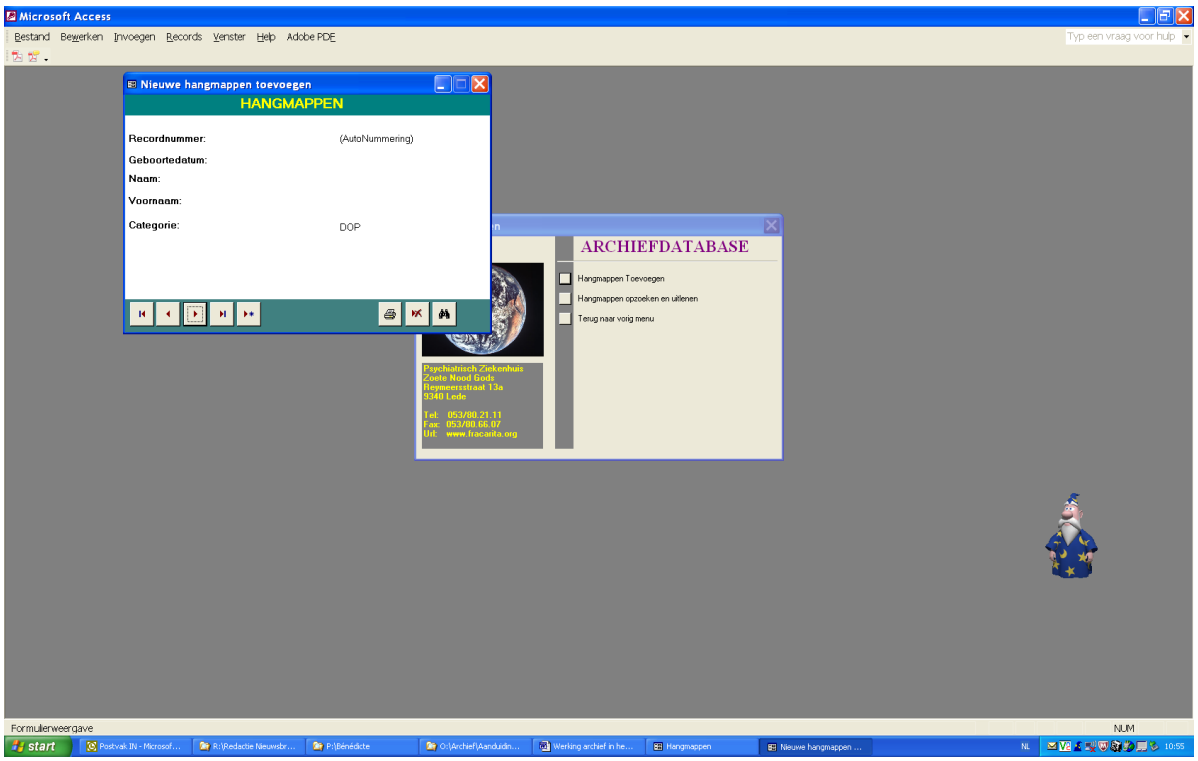
4.2. Hangmappen

Elke hangmap krijgt bij archivering automatisch een recordnummer toegewezen. De andere velden zijn

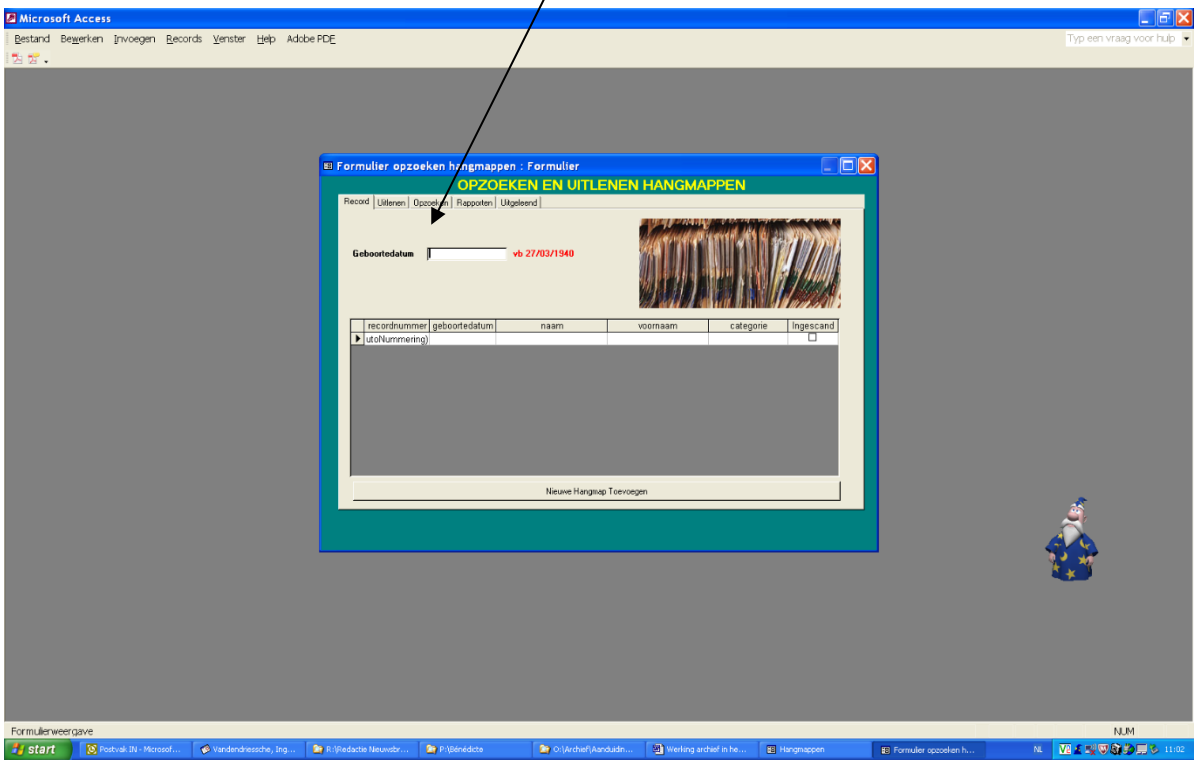
a) Geboortedatum
b) Naam
c) Voornaam
d) Categorie

Het is de archivaris die deze informatie ingeeft.

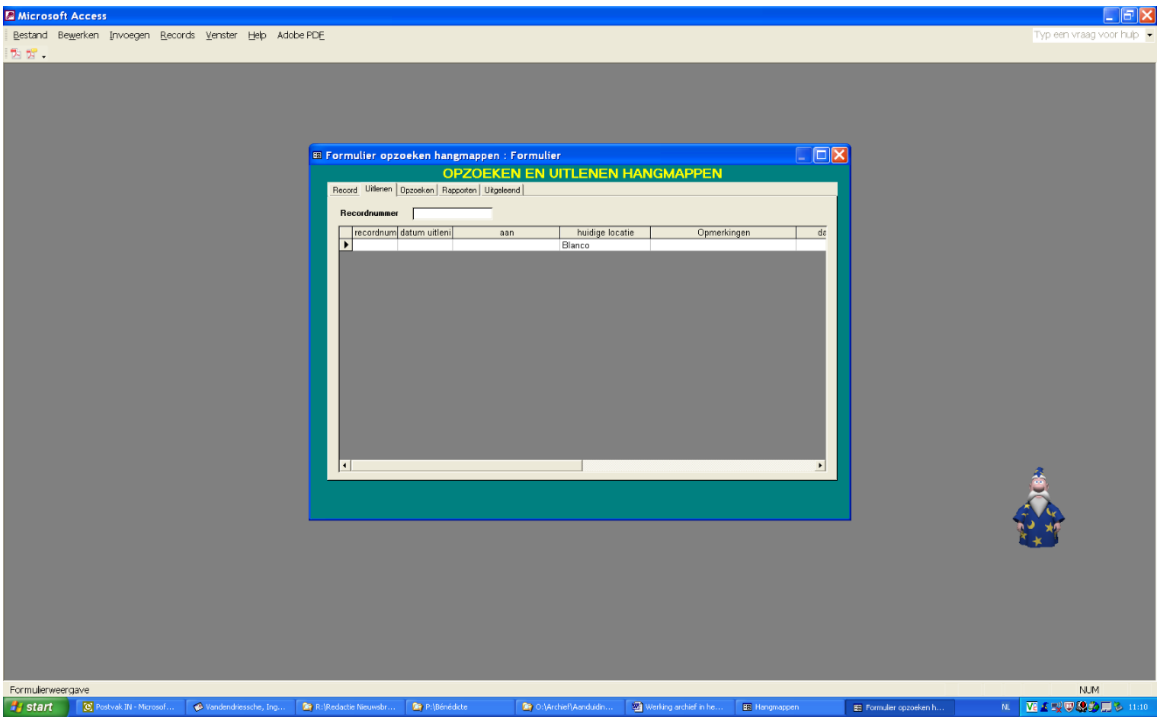
Bij opname van een patiënt of bewoner worden het medische en sociale dossier gemaakt op het medisch secretariaat. Enkel het medische en sociale dossier worden in de archiefdatabase genummerd. Het psychologische dossier, dat een onderdeel is van het medische dossier, en het administratieve dossier worden niet apart gearchiveerd. Het aanmaken van een dossier houdt in dat de data, zoals hieronder aangegeven, ingegeven worden en vervolgens afgedrukt worden op een etiket dat aangebracht wordt op de bruine hangmap. De mappen gaan vervolgens naar de betrokken diensten. Bij ontslag van de patiënt of bewoner gaat het dossier naar het archief.



