NEDERDUITSE GEREFORMEERDE KERK
Een Liggaam en Een Gees

POPIA HANDLEIDING VAN DIE NG GEMEENTE DOMUS DEI RANDBURG-SUID ('die Gemeente')

WET OP BESKERMING VAN PERSOONLIKE INLIGTING

WET NO.4 VAN 2013

PROTECTION OF PERSONAL INFORMATION

ACT 4 OF 2013

POPIA HANDLEIDING VIR DIE NG GEMEENTE

DOMUS DEI RANDBURG SUID

INLIGTINSREGULEERDER	Adv Pansy Tlakula	JD House Stiemensstraat 27 Braamfontein Johannesburg Posbus 31533 Braamfontein Johannesburg 2017 info@justice.gov.za
HOOFINLIGTINGSBEAMPTE	Dr Gustav Claassen	Posbus 13528 Hatfield 0028 Tel 012 342 0092 info@ngkerk.org.za gensecdrc@ngkerk.org.za
ADJUNKINLIGTINGSBEAMPTE	Dr Andrew Kok	NG Kerk Argief Noordwal-Wes 1 Stellenbosch Posbus 34 Stellenbosch 7599 021 882 9923 argief@kaapkerk.co.za
GEMEENTE INLIGTINGSBEAMPTE	Esti Esterhuizen	Domus Dei Randburg Suid Jeanweg 30 Blairgowrie Tel 011 787 4004 072 367 4739 kantoor@domusdei.co.za

INLEIDING

WET OP BESKERMING VAN PEROONLIKE INLIGTING, No. 4 van 2013

('die Wet')

Oorsig van die Wet

1. Doel van die Wet

Ter bevordering van die beskerming van persoonlike inligting wat deur openbare en privaatliggame geprosesseer word.

Dit beteken dat:

- Sekere voorwaardes daargestel word ten einde minimum vereistes vir die prosessering van persoonlike inligting te vestig;
- Die Wet voorsiening maak vir die instelling van 'n Inligtingsreguleerder om sekere bevoegdhede uit te oefen en om sekere pligte en werksaamhede ingevolge hierdie Wet en die Wet op die Bevordering van Toegang tot Inligting, 2000, te verrig;
- Die Wet voorsiening te maak vir die uitreiking van gedragkodes;
- Die Wet voorsiening maak vir die regte van persone met betrekking tot ongeoorloofde elektroniese kommunikasie en geoutomatiseerde besluitneming;
- Die Wet die vloei van persoonlike inligting oor die grense van die Republiek reguleer;
- En dat die Wet voorsiening maak vir aangeleenthede wat daarmee in verband staan.

Die Wet verleen erkenning aan –

- Artikel 14 van die Grondwet van die Republiek van Suid-Afrika, 1996, wat voorsiening maak dat elke persoon die reg op privaatheid het;
- Die reg op privaatheid asook die reg op die beskerming teen onregmatige insameling, behoud (berging), verspreiding en gebruik van persoonlike inligting behels;
- Die feit dat die Staat die regte in die Handves van Menseregte moet eerbiedig, beskerm, bevorder en verwesentlik.

Die Wet is verder opgestel gedagtig daaraan dat –

- In ooreenstemming met die grondwetlike waardes van demokrasie en openheid, die noodsaaklikheid vir ekonomiese en sosiale vooruitgang, binne die raamwerk van die inligtingsamelewing, vereis dat onnodige struikelblokke ten opsigte van die vrye vloei van inligting, met inbegrip van persoonlike inligting, verwyder word.

Ten einde –

- Die prosessering van persoonlike inligting deur openbare en privaat liggame te reguleer, in harmonie met internasionale standaarde, op 'n wyse wat gevolg gee aan die reg op privaatheid onderhewig aan regverdigbare beperkings wat daarop gemik is om ander regte en belangrike belange te beskerm

2. Hooftrekke van die Wet

Die Wet is in November 2013 onderteken en gedeeltes het in werking getree in April 2014. In Desember 2016 is die Inligtingsreguleerder aangestel. Die res van die regulasies het op 1 Julie 2020 in werking getree en organisasies (soos bv gemeentes / sinodes) moet teen 30 Junie 2021 aan alle wetlike vereistes voldoen.

