EKKLESIA en de AVG

(Algemene Verordening Gegevensbescherming)

EFKASOFT, januari 2018

Inhoudsopgave

1 Inleiding

De tekst in dit hoofdstuk is grotendeels overgenomen uit de nieuwsbrief van het dienstenbureau CGK van december 2017 en aangevuld met informatie over EKKLESIA/EFKASOFT.

Per 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG) in werking. Deze Europese verordening, die de Wet PersoonsBescherming (WBP) vervangt, heeft betrekking op de rechten op bescherming van de persoon waarvan de persoonsgegevens gebruikt worden, en de plichten die de organisatie heeft die deze gegevens gebruikt.

Ook kerkelijke ledenadministraties vallen onder deze verordening. Dat betekent dat kerkelijke ledenadministratie aan bepaalde eisen moet voldoen.

1.1 Privacy in de kerk

De waarborging van privacy is een belangrijk onderwerp. De Autoriteit Persoonsgegevens kan voor overtreding van de WBP (per mei 2018 AVG) boetes uitdelen. Het is belangrijk om zorgvuldig om te gaan met persoonsgegevens van kerkleden.

De kerk moet daarom in eenvoudige taal precies en volledig uitleggen (in een privacyverklaring) wat zij doet met persoonlijke gegevens. Ook moet zij gebruikers/bezoekers wijzen op hun rechten, zoals het aanpassen van gegevens, inzage in dossiers of zelfs het laten vernietigen daarvan.

Vanuit de gedachte van risicobeheersing vereist de AVG dat u het minimale aan persoonsgegevens bewaart. U moet dus actief informatie weggooien wanneer deze niet meer relevant is.

1.2 Binnen eigen kerk

Uw kerkelijk bureau, ledenadministratie of commissie van beheer verzamelt de persoonsgegevens. Meestal in een softwaresysteem. Kerkleden kunnen individueel bezwaar aantekenen tegen registratie van persoonsgegevens binnen de eigen kerk.

Persoonsgegevens mogen doorgegeven worden aan leden binnen de eigen kerk. Denk bijvoorbeeld aan uitwisseling van adressen of relevantie informatie voor organisatoren van activiteiten in de kerk. Een afgeschermde ledenpagina op het internet is een veilige en praktische optie voor het registeren en verzamelen van noodzakelijke persoonsgegevens.

In het Vrijstellingsbesluit WBP, artikel 4, vindt u welke gegevens u onder welke voorwaarden mag verzamelen als kerk.

1.3 Buiten eigen kerk

Voor het verstrekken van persoonsgegevens buiten eigen kerk is een wettelijke basis nodig. In de Wbp staat op welke gronden. De meest voorkomende grondslag is toestemming. Dat betekent dat uw persoonsgegevens alleen buiten de kerk gepubliceerd mogen worden als daarvoor expliciet toestemming is gegeven.

1.4 Gegevens en bewerkers

Daarnaast blijft de kerk verantwoordelijk voor persoonsgegevens die zij geeft aan ‘bewerkers’. Een bewerker is een persoon of organisatie aan wie de verantwoordelijke, in dit geval de kerk, gegevensverwerking heeft uitbesteed. Bijvoorbeeld het personeelsadministratiekantoor of een softwarebedrijf.

Wanneer u gebruik maakt van een softwarepakket, controleer dan of het bedrijf ISO 27001 gecertificeerd is. Dit certificaat garandeert een onafhankelijke controle op de naleving van de nieuwe privacywetgeving (bewerkersovereenkomst AVG). *)

***)**
EFKASOFT is niet ISO 27001 gecertificeerd. Dit is ook geen vereiste om te kunnen voldoen aan de AVG. Een formele certificering door een externe partij is een kostbare zaak, waardoor EKKLESIA niet meer voor een betaalbare prijs zou kunnen worden aangeboden.

Wel legt EFKASOFT in dit document uitgebreid verantwoording af van de inspanning die is gepleegd ten aanzien van de beveiliging en waarborg van de privacy.