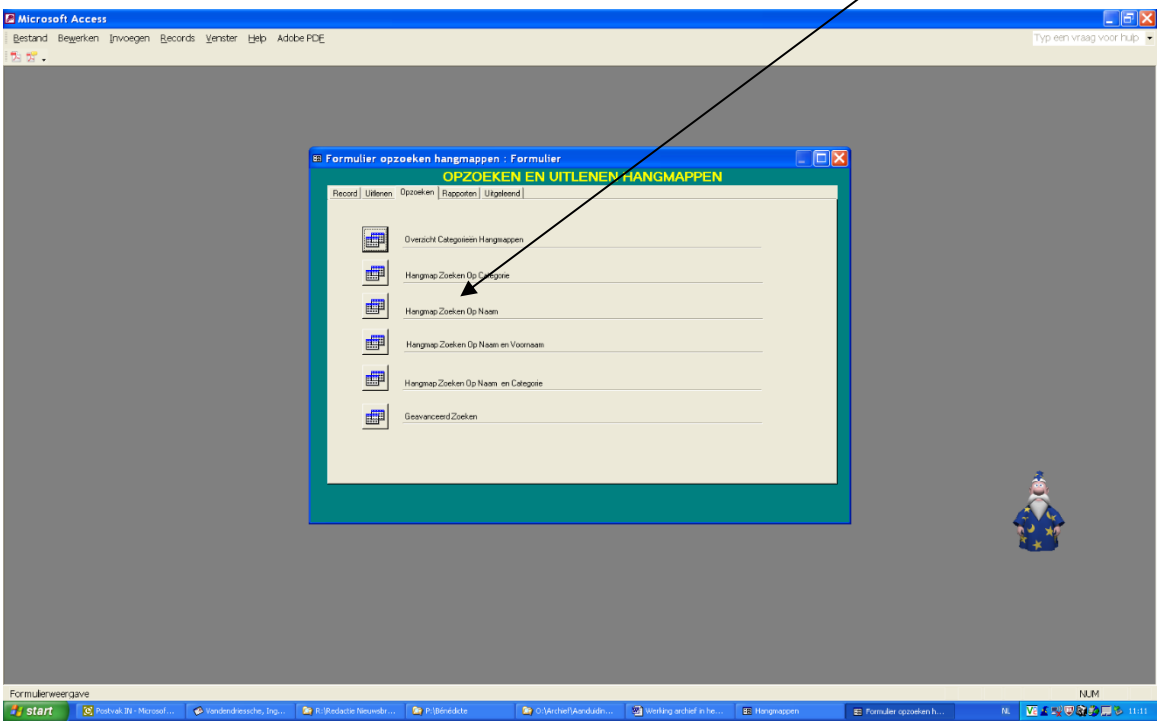
Bij bijvoorbeeld een heropname van een patiënt of bewoner zijn er meerdere mogelijkheden om een medisch of sociaal dossier te lokaliseren. Indien je de geboortedatum weet, kan je meteen nagaan of het dossier al dan niet gearchiveerd is.



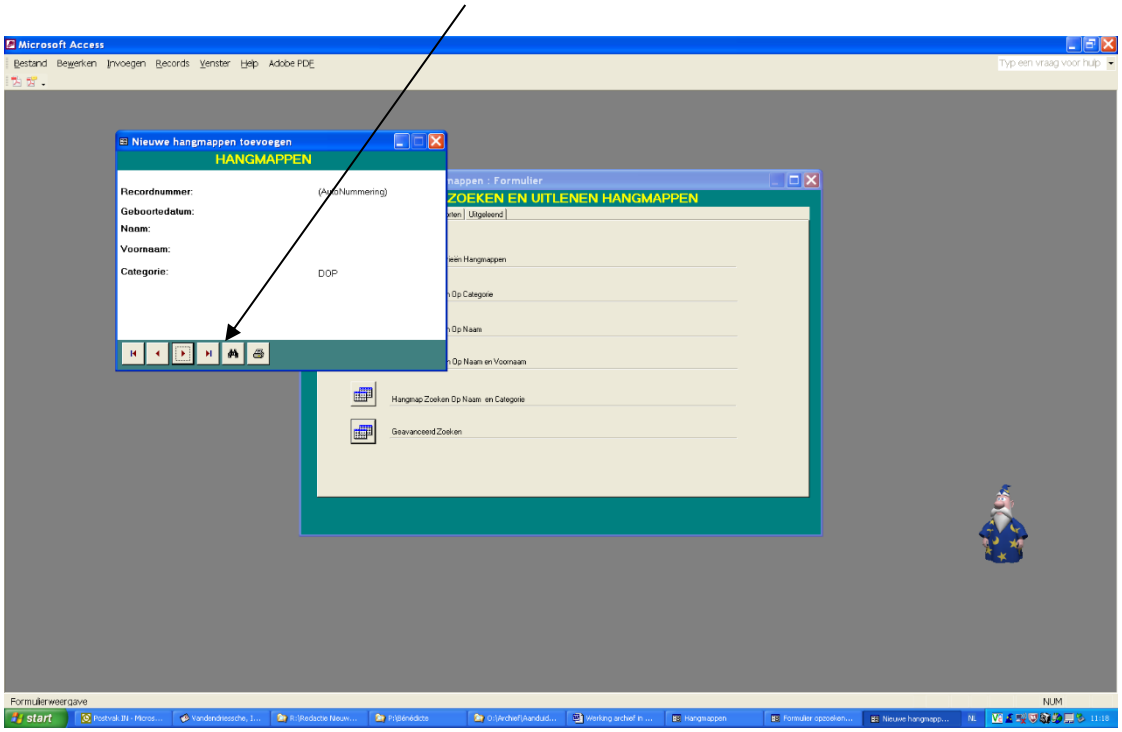
De aanwezigheid van een dossier in het archief kan je nagaan via het tweede tabblad ‘uitlenen’. Daartoe geef je het recordnummer in.



Indien de geboortedatum niet gekend is, wordt het dossier het meest frequent gezocht via ‘hangmap zoeken op naam’ bij het derde tabblad ‘opzoeken’.

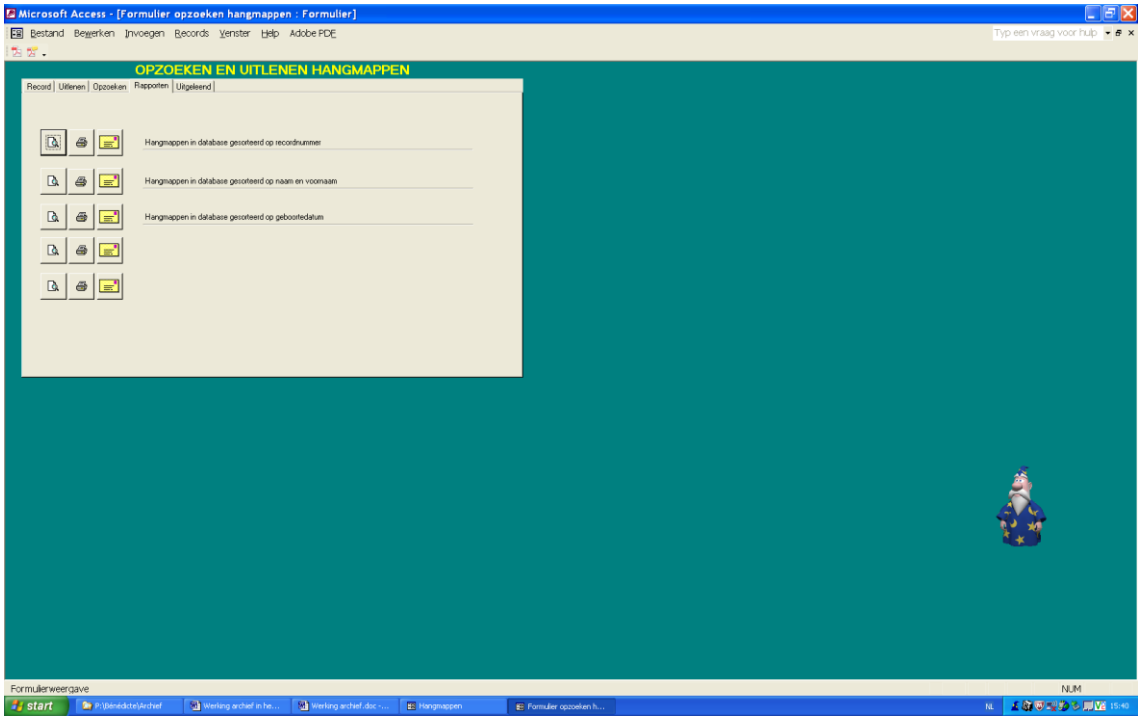


De parameter hier is de familienaam van de patiënt of de bewoner. Belangrijk hierbij is dat je de juiste schrijfwijze van de naam kent. Bij twijfel, moet je de verschillende mogelijke schrijfwijzen apart ingeven. Je krijgt dan een overzicht van alle dossiers – sociale en medische dossiers, maar ook personeelsdossiers en dossiers van de arbeidsarts – met deze familienaam.
Een andere mogelijkheid is het zoeken van een dossier via 'geavanceerd zoeken'. Je zet de cursor in het veld 'naam' en klikt vervolgens op de knop 'zoeken'.