In die omgangstaal word verwys na die wet as **POPIA** en ons sal deurgaans die afkorting gebruik .

2.1 Wie moet voldoen aan POPIA?

POPIA is van toepassing op enige instansie, maatskappy of organisasie wat op een of ander wyse persoonlike inligting prosesseer. Die Wet geld dus vir openbare liggame (bv. Binnelandse Sake, SAID) en privaat instansies (bv. finansiële instellings; gesondheidsorg instansies; besighede; direkte bemarkers; asook kerke).

Die Wet is dus van toepassing op gemeentes, ringe, sinodale en ander kerklike instansies wat op een of ander wyse persoonlike inligting hanteer. Gemeentes wat ander bedrywighede (bv. 'n kleuterskool of ouetehuis) bedryf moet ook daarvan bewus wees dat die persoonlike inligting van daardie mense en personeel ook onder POPIA val. Dit moet in gedagte gehou word dat enige inligting wat 'n gemeente van minderjarige kinders berg, die vooraf toestemming van ouers verg.

2.2 Wat beteken die prosessering van data / inligting?

Die prosessering van inligting word baie wyd deur die Wet gedefinieer. In terme van POPIA beteken prosessering van inligting enige aksie of aktiwiteit (meganies, outomaties of elektronies) wat die volgende insluit, maar nie daartoe beperk is nie:

Versameling, ontvangs, opname, organisering, berging, opdatering, herwinning verspreiding, samesmelting, vernietiging en uitwissing van data.

Die beskerming van persoonlike inligting is nou meer as ooit noodsaaklik omdat die ontwikkeling van die elektronika die risiko nog groter maak dat dit misbruik kan word en mense se privaatheid geskend kan word.

2.3 Kan kerke steeds data insamel en prosesseer?

Die Wet verbeid niemand om enige persoonlike inligting in te samel en daarmee te handel nie. POPIA skryf net die regmatige handelinge voor om persone te beskerm. Die Wet help om data op die korrekte wyse te prosesseer sonder om vervolging te vrees.

Daarom moet die voldoening aan die vereistes van die Wet nie as las beskou word nie, maar werk dit mee om individue, ander persone en die kerk te beskerm.

2.4 Wat word beskou as persoonlike inligting?

Uit die onderstaande lys van tipes persoonlike inligting is dit duidelik dat kerklike kantore oor baie persoonlike inligting van lidmate beskik en derhalwe moet daar met sorg daarmee omgegaan word. Hierdie lys dui op die mees algemene inligting waaroor kerkkantore beskik, maar is nie volledig nie.

- Identiteitsnommers / paspoortnommers
- Geboortedatums / ouderdomme
- Telefoonnommers
- E-posadresse
- Fisiese adresse
- Geslag, ras en etniese oorspring
- Foto’s, stemopnames, video-opnames (ook CCTV), biometriese data
- Huwelikstatus en familieverwantskappe
- Kriminele rekords
- Private korrespondensie
- Godsdienstige en filosofiese oortuigings en politieke opinies
- Indiensnemingsrekords en vergoedingsinligting
- Finansiële inligting
- Opvoedkundige inligting
- Fisiese en psigiese gesondheidsinligting, mediese geskiedenis, bloedgroep en seksualiteit

- Lidmaatskap van verenigings en organisasies

Nota: Neem asseblief kennis dat hierdie inligting net van lewendige persone versamel, geberg en gebruik moet word. Inligting wat van persone geberg word wat oorlede is, moet vernietig word (vergelyk voorwaarde 7).