1.5 Wet Meldplicht Datalekken

De wet meldplicht datalekken bepaalt dat er melding gemaakt moet worden bij inbreuk op persoonsgegevens van gevoelige aard met mogelijk ernstige gevolgen. Een inbreuk is een hack, technisch falen, verlies of diefstal van een laptop waarop persoonsgegevens van de kerk zijn opgeslagen. Persoonsgegevens van gevoelige aard gaan o.a. over betalingsgegevens, verslavingen, werk- of relatieproblemen of gegevens die kunnen worden misbruikt voor (identiteits)fraude. Een andere reden voor melding is wanneer persoonsgegevens uitlekken die media gevoelig zijn.

Volgens de huidige privacywet hoeft u alleen datalekken bij te houden wanneer u ze ook moet melden aan de toezichthouder. De nieuwe regels van de AVG stellen het verplicht alle datalekken intern te documenteren, óók datalekken die niet aan de toezichthouder gemeld hoeven te worden.

2 AVG: Algemene Verordening Gegevensbescherming

De tekst in dit hoofdstuk is grotendeels overgenomen uit de nieuwsbrief van het dienstenbureau CGK van december 2017 en aangevuld met informatie over EKKLESIA/EFKASOFT.

Een nieuwe privacywet voor heel Europa, dat is wat de Algemene Verordening Gegevensbescherming (AVG) ons brengt. Vanaf 25 mei 2018 moet elke organisatie voldoen aan deze strenge nieuwe wet. Wat gaat er allemaal veranderen? De AVG in negen overzichtelijke stappen:

2.1 Bewustwording

Zorg dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen.

Let op : persoonsgegevens worden niet alleen in gedocumenteerde, gestructureerde en formele systemen vastgelegd. Ook worden kladlijstjes, geprinte wijk- of verenigingsgegevens en dergelijke bijgehouden en opgeslagen. Een zorgvuldige omgang met persoonsgegevens betekent niet alleen dat de automatiseringssystemen zijn afgeschermd; het betekent ook dat men zich bewust moet zijn van de gevoeligheid van de gegevens en de risico's die kleven aan het gebruiken van geautomatiseerde hulpmiddelen. Iedereen moet bewust zorgvuldig omgaan met gegevens en helemaal met persoonsgegevens.

Zorgvuldig gedrag kan worden bevorderd door hiervoor een aantal gedragsregels op te stellen. Gedragsregels over bijvoorbeeld het aanzetten van een slot (lock) op de computer als je niet op je plek zit, het hanteren van een clean desk policy, het afsluiten van kasten, niet laten slingeren van papier en dergelijke.

2.2 Rechten van betrokkenen

Personen krijgen recht op inzage, correctie en verwijdering van hun gegevens. Nieuw daarbij zijn:

- het klachtrecht van betrokkene bij de Autoriteit Persoonsgegevens (AP);
- het recht op dataportabiliteit: betrokkene heeft het recht de gegevens die een organisatie van hem/haar gebruikt op te vragen. Zo kan hij zijn gegevens bijvoorbeeld makkelijk doorgeven aan een vergelijkbare organisatie;
- het recht op vergetelheid: in een aantal gevallen moeten organisaties persoonsgegevens wissen als een betrokkene hierom vraagt.

De organisatie moet tijdig kunnen reageren, vooraf bedenken hoe ze met deze rechten omgaat. Verouderde gegevens van een persoon moeten worden gewist op diens verzoek. Een verzoek van een betrokkene over zijn persoonsgegevens moet normaal binnen een maand inhoudelijk afgehandeld zijn.

2.3 Gegevensbewerking

De AVG stelt een documentatieplicht voor de verwerking van de persoonsinformatie. Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt.

Onder de AVG heeft u ook een verantwoordingsplicht, wat inhoudt dat u kunt aantonen dat uw organisatie in overeenstemming met de AVG handelt. Het bijhouden van een register van verwerkingsactiviteiten (verwerkingsregister) is onderdeel van de verantwoordingsplicht.

U kunt het verwerkingsregister ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties

waarmee u hun gegevens heeft gedeeld.

2.4 Data Protection Impact Assesment (DPIA)

Onder de AVG kunt u verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Voor kerken zal dit in het algemeen niet spelen.

2.5 Gegevensbescherming door ontwerp en door standaardinstellingen

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat u niet meer gegevens verzamelt dan noodzakelijk is voor het doel van de verwerking. En dat u de gegevens niet langer bewaart dan nodig. Privacy by default houdt in dat u technische en organisatorische maatregelen neemt om te zorgen dat u standaard alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken.

2.6 Functionaris gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Voor kerken lijkt dit niet verplicht te zijn. Wel kan het verstandig zijn om iemand de taak te geven om er op toe te zien dat de organisatie haar verplichtingen op het gebied van gegevensbescherming nakomt. Hij of zij is het eerste aanspreekpunt bij vragen over privacy en adviseert de organisatie over de toepassing van de regelgeving. Ook de bewustwording van de organisatie op het gebied van privacy, gegevensbescherming behoort tot haar/zijn taak.

2.7 Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren (incidentenregister). Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan.

2.8 Bewerkersovereenkomsten

Heeft u uw gegevensverwerking uitbesteed aan een bewerker? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn. En of deze voldoen aan de eisen die de AVG aan verwerkersovereenkomsten stelt. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan. Belangrijke aandachtspunten zijn daarbij: goede afspraken over gebruik, over beveiliging van de gegevens, over het melden van datalekken en geheimhouding door de verwerker.

2.9 Toestemmingsvereisten uitgebreid

Uw gegevensverwerking kan gebaseerd zijn op toestemming van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Privacygegevens moeten uit vrije wil, niet onder een voorwendsel of onder druk, gegeven zijn. In de toestemming moet duidelijk zijn voor welke specifieke verwerking en/of specifiek doel gegevens gebruikt worden. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan.

Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

3 EKKLESIA en bescherming persoonsgegevens volgens AVG

3.1 Encryptie

Zoals in hoofdstuk 4 is uitgelegd, is de database niet buiten EKKLESIA om toegankelijk. Dit garandeert een hoge mate van bescherming van de gegevens.

3.2 Geregistreerde gegevens

In de database van EKKLESIA kunnen de volgende gegevens worden geregistreerd. Niet iedere klant hoeft al deze gegevens in te vullen, sommige kunnen dus ook leeggelaten zijn.

Het bestand KG.DBF bevat de gezinstabel.

Veldnaam:	**Omschrijving gebruik:**
GEZINSNAAM	Achternaam waarmee het gezin wordt aangesproken op briefpost.
GEZAANHEF	De aanhef: dhr./mw/fam.
GEZVOORVGS	De voorletters van het gezinshoofd en 'v.d.' e.d.
EXTRAADRES	Extra adresregel, bijv. naam van een tehuis of nadere aanduiding van de locatie.
STRAAT	Straat plus huisnummer.
POSTCODE	Postcode.
WOONPLAATS	Woonplaats.
TELEFOON	Telefoonnummer
WIJK	Wijkcodering.
GEZINSNR	Automatisch gegenereerd door programma. Wordt gebruikt voor koppeling tussen leden en gezinnen.
LAATSTGMUT	laatste gezinsmut. datum, automatisch gegenereerd bij wijzigingen
NIX	Naamindex hulpveld, automatisch gegenereerd. Is voor intern gebruik door het programma.
GEZINSKENM	Kenmerken behorende bij het gehele gezin of adres. Dit veld is voor veel toepassingen te gebruiken. Het bestaat uit een serie tekens, waarbij aan elk afzonderlijk een bepaalde betekenis kan worden toegekend. Elk teken kan slechts éénmaal in het veld voorkomen, dubbele worden eruit verwijderd. Ook de volgorde van de tekens wordt door het programma bepaald.
GEZINBIJZH	Extra veld voor gezinsgegevens, bijv. te gebruiken voor een bezorgwijk nummering of zoiets.
GSTATUS	gezinsstatus, voor intern gebruik
GMUTREDEN	gezinsmutatie reden
GMUTBRON	gezinsmutatie bron
GMUTOPMERK	gezinsmutatie opmerkingen
GMARKEER	gezinsmarkering
SECTIE	sectie waarin adres zich bevindt
BEZORGWIJK	bezorgwijk waarin adres zich bevindt

Het bestand KL.DBF bevat de ledentabel.

Veldnaam:	**Omschrijving gegevens:**
ACHTERNAAM	Achternaam van het lid.
VOORVGSELS	Voorvoegsels, zoals 'van der', enz.
VOORNAMEN	Voornamen voluit, gescheiden door een spatie. Vanuit dit veld genereert het programma automatisch de voorletters, namelijk de beginletters van elk woord.

ROEPNAAM	De roepnaam.
VOORLETTER	Automatisch gegenereerd vanuit VOORNAMEN.
GESLACHT	M=man, V=vrouw
GEBDATUM	Geboortedatum.
SOORTLID	Lid code, standaard: B=belijdend lid, D=dooplid, G=geen lid. Andere codetekens zijn hier ook toegestaan.
BURGSTAAT	Burgerlijke staat: O=ongehuwd, G=gehuwd, W=weduw(naar), S=gescheiden. Andere codes zijn hier ook toegestaan.
KENMERKEN	Kenmerken behorende bij het individuele gezinslid. Dit veld is voor veel toepassingen te gebruiken. Het bestaat uit een serie tekens, waarbij aan elk afzonderlijk een bepaalde betekenis kan worden toegekend. Elk teken kan slechts éénmaal in het veld voorkomen, dubbele worden eruit verwijderd.
GEBPLAATS	Geboorteplaats.
VADER	Voor- en achternaam van de vader
MOEDER	Voor- en achternaam van de moeder
INDATUM	Datum van binnenkomst in de gemeente, in geval van verhuizing van elders.
INKERK	Kerkgenootschap vanwaar lid is binnengekomen
INPLAATS	Plaats van de kerk vanwaar lid is binnengekomen
INOPMERK	Opmerking bij binnenkomst gegevens
DOOPDATUM	Datum waarop de doop heeft plaatsgevonden
DOOPKERK	Kerkgenootschap waar de doop heeft plaatsgevonden
DOOPPLAATS	Plaats van de kerk waar de doop heeft plaatsgevonden
DOOPOPMERK	Opmerking bij de doop
BELDATUM	Datum waarop belijdenis des geloofs is afgelegd
BELKERK	Kerkgenootschap waar de geloofsbelijdenis is afgelegd
BELPLAATS	Plaats van de kerk waar de geloofsbelijdenis is afgelegd
BELOPMERK	Opmerking bij geloofsbelijdenis
ECHTGEN	Voor- en achternaam van de echtgeno(o)t(e)
HUWDATUM	Datum waarop het huwelijk is voltrokken
HUWKERK	Kerkgenootschap waarin huwelijksbevestiging heeft plaatsgevonden
HUWPLAATS	Plaats van de kerk waar de huwelijksbevestiging heeft plaatsgevonden
HUWOPMERK	Opmerking bij huwelijk
UITDATUM	Datum waarop het lid is vertrokken
UITKERK	Kerkgenootschap waarnaar lid is vertrokken (leeg bij onttrekking)
UITPLAATS	Plaats waarnaar het lid is vertrokken
UITOPMERK	Opmerking bij vertrek
BIJZHEDEN	Bijzonderheden, zoals de datum van overlijden van de echtgenoot, speciale wetenswaardigheden, censuur, enz. Bij verwijderen van het lid wordt hier de reden van verwijdering ingevuld
LIDNR	Automatisch gegenereerd door programma.
GEZINSNR	Automatisch gegenereerd door programma. Wordt gebruikt voor de koppeling tussen leden en gezinsgegevens.
GVOLGORDE	Gezinsvolgorde, automatisch gegenereerd. Bij ongehuwden is de volgorde op geboortedatum, bij gehuwden / gescheidenen / weduw(naars) is positie 1 altijd voor de man en positie 2 voor de vrouw, vanaf 3 voor kinderen. Verwijderde leden worden op positie 99 gezet.
LAATSTEMUT	Datum van de laatste lid mutatie, wordt automatisch door programma bijgehouden
NIX	Naam index veld. Wordt automatisch door het programma gegenereerd. Is voor intern gebruik door het programma.
LSTATUS	lidstatus, voor intern gebruik
LMUTREDEN	lidmutatie reden
LMUTBRON	lidmutatie bron
LMUTOPMERK	lidmutatie opmerkingen
OVERLEDEN	overlijdensdatum

TITEL	titulatuur: dhr, mw, Ir, Ds enz.
EMAIL	e-mail adres
LTELEFOON	(mobiele) telefoonnummer van lid
BEROEP	dagelijks beroep van lid
LMARKEER	markering

De bestanden KN*.DBF + KN*.FPT bevatten de notities en eigen velden.

Veldnaam:	**Omschrijving gegevens:**
LIDNR	automatisch gegenereerd
EIGENVELD	verwijzing naar de plaats van de de eigen velden in KN.FPT
NOTITIES	verwijzing naar de plaats van de notities tekst in KN.FPT

De notitiesbestanden vormen een bijzondere categorie. Als gebruik gemaakt wordt van één notities bestand, dan dient dit KN.DBF/KN.FPT te heten. Wordt gebruik gemaakt van meerdere notities bestanden, dan dient de naam te beginnen met KN, gevolgd door max. 6 letters. Notities kunnen een ongelimiteerde hoeveelheid tekst bevatten, zoals pastorale aantekeningen of huisbezoek gegevens. Notities bestanden bevatten ook de zogenaamde 'eigen velden'. Deze worden op de 'eigen velden kaart' zichtbaar door ze met de menu-editor te definiëren. Ook andere gebruikers kunnen hun eigen notitiesbestand (+eigen velden) definiëren. Deze worden steeds, bijv. na een update van de basisgegevens (=inlezen actuele backup) automatisch aan de juiste persoon gekoppeld, op basis van het lidnummer.

HL.DBF en HG.DBF dienen voor het bijhouden van wijzigingshistorie. Ze hebben dezelfde recordstructuur als resp. KL.DBF en KG.DBF.

KA.DBF bevat de algemene kerkgegevens.

Veldnaam:	**Omschrijving gegevens:**
SECTIE	sectie-indeling van de sleutel
SLEUTEL	sleutelnaam
WAARDE	waarde van de sleutel

KM.DBF bevat een aantal interne velden ten behoeve van het programma, zoals bestandssleutelcode, naam van eigenaar van het programma, toegangsrechten, en dergelijke. De inhoud van dit bestand wordt om begrijpelijke redenen niet bekendgemaakt.

MUTATIES.DBF wordt automatisch door EklReport aangemaakt wanneer dat nodig is. Het bevat in principe alle velden van zowel KG.DBF als KL.DBF 2x naast elkaar, waarbij de 2e keer alle velden achteraan een "1" toegevoegd hebben. Deze afgeleide tabel wordt gebruikt om de mutatieoverzichten op eenvoudige wijze te kunnen genereren.

3.3 Verwijderde gegevens

Verwijderde gezins- of persoons-records krijgen in EKKLESIA de status DELETED. Het programma bevat een functie om deze records weer zichtbaar te maken, bijv. voor historische raadpleging. Ook kunnen deze gegevens weer worden teruggezet naar de status 'actueel', bijv. wanneer per ongeluk een record zou zijn verwijderd, of wanneer een vertrokken lid later weer terugkomt binnen de gemeente.

De AVG schrijft voor dat verwijderde gegevens niet langer bewaard mogen worden dan noodzakelijk (max. 2 jaar), tenzij aantoonbaar is dat deze voor historisch archief nut hebben. Kerkelijke gegevens hebben in het verleden altijd deze functie gehad (doopregisters e.d.), dus waarschijnlijk kan in het kader van de AVG aantoonbaar worden gemaakt dat deze bewaard moeten worden.

Indien deze gegevens toch uit de database moeten worden verwijderd (bijv. wegens te brede toegankelijkheid, tenslotte zijn ze aanwezig in de database), dan kan worden gekozen voor de systeemonderhoudsfunctie 'Definitief opschonen'. Hiermee worden álle verwijderde records definitief uit de database verwijderd, zonder onderscheid op ouderdom ervan. (Opschonen van alle

records die langer dan 2 jaar geleden verwijderd zijn, is dus niét mogelijk.)

Wanneer er desondanks een historisch archief vereist/gewenst is, verdient het aanbeveling om bijv. aan het einde van elk jaar de lidkaarten van alle verwijderde leden af te drukken op papier (met inktjetprinter, laserprinter afdrukken zijn niet duurzaam genoeg) en deze afdrukken in een map onder goed geconditioneerde omstandigheden te bewaren, waarna vervolgens de functie 'definitief opschonen' kan worden uitgevoerd.

3.4 Inzage / correctie eigen gegevens

Indien iemand inzage wenst in zijn eigen persoonlijke gegevens, dan kan eenvoudig via het rapport 'lidkaart' of 'gezinskaart' een uitdraai worden gemaakt van alle gegevens die over hem/haar opgeslagen zijn. De eventuele geretourneerde correcties kunnen door de ledenadministrateur worden verwerkt.

3.5 Mutatiehistorie / mutatiebron

In het programma is het mogelijk om de historie van mutaties terug te vragen. Bij iedere mutatie kan worden opgegeven wat de bron van deze mutatie is geweest: ledenadministrateur, scriba, betrokkene, familie van betrokkene, enz. Zo kan achteraf worden nagegaan wie het initiatief tot de mutatie heeft genomen.

3.6 Actief vernietigen van niet relevante gegevens

Soms wordt informatie verzameld ten behoeve van bijv. een kerkelijke actie. Deze informatie blijft gemakkelijk jaren staan. De nieuwe AVG vereist dat dergelijke niet (meer) relevante informatie actief wordt verwijderd. EKKLESIA biedt de mogelijkheid, door middel van de zoek/vervang optie om eenvoudig en efficiënt bepaalde velden op te schonen.

4 EKKLESIA en beschikbaarheid, integriteit en vertrouwelijkheid (ISO-27001)

Wanneer het gaat om de AVG, wordt vaak verwezen naar de zogenaamde ISO-27001 certificering. De exacte tekst van deze certificering is niet vrij verkrijgbaar, alleen tegen betaling. Wel is informatie beschikbaar over de uitwerking hiervan. Eén van de uitwerkingen is een matrix van 56 mogelijke bedreigingen waarvoor een verklaring moet worden gegeven hoe hiermee omgegaan wordt. In de matrices in de bijlage bij dit document komen de onderwerpen aan de orde en is een kruisverwijzing naar de betreffende artikelen in de ISO norm opgenomen.

4.1 Database / Encryptie

De EKKLESIA database is een dBase-III/FoxPro databasestructuur, een zeer wijd verbreid opslagformaat, bestaande uit .dbf en .fpt bestanden. Het is een zeer stabiel bestandsformaat, dat al meer dan 25 jaar zijn betrouwbaarheid heeft bewezen.

Er zijn vele tools beschikbaar om dit databaseformaat te openen. Om directe toegang tot de vertrouwelijke gegevens tegen te gaan, worden door EKKLESIA de gegevens versleuteld opgeslagen in de database, met een sleutel die uniek is per klant (kerk). Dat betekent dat de database uitsluitend benaderbaar is via het bijbehorende EKKLESIA programma.

4.2 Toegangscontrole

Het EKKLESIA programma is voorzien van een loginscherm waarin gebruikersnaam en wachtwoord moet worden ingevoerd om toegang te krijgen tot de gegevens. EKKLESIA wordt geleverd met een standaard gebruikersnaam/wachtwoord combinatie. Het wordt de gebruiker aangeraden om deze meteen na installatie te wijzigen. Dit wordt echter aan de verantwoordelijkheid van de gebruiker overgelaten. De hoofdgebruiker (de ledenadministrateur) heeft de mogelijkheid om meer gebruikers aan te maken, elk met eigen gebruikersnaam en wachtwoord. Het is ook nu de verantwoordelijkheid van de hoofdgebruiker om sterke wachtwoorden uit te delen.

Daarnaast is het mogelijk om velden uit de database en/of functies van het programma uit te sluiten van toegang, door toegangsrechten te definiëren en deze te koppelen aan een groep, die vervolgens kan worden toegewezen aan gebruikers.

Wanneer gebruik wordt gemaakt van notitiesbestanden, door ledenadministrateur of door één van de andere gebruikers, dan kan indien hierin gevoelige informatie wordt opgeslagen (bijv. huisbezoek notities) dit notitiesbestand onafhankelijk van de basisgegevens worden versleuteld met een eigen gedefinieerd wachtwoord, dat naast het toegewezen wachtwoord moet worden ingevuld.

Dit betekent dat de ledenadministrateur verantwoordelijk is voor wie toegang heeft tot welke gegevens.

4.3 Back-up

Voor het veiligstellen van de gegevens ingeval van een crash, is EKKLESIA voorzien van een back-up functie, waarmee een kopie van de database kan worden gemaakt. Dit bevat dezelfde, versleuteld opgeslagen, gegevens als de database, waarbij de afzonderlijke bestanden gecomprimeerd en gecombineerd worden tot één bestand in het gangbare zip-formaat. Dat betekent dat eenvoudig het zip-bestand kan worden uitgepakt, eventueel ook buiten het programma EKKLESIA om, maar de resulterende databasebestanden bevatten dan nog steeds de versleutelde gegevens.

Iedere keer wanneer sinds de laatstgemaakte back-up wijzigingen zijn aangebracht aan de gegevens, zal het programma net voor afsluiten de gebruiker er aan herinneren dat het verstandig is om een nieuwe, actuele backup te maken. Het meest actuele back-up bestand heeft altijd de naam 'EklData.zip'. Wanneer er al een bestand bestaat met die naam, dan zal het programma dit bestand

eerst hernoemen naar 'EklData_YYYYMMDD_HHMM.zip', waarby YYMMDD de datum en HHMM de tijd is waarop het betreffende back-up bestand destijds is gemaakt. Hierdoor wordt een historie opgebouwd van back-up bestanden, zodat altijd in de tijd terug kan worden gegaan.

Zeker wanneer er in de gemeente ook EKKLIDON gebruikers zijn, die periodiek een update krijgen van het gegevensbestand via een back-up, is de zekerstelling van de gegevens gewaarborgd, omdat deze dan vanzelfsprekend op meerdere plekken / pc's worden bewaard.

Ook van de rapporten en selectie bestanden, die door de gebruiker van het programma naar wens kunnen worden aangepast, kan een afzonderlijke back-up worden gemaakt in een zip-bestand.

4.4 Programmaverspreiding

Direct na het installeren van EKKLESIA op een computer, wordt een registratieprocedure gestart. Het programma kan 30 dagen worden gebruikt, binnen die termijn moet worden geregistreerd om toegang te behouden. Ten behoeve van de registratie wordt gevraagd om de adresgegevens van de gebruiker. De registratieprocedure is een handmatig proces, dus EFKASOFT is goed op de hoogte van waar het programma is geïnstalleerd.

Bij overdracht van het programma naar een andere PC zal opnieuw geregistreerd moeten worden, zodat deze contactgegevens bij EFKASOFT actueel kunnen blijven.

Om te voorkomen dat het programma volledig ontoegankelijk zou worden wanneer EFKASOFT permanent onbereikbaar zou zijn, dus niet geregistreerd zou kunnen worden, is vanaf versie 6 de volledige blokkade vervangen door een zogenaamd 'nag-screen', dat vereist dat er max. 30 seconden na opstarten pas met het programma kan worden gewerkt; maar daarna is wél de volledige functionaliteit weer beschikbaar. De rapportagemodule blokkeert nooit, dus het is altijd mogelijk om via rapportages de gegevens weer in leesbare vorm beschikbaar te krijgen.

Binnen de gemeente kunnen wel onbeperkt EKKLIDON (is EKKLESIA 'kijkversie') worden verspreid, waarmee niet de basisgegevens maar wel aanvullende notities kunnen worden gemuteerd. De toegang wordt ook hier bewaakt door middel van een gebruikersnaam / wachtwoord combinatie die door de ledenadministrateur wordt verstrekt.

4.5 Rapportages

Een belangrijk aandachtspunt voor de gebruiker vormen de rapportages, die vanuit EKKLESIA kunnen worden gemaakt. Vanuit EKKLESIA kunnen rapporten gemaakt worden voor afdrukken, maar ook voor opslag in leesbare digitale bestanden, zoals tekstbestanden (.txt), kommagescheiden data (.csv), MS Word, MS Excel, Adobe PDF. Afhankelijk van het soort rapport, kan een dergelijk bestand gevoelige informatie bevatten. Zo zijn er rapporten voor volledige export van alle gegevens beschikbaar, volledige lidkaart rapporten, e.d.

Ondanks het feit dat de EKKLESIA gegevensbestanden versleuteld zijn, zijn deze rapportages volledig toegankelijk. Het is dus van belang dat hiermee zorgvuldig wordt omgegaan. Het verdient aanbeveling om oude rapportages tijdig op te ruimen (niet op afgedankte opslagmedia te laten slingeren) en zorg te dragen voor een veilige verspreiding van benodigde documenten (niet op breed toegankelijke (web-)servers op te slaan).

4.6 Mogelijke calamiteiten en oplossingen

4.6.1 Calamiteit: (hoofd-)wachtwoord kwijt

Mocht zich een calamiteit voordoen waardoor het (hoofd-)wachtwoord bij de gebruiker niet meer bekend is, dan kan (een back-up van) het gegevensbestand worden opgestuurd naar EFKASOFT. Op basis van de versleuteling per klant is EFKASOFT in staat om het hoofdwachtwoord uit te lezen. Indien omwille van de privacy dit ongewenst is, kan hierbij worden volstaan met slechts één enkele tabel, KM.DBF, die alleen de toegangsgegevens bevat en niet de persoonlijke gegevens.

4.6.2 Calamiteit: programma niet meer beschikbaar

Er zou zich het geval kunnen voordoen dat het EKKLESIA programma niet meer foutloos uitgevoerd kan worden, bijv. omdat de (nieuwe) pc met een incompatibele versie van het operating system werkt en er geen updates meer door EFKASOFT voor worden verstrekt. Dan zouden de gegevens ontoegankelijk kunnen worden.

Hiervoor zijn de volgende oplossingen mogelijk:

1. Het EKKLESIA programma alsnog installeren op een pc waarop het wél wil draaien. Vervolgens door middel van de rapportagemodule een volledige export uitvoeren van de gegevens. Hiervoor zijn speciale export-rapporten beschikbaar gesteld. De gegevens kunnen dan weer ingelezen worden in een ander programma/database voor dit doel.
2. Indien EFKASOFT wel bereikbaar is, zou die kunnen worden gevraagd om bovenstaande export te verzorgen, op basis van toegestuurd back-up bestand.

4.6.3 Calamiteit: programma kan niet meer worden geregistreerd

Er zou zich het geval kunnen voordoen dat het programma niet meer geregistreerd kan worden omdat EFKASOFT onbereikbaar is geworden (bijv. door overlijden). In dat geval kan altijd via de rapportagemodule een export worden gemaakt naar leesbaar formaat, zodat de gegevens kunnen worden ingelezen in een ander programma. Mocht er onverhoopt sprake zijn van overlijden of van stoppen van EFKASOFT, dan zal (zo nodig door de nabestaanden van EFKASOFT) een niet-registreerbare versie van het programma worden verstrekt, zodat de acute noodzaak tot overstappen op een ander programma wordt verminderd.

4.6.4 Calamiteit: database is uitgelekt naar onbevoegden

Indien het gegevensbestand in onbevoegde handen komt, bijv. doordat een gemaild back-up bestand wordt onderschept, of doordat een afgedankte harde schijf deze gegevens bevat, dan worden deze beschermd door het versleutelingsalgoritme.