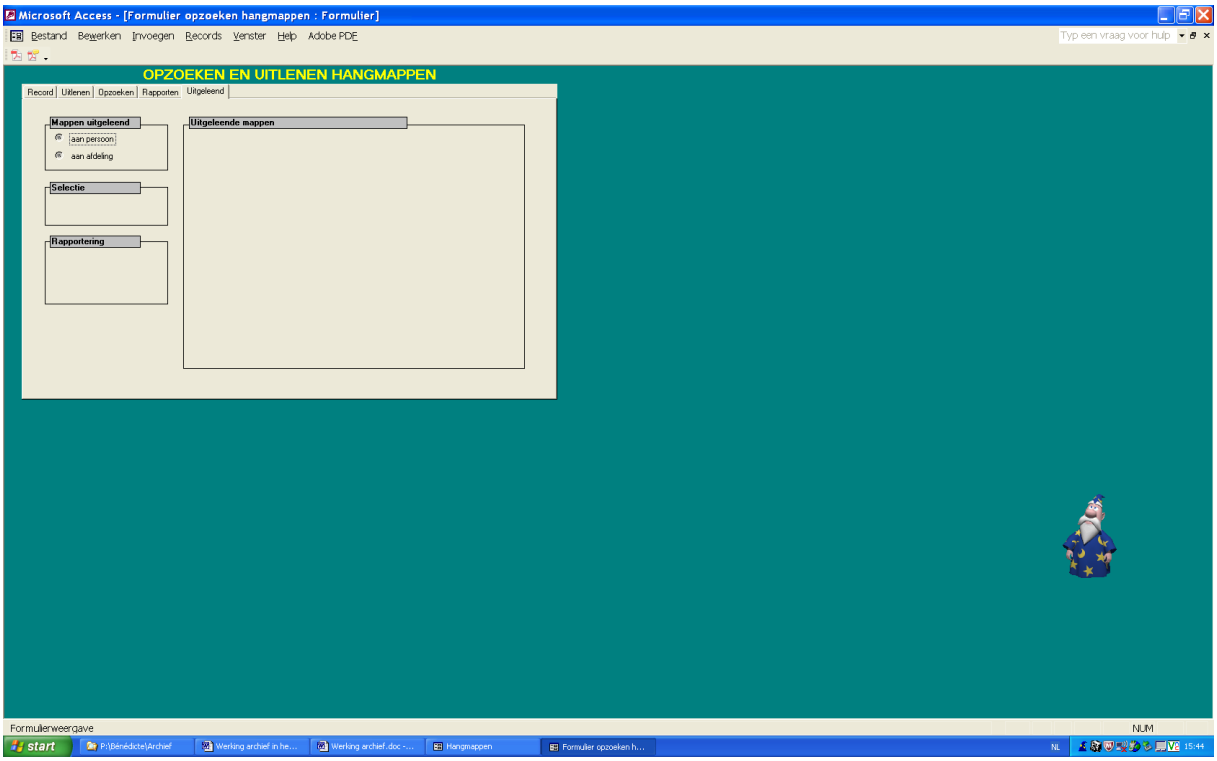


Hier heb je de mogelijkheid om een gedeelte van de naam in te geven waardoor alle records met dit gedeelte meteen op het scherm verschijnen. Dit is vooral interessant wanneer je niet de precieze schrijfwijze kent.

Het tabblad 'rapporten' maakt het mogelijk om allerlei overzichten te maken. Deze mogelijkheid wordt echter weinig gebruikt.



Het laatste tabblad ‘uitgeleend’ biedt de mogelijkheid om een rapport te maken van alle uitgeleende dossiers per persoon of per afdeling.



Bijlage 2

Informatieveiligheidsbeleid van de organisatie Broeders van Liefde

Provincialaat der Broeders van Liefde vzw

Stropstraat 119 - 9000 Gent

☏ 09 221 45 45

🖷 09 221 98 89

Broeders van Liefde

Informatieveiligheidsbeleid van de organisatie Broeders van Liefde

Classificatie: Intern
Datum: 01/01/2018

Inleiding

In deze nota beschrijven we het beleid dat de vzw Provincialaat der Broeders van Liefde voert op vlak van informatieveiligheid.

In essentie bewaakt informatieveiligheid 3 kwaliteiten van gegevens:

- vertrouwelijkheid: zijn de gegevens enkel beschikbaar voor bevoegde personen?
- betrouwbaarheid: zijn de gegevens correct en up-to-date en zijn ze enkel door bevoegde personen gemaakt of aangepast?
- beschikbaarheid: kunnen we de gegevens gebruiken op het moment dat we ze nodig hebben?

De informatie die we beheren kunnen we naar inhoud 2 soorten onderscheiden:

- persoonsgegevens
- bedrijfsgegevens

Een gegeven is een persoonsgegeven als het over een identificeerbare, natuurlijke persoon gaat. Deze persoon wordt **betrokkene** genoemd. In dit document onderscheiden we 2 grote groepen:

- De cliënten: de personen aan wie wij diensten (zorg, onderwijs, een leefomgeving, arbeidskansen, …) verlenen. Naar gelang de sector waarin een entiteit werkt kan dat bijvoorbeeld zijn: een patiënt, een leerling, een bewoner, een doelgroepmedewerker, … Soms kan de cliënt niet zelf zijn rechten beheren (bijvoorbeeld een kind of iemand die onbekwaam is). Dan treedt een vertegenwoordiger op in zijn plaats. In bepaalde gevallen betreft een persoonsgegeven niet de cliënt zelf, maar iemand uit zijn omgeving (familie, een bezoeker, een voogd,…).
- De medewerkers: de personen die deze diensten (zullen) leveren. Vaak zijn dat loontrekkenden, maar ook stagiairs, sollicitanten, externen, vrijwilligers en zelfstandige dienstverleners horen in deze groep.

Wat geen persoonsgegeven is, is per definitie een bedrijfsgegeven.

Informatieveiligheid streven we na zowel voor gegevens op papier als voor elektronische gegevens, bijvoorbeeld ook foto's, camerabeelden en geluidsopnames.

We geven in deze beleidsnota dus aan welke doelen we onszelf stellen op vlak van informatieveiligheid en welke instrumenten we daarvoor voorzien.

Naast gegevens die in elke organisatie beschermd moeten worden (bedrijfsdocumenten, personeelsgegevens,…), verzamelen en verwerken we ook (bijzonder) gevoelige persoonsgegevens van cliënten[1]. Dit soort gegevens is onderworpen aan een zeer strikte regelgeving van de overheden (vooral Europa). Veel van onze cliënten hebben een aandoening of een beperking en worden daarom soms het doelwit van stigmatisering en discriminatie. Dit motiveert ons extra om hun rechten te beschermen.

Als beleidsinstrument geeft deze nota geen concrete maatregelen die voorzien zijn voor een bepaalde periode. Dergelijke maatregelen beschrijven we in een apart document - het actieplan - dat we zien als een vertaling naar concrete stappen van deze beleidsnota. Elke sector heeft zijn eigen jaarlijkse actieplan.

Visie

A. Kwaliteit

De organisatie Broeders Van Liefde wil kwalitatieve diensten leveren in de verschillende sectoren en ons informatieveiligheidsbeleid maakt integraal deel uit van deze focus op kwaliteit. Dit wil enerzijds zeggen dat de kwaliteit van de dienstverlening in het gedrang komt als de informatieveiligheid onvoldoende gegarandeerd is en anderzijds dat informatieveiligheid geen doel op zich is maar altijd deel uitmaakt van onze focus op de kwaliteit van de werking.

B. Regelgeving en ethiek

Het registreren en beheren van persoonsgegevens is strikt gereglementeerd door overheden (vooral de Europese en de Belgische, in mindere mate de Vlaamse)[2]. Wij volgen de bepalingen van de overheden stipt op en engageren ons om bij wijziging van de regelgeving op tijd de nodige aanpassingen door te voeren in de organisatie.

Bovenop deze wettelijke vereisten vinden wij het ook vanuit ethisch standpunt onze opdracht om de persoonlijke levenssfeer van de cliënten en de medewerkers te respecteren. We streven daarin zorgvuldigheid na en overleg met de betrokkenen. We hechten ook groot belang aan het respecteren van het beroepsgeheim en de discretie.

C. Een lerende organisatie

We zijn er ons van bewust dat informatieveiligheid net als veiligheid op andere terreinen niet voor 100% haalbaar is. Daaruit leiden we af dat verbeteringen altijd mogelijk zijn en dat we dus blijvend kunnen bijleren. We beschouwen onszelf daarom als een lerende organisatie die bij incidenten de mogelijke oorzaken analyseert en preventiemaatregelen uitwerkt en niet in de eerste plaats een 'dader' zoekt. Een lerende organisatie zijn betekent

[1] De begrippen 'gevoelige persoonsgegevens' en ' bijzonder gevoelige persoonsgegevens' worden verder in dit document gedefinieerd, namelijk in hoofdstuk 3 'Doelstellingen' paragraaf A 'Gegevensbeveiliging'

[2] De belangrijkste algemene wettelijke bepalingen zijn:

- de Europese directieve "General Data Proctection Regulation" (hierna GDPR genoemd) - gepubliceerd in mei 2016 - en waaraan we uiterlijk in mei 2018 volledig moeten conformeren. Merk op dat GDPR enkel de rechten van levende personen beschermt. De persoonsgegevens van overledenen worden in bepaalde gevallen wel nog door een Belgische wet beschermd.
- de wet van 8 december 1992 voor het beveiligen van de privacy met betrekking tot het verwerken van persoonlijke informatie en het KB van 13 feb 2001 voor het uitvoeren van deze Wet (hierna Privacywet).
-

ook medewerkers sensibiliseren voor risico's en zorgvuldig gedrag promoten. We willen dus ook op vlak van informatieveiligheid een leer- en verbetercultuur bevorderen.

D. Realisme

Ons informatieveiligheidsbeleid gaat voor een realistische aanpak. Daar zijn 2 aspecten aan. Ten eerste: zonder inzet van middelen (personeel en geld) kunnen we geen beleid voeren dat informatiesystemen passend beveiligt. Ten tweede kunnen maatregelen op vlak van informatieveiligheid soms financiële kosten impliceren of een impact hebben op de tijd die medewerkers aan hun kernopdracht kunnen besteden. De middelen zijn niet onbeperkt en een afweging van de kosten in geld en tijd is nodig.

We gaan dus voor een zo hoog mogelijk beschikbaarheid, betrouwbaarheid en vertrouwelijkheid van **cliënt- , personeels- en bedrijfsgegevens** en voor een efficiënt gebruik van de beschikbare middelen.

Doelstellingen

In deze paragraaf zullen we onze visie uitwerken in doelstellingen die we nastreven. We groeperen deze doelstellingen in de volgende 8 actiedomeinen:

1. Gegevensbeveiliging
2. Toegangenbeheer
3. Risicobeheer
4. Incidentenbeheer
5. Bewustmaking van de medewerkers
6. Beveiliging van infrastructuur en netwerk
7. Fysieke beveiliging
8. Beheer van afspraken met externe partijen

In de bepaalde gevallen worden deze doelstellingen concreter gemaakt in aparte beleidsnota's of procedures.

Hier volgt een beschrijving per actiedomein van de doelen.

A. Gegevensbeveiliging

i. Gegevens classificeren we in 2 soorten: **persoonsgegevens** en **bedrijfsgegevens**.

De persoonsgegevens zijn opgedeeld in 3 subcategorieën:

- Gewone Persoonsgegevens
- Gevoelige Persoonsgegevens en
- Bijzonder Gevoelige Persoonsgegevens.

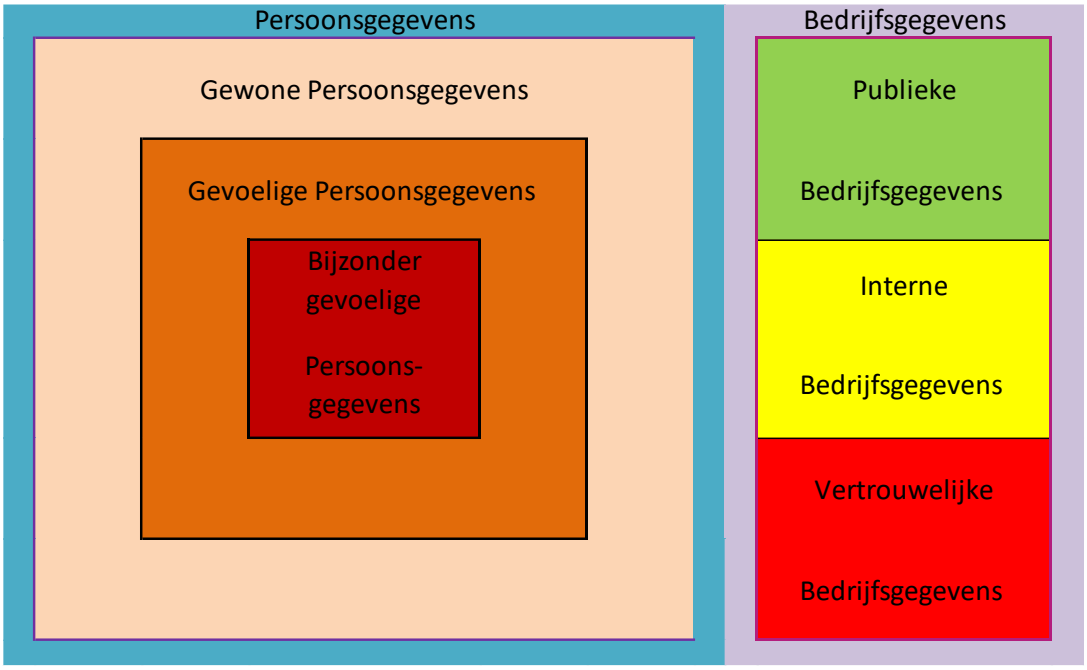
Een persoonsgegeven dat nog niet expliciet geclassificeerd is, krijgt voorlopig het label 'gevoelig persoonsgegeven'.

Bedrijfsgegevens zijn ook opgedeeld in 3 subcategorieën:

- Publieke bedrijfsgegevens,
- Interne bedrijfsgegevens en
- Vertrouwelijke bedrijfsgegevens.

Een bedrijfsgegeven dat nog niet expliciet geclassificeerd is, krijgt voorlopig het label 'intern bedrijfsgegeven'.

Deze onderverdelingen gelden zowel voor gestructureerde gegevens (gegevens opgeslagen in databanken en toegankelijk via applicaties) als voor ongestructureerde gegevens (gegevens in aparte bestanden op schijven, toegankelijk via bureauticatoepassingen zoals tekstverwerkers, rekenbladen, mails,…) als ook voor gegevens op papier.



a. Alles wat geen persoonsgegeven is, is een bedrijfsgegeven.
b. Iedereen mag publieke bedrijfsgegevens lezen. Ze mogen verspreid worden, ook buiten de organisatie.
c. Medewerkers mogen interne bedrijfsgegevens lezen, maar ze niet verspreiden buiten de organisatie. Bedrijfsgegevens die (nog) niet geclassificeerd is, beschouwen we als intern.
d. Vertrouwelijke bedrijfsgegevens mogen enkel beschikbaar zijn voor bij functie of bij naam genoemde personen of groepen van personen.

ii. Gewone persoonsgegevens zijn persoonsgegevens die ook buiten de organisatie bekend zijn of gemakkelijk op te zoeken zijn, bijvoorbeeld het postadres, het mailadres, het telefoonnummer. Ook elk persoonsgegeven dat de betrokkene zelf publiek heeft gemaakt valt hieronder.

iii. Gevoelige persoonsgegevens zijn persoonsgegevens die noch bijzonder gevoelige persoonsgegevens (zie volgend punt), noch gewone persoonsgegevens zijn. Het gaat vooral over informatie die een voorzichtige persoon niet over zichzelf publiek zou maken, bijvoorbeeld een bankrekeningnummer of de verrichtingen daarop, schoolresultaten, loon of barema, samenstelling van het gezin, enzovoort.

iv. GDPR - de Europese regelgeving op vlak van privacy - somt in Art.9 en 10 negen soorten bijzonder gevoelige persoonsgegevens op namelijk:
   a. ras/etnische afkomst,
   b. politieke opvattingen,
   c. syndicaal lidmaatschap,
   d. biometrische gegevens,
   e. genetische gegevens,
   f. medische gegevens,
   g. gegevens over iemands seksueel gedrag of gerichtheid,
   h. religieuze of levensbeschouwelijke overtuiging
   i. strafrechtelijke veroordelingen/strafbare feiten.

   De eerste 5 slaan we niet op. De laatste 4 wel als ze noodzakelijk zijn voor de dienst aan de cliënt of als het bijhouden door een overheid is opgelegd. Deze bijzonder gevoelige persoonsgegevens zijn enkel beschikbaar voor personen die persoonlijk een zorg-, onderwijs- of hulpverlenersrelatie hebben met de betrokkene.

v. Alle persoonsgegevens over een betrokkene (cliënt, personeelslid) zullen we op zijn vraag aan hem binnen de maand leveren[3], naargelang zijn keuze elektronisch of op papier. De betrokkene hoeft deze vraag niet te motiveren. De betrokkene tekent voor ontvangst.

vi. Persoonsgegevens zullen we op vraag van de betrokkene corrigeren. De vraag van de betrokkene om medische gegevens te corrigeren wordt genoteerd in het dossier. Punctuele fouten worden gecorrigeerd, medische opinies meestal niet, omdat het moeilijk te bewijzen is dat een medische opinie niet correct is.

vii. Persoonsgegevens zullen we op vraag van de betrokkene wissen in de gevallen waarin de regelgeving dat voorziet.

viii. Persoonsgegevens kunnen we op ons initiatief wissen in de gevallen waarin de regelgeving dat toelaat. In de regel doen we dit wanneer het bijhouden van deze gegevens niet meer nodig is om het doel van de verwerking te bereiken. Papieren documenten met vertrouwelijke persoonsgegevens worden onder toezicht van de databeheerder versnipperd hetzij in de voorziening zelf hetzij door een leverancier die een attest aflevert.

ix. De verwerking van persoonsgegevens zullen we op vraag van de betrokkene beperken in de gevallen waarin de regelgeving dat voorziet.

x. Een bestand mag in principe alleen gegevens bevatten van dezelfde classificatie, namelijk persoonsgegevens of bedrijfsgegevens. Een bestand dat hoofdzakelijk bedrijfsgegevens bevat en slechts enkele gewone persoonsgegevens (bv het mailadres van een medewerker van een leverancier) mag wel nog als een bestand van bedrijfsgegevens beschouwd worden.

Als een bestand met persoonsgegevens gegevens bevat van meer dan 1 subcategorie dan zullen we dit bestand classificeren op het striktere niveau. Dus:

- een bestand met gewone en gevoelige persoonsgegevens valt in de subcategorie gevoelige persoonsgegevens en
- een bestand met gevoelige en bijzonder gevoelige persoonsgegevens valt in de subcategorie bijzonder gevoelige persoonsgegevens.

Als een bestand bedrijfsgegevens bevat van meer dan 1 subcategorie dan zullen we dit bestand ook classificeren op het hogere niveau. Dus:

- een bestand met publieke en interne bedrijfsgegevens valt in de subcategorie interne bedrijfsgegevens en
- een bestand met interne en vertrouwelijke bedrijfsgegevens valt in de subcategorie vertrouwelijke bedrijfsgegevens

xi. GDPR bepaalt dat we alle “verwerkingsactiviteiten” op persoonsgegevens moeten beschrijven in een ’ verwerkingsregister’. Daarin staat welk doel de verwerking dient en welke rechtsgrond de verwerking rechtvaardigt.

xii. Wij volgen de lijst van rechtsgronden die in GDPR opgesomd zijn. Degene die we het meest gebruiken zijn:

a. We hebben die gegevens nodig voor het verlenen van **medische zorgen**
b. We hebben die gegevens nodig voor de uitvoering van een **overeenkomst** met de betrokkene. Bijvoorbeeld: facturatie van de geleverde diensten.
c. Er is een **wettelijke verplichting** om die gegevens bij te houden. Zo is bijvoorbeeld een school verplicht om bij te houden wie welk diploma heeft gehaald of is een ziekenhuis verplicht om een geval van tbc te melden aan de bevoegde instanties.

[3] De Wet op de patiëntenrechten voorziet voor de sector GGZ een uitzondering voor wilsonbekwame personen. Het is ook niet verplicht om de patiënt inzage te geven als hem dat ernstig nadeel zou berokkenen.

d. We hebben de **toestemming** van de cliënt. Dergelijke toestemming moet een cliënt vrij kunnen geven, wat onder meer willen zeggen dat de verlening van zorg of onderwijs of een andere dienst niet als voorwaarde mag hebben dat de cliënt zijn toestemming heeft gegeven voor een bepaalde gegevensverwerking. Een cliënt kan de gegeven toestemming op elk moment intrekken. Voor bijzonder gevoelige persoonsgegevens moet de toestemming bovendien **schriftelijk** zijn.

xiii. In de sector GGZ worden medische gegevens opgeslagen in het elektronisch patiëntendossier (EPD) en gedeeld in het behandelteam. We brengen de patiënt hiervan op de hoogte. Alle lees- en schrijfacties op het elektronisch patiëntendossier worden gelogd.

xiv. Alle persoonsgegevens worden beheerd (verzameld, opgeslagen, verwerkt, ter beschikking gesteld, vernietigd) in strikte naleving van de wetten en reglementeringen van de verschillende bevoegde overheden.

xv. De dienst informatica zorgt voor een back-up van alle gegevens op servers. Zij zorgen ook voor het geregeld testen van het restoren.

xvi. Gegevens die nuttig zijn voor de bedrijfsvoering mogen enkel op netwerkschijven opgeslagen worden. Lokale of verwisselbare schijven worden immers niet geback-upt.

xvii. Gegevens op verwisselbare media (mobiele schijven, cd's, usb's, tapes) die uit onze gebouwen kunnen meegenomen worden moeten versleuteld worden als ze (bijzonder) gevoelige persoonsgegevens bevatten of vertrouwelijke bedrijfsgegevens.

xviii. Opslagmedia (harde schijven, tapes, usb-sticks,…) waarop gegevens staan of hebben gestaan mogen de organisatie niet verlaten zonder dat de gegevens onherstelbaar zijn gewist.

xix. Voor alle gegevens is iemand aangesteld die ze beheert, de databeheerder. De persoon die deze rol opneemt, beslist over de classificatie van de gegevens en over wie op basis van zijn functie of rol bepaalde toegangen krijgt.

xx. Voor bijzonder gevoelige persoonsgegevens registreren we de lees- en schrijfacties. Lees- en schrijfacties op andere gegevens worden alleen gelogd als er een noodzaak is.

xxi. Persoonsgegevens geven we niet zonder toestemming van de betrokkene door aan externe partijen behalve in de gevallen voorzien in de wet of in GDPR.

xxii. Persoonsgegevens kunnen geanonimiseerd worden waardoor het niet langer mogelijk is (zelfs niet in combinatie met publieke gegevens) om een verband te leggen tussen het geanonimiseerde gegeven en de oorspronkelijke persoon. Daardoor vallen volledig geanonimiseerde gegevens niet meer onder de privacywetgeving en kunnen we ze ook voor andere doeleinden gebruiken dan de oorspronkelijke gegevens.

xxiii. Persoonsgegevens uit de productie-omgeving worden strikt gescheiden gehouden van gegevens die voor andere doelen dienen (zoals voor het testen van programma's of voor opleiding). Hiermee voorkomen we enerzijds dat we de productie-omgeving besmetten met niet-reële gegevens en anderzijds dat persoonsgegevens gebruikt worden voor verwerkingen waarvoor we geen rechtsgrond hebben.

xxiv. Persoonsgegevens en vertrouwelijke bedrijfsgegevens slaan we in principe op op media die zich in de gebouwen van onze organisatie bevinden. Persoonsgegevens kunnen enkel bij een leverancier opgeslagen en verwerkt worden (bv in de "cloud"), als uit gedetailleerd, voorafgaand onderzoek blijkt dat deze leverancier voldoende garanties

biedt op vlak informatieveiligheid. Ook na het sluiten van het contract evalueren we de informatieveiligheid van de geleverde diensten geregeld.

xxv. Persoonsgegevens en vertrouwelijke bedrijfsgegevens gegevens kunnen versleuteld worden. Daarbij maken we eerst een afweging van enerzijds de impact en de waarschijnlijkheid van sleutelverlies en anderzijds de impact en waarschijnlijkheid van een lek.

xxvi. Gevoelige persoonsgegevens mogen niet onbeveiligd elektronisch (bijvoorbeeld via mail) verstuurd worden buiten de organisatie. Ofwel moeten die gegevens versleuteld zijn ofwel moet de verbinding zo beveiligd zijn dat de gegevens niet kunnen onderschept worden. Vertrouwelijke gegevens mogen binnen de organisatie onversleuteld verstuurd worden bijvoorbeeld via mail als deze gegevens enkel over onze eigen netwerken gaan.

xxvii. We respecteren de wettelijke bewaartermijnen voor persoonsgegevens.

We respecteren de regelgeving betreffende het melden van datalekken aan de betrokkene en/of aan een bevoegde instantie.

B. Toegangenbeheer

i. De gebruiker krijgt toegang tot gegevens of toepassingen in de mate dat hij die gegevens nodig heeft om zijn taken uit te voeren. Hij krijgt dus niet meer toegang dan nodig.
ii. Bij vertrek verliest de gebruiker alle toegangen die verbonden waren met zijn functies in de organisatie.
iii. Bij mutatie verliest de gebruiker de toegangen die verbonden waren met zijn vorige functies of dienst.
iv. De gebruiker krijgt enkel toegang via zijn persoonlijk gebruikersaccount en een moeilijk te raden wachtwoord dat hij zelf kiest en dat hij niet deelt met anderen. De ingelogde gebruiker voorkomt dat een ander kan werken gebruik makend van de sessie van de ingelogde gebruiker. Het wachtwoordenbeleid wordt in een apart document verder gespecifieerd.
v. Sommige medewerkers (vooral IT-ers) hebben een tweede gebruikersaccount met extra rechten om systemen of toepassingen te kunnen beheren. Deze geprivilegieerde accounts mogen enkel daarvoor gebruikt worden en worden gemonitord.
vi. De dienst IT zorgt ervoor dat geprivilegieerde accounts die met de hardware of software meegeleverd werden onbruikbaar zijn gemaakt.
vii. HR meldt mutaties en uitdiensttredingen aan IT en aan de databeheerder zodat deze de toegangen kunnen aanpassen of wegnemen. In deze context van toegangenbeheer onderscheiden we de volgende soorten gegevens:
    a. Interne, gestructureerde gegevens. Dat zijn gegevens in toepassingen en databanken die we zelf beheren. De toegangen tot deze gegevens worden beheerd in de toepassing zelf door de persoon aan wie de directie de rol van databeheerder gaf.
    b. Interne, ongestructureerde gegevens. Dat zijn gegevens die we lezen en bewerken met bureauticatoepassingen zoals tekstverwerkers, rekenbladen en mail. De dienst IT beheert in dit geval de toegangen.
    c. Externe gegevens. Dit zijn gegevens die op de infrastructuur van een extern partij (vaak een overheidsinstantie) staan en die zij aanbieden via een toepassing op het internet. Het beheer deze toegangen behoort tot de rol van de databeheerder die is aangeduid door de directie.

viii. In grote lijnen bevat dit externe toegangenbeheer de volgende rollen en taken:
    a. De gebruiker vraagt een toegang aan op bepaalde gegevens of op een toepassing.
    b. De leidinggevende beoordeelt of de vraag aansluit bij een taak uit het takenpakket van de gebruiker.
    c. De databeheerder verleent de gevraagde toegangen en neemt ze weer weg als de gebruiker van functie verandert of als hij vertrekt.
    d. De databeheerder voert periodiek controles uit.

C. Risicobeheer

Informatiesystemen zijn net als andere bedrijfsmiddelen onderhevig aan risico's.
Deze risico's zijn deels vergelijkbaar met deze in andere, even grote organisaties (bedrijven, overheden). Anderzijds werkt de vzw Provincialaat der Broeders van Liefde ook sterk gedecentraliseerd. Deze kleinere entiteiten hebben niet de middelen om een apart risicobeheer uit te werken. Daarom kiezen we ervoor om de risico's in kaart te brengen naargelang ze aan bod komen bij de andere elementen van informatieveiligheidsbeleid (databeveiliging, toegangen, incidenten, bewustmaking, …) uit dit hoofdstuk en om dus geen apart formeel risicobeheer in te voeren.

Daar is een belangrijke uitzondering op: de gegevensbeschermingeffectbeoordeling (= PIA = Privacy Impact Assessment) zoals beschreven in GDPR[4].

[4] GDPR art 35 en 36

Wanneer we een nieuwe grootschalige verwerking van bijzonder gevoelige gegevens voorzien, zullen we de risico's inschatten en maatregelen uitwerken om die risico's onder controle te houden. We zullen de Belgische gegevensbeschermingsautoriteit[5] vooraf raadplegen.

D. Incidentenbeheer

Een informatieveiligheidsincident is een gebeurtenis binnen de organisatie waarbij er risico's ontstaan op vlak confidentialiteit, betrouwbaarheid of beschikbaarheid van gegevens of informatiesystemen.
Het volstaat dus dat er een risico ontstaat om van een informatieveiligheidsincident te spreken, het is niet noodzakelijk dat er schade is.

We moedigen medewerkers aan om incidenten op vlak van informatieveiligheid te melden. Medewerkers zijn verplicht om incidenten te melden waarbij het waarschijnlijk is dat persoonsgegevens bij onbevoegden zijn beland. Alle incidenten houden we bij in een incidentenbeheersysteem of incidentenbestand.
De informatieveiligheidsconsulent analyseert het incident, stelt een remediëring voor en volgt de uitvoering van de remedie op. Vaak zal voor de technische aspecten van de diagnose of de remediëring op de IT-dienst beroep moeten worden gedaan. Ze zal de nodige prioriteit geven aan de nodige acties in overleg met de directie. De medewerker krijgt feedback over het incident dat hij had gemeld. De informatieveiligheidsconsulent bespreekt frequente of zware incidenten met de directie.

E. Bewustmaking van de medewerkers

Elke medewerker[6] wordt bij het aangaan van een samenwerking gewezen op hun verplichting tot discretie en respect voor de privacy, zelfs na het beëindigen van de samenwerking. We houden deze boodschap levendig via verschillende kanalen, via opleiding of via opeenvolgende campagnes.
Een medewerker die gevoelige persoonsgegevens of vertrouwelijke (of interne) bedrijfsgegevens leest, gaat daar discreet mee om. Bij het opslaan zorgt hij voor de correctheid en de actualiteit van deze gegevens. In geval van niet respecteren van de privacy kunnen loontrekkende medewerkers gesanctioneerd worden zoals voorzien in het arbeidsreglement.
In het bijzonder vragen wij medewerkers om ieders portretrecht te respecteren en om vooral ook op de sociale media oog te hebben voor de privacy van cliënten en collega's. Een toestemming van de betrokkene is nodig zowel voor het nemen als voor het verspreiden van beeldmateriaal met herkenbare personen. Die toestemming moet schriftelijk zijn als het over beelden gaat waaruit men zeer gevoelige persoonsgegevens kan afleiden (bijvoorbeeld over iemands gezondheid).

F. Beveiliging van de eigen elektronische infrastructuur en de eigen netwerken

Elektronische gegevens worden opgeslagen op dragers (schijven, tapes, ...) en worden toegankelijk gemaakt met behulp van servers, netwerken, software enzovoort. Het is van groot belang dat we deze infrastructuur veilig beheren.
Belangrijke elementen hierin zijn:

- Een configuratie met strikte beveiliging van netwerkapparaten, servers, pc's, laptops en mobiele apparaten.
- Een up-to-date documentatie van de netwerken.
- Een strikte scheiding tussen het bedrijfsnetwerk enerzijds en anderzijds het netwerk dat we in sommige entiteiten aan cliënten en bezoekers aanbieden.
- Een up-to-date bescherming tegen malware (o.a. virussen).
- Waar nodig worden elektronische communicatiekanalen versleuteld om de vertrouwelijkheid, authenticiteit en integriteit van de informatie die over die

[5] In 2017 heet die nog de Privacycommissie.
[6] In de inleiding werd uitgelegd wie we in deze context allemaal als medewerker beschouwen

kanalen gaan te verzekeren. De IT-dienst beheert de sleutels hiervoor zorgvuldig.

- Enkel apparatuur die wij beheren, mag verbonden worden met het interne netwerk. Een uitzondering kan, mits overleg vooraf met de informatieveiligheidsconsulent. Deze evalueert de risico's en de technische en organisatorische maatregelen om die risico's op te vangen en geeft een advies aan de aanvrager en diens directie. Bij blijvend verschil van mening beslist de directie.
- De dienst IT houdt de software (operating systemen en applicaties) up-to-date qua beveiliging, conform de aanbevelingen van de leverancier.
- Enkel de IT-diensten en leveranciers mogen software installeren, eindgebruikers niet.
- De dienst IT wist de gegevensdragers op afgedankte apparatuur onherstelbaar vooraleer die apparatuur de organisatie verlaat.
- Bedrijfsnetwerken worden gescheiden van het internet met strikt geconfigureerde firewalls. Apparaten op de bedrijfsnetwerken die toegang tot het internet nodig hebben, worden extra beveiligd bijvoorbeeld door ze in een DMZ(=DeMilitarized Zone) te zetten, zodat ze geen risico vormen voor de andere apparaten op de interne netwerken.
- Mobiele apparaten zoals laptops en smartphones worden extra beveiligd zodat de gegevens bij verlies of diefstal niet leesbaar zijn voor derden.
- De dienst IT zorgt voor een Disaster Recovery Plan waarin ze de kritische toepassingen die ze beheert opsomt en waarin ze de preventieve en curatieve maatregelen beschrijft om de onbeschikbaarheid kort te houden. Jaarlijks neemt de IT-dienst het initiatief om minimaal één test uit dat plan uit te voeren.
- Bij de eerste fase van een business- of IT-project zal geëvalueerd worden of het project een impact kan hebben op de veiligheid van de informatica-infrastructuur. Zo ja, dan wordt de informatieveiligheidsconsulent erbij betrokken om gedurende het project advies en ondersteuning te geven op vlak van informatieveiligheid.
- Om de beschikbaarheid van de informatie maximaal te verzekeren beheert IT de capaciteit van systemen (cpu-verbruik, geheugen, schijfruimte) en bandbreedte en stabiliteit van de transportkanalen.

G. <u>Fysieke beveiliging</u>

We zorgen ervoor dat de hardware in beveiligde lokalen staat. De veiligheid betreft hier 2 aspecten:

a. Geen toegang voor onbevoegden.
   i. Wie toegang heeft tot een lokaal waar servers, routers en switchen van het bedrijfsnetwerk staan, sluit de deuren van dat lokaal bij vertrek.
   ii. De sleutels van die lokalen worden beheerd door de dienst die ook verantwoordelijk is voor de andere sleutels van dat gebouw.

b. De apparaten in de beveiligde lokalen zijn beschermd tegen stroomuitval, brand en wateroverlast.

Wat betreft informatie <u>op papier</u> bepalen we dat we gevoelige persoonsgegevens en vertrouwelijk bedrijfsgegevens achter slot bewaren.

H. <u>Beheer van afspraken met externe partijen</u>

a. Leveranciers met een opdracht in het kader van informatieverwerking.

De organisatie Broeders van Liefde legt aan potentiële leveranciers tijdens de besprekingen voorafgaand aan elk contract een verwerkingsovereenkomst voor. Dat document wijst de potentiële leverancier op zijn aansprakelijkheid als 'verwerker' zoals beschreven in GDPR. Het bevat o.m. de verplichting om ons meteen te verwittigen bij een veiligheidsinbreuk of het vermoeden van een gegevenslek, de vraag dat de leverancier de passende technische en organisatorische maatregelen waarborgt voor de veiligheid van gegevens en de garantie dat hij zal meewerken aan controles die we nodig achten. Potentiële leveranciers die onvoldoende garanties bieden op vlak van informatieveiligheid komen niet verder in aanmerking voor een contract. Een leverancier zal aantonen dat hij zijn medewerkers die in contact kunnen komen met vertrouwelijke informatie die we beheren, op de hoogte heeft gebracht van onze vereisten op vlak van zorgvuldigheid, discretie en het respect voor de privacy. De verwerkingsovereenkomst preciseert die vereisten.

b. Niet-loontrekkende medewerkers.

Sommige medewerkers zijn geen loontrekkende maar stagiair, medewerker in dienst van een leverancier, vrijwilliger of zelfstandige dienstverlener (bijvoorbeeld dokters in ziekenhuizen of OC's, sommige therapeuten in scholen van het Buitengewoon Onderwijs of de kapster in een woonzorgcentrum). Ook van hen verwachten we zorgvuldigheid, discretie en het respect voor de privacy. We leggen hen daarom bij de start van de samenwerking een document met onze verwachtingen op dit vlak voor. Als de samenwerking meer dan een maand zal duren, vragen we hen om een kopie te ondertekenen voor ontvangst.
Wanneer de samenwerking geregeld wordt in een schriftelijk contract met een zelfstandige, zal dit document deel uitmaken van dit contract.
Wanneer de samenwerking geregeld wordt in een schriftelijk contract met een leverancier wiens medewerker(s) bij ons werken,

- zal dit document bepalen dat de leverancier instaat voor de naleving door zijn personeel van onze eisen op vlak van informatieveiligheid en respect voor de privacy en
- zal dit document deel uitmaken van dit contract.

Zij krijgen enkel toegang tot persoonsgegevens van de cliënten aan wie zij diensten verlenen en ook enkel aan die gegevens die nodig zijn om hun taak uit te voeren.

c. Samenwerkingsverbanden .

Persoonsgegevens doorgeven aan derden kan enkel in de volgende omstandigheden:

* Er is een Europese, Belgische of Vlaamse wetgeving die dat doorgeven toelaat of zelfs verplicht (de betrokkene moet wel geïnformeerd worden), of
* De betrokkene stemt in met dit doorgeven van zijn persoonsgegevens. Voor gevoelige persoonsgegevens moet die toestemming schriftelijk zijn.

Wanneer een entiteit van BVL in een samenwerkingsverband stapt met een of meer (entiteiten van) andere organisaties, onderzoekt de lokale directie of cliëntgegevens kunnen gedeeld worden. Zo ja bepaalt ze welke gegevens daarvoor in aanmerking komen en welke rechtsgrondgrond hiervoor bestaat. Afspraken hierover laten de lokale directies op papier zetten. Er wordt ook afgesproken wie als 'functionaris voor gegevensbescherming' (zie verder) zal fungeren in dit samenwerkingsverband.

Rollen en verantwoordelijkheden

A. De Raad van Bestuur

De Raad van Bestuur van de vzw Provincialaat der Broeders Van Liefde (verder het bestuur genoemd) neemt in het kader van informatieveiligheid de volgende verantwoordlijkheden op:

Het bestuur is eindverantwoordelijke op vlak van informatieveiligheid.
Het bepaalt het informatieveiligheidsbeleid. Dit werd uitgeschreven in onderhavige beleidsnota die actueel wordt gehouden en die intern gepubliceerd wordt.
Het zorgt voor de materiële middelen om de geplande acties te realiseren en volgt de realisaties op.
Het bestuur stelt het organisatorisch kader op en geeft aan welke personen welke verantwoordelijkheden op vlak van informatieveiligheid zullen opnemen.
Het bestuur beslist welke verantwoordelijkheden op vlak van informatieveiligheid bij de lokale directies liggen en welke centraal opgenomen worden.

B. De centrale stuurgroep informatieveiligheid (CSGIV)

De CSGIV is een overlegorgaan dat de volgende taken op zich neemt:

- Zij bespreekt en verbetert de voorgestelde aanpassingen aan deze beleidsnota vooraleer de aanpassingen aan het bestuur worden voorgelegd.
- De CSGIV bespreekt het IV-actieplan dat de centrale informatieveiligheidsconsulent heeft opgesteld, past het waar nodig aan en bezorgt het aan het bestuur dat het uiteindelijk goed- of afkeurt.
- DE CSGIV volgt de realisaties van de goedgekeurde actieplannen op en rapporteert hierover jaarlijks aan het bestuur.

In de CSGIV zijn de volgende instanties vertegenwoordigd:

Het beleid van de sector verzorgingsinstellingen
Het beleid van de sector onderwijs
Het beleid van de sector welzijn en buitengewoon onderwijs
De hoofdartsen
De centrale dienst IT
De juridische dienst
De interne audit
De informatieveiligheidsconsulenten

C. De lokale directies

De directies in de entiteiten zijn verantwoordelijk voor de lokale informatieveiligheid. Ze laten zich adviseren door de lokale informatieveiligheidsconsulent, volgen de evolutie in het beleid op en ook de actieplannen, ze ondersteunen de lokale informatieveiligheidsconsulent in diens werk, bijvoorbeeld op vlak van bewustmaking en incidentbeheer.

D. De informatieveiligheidsconsulenten (IVC's) en de data protection officer (DPO)

Binnen de Centrale Diensten Broeders van Liefde is is er een centrale informatieveiligheidsconsulent (CIVC) die ter beschikking staat van de hele vzw. Voor entiteiten waar dit wettelijk verplicht is, is er ook een lokale informatieveiligheidsconsulent (LIVC) aangesteld. In de andere gevallen is er enkel een lokale contactpersoon voor informatieveiligheid en GDPR. De CIVC en de LIVC's hebben in de eerste plaats adviserende, maar daarnaast ook stimulerende, documenterende en controlerende rol. Daarbij neemt de LIVC de taken op die een grote lokale betrokkenheid vereisen, de CIVC neemt de taken op die we het efficiëntst centraal kunnen realiseren, omdat ze zeer gelijklopend zijn voor alle entiteiten. De CIVC adviseert in alle onafhankelijkheid het bestuur op vlak van informatieveiligheid.
De CIVC stelt een centraal meerjarig actieplan voor om de beleidsdoelen te realiseren en legt dit voor aan de CSGIV.
De LIVC stelt een lokaal actieplan voor aan zijn directie. Hij inspireert zich daarvoor op het centrale actieplan en op de lokale noden. Hij rapporteert aan zijn directie over de vorderingen in dit actieplan.
De LIVC's kunnen bij de CIVC terecht voor advies en bronnenmateriaal.

IVC beheert het meldsysteem voor informatieveiligheidsincidenten en neemt de leiding in bewustmakingscampagnes.
Bij ernstige incidenten contacteert de LIVC de lokale directie en de CIVC het bestuur. Het begrip 'ernstig incident' moet nog duidelijk afgebakend worden.
De CIVC organiseert regelmatig intervisie-overleg met LIVC's coacht en ondersteunt hen.
De CIVC volgt van nabij de evoluties op vlak van wetgeving, bedreigingen en technologie op voor zover ze impact kunnen hebben op informatieveiligheid.
De CIVC leidt de CSGIV.
De CIVC zorgt voor een goede doorstroming van informatie op vlak van informatieveiligheid vanuit de entiteiten naar de CSGIV en omgekeerd.
De IVC's beheren de documentatie over de informatieveiligheid. Dit houdt onder meer in dat ze een eerste versie van documenten maken, dat ze overleggen met betrokken partijen en dat ze de definitieve versie laten goedkeuren en publiceren.
De LIVC bewaakt in samenspraak met de lokale directie de informatieveiligheid wanneer de voorziening een samenwerkingsverband met een derde partij aangaat en volgt dit verder op tijdens de samenwerking.
De LIVC meldt een eventuele gegevenslek aan zijn directie en aan het centrale niveau.
De CIVC neemt de rol van 'functionaris voor gegevensbescherming' (=Data Protection Officer) zoals beschreven in GDPR op. De DPO is onder meer het aanspreekpunt voor betrokkenen die meer informatie willen over de bescherming van hun gegevens of over hun rechten, of die een klacht willen indienen. Hij is ook het contactpunt voor de Belgische gegevensbeschermingsautoriteit.
De DPO contacteert in geval van een gegevenslek van persoonsgegevens de Belgische gegevensbeschermingsautoriteit binnen de 72 uur na kennisname. Hij brengt elke betrokkene op de hoogte (hetzij individueel, hetzij via een openbare mededeling) tenzij aan één van de volgende voorwaarden wordt voldaan:

1) De gegevens zijn onleesbaar voor onbevoegden (bijvoorbeeld omdat ze versleuteld zijn)
2) Er zijn achteraf maatregelen genomen die het hoge risico te niet doen

E. Lokale contactpersoon voor informatieveiligheid

In entiteiten waar een IVC wettelijk niet verplicht is, werken we met mensen die de rol van lokaal contactpersoon voor informatieveiligheid opnemen. Zij zorgen samen met de lokale directie voor:

1) het plannen en uitvoeren van acties die op lokaal niveau nodig zij om GDPR te realiseren
2) voor het melden aan het centrale niveau van een eventuele gegevenslek.

F. De IT-diensten

Lokale en centrale IT-diensten zorgen voor de technische implementatie van de beveiliging van elektronische gegevens en van de systemen die deze gegevens ter beschikking stellen. Zij vertalen de aanbevelingen of vereisten van het beleid in concrete maatregelen op systemen, netwerken, databanken en applicaties. Daartoe hebben zij vaak geprivilegieerde toegangsrechten, waarvan ze zorgzaam gebruik maken, zodat beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens verzekerd blijven.
Zij onderzoeken de eventuele informatica-aspecten van informatieveiligheidsincidenten (diagnose) en stellen technische oplossingen voor (remediëring).
Ze geven incidenten die ze zelf constateren of die anderen aan hen melden door aan de IVC.
Bij aanpassingen aan systemen en toepassingen – bijvoorbeeld tijdens projecten of support - die een impact kunnen hebben op de beveiliging of op de privacy contacteren ze vooraf de IVC.

G. De gebruikers

Gebruikers gaan zorgvuldig en discreet om met de gegevens waar ze toegang toe hebben. Ze melden incidenten op vlak van informatieveiligheid.
De lokale directie kan een bepaalde gebruiker de rol van databeheerder geven.

H. Beheer van archief met historische en erfgoedkundige waarde

Zowel lokaal (in een voorziening, school) als op de centrale diensten bevinden er zich documenten en bestanden (op papier of digitaal) die een historisch, erfgoedkundig en wetenschappelijk belang hebben en die bijgevolg blijvend bewaard mogen worden.7
Deze documenten en bestanden kunnen zowel gewone, gevoelige of bijzonder gevoelige persoonsgegevens bevatten als ook publieke, interne en vertrouwelijke bedrijfsgegevens.
De archiefverantwoordelijken selecteren en zorgen voor de bewaring van de documenten en bestanden die deze gegevens bevatten, in de bewaaromstandigheden en de beveiligingsgraad beschreven in de vademecums van het archief.8
De inzage voor externen (personen van buiten de voorziening of school) is als volgt geregeld:

- De externe vraagt schriftelijk toegang en beschrijft daarin het doel van zijn opzoeking en de aard van de gezochte gegevens.
- Voor publieke en interne bedrijfsgegevens en voor gewone persoonsgegevens geeft de archiefverantwoordelijke al dan niet zijn/haar akkoord.
- Voor vertrouwelijke bedrijfsgegevens en voor gevoelige persoonsgegevens geeft de directie al dan niet haar akkoord.
- Voor bijzonder gevoelige persoonsgegevens geven de directie en de DPO gezamenlijk al dan niet hun akkoord. In geval van medische gegevens beslist de (hoofd)arts.
- De externe ondertekent een verklaring waarin hij/zij garandeert om de persoonsgegevens niet te verspreiden.

De vademecums beschrijven ook welke interne personen welke documenten mogen inkijken.

Werkwijzen en middelen

Informatie veilig beheren vereist zowel een continuïteit in de werking als een projectmatige aanpak. Die continuïteit houdt in dat we willen bewaken en versterken wat in het verleden al gerealiseerd is op vlak van bijvoorbeeld toegangenbeheer, databeheer, incidentenbeheer, enzovoort.
Voor continuïteit heb je goed gedocumenteerde procedures nodig, waarover de betrokkenen goed geïnformeerd zijn. Deze documentatie wordt gepubliceerd op een voor de verschillende doelgroepen vlot toegankelijk platform en jaarlijks kijkt de IVC of er aanpassingen nodig zijn.
De projectmatige aanpak dient om antwoord te kunnen bieden op nieuwe noden op vlak van informatieveiligheid.
Het is van belang dat de IVC snel (dit wil zeggen ten laatste op het moment dat het lastenboek wordt opgemaakt) betrokken wordt bij projecten die de entiteiten of de hoofdzetel lanceren, zodat hij meteen kan onderzoeken of deze projecten ondersteuning nodig hebben op vlak van informatieveiligheid. De lokale of centrale directies onderzoeken bij de indieners van projecten of de informatieveiligheidsconsulent erover moet geïnformeerd worden. Zo voorkomen we dat we onveilige oplossingen kiezen of dat we achteraf extra kosten hebben om de realisatie conform te maken aan onze noden op vlak van informatieveiligheid.
Voor eigen projecten op vlak van informatieveiligheid zal de IVC werken volgens de cyclus: plan – do – check – act.
Bij de opstart van projecten (lokaal of centraal) moet ervoor gezorgd worden dat eventuele kosten die nodig zijn om een informatieveilige oplossing te realiseren worden meegerekend in de projectkost.

Voor acties op vlak van informatieveiligheid die in essentie lokaal zijn, spreken we de lokale middelen aan, voor centrale acties centrale middelen, hetzij via vooraf opgestelde budgetten, hetzij via ad hoc vragen.

[7] Zie het KB van 13 februari 2001 en GDPR.
[8] Momenteel zijn de volgende vademecums beschikbaar: 'Vademecum archivering sector geestelijke gezondheidszorg' en het 'Vademecum archivering orthopedagogische zorg'.

Evaluatie

Wetgeving, bedreigingen en technologie evolueren snel. Driejaarlijks stelt de CIVC een document op met de aanpassingsvoorstellen aan deze beleidsnota die hij nodig acht om gepast te kunnen inspelen op deze evoluties.
De nota met aanpassingsvoorstellen wordt eerst op de centrale stuurgroep informatieveiligheid besproken en daarna aan het bestuur voorgelegd.
Dan worden de nodige acties ingepland om werkwijzen en procedures in lijn te brengen met de veranderingen uit de nota en om de nieuwe versies te publiceren.