2.5 Hoe kan daar aan POPIA se vereistes voldoen word?

Elke gemeente of kerklike instansie moet aan die volgende aandag gee:

- Die gemeente moet ’n bewusmakingsprogram saamstel en volg
- ’n POPIA handleiding moet opgestel word
- ’n Inligtingsbeampte moet aangestel word om toe te sien dat daar aan die eise van die Wet voldoen word
- Lidmate moet toestemming aan die kerk- of sinodale kantoor verleen om persoonlike data te prosesseer

2.6 Wat gebeur as daar nie voldoen word aan die wet nie?

Die Wet bepaal dat daar ’n maksimum boete van tot en met R 10 miljoen opgelê kan word indien ’n verantwoordelike party nie uitvoering gee aan die bepalings van die Wet nie. Datasubjekte het die reg om ’n regsaksies teen die verantwoordelike party in te stel en dit sou selfs moontlik wees dat, onder sekere omstandighede, die Inligtingsbeampte gevangenisskap opgelê kan word

2.7 Voorwaardes vir voldoening aan die Wet?

Verder voorsien die Wet agt (8) voorwaardes waaraan voldoen moet word om persoonlike inligting wettig in te samel, te verwerk, te berg en te gebruik.

Hierdie voorwaardes sal in die volgende hoofstukke bespreek word:

1. Verantwoordingspligtigheid (accountibility)
2. Beperkte prosessering (processing limitation)
3. Oogmerkspesfikasie (purpose spesific)
4. Beperkte verdere prosessering (further processing limitation)

5. Inligtingsgehalte (information quality)
6. Openheid (openness)
7. Veiligheidsvoorsorgmaatreëls (security safeguards)
8. Deelname deur “datasubjek”*

_____

*“datasubjek” – die persoon op wie persoonlike inligting betrekking het

VOORWAARDE 1: VERANTWOORDINGSPLIGTIGHEID

Laai eerstens die Wet af (Afrikaans)

Wet_2013_4.pdf

Die POPI Inligtingsbeampte is verantwoordelik is vir die insameling, bewaring en gebruik van lidmate se inligting.

1.1 POPIA INLIGTINGSBEAMPTE

Elke gemeente of kerklike instansie moet 'n Inligtingsbeampte aanstel soos uiteengesit in die Wet, artikel 55.

Die Inligtingsbeampte van die NG Gemeente Domus Dei Randburg-Suid is Esti Esterhuizen (of enige opvolger wat deur die Kerkraad vir die doel aangestel word).

Die verantwoordelikhede van die Inligtingsbeampte sluit die volgende in:

- Aanmoediging tot voldoening, deur die instansie, aan die voorwaardes vir die regmatige prosessering van persoonlike inligting;
- Die hantering van versoeke wat ooreenkomstig hierdie Wet aan die liggaam (die Gemeente) gerig word;
- Om met die Reguleerder saam te werk in verband met ondersoeke wat ooreenstem met Hoofstuk 6 met betrekking tot die instansie gedoen word;
- Om andersins, voldoening deur die instansie aan die bepalings van hierdie Wet te verseker;
- Ander verantwoordelikhede soos wat voorgeskryf mag word van tyd to tyd.

Artikel 55 (2) dat die Inligtingsbeampte slegs sy / haar werksaamhede ingevolge hierdie Wet mag opneem nadat die verantwoordelike party hulle by die Reguleerder geregistreer het.

Naas die Wet (artikel 55) moet die Inligtingsbeampte ook aan die volgende bykomende vereistes voldoen (Regulasie in Staatskoerant van 14 Desember 2018):

- 'n Voldoeningsraamwerk ontwikkel, implementeer, monitor en onderhou;
- 'n Persoonlike inligtingsimpakassessering doen 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, monitor, onderhou en beskikbaar stel soos in artikel 11 en 51 van die wet op die Bevordering van Toegang tot Inligting, 2000 voorgeskryf

- Interne maatreëls ontwikkel tesame met voldoende stelsels om versoeke om inligting of toegang te verwerk;
- Die fasilitering van interne bewustheidsessies oor: die bepaling van die Wet; regulasies ingevolge die Wet uitgevaardig; en gedragskodes of inligting van die Reguleerder af verkry;

Die Inligtingsbeampte moet in oorleg met die Kerkraad ’n Inligtingsbeleid saamstel.

Die doel van die hierdie handleiding is om die Gemeente se privaatheidsbeleid uit te spel tov:

a. <u>Data insameling</u> (Maw hoe gaan die data ingesamel word in ons gemeente) ten opsgite van:

i Tipe data

Die tipe data wat ingesamel sal word van lidmate is soos aangedui op die nuwe intrekkersvorm (“Sensusvorm”). Hierdie vorm is beskikbaar op ons webblad en is ook hierby aangeheg. Hierdie vorm kan vooraf uitgedruk word en voltooi word deur lede tydens besoeke vanaf kerkraadslede / dominee. Die vorm is ook in die kerkgebou / kantoor beskikbaar waar lidmate dit kan kom voltooi. Elektroniese vorms is ook beskikbaar en is baie meer vertroulik. Lidmate kan dit na die kerkkantoor toe teruggestuur dmv ‘n epos, of dit kan op die webblad voltooi word. Debietorder vorms kan ook apart ingevul word en is ook elektronies beskikbaar op die webblad. Op hierdie wyse gee lidmate instemming dat hulle inligting versamel, geberg en gebruik mag word. Ouers gee ook toestemming op die Sensusvorm dat inligting van minderjariges hanteer mag word. Indien wysigings van inligting verkry word vanaf die lidmate (datasubjekte) sal die Inligtingsbeampte die nodige verandering aanbring op die databasis en dan die vorms vernietig indien nodig. Hierdie vorm word slegs deur die kantoorpersoneel hanteer.

ii Doel waarvoor die data ingesamel word

Die doel van data insameling is om nuwe lidmate se inligting op ons databasis te plaas vir interne funksionering van ons gemeente. Hierdie inligting word slegs gebruik deur die leraar, jeugwerker, kantoorbestuurder en kerkraadslede. Hierdie inlgting sluit die volgende in: verjaarsdagdatums en huweliksdatums (vir gelukwensing), adresse vir huis besoeke, ens.

iii Toestemming van datasubjek (lidmate)

Wanneer lidmate die Sensusvorm voltooi moet hulle teken by "Toestemming van Lidmaat" dat hy / sy toestemming gee dat die gemeente hulle inligting mag stoor in die Winkerk program vir solank as wat die gemeente of sinode die inligting benodig. Verder gee lidmate ook toestemming dat hulle minderjarige kind(ers) se inligting op die keersy van hierdie dokument onder dieselfde voorwaardes gestoor/gebruik mag word.

iv Berging van data

Lidmate se data word geberg in die kerkkantoor, die kluis in die kerkkantoor asook op die rekenaar / personeel se skootrekenaars. Dit word ook op harde kopie asook elektronies geberg.

b. Data gebruik en beperkings (Maw hoe gaan ons die data deel)

Ons data word elektronies asook op papier gedeel. Data word gedeel met die predikant, jeugleier asook gemeenteraadslede wat besoeke doen aan lidmate. Die data wat gedeel word is naam, van, adres, telefoonnommer, epos, ID.(verwys na die Sensusvorm). Hierdie data word gedeel dmv eposse, asook harde kopieë. Hierdie inligting mag met geen ongemagtigde persone buite die gemeente gedeel word, sonder die datasubjek se toestemming nie.

c. Data beveiliging (Maw die metodes/manier hoe data beveilig word bv fisiese sekuriteit en elektroniese sekuriteit)

Fisiese sekuriteit: Data word beveilig in die kerkkantoor wat sekuriteitshekke het.
Elektroniese sekuriteit: Personeel se rekenaars / skootrekenaars waar toegang tot die inligting met wagwoorde en sekuriteitskodes beheer word.

d. Data retensie (Maw hoe lank moet data gehou word)

Inligting word geberg solank die lidmaat in die gemeente is. Argiefinligting word geberg slegs vir navorsing. Statistiese-inligting / navorsingsinligting word vir 'n onbeperkte tyd gestoor. Sodanige inligting hoef slegs in Winkerk se argief register gestoor te word. (Sien lys aangeheg vanaf Argief kantoor ontvang vir bewaring van inligting.)

e. Data vernietiging (Beskryf volledig hoe die onbenutte en/of verouderde data vernietig gaan word)

Vernietiging van Harde kopie wat nie meer benodig word/verval - Word versnipper.
Elektroniese rekords – Moet vanaf die rekenaar / skootrekenaar verwyder word (insluitend vanuit die betrokke herwinningsmandjie (recycle bin).

Hardeware (bv ou rekenaars wat nie meer gebruik word nie) se harde skywe moet vernietig word of behoorlike uitgevee word (wiped) dat dit nie weer herwin kan word nie.

f. Personeelbewustheidsopleiding

Sodra die inligtingbeampte die inligtingsbeleid en prosedure handleiding gefinaliseer het, moet alle personeellede wat op een of ander wyse van die data gebruik maak opleiding ontvang om hulle bewus te maak van die vereistes van die Wet en hoe daar voortaan met data gewerk gaan word. Voortgaande opleiding sal ook gedoen word met die aanstel van nuwe personeel.

Wie moet almal opgelei word:
Betaalde amptenare
Kerkraadslede wat met die data gaan werk

g. Publisering van die handleiding
Die handleiding is beskikbaar op ons webblad.

VOORWAARDE 2: BEPERKTE PROSESSERING

Artikels 9-12 van die Wet handel oor beperkte prosessering.

Daar is 4 hoekstene vir beperkte prosessering:

A Redelike wyse

B Minimalistiese inligting

C Toestemming van lidmaat

D Direk vanaf lidmaat

Op die Sensusvorm is daar net sekere basiesiese inligting wat verskyn. Daar is wel ekstra inligting wat die gemeente mag benodig soos bv bankbesonderhede, mediese inligting of ander kerklike inligting wat nie op die Sensusvorm verskryn nie. In die geval waar ‘n lidmaat ‘n debietorder wil teken, is daar ‘n aparte vorm wat voltooi moet word en teruggestuur moet word na die kantoor. Op hierdie vorm teken die lidmaat ook dat hy toestemming gee dat ons sy bankbesonderhede mag stoor. Wanneer daar ‘n Sondagskooluitstappie is, is die mediese inligting nodig vir in geval van nood. Dis nie nodig om alle mediese kondisies te stoor nie, slegs dit wat van toepassing is. Jaarliks moet ons lidmaatbewegins aan die Sinode stuur met die nodige inligting. Ons kan ook op die attestate wat ons aanstuur na ander gemeentes aantoon dat die persoon op die kerkraad was. Dit is belangrik vir die ander gemeente om dit te weet.

VOORWAARDE 3: OOGMERKSPESIFIKASIE

Inligting moet versamel word vir ‘n spesifieke oogmerk wat verband hou met ‘n werksaamheid van die instansie.

1. Watter inligting van lidmate ingesamel gaan word soos bv.:
    a. Persoonlike inligting bv.: volle name, van, geboortedatum en identiteitsnommer
    b. Adresbesonderhede bv.: woon- en posadres
    c. Kontakbesonderhede bv.: telefoon, en selfoonnommers; epos adresse
    d. Ander inligting bv.: geslag, taalvoorkeur, beroep
    e. Finansiële inligting, bv.: bankbesonderhede

2. Bepaling van doeleindes waarvoor die inligting gebruik gaan word
    -Epos adresse word gebruik tov kommunikasie.
    -Huweliksdatum word gebruik tov gelukwensing of dalk huweliksverrykingsseminare. Geboortedatums word gebruik vir gelukwensing van verjaarsdae.
    -Alle inligting wat ons dus bymekaar maak kan ons motiveer

VOORWAARDE 4: BEPERKTE VERDERE PROSESSERING

Wie kry tans toegang tot die data?

1. Kerkkantoor personeel

   Administratiewe/finansiële personeel kan toegang kry tot die data. Hulle werk dag tot dag met lidmate se data. Die minimalistiese beginsel moet nogsteeds toegepas word. Slegs een gebruiker, die "meester gebruiker" moet aangestel word om toegang tot Winkerk 7 om data te kan laai en te wysig. Hierdie "meester gebruiker" is die enigste gebruiker wat ander gebruikers se regte kan verander. Hierdie "ander" gebruikers het slegs beperkte toegang met beperkte regte. Hulle word ook verplig om 'n skerm te onderteken waarin hulle onderneem om die inligting van lidmate te beskerm en nie aan enige ongemagtigde persoon/instansies ooit sal bekend maak nie.

2. Predikant (slegs die minimum inligting bv Winkerk online, indien hulle meer inligting benodig kan dit aangevra word vanaf die inligtingsbeampte)

   Hoe word inligting aan predikante voorsien:

   -Harde kopieë. Wanneer harde kopieë voorsien word, moet dit genommerde kopieë wees. Die kerkkantoor moet rekord hou nadat dit nie meer nodig geword het of verouderd geword het en na die kerkkantoor moet terugkom om vernietig te word.

   -Elektronies. Wanneer elektroniese dokumente aangestuur word, is dit goed om dit met 'n wagwoord aan te stuur. Stuur die wagwoord apart aan deur 'n ander media bv sms/whatsapp.

3. Kerkraadslede

   Hulle het ook sekere data nodig vir die uitvoer van hulle pligte. Die data moet ook tot die minimum beperk word. Die riglyne soos vir predikante moet ook nagekom word. Die inligting moet beperk word tot hulle wyk of die kleingroep wat hulle bedien. Dis nie nodig dat hulle ander lidmate se inligting van 'n ander wyk hoef te he nie.

4. Jeugwerkers en Sondagskoolpersoneel

   Jeugwerker en sondagskool personeel het ook data van lidmate nodig, veral kinders. Hierdie inligting moet ook tot die minimum beperk word. Die riglyne soos vir predikante moet ook nagekom word. Dit is veral belangrik dat kinders se inligting tov die wet baie beperk moet word. Die wet vereis dat enige inligting van kinders deur die ouers goedgekeur/toestemming gegee moet word om te kan berg.

5. Lidmate

Lidmate is ook beperk om sekere inligting van ander lidmate te kan kry. Bv verjaarsdae. Hierdie inligting is nie net vir die gemeentelede sigbaar nie, maar ook vir die publiek. Dit is dus baie belangrik dat inligting wat gebruik/geplaas word in nuusbriewe, afkondigings, verjaarsdae, sms, webblaaie, whatsapp ens daar eers toestemming vooraf gekry moet word vanaf die lidmaat voordat dit geplaas kan word.

VOORWAARDE 5: INLIGTINGSGEHALTE

Die verantwoordelike party moet redelike stappe doen om te verseker dat die persoonlike inligting wat ingesamel word volledig, akkuraat, nie misleidend is nie en opgedateer moet word volgens artikel 16

VOORWAARDE 6: OPENHEID

Artikel 18 bepaal dat die verantwoordelike partye redelikerwys moet verseker dat die datasubjek bewus is dat inligting oor hom ingesamel is asook watter inligting.

Winkerk online is ‘n baie handige hulpmiddel. Lidmate kan registreer by Winkerk online en kan op hierdie manier sien wat se inligting die gemeente van hulle hou. Hulle kan ook dadelik ‘n versoek rig dat foutiewe inligting reggestel/opgedateer moet word.

VOORWAARDE 7: VEILIGHEIDSVOORSORGMAATREELS

Winkerk 7

Daar moet bepaal word op watter toestelle hierdie sagteware beskikbaar is bv tafelrekenaar, skootrekenaar, tablette en selfone. Die nodige sekuriteit moet in plek wees – nie net fisiese berging nie, maar ook toegang tot die elektroniese data.

Berging van data
Elektroniese berging:

1. Winkerk 7

   Winkerk 7 is ten volle POPI aanpasbaar. Gebruikers het elkeen hulle eie gebruikersnaam en wagwoord. Elke gebruiker wat vir die eerste keer aanteken in Winkerk online moet die POPPI gebruikersvoorwaarde skerm kry, en die voorwaardes aanvaar wat in die databasis ook gestoor word. Die rede hiervoor is om voorsiening te maak vir moontlike ondersoeke om vas te stel of ‘n spesifieke amptenaar data volgens die Wet hanteer het. So ‘n persoon kan dan nie sê dat hy / sy nie hiervan geweet het nie.

2. Kerkkantoor bv tafelrekenaar

3. Addisionele installasies

4. Admin personeel se persoonlike rekenaars

   Die inligingsbeampte moet weet op watter amptenare se persoonlike rekenaars die program gelaai word. Die POPPI inligtingsbeampte moet toesien dat die program daar onder baie streng voorwaardes en met die nodige veiligheidsprotokole in plek daar gebruik mag word.

   Indien die amptenaar nie meer in diens van die gemeente is nie / of benodig word nie, moet dit verwyder word van die amptenaar se rekenaar. Alle inligting van lidmate moet verwyder word van daardie rekenaar.

5. Predikante se persoonlike rekenaars

   Die POPI inligtingsbeampte moet toesien dat die program onder baie streng voorwaardes en met die nodige veiligheidsprotokole gebruik word. Indien die amptenaar nie meer in diens van die gemeente is nie / of benodig word nie, moet dit verwyder word van die amptenaar se rekenaar. Alle inligting van lidmate moet verwyder word van daardie rekenaar.

Ander programme

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

Elektroniese berging:

1. Finkerk

   Lidmate se inligting word net so oorgedra vanaf Winkerk 7 na Finkerk. Bankbesonderhede van lidmate kan ook in Finkerk gestoor word. Hier word ook ‘n wagwoord gebruik wat slegs aan enkele van Infokerk se personeellede bekend is.
   Die volgende persone kry toegang tot die Finkerk: Kerkantoor personeel; predikante; en ouditeure van die gemeente.

2. Winkerk online

   Data word ook in Winkerk online geberg. Enige gemeente kan aansoek doen by Winkerk online om toegang te kry wat backup buddy gebruik. Die gemeente doen aansoek en Infokerk gee dan toegang. Een amptenaar word toegang gegee tot Winkerk 7 se spesiale funksies waar amptenare wat aansoek doen by Winkerk online se goedkeuring gedoen kan word. ‘n Amptenaar wat dan toegang tot Winker online wil hê moet self op Winkerk online se webwerf ingaan en registreer. Hierdie inligting word dan deurgestuur na Winkerk 7 se program waarop die gemagtigde amptenaar dan op Winker 7 hierdie aansoek moet goedkeur.
   Daar is 3 soorte gebruiker wat toegang kan kry tot Winkerk online: Kerkkantoorpersoneel; predikante; jeugwerkers; lidmate (om verouderde inligting reg te stel / op te dateer). Die POPPI inligtingsbeampte moet weet wie almal toegang to Winkerk online het.

3. E-pos programme

   Persoonlike inligting van lidmate kan ook gestoor word in epos programme. Gemeentes gebruik gewoonlik Outlook. Daar moet geweet word waar die data van Outlook gestoor word. Dit word gestoor onder die “users folder” en die databasis se naam is Outlook.pst Die POPI beampte moet ook bewus wees van elke persoon wat in die gemeente epos programme gebruik en wat se inligting daar gestoor word. Ander gemeentