POPIA Beleid

Die Kerkraad (KR) aanvaar hiermee die volgende beleid vir gemeente [naam van gemeente] rakende die POPI wetgewing, ook genoem die wet op die beskerming van persoonlike inligting:

1. Oorsig en Agtergrond

Met die koms van kragtige elektroniese toestelle is die beskerming van persoonlike inligting belangriker as ooit. Die oogmerk van die POPI Wet is juis om persoonlike inligting te beskerm wanneer dit deur ’n ENIGE verantwoordelike party – insluitend kerke – geprosesseer word.

Dit is gerig op die balansering van die reg op privaatheid teenoor die reg op toegang tot inligting asook die vrye vloei van inligting binne die Republiek en oor internasionale grense.

Hierdie is dus kommende ’n wet wat reeds in 2013 (Wet nr. 4 van 2013) deur die SuidAfrikaanse regering goedgekeur is waarin die voorwaardes gereguleer en wetlik bepaal word, wat instansies moet volg om die persoonlike inligting van hulle lede / kliënte, (volgens bg. wet ’n “Datasubjek” en in ons geval die lidmate en personeel), se persoonlike inligting wettig te mag versamel / ontvang, verwerk, opdateer, aanwend, versprei en te stoor / bewaar / berg, asook die vernietiging of uitvee van hierdie data. Die wet vereis ook dat wanneer ’n instansie kinders se inligting hanteer, die ouers daartoe vooraf toestemming moet gee. Dit geld ook vir enige ander persoonlike inligting wat deur die gemeente en affiliasies versamel sou word vir watter doel ook al. (Bv. Sunrise Na-skool). Die POPI wet is dus van toepassing op almal wat persoonlike inligting prosesseer, ook die kerke. Die wet beperk egter nie instansies om inligting te mag verwerk nie, dit vereis net dat dit op die regte manier hanteer en reguleer sal word.

Hierdie wet het in werking getree op 01 Julie 2020, (met ’n een jaar grasie tydperk vir instansies om daaraan te voldoen). Dit reguleer die wyse waarop persoonlike inligting geprosesseer mag word en skryf die minimum vereistes vir die regmatige prosessering van persoonlike inligting voor deur vrywillige en verpligte maatreëls wat verseker dat persoonlike inligting met die nodige respek hanteer word.

Die volgende 8 voorwaardes, wat deur die POPI wet vereis word, waaraan instansies moet voldoen, sal nou soos vanuit hierdie wet, soos volg verdeel word vir die doel van die uitleg van hierdie dokument / beleid:

1. Verantwoordingspligtigheid. (“Accountability”)
2. Beperkte prosessering. (“Processing limitations”)
3. Oogmerk Spesifikasie. (“Purpose Specific”)
4. Beperkte verdere prosessering. (“Further Processing Limitations”)
5. Inligtingsgehalte. (“Information quality”)
6. Openheid. (“Openness”)
7. Veiligheidsvoorsorgmaatreëls. (“Security Safeguards”)
8. Deelname deur die lede / Datasubjek. (“Data subject Participation”)

2. VERANTWOORDINGSPLIGTIGHEID:

Elke instansie wat persoonlike inligting hanteer, moet kennis dra van die POPI wet. ’n Bewustheidsveldtog moet van stapel gestuur word en ’n inligtingsoudit (status risiko assessering) voltooi word. Uit hierdie inligting word die POPI prosedurehandleiding saamgestel.

Elke instansie moet ook ‘n amptelike enkel verantwoordelike persone vir die doel, by die instansie gaan aanwys as die Nakomingsbeampte, met die volgende pligte en verantwoordelikhede, soos dit uiteen

gesit word in Artikel 55 van die wet soos volg: (Die wet bepaal dat hierdie persoon, so ver dit moontlik kan, 'n werknemer in diens van die gemeente moet wees en verkieslik die hoogste rang sal beklee.)

Toesien dat die instansie die 8 voorwaardes, (soos in punt 1 hierbo genoem), van die wet nakom met betrekking tot die regmatige verwerking van persoonlike inligting van datasubjekte (lidmate).

1. Die hantering van versoeke wat aan die gemeente gerig word in terme van die wet.
2. Om saam met die inligtingsreguleerders te werk met ondersoeke teen die gemeente.
3. Toesien dat die gemeente heeltemal aan al die voorskrifte van die wet voldoen.

Regulasies in die staatskoerant van 14 Desember 2018 bepaal verder dat die nakomingsbeampte, saam met die inligtingsbeamptes, moet bykomend tot voorskrifte van die wet in Artikel 55(1) verseker dat:

- 'n Voldoeningsraamwerk ontwikkel, geïmplementeer, gemonitor en onderhou word. (Hierdie dokument / beleid moet dan ook hieraan voldoen.)
- 'n Persoonlike inligtingsimpakassessering gedoen word om te verseker dat voldoende maatreëls en standaarde bestaan ten einde te voldoen aan die voorwaardes vir die wettige verwerking van persoonlike inligting.
- 'n Handleiding ontwikkel, gemonitor, onderhou en beskikbaar gestel word soos in artikels 14 en 51 van die Wet op Bevordering van Toegang tot Inligting, 2000 (Wet No. 2 van 2000), voorgeskryf.
- Interne maatreëls ontwikkel word saam met voldoende stelsels om versoeke om inligting of toegang daartoe te verwerk.
- Interne bewustheidsessies oor die bepalings van die Wet, regulasies ingevolge die Wet uitgevaardig, gedragskode, of inligting van die Reguleerder verkry, gehou word.

BELEID: VERANTWOORDINGSPLIGTIGHEID

1. Dat die voorsitter van die Bedryfsbediening die rol van die amptelike nakomingsbeampte by Gereformeerde Gemeente Linden sal vul.
2. Dat die volgende personeellede ook in die rol van inligtingsbeamptes aangewys word en dus met die inligting mag werk:
    a. Alle administratiewe en bedienings-koördineerder poste wat met die lidmaatdata werk.
    b. Alle leraars wat die inligting van die lidmate benodig.
3. Dat al bogenoemde persone in die begin van hierdie proses se implementering, ook aandag sal gee aan:
    a. 'n Bewusmakingsveldtog in die gemeente, (veral onder die leierskorps), dat daar so 'n wet bestaan en wat die vereistes uit die wet is en dat daar gewerk gaan word daaraan om 'n beleid daarvoor op te stel.
    b. 'n Statusrisiko – assessering gedoen moet word, wat o.a insluit, 'n register van die tipe inligting wat tans reeds versamel is. (Bv. Adres, telefoon nrs, beroepe, bankbesonderhede, ens. Hoe is dit versamel / bekom? Met wie was dit in die verlede en gaan dit in die toekoms mee gedeel word?)
    c. Die Opstel van 'n POPI prosedurehandleiding, wat hierna gebruik sal word as deel van die gemeente se beleid hoe die data in die toekoms hanteer gaan word.

3. BEPERKTE PROSESSERING:

Artikels 9 tot 12 van die spesifieke wet handel oor beperkte prosessering. Daar is 4 hoekstene waarop hierdie voorwaarde gebou is:

a) Die versameling van inligting moet op 'n redelike wyse gedoen word, sonder om inbreuk te maak op die lidmaat se privaatheid.

b) Minimalisties. ("Less is more"). Ons is geregtig om wel alle soort inligting van die lidmate in te samel, maar die voorskrif stel dat ons nie meer inligting as wat benodig gaan word moet probeer insamel nie.

Daar mag ook addisionele inligting ingesamel word, net van sekere van die lede, vir 'n spesifieke doel, wat gemotiveer kan word as belangrik vir 'n kerk. (Maar dit is spesifieke inligting en sal dus nie nodig wees om al hierdie soort inligting by al jou lede te moet kry nie.) Bv. Bankbesonderhede wanneer 'n debietorder ingestel moet word, of mediese toestande as 'n lidmaat / kinders op 'n kamp of uitstappie moet gaan, of ander kerklike inligting soos dat die lid in spesifieke leiersposisies al gedien het.

c) Toestemming van die lidmaat moet verkry word om wel hulle inligting te mag versamel en te stoor en dit daarna te mag aanwend vir die doel van die funksionering van die gemeente.

d) Inligting mag slegs vanaf die lidmaat self, direk ingesamel word en nie by 'n 2de party gekry word nie. Behalwe natuurlik dit wat ander gemeentes reeds ingesamel het en aan ons moet deurgee, wanneer daar van gemeentes verwissel word.

BELEID: BEPERKTE PROSESSERING

Dat die onderskeie inligting wat benodig sal word van lidmate, so hanteer sal word:

1. Bankbesonderhede van lidmate sal slegs deur een lid in die Kerkkantoor hanteer en gestor word. Die pos wat verantwoordelik is vir die insleuteling van debietorders. (Toestemming word in elk geval verkry by lidmate vir die gebruik en doel daarvan op die debietorder aansoek)
2. Alle nuwe lidmate moet in die toekoms toestemming gee dat ons hulle inligting mag versamel en gebruik slegs vir die doel van die funksionering van die gemeente. (Hierdie sal dus op die lidmaat aansoek vorm aangebring moet word.
3. Die kerkkantoor moet ook 'n stelsel in plek kry om al die bestaande lidmate se toestemmings ook vir bg. doel te kry.

4. OOGMERK SPESIFIKASIE:

Die doel van die versameling van persoonlike data van lidmate is tweeledig van aard.

a) Dit word eerstens benodig omdat die persoon 'n lid van die organisasie is, wat dan verband hou met die werksaamhede van die organisasie. (Indien daar 'n goeie rede is, met goeie motivering, vir sekere inligting wat benodig gaan word daarvoor, kan dit versamel word.)

b) Die data van individue wat benodig word moet natuurlik ook voortdurend hersien of verander word soos wat dit verouderd raak en weer opdateer moet word. Daarom is dit noodsaaklik dat daar 'n proses van instandhouding van data moet wees.

Die bogenoemde motivering is meer as genoeg rede om hierdie inligting van lidmate te versamel en te gebruik. Hoewel Artikel 26 instansies verbied om inligting rakende 'n datasubjek se geloofsoortuigings te

prosesseer, gee Artikel 28(1) van die wet spesifiek vir kerke die toestemming om wel lidmate se inligting te mag versamel en te bewaar.

BELEID: OOGMERK SPESIFIKASIE

Dat die Kerkkantoor gereelde opnames onder die lidmate sal hou om die verandering van lidmate se inligting, (soos gelys in Bylaag B), op te spoor en op die databasis op te dateer.

Dat die gemeente geregtig is om hierdie inligting in te samel wanneer lidmate aangedui het dat hulle lede wil wees van hierdie gemeente / organisasie.

5. BEPERKTE VERDERE PROSESSERING:

Dit is belangrik om te weet wie toegang kry tot die data, hetsy dit genommerde harde- of wagwoordbeskermde elektroniese kopieë is. Hier volg ŉ lys van watter persone of instansies binne die gemeente tans toegang tot die lidmate se data het en op watter wyse hulle dit gebruik:

a) Kerkkantoor personeel.

Die administratiewe en finansiële personeel kan toegang tot die data verkry, hoewel die minimalistiese beginsel, (sien 3b hierbo) steeds toegepas moet word. In die verband is dit baie belangrik dat gemeentes tyd moet begroot om die toegang van amptenare wat die databasis mag gebruik, behoort te ondersoek en seker te maak dat slegs amptenare wat werklik toegang tot alle data moet kry sodanige regte binne in die databasis moet ontvang wat hulle toegang tot alle data gee. Om toegang tot alle data te ontvang, beteken nie noodwendig dat so 'n amptenaar enige data moet kan verander nie. Dit is heeltemal moontlik dat 'n databasis gebruiker wel alle data kan sien, maar nie wysig nie.

Dit is baie belangrik dat slegs een gebruiker as "meester gebruiker" aangestel moet word. Die meester gebruiker is dan die enigste gebruiker wat ander gebruikers se regte kan verander. Alle ander amptenare se regte kan individueel verstel word onder die "Stelsel opsie" by die afdeling "Gebruikers" om slegs beperkte toegang met beperkte regte aan hulle toe te ken. Elke gebruiker wat in die databasis aanteken / gebruik, moet verplig word om 'n dokument te "onderteken" waarin hulle onderneem om die inligting van lidmate te beskerm en nie aan enige ongemagtigde persoon of instansie ooit sal bekend maak nie. Ons noem dit die gebruiksvoorwaardes vir POPI aanpasbaarheid binne in die sisteem / stelsel / program / beleid.

b) Leraars.

Dit is noodsaaklik dat leraars wel toegang tot die data van alle lidmate moet kan kry om hulle ampsverpligtinge ten volle te kan nakom. Natuurlik moet die minimalistiese beginsel ook hier toegepas word. Leraars en ander amptenare moet net van die minimum inligting voorsien word, en sou die behoefte later verander dat hulle meer inligting nodig kry om hulle werk te kan doen, kan dit op daardie stadium aan hulle beskikbaar gestel word. Die lidmaatinligting kan op een of meer van die volgende metodes aan leraars voorsien word:

i. Harde kopieë.
ii. Elektronies.

Maak seker dat wanneer harde kopieë voorsien word, dit verkieslik as genommerde kopieë voorsien moet word, en die kerkkantoor moet rekord hou dat kopieë, nadat dit nie meer benodig word nie, of verouderd geraak het, na die kerkkantoor moet terugkom om vernietig te word.

Wanneer elektroniese kopieë voorsien word, is dit beter om die elektroniese dokumente met 'n wagwoord te beskerm en die wagwoord apart aan die leraar via 'n ander medium soos bv. 'n SMS te voorsien.

c) Kerkraadslede en ander leiersposisies.

Dit is natuurlik ook noodsaaklik dat kerkraadslede en ander leiers in die uitvoering van hulle pligte sekere inligting van lidmate moet hê. Maak seker dat hierdie inligting ook tot die minimum beperk word, en dat die riglyne soos hierbo vir leraars ook nagekom word. Inligting wat aan kerkraadslede voorsien word, behoort verder beperk te word, tot die lidmate van hulle groep waarvoor hulle verantwoordelik is. Dit is nie nodig dat 'n kerkraadslid inligting van lidmate in ander groepe hoef te hê nie behalwe waar die kerkraadslid verantwoordelik is vir meer as groep.

Dit is verder ook baie belangrik om daarop te let dat die inligting van kinders spesifiek baie meer beperk word deur die wet en dat daar oor die algemeen baie versigtiger met die inligting van kinders omgegaan moet word. Die wet vereis ook dat, om die inligting van minderjarige kinders te mag prosesseer, die toestemming van die ouers nodig is. Maak dus voorsiening daarvoor op die lidmaat aansoek vorm.

d) Lidmate.

Lidmate kan natuurlik ook soms beperkte toegang tot inligting van ander lidmate kry. Dit gebeur baie maal dat herdenkings of verjaardae op die gemeente se afkondigings verskyn. Hierdie inligting is dan nie alleen vir die gemeente sigbaar nie, maar ook vir die wyer publiek.
Dit is daarom noodsaaklik dat persoonlike inligting van lidmate wat op openbare platforms soos webwerwe, sosiale media of selfs WhatsApp, asook afkondigings voorkom, slegs gepubliseer mag word met die toestemming van die lidmaat.

BELEID: BEPERKTE VERDERE PROSESSERING

1. Die admin poste in die Kerkkantoor sal dien as die Hoof Inligtingsbeamptes wat saam met die Nakomingsbeampte ook sal toesien dat die volgende deel van die beleid (soos in die res van hierdie dokument), tot uitvoer gebring word.
2. Die volgende poste / lede / funksionarisse / lidmate mag ook die ander lede se persoonlike inligting hanteer:
    a. Leraars.
    b. Ander personeel en lede van die Bedryfsbediening.
    c. Groei-groep leiers.
    d. BlinC mentors en Ark Toerleiers.
    e. Ouderlinge.
    f. Voorsitters van die bedieninge.
3. Vir die doel daarvan om die hantering daarvan reg te doen, moet elkeen eers deur ’n POPI inligting / opleidingsessie gaan.
4. Dat die Kerkkantoor ’n register sal opstel en byhou van harde kopieë wat uitgegee word, en wanneer dit nie meer gebruik woed nie, dit terug gekry moet word en daarna vernietig moet word deur die kerkkantoor personeel. Indien daar ’n elektroniese weergawe uitgereik word, moet die kerkkantoor verseker dat die inligting met ‘n wagwoord beskerm word.
5. Toestemming vir die gebruik van die kinders se inligting moet eers verkry word.
6. Toestemming moet ook eers verkry word van die lidmate voordat hulle verjaardae bekend gemaak mag word.

6. INLIGTINGSGEHALTE:

Die wet stel dit dat die verantwoordelike party moet redelike stappe neem om te verseker dat die persoonlike inligting van lidmate wat so ingesamel word, volledig, akkuraat, nie misleidend is nie en gereeld opgedateer word, volgens artikel 16.

BELEID: INLIGTINGS-GEHALTE

Dat die Kerkkantoor se admin personeel, wat die opdatering van die databasis hanteer, voordurend sal probeer verseker dat die nuutste inligting van lidmate verkry word en gevolglik verander word op die databasis.

7. OPENHEID:

Artikel 18 van die wet bepaal dat die verantwoordelike party redelike wyse verseker dat die datasubjekte / lidmate bewus is dat inligting oor hulle ingesamel is / word en watter inligting dit dan ook sal wees.

BELEID: OPENHEID

Dat die lidmate gereeld ingelig sal word, op verskeie metodes, van die verskillende persoonlike data wat deur die kerkkantoor gehou word en dat dit volgens die POPI wetgewing hanteer word.

8. VEILIGHEIDSVOORSORGMAATREËLS:

Dit is belangrik dat die volgende 5 aspekte wat alles te doen het met die veiligheidsvoorsorgmaatreëls ten opsigte van lidmate se data nagekom word. Die 5 aspekte is:

A. Berging.
B. Beveiliging.
C. Retensie.
D. Vernietiging.
E. Bewusmaking van personeel.

A. BERGING.
    a. Op rekenaars:

'n Volledige analise moet gedoen word oor die berging van data en waar die data geberg word. Persoonlike inligting van lidmate kan op papier geberg word, of dit kan elektronies bewaar word. Daar moet verder bepaal word wie kry almal toegang tot papier kopieë asook wie kry almal toegang tot die elektroniese data. Die elektroniese data moet verkieslik net op een rekenaar geberg word, met al die nodige beskermingsmaatreëls in plek. Daar mag wel verskeie, vooraf goedgekeurde persone, toegang daartoe verkry vanaf ander rekenaar of toestelle. (Bv. op 'n netwerk).
Elke toestel / gebruiker moet voorsien word van sy eie unieke gebruikersname en wagwoorde om in die stelsel in te teken. Elke verbruiker daarvan moet ook 'n onderneming onderteken dat hulle die data sal beskerm en nie wederregtelik sal versprei nie. Dit is belangrik dat die Nakomingsbeampte ingelig sal word van waar, hoe en met wie die data geberg en gedeel word. Veral waar die data op tuisrekenaars geberg gaan word, sodat hy / sy kan verseker dat:

- Onder streng voorwaardes en met die nodige veiligheidsprotokolle in plek, op amptenare se tuisrekenaars gebruik mag word, en;
- Sou die amptenaar nie meer in diens van die gemeente staan nie, of die program nie meer deur die amptenaar benodig word nie, verwyder word van 'n amptenaar se tuisrekenaar. Onthou ook dat alle

rugsteun kopieë van die data, sowel as enige ander elektroniese dokument wat moontlik inligting van lidmate

- mag bevat ook verwyder moet word.

b. Ander metodes en plekke:

Data van lidmate kan ook in die volgende programme of plekke gestoor word:

- Finansiële sagteware.

Die sagteware wat gebruik word om die lidmate se finansiële bydraes te boekstaaf en vanaf te bestuur, word slegs op die kantoorbestuurder se rekenaar gelaai. Beskerming hiervoor moet in plek wees.

- Anatomy Church Management.

Amptenaar / Personeel / Sommige Funksionarisse kan dmv Anatomy toegang kry tot al die nuutste data deur op die diens aan te teken met sy/haar gebruikersnaam en wagwoord. (Die Nakomingsbeampte moet ook hiervan ingelig word om te weet wie almal het ook so toegang verkry, sodat hy/sy ook kan verseker dat persone se toegang herroep kan word, indien hulle nie meer die toegang benodig nie.)
Lidmate van die gemeente kan ook toegang gegee word tot Anatomy, maar is hoofsaaklik net om hulle eie inligting te kan sien en te kontroleer. Die toegang van lidmate tot hulle eie data is juis inlyn met die POPI wet se voorwaardes 5 en 6 nl. Inligtingsgehalte en Openheid, omdat lidmate ook verouderde data kan regstel, of ten minste 'n versoek rig tot die regstelling van hulle data.

- E-Pos programme.

Die POPI Nakomingsbeampte moet ook ondersoek instel na watter persoonlike inligting van lidmate en ander datasubjekte in gemeentes se e-Pos Programme gestoor word. Onthou ook dat dit nie net lidmate se inligting is wat in e-pos programme gestoor word nie, maar baie ander datasubjekte se inligting soos bv. Klassis predikante, of Sinodale amptenare, of diensverskaffers ens.
Die POPI Inligtingsbeampte moet ook ondersoek instel na waar die data van die betrokke e-pos program gestoor word, sodat dit beveilig kan word. (Later in hierdie dokument meer inligting oor die beveiliging van data in e-pos programme.)

- Microsoft Word en Excel.

Microsoft Word en Excel is seker van die programme wat die meeste deur gemeentes gebruik word. Dit is daarom ook raadsaam om presies vas te stel watter inligting daar in hierdie programme ingetik word. Microsoft Word word sekerlik daagliks gebruik om afkondigings, agendas, notules en korrespondensie mee te tik. Baie gemeentes plaas lidmate se verjaarsdae op die afkondigings. Daarmee saam word daar dikwels ook die lidmate wat verjaar se telefoonnommers en ander persoonlike inligting in die afkondigings bekend gemaak. Hoewel dit verstaanbaar is dat ons graag wil hê dat lidmate onderling met mekaar moet kan kontak maak, sal die Kerkkantoor nou baie versigtiger moet wees met die publikasie van identifiseerbare persoonlike besonderhede.

- PDF lêers en ander dokumente.

Gemeentes ontvang dikwels dokumente in PDF formaat wat, sou dit verlore raak wel 'n probleem kon veroorsaak. Dit gebeur ook dat lyste met lidmaatinligting in PDF formaat aan amptenare of ander belanghebbendes beskikbaar gestel word. Die Kerkkantoor sal ook hierop moet begin let om dit te verminder of te beskerm.

- Gemeentelike webwerwe.

Dit gebeur soms dat gemeentes op hulle webwerwe sekere identifiseerbare besonderhede van lidmate of amptenare plaas. Dit is nie noodwendig verkeerd nie, maar sodanige plasing(s) moet met uitdruklike goedkeuring van die lidmaat of lidmate gedoen word. Die Kerkkantoor en webmeesters sal ook hierop moet begin let om dit te verminder of om die nodige toestemming te verkry.

- Sosiale media.

Dieselfde beginsel wat hierbo vir gemeentelike webwerwe genoem was, is ook van toepassing op sosiale media plasings. Veral in die skep van WhatsApp groepe wat eintlik geweldige ernstige gevolge kan inhou. Almal weet hoe WhatsApp groepewerk. Dit koppel aan die kontakte op iemand se selfoon. Baie gemeentes voer nou lidmate as kontakte op 'n selfoon in en skep dan 'n groep of groepe waarmee daar met lidmate mee gekommunikeer word. Die goue reël sou egter wees dat lidmate se toestemming eers verkry moet word voordat hulle op die groep bygevoeg word. Voor POPI sou dit goed genoeg gewees het om lidmate voor die voet by te voeg, want 'n lidmaat kan mos die groep "leave" as hy/sy nie op die groep wil wees nie. Na POPI sal jy egter lidmate se goedkeuring moet kry alvorens jy hulle op 'n groep mag byvoeg. Die kerkkantoor sal

hierop moet konsentreer om eers die nodige toestemming te kry vir die skep van groepe en hele gemeente sal hieroor ingelig moet word.

- Selfone.

Die tegnologie maak dit al hoe makliker vir administratiewe personeel en predikante om inligting van lidmate op hulle selfone te laai. Een van die grootste probleme met selfone is dat dit baie maklik wegraak. As daar nie genoegsame beskerming op die selfoon is nie, en dit sou wegraak kan dit beslis 'n oortreding in terme van die wet wees.

- Harde Kopieë.

Die POPI Nakomingsbeampte moet ook ondersoek instel na hoe en waar harde kopieë in die kantoor geberg moet word (in lessenaarlaaie of kabinette). Die grootste probleem kom egter waar geberg word. (Meer inligting hoe om harde kopieë ook te beskerm volg later in die dokument) Papier weergawes van die data moet dus ook streng beheer en geberg word.

B. BEVEILIGING.

Die beveiliging van data is die grootste taak wat 'n gemeente moet uitvoer om binne die voorskrifte van die wet te bly. Daar is 2 tipes beveiliging waaraan gemeentes moet aandag gee en dit is:

a. Fisiese Sekuriteit.
b. Elektroniese Sekuriteit.

a. Fisiese Sekuriteit:

- Diefwering en veiligheidshekke.

Indien daar nie diefwering en of veiligheidshekke is nie, sal dit eintlik noodsaaklik wees om dit te laat aanbring as eerste stap in die fisiese beveiliging van die kantore. Indien daar wel reeds is, sal dit 'n goeie idee wees om dit na te gaan om te verseker dat dit wel voldoende is.

- Alarmstelsel.

'n Goeie alarmstelsel, wat verkieslik aan 'n reaksiemag gekoppel is sal eintlik 'n noodsaaklikheid wees in die beveiliging van die kantoor. Dit is dalk ook nou 'n goeie tyd om die alarmstelsel te laat nagaan of dit nog voldoende is en of dit nie dalk opgegradeer behoort te word nie.

- Sekuriteitskameras.

As die gemeente se begroting dit toelaat sal sekuriteitskameras 'n verdere bonus wees en die ideaal sal natuurlik wees dat dit 'n stelsel is wat 'n video opname van beweging kan maak, sodat sou dit nodig wees, daar agterna na die opnames gekyk kan word.

- Brandkluis.

'n Groot genoeg brandkluis is werklik noodsaaklik. Die meeste gemeentes beskik wel oor 'n brandkluis veral om o.a. kontant in toe te sluit, maar dit sal 'n goeie idee wees om bv. die rekenaar waarop die data gestoor word ook in die kluis toe te sluit as die kluis groot genoeg is om dit te kan doen. Verder is dit ook 'n goeie gebruik om bv. laptops en eksterne hardeskywe en ander elektroniese bergingstoestelle in die kluis toe te sluit wanneer dit nie in gebruik is nie. Dit moet natuurlik by die personeel ingeskerp word dat veiligheidshekke gesluit moet wees en alarmstelsels geaktiveer moet word sodra die kantoor verlaat word. Dit help niks as die kantoor die beste veiligheidsmaatreëls het, maar dit word nie gebruik nie.

b. Elektroniese Sekuriteit:

- Wagwoorde.

Dit het ’n algemene praktyk geword dat wagwoorde jou harde- en sagteware moet en kan beskerm. Alhoewel die meeste hiervan dit outomaties vereis, is daar soms ’n keuse om dit oor te slaan. Hierteen oor word dit dus nou agv die POPI wetgewing ten sterktes aanbeveel en vereis dat wagwoorde in plek gestel word om die Data te help beskerm wat op die toestelle en in die sagteware gestoor is. Die POPI wet vereis dus dat alle toerusting waarop Data gestoor word moet met ’n wagwoord ook beskerm word. (Alle rekenaars met Windows moet nou ook ’n wagwoord kry.)

- Goeie wagwoord praktyke.

i.) Verskillende wagwoorde.

Die eerste belangrike beginsel is dat 'n mens nie dieselfde wagwoord vir al jou programme en webwerwe moet gebruik nie. Maak seker dat jy vir elke webwerf of program 'n ander wagwoord gebruik. 'n Gebruik wat

baie mense onwetend doen en wat eintlik 'n baie gevaarlike en riskante gebruik is, is om vir jou "Browser" die reg te gee om 'n webwerf se Gebruikersnaam en/of wagwoord te onthou. Die gerief daaraan is natuurlik dat dit vir die gebruiker baie tyd spaar om toegang te verkry tot webwerwe wat baie besoek word, maar die gevaar hieraan verbonde is dat enige ongemagtigde persoon toegang tot jou webwerwe kan verkry sonder om die gebruikersnaam of wagwoord in te vul op die webwerf.

ii.) Sterk wagwoorde.
Gebruik wagwoorde wat moeilik geraai kan word. Vermy wagwoorde wat name of vanne of geboortedatums bevat. Vermy ook wagwoorde wat goed bevat soos "password" of "wagwoord" of "admin" of "abc" of "123" ens. Hoe moeiliker wagwoorde word, hoe moeiliker word dit natuurlik om dit te onthou. Dit is dan natuurlik die rede waarom mense sommer eenvoudige en maklike wagwoorde gebruik. Dit is gelukkig nie baie moeilik om hierdie praktyk reg te maak nie. Die meeste webwerwe wat wagwoorde vereis, gee ook aan die gebruiker die geleentheid om sy of haar wagwoord te verander. Dit is dus binne enigiemand se vermoë om sterk wagwoorde vir alle plekke waar wagwoorde vereis word, te skep. Die gebruik van sterk wagwoorde is natuurlik 'n groot uitdaging. Die uitdaging is natuurlik om 'n manier te vind om die wagwoorde iewers neer te skryf waar dit veilig is. Verkieslik kan wagwoorde ook gestoor word op rekenaarprogramme, maar dan moet daar ook ’n sterk wagwoord beskerming wees daarvoor.

iii.) Verander wagwoorde gereeld.
Wagwoorde behoort nie net sterk te wees nie, maar behoort ook van tyd tot tyd verander te word. Sonder die gebruik van ’n wagwoordbestuurder sal dit 'n omslagtige en moeilike taak wees wat mense baie maklik ter syde sal stel, maar met die gebruik van 'n wagwoordbestuurder word die taak makliker gemaak.

- Wagwoord bestuurder programme.

Die aanbeveling vanaf Infokerk is dat elke gebruiker van die elektroniese data ’n Wagwoord bestuurder sagteware program begin gebruik op al die toestelle. Die Nakomingsbeampte sal dit moet kontroleer by almal.

- Enkripsie van hardeskywe.

Hierdie aksie word ook sterk aanbeveel om te oorweeg dat alle rekenaar hardeskywe wat die onderskeie data op het, ook met ’n Enkripsie sagteware program enkripteer word om die data en inhou van die hardeskywe so te beskerm. Die Nakomingsbeampte sal dit moet kontroleer by almal.

- Enkripsie van lêers.

Indien die Enkripsie van hardeskywe nie moontlik gaan wees nie, kan ook oorweeg word die leërs op die rekenaar te enkripteer en so te beskerm en steeds gemaklik binne die wet te kan funksioneer. Dit is nie nodig om al die leërs / dokumente op ’n rekenaar so te hanteer nie, sleg die wat persoonlike inligting van mense bevat. Die Nakomingsbeampte sal dit moet kontroleer by almal.

C. RETENSIE.

Die wet vereis dat data van datasubjekte / lidmate nie langer gestoor mag word as die oorspronklike oogmerk waarvoor dit ingesamel was nie. Daar is egter ook 'n aantal uitsonderings soos in Artikel 14 (1) en (2) van die wet:
1. Gemeentelike werksaamhede:
Die wet noem duidelik in Artikel 14(1)(b) dat indien die verantwoordelike party die rekords redelikerwys benodig vir regmatige oogmerke wat met daardie verantwoordelike party se werksaamhede of aktiwiteite verband hou dan mag dit langer bewaar word. (Dit is wel nodig om lidmate wat nie meer lede is nie, wel in ’n argief te behou en word ook so deur die GKSA Admin Buro vereis, veral as dit handel oor die uitreik van attestate.)
2. Historiese, statistiese of navorsingsoogmerke:
Artikel 14(2) noem dat as rekords van persoonlike inligting vir historiese, statistiese of navorsingsoogmerke benodig word, dit vir langer tydperke as die waarvoor dit oorspronklik ingesamel was, gehou mag word, indien die verantwoordelike party geskikte voorsorgmaatreëls teen die gebruik van die rekords vir enige ander oogmerke ingestel het.
3. Anatomy (Lidmaatdatabasis):

Die Anatomy program is juis sodanig ontwerp, dat gebruikers van die program outomaties aan die vereistes van Artikel 14 van die wet voldoen. Die hele argiveringsproses waardeur die gebruiker geneem word wanneer 'n lidmaat verwyder moet word, maak seker dat slegs 'n persoon wat as "lidmaat" geklassifiseer is, oorgeplaas kan word na 'n ander gemeente of kerk. Persone wat nie as "lidmate" geklassifiseer word nie, kan nie oorgeplaas word nie, en word net van die stelsel verwyder. Die inligting van sodanige persoon is onherroeplik verwyder. Die argiveringsproses is dus 100% in lyn met Artikel 14 (2).

4. Rugsteun Kopieë:

Ou rugsteun kopieë wat op eksterne hardeskywe of geheue stokkies geberg word, behoort ook van tyd tot tyd verwyder te word. ’n Goeie praktyk sou wees dat die POPI Nakomingsbeampte saam met die inligtingsbeamptes 'n skedule moet opstel waarvolgens alle rugsteun kopieë elke einde van die boekjaar nagegaan moet word en ou inligting wat nie meer benodig word nie vernietig moet word. Sien ook die volgende hoofstuk oor "Data vernietiging".

5. Elektroniese dokumente wat aan amptenare voorsien was:

Dit is 'n goeie praktyk om enige elektroniese dokumente wat aan derde partye voorsien was, onmiddellik nadat dit die ontvanger bereik het, te vernietig. Sodanige inligting sou in elk geval baie vinnig verouderd raak as dit net iewers op die hardeskyf gestoor word. Indien ou inligting nie vernietig word nie, is dit nie in lyn met die POPI wet nie, en dit mors ook spasie op die hardeskyf.

6. Harde Kopieë:

Harde kopieë behoort ook op 'n baie gereelde basis nagegaan te word om te verseker dat dit nie verouderde inligting bevat nie. Die POPI Nakomingsbeampte saam met die inligtingsbeamptes van die gemeente behoort in die inligtingshandleiding 'n beleid voor te skryf hoe daar met ou harde kopieë te werk gegaan moet word wat betref die tydsduur wat dit behou moet word. Sien ook die hoofstuk oor datavernietiging.

7. Argief voorskrifte:

Dit is baie belangrik om daarop te let dat daar wel ander dokumente is wat nie persoonlike inligting van lidmate bevat nie, en waarvan die bewaringstydperke deur die argief voorgeskryf word. Sommige sodanige dokumente moet in harde kopie formaat wees en mag nooit vernietig word nie, en ander dokumente moet vir tydperke wat wissel tussen 1 jaar en 15 jaar bewaar word. (GKSA kerkargief sal hieroor geraadpleeg moet word.)

D. VERNIETIGING.

Die POPI Nakomingsbeampte saam met die inligtingsbeamptes van die gemeente, moet aandag gee aan die vernietiging van elektroniese data sowel as inligting wat op harde kopieë voorkom en 'n data-vernietigingsbeleid opstel en implementeer. In hierdie beleid sal die volgende uiteengesit moet word:

a.) Prosedures en metodes hoe die Elektroniese inligting van hardeskywe verwyder moet word. (Onthou dat Data nie noodwendig verwyder is as die “delete” of formateringsfunksies gebruik is nie. ’n Baie meer deeglike metode sal gevolg moet word soos om Digitale sanitasie toe te pas of die fisiese vernietiging van die hardeware.)

b) Prosedures en metodes hoe die harde kopieë, (dus op papier), vernietig moet word. Versnippering daarvan gaan dus die beste werk, maar die gehalte en die toerusting wat hiervoor benodig gaan word, gaan ook bepaal en gevolglik aangekoop moet word.

E. BEWUSMAKING VAN PERSONEEL.

Alle personeel en gevolmagtigdes wat met die data gaan werk moet gereeld heropgelei word in die vereistes van die wetgewing.

BELEID: VEILIGHEIDS-VOORSORGMAATREëLS

BERGING

- Dat alle lidmaat informasie as data op een sentrale rekenaar in die Kerkkantoor, op databasis sagteware gelaai mag word. Die Kerkkantoor admin personeel sal ook dien as die enigste gevolmagtigdes om die data te wysig daarin.
- Dat daar wel ander elektroniese toestelle daaraan gekoppel mag word vir data onttrekking, deur vooraf goedgekeurde proses aan personeellede of ander funksionarisse / amptenare. (Die Nakomingsbeampte moet altyd op hoogte gehou word van enige verandering wat hier sou plaasvind)
- ’n Register moet gehou word in die Kerkkantoor van al bg. persone en watter tipe toegang hulle het.
- Elke toestel / gebruiker moet voorsien word van sy eie unieke gebruikersname en wagwoorde om in die stelsel in te teken.
- Elke verbruiker daarvan moet ook ’n onderneming onderteken dat hulle die data sal beskerm en nie wederregtelik sal versprei nie.
- Data mag in harde kopieë, (papier), uitgedruk en gehou word, maar moet sover moontlik beperk word:
    - Alle harde kopieë moet genommer word en op ’n register aangeteken word.
    - Sodra hierdie kopieë nie meer gebruik word nie, moet dit ingehandig word by die Kerkkantoor vir vernietiging.
    - Nuwe Lidmaat aansoekvorms en Debietorder aansoekvorms mag wel geberg word, maar moet voldoen aan die beveiligings maatreëls soos genoem.
- Lidmate se inligting mag ook op / in die volgende sagteware en hardeware gestoor word:
    - Finansiële sagteware.

  Om die lidmate se finansiële bydraes te boekstaaf en vanaf te bestuur en word slegs op die kantoorbestuurder se rekenaar gelaai. Beskerming hiervoor moet in plek wees. Sowel as vir die boekhouding en die personeel salarisuitbetalings.
    - Anatomy.
    - E-Pos programme.

  Lidmate se inligting asook ander datasubjekte se inligting soos bv. Klassis predikante, of Sinodale amptenare, of diensverskaffers ens., mag in e-pos programme gestoor word. Mits dit voldoende beveilig word.
    - Microsoft Word, Excel, PDF lêers en ander dokumente.

  Lidmate se inligting mag op rekenaars / ander elektroniese toestelle, in die verskillende elektroniese formate gestoor word. Mits dit ook voldoende beveilig word. (Die Kerkkantoor en ander verantwoordelike persone sal ook hierop moet begin let om dit te verminder, te beskerm of te vernietig wanneer die doel daarvan bereik is.) Dit mag ook harde kopieë gestoor word, maar dit sal streng beheer moet word en geberg word in kluise, lessenaarlaaie of kabinette wat gesluit kan word.
    - Gemeentelike webwerwe.

  Enige plasing(s) van lidmate se inligting op die gemeente se webblad mag slegs met uitdruklike goedkeuring van die lidmaat of lidmate gedoen word. (Die Kerkkantoor en webmeesters sal ook hierop moet begin let om dit te verminder of om die nodige toestemming te verkry.)
    - Sosiale media. (Veral WhatsApp)

  Sosiale media mag gebruik word, maar sal ook daaraan onderworpe wees dat lidmate se toestemming eers verkry moet word voordat hulle op die groep bygevoeg word. (Die kerkkantoor sal hierop moet konsentreer om eers die nodige toestemming te kry vir die skep van groepe en hele gemeente sal hieroor ingelig moet word.)
    - Selfone.

  Lidmate se inligting mag op selfone gestoor word. Die verantwoordelike persone moet verseker dat genoegsame beskerming op die selfoon is.

BELEID: VEILIGHEIDS-VOORSORGMAATREëLS (vervolg)

BEVEILIGING

- Dat die fisiese sekuriteit by die Kantore altyd gemonitor sal word om te bepaal of dit nog voldoende te wees.
- Elektroniese Sekuriteit, van alle elektroniese toestelle wat lidmaat inligting bevat, moet in plek gestel word met die volgende:
    - Alle toestelle en sagteware moet van sterk wagwoorde voorsien word.
    - Enkripsie van hardeskywe en / of lêers moet op alle elektroniese toerusting wat data berg, installeer en geïmplementeer word. Dit sal van toepassing wees op elke Laptops , Desktop rekenaars, Eksterne hardeskywe en Flash Drives. (Geheuestokkies)
    - Bg. sal insluit dat daar op elke toestel ’n goeie opgedateerde antivirusprogram gelaai moet word.

RETENSIE

- Dat data gehou mag word, maar dat data van lidmate nie langer gestoor mag word as die oorspronklike oogmerk waarvoor dit ingesamel was nie.
- Vir die doel van die argief sal die volgende inligting wel gehou word:
    - Nuwe lidmaat aansoek vorms en attestate ontvang.
    - Attestate uitgereik vir lidmate wat vertrek het.

VERNIETIGING

- Dat daar ’n beleid met prosedures en riglyne opgestel moet word om die bestuur van die van uitgediende data in elektroniese en harde kopie formaat se metodes van vernietig bepaal kan word.
- Bg. beleid moet die Prosedures en metodes insluit hoe die Elektroniese inligting van hardeskywe verwyder moet word.
- Bg. beleid moet die Prosedures en metodes insluit hoe die harde kopieë, (dus op papier), vernietig moet word.

BEWUSMAKING VAN PERSONEEL

- Dat almal wat met die betrokke data van die gemeente gaan werk, moet gereeld daaraan herinner word dat hulle almal ’n verantwoordelikheid het in die hantering van die betrokke data en dan veral ook die vernietig daarvan wanneer dit nie meer gebruik word nie.
- Gereelde opleiding en besprekings hieroor gehou sal word.

9. DEELNAME DEUR DIE LEDE / DATASUBJEK:

Lidmate mag, met verskaffing van bewys van identiteit, ter eniger tyd vra dat die kerk bevestig dat dit ook persoonlike inligting beskik asook watter inligting dit is. Lidmate mag vra dat inligting reggestel moet word.

BELEID: DEELNAME DEUR LIDMATE

- Dat die Kerkkantoor enige navraag gepaardgaande die POPI wetgewing, asook vanaf lidmate rakende die Lidmate se besonderhede wat geberg word, sal hanteer.
- Dat die lidmate ook gereeld bewus gemaak moet word van die uitwerking en gevolge van die POPI wetgewing en hulle rol daar binne.

Goedgekeur deur:  **Datum: 29 Junie 2021**

Bylaag A: Gids vir die opstel van 'n POPI Prosedure Handleiding

Die opstellers van die Gemeente se POPI prosedurehandleiding moet die volgende in ag neem hiervoor en moet die gemeente se privaatheidsbeleid uitspel ten opsigte van:

1. Data Insameling:

Alles rakende die tipe inligting wat versamel word, sowel as die verskillende tipe metodes wat hiervoor gebruik word, moet in die handleiding beskryf word. (Indien dit op papier geskryf word moet ook verseker kan word dat dit nie in verkeerde hande kan land na voltooiing daarvan nie.)

   a. Tipe data
   b. Doel waarvoor data benodig word
   c. Toestemming van lidmate
   d. Minimalistiese berging
   e. Deursigtigheid
   f. Toegang tot data

2. Data gebruik en beperkings:

Dit moet in die handleiding beskryf word hoe die data gebruik gaan word. Veral dan ook "Hoe" word die data gedeel:

   a. Met wie deel ons dit?
   b. Waarop deel ons dit?
   c. Watter spesifieke data, (bv. Adresse, telefoon nrs, ens.), word gedeel / versprei?

(Dit behoort genoem te word dat dit aangewend word vir die interne funksionering van die gemeente en dat dit met geen ongemagtigde persone buite die gemeente gedeel sal word nie.)

3. Data Berging:

Een van die belangrikste onderafdelings van die handleiding moet die hoofstuk oor die berging van data wees. "Hoe" en "Waar" word die data geberg? Beskryf in die handleiding of dit op 'n rekenaar geberg word, en of dit op papier geberg word? Lys ook al die plekke waar dit gaan wees. (Bv. Leraars, ander personeel, leiers, verskeie funksionarisse, vrywilligers, ens.)

4. Data Beveiliging:

Bespreek volledig in die handleiding die metodes van data beveiliging word, met in ag genome ook vir elke van bg. bergings plekke, met verwysing na die onderstaande twee punte:

   a. Fisiese Sekuriteit
   b. Elektroniese Sekuriteit

5. Data Retensie:
   a. Hoe lank moet data gehou word.
   b. Die meeste van die inligting word geberg solank as die lidmaat in die gemeente is.
   c. Argief inligting vir navorsings- en statistiese doeleindes word onbeperk gestoor. Sodanige inligting hoef slegs in die kerk se Argief register gestoor te word.
   d. Ander inligting moet direk nadat dit nie meer benodig word nie, vernietig word.

6. Data Vernietiging:

Die handleiding moet volledig beskryf hoe data vernietig moet word. Dit geld vir elektroniese sowel as papier dokumente. Selfs die hardeware van rekenaar wat nie meer gebruik gaan word vir die doel daarvoor nie, moet daar beleid voor wees oor die metodes van die vernietiging daarvan op die regte manier.

7. Personeel bewustheidsopleiding:

Die detail, frekwensie en tipe opleiding van die betaalde personeel, maar ook almal (Lidmate) wat met die data bemoei gaan wees, se opleiding moet ook hierin uiteengesit word. Veral ook nuwe gebruikers wat elke

keer by kom. Dus die aanvanklike opleiding na die goedkeuring van hierdie beleid, maar ook hoe die voortgaande opleiding daarna gedoen moet word.

8. Publisering van die handleiding:

Wanneer dit die eerste keer publiseer gaan word en waar dit daarna beskikbaar gestel gaan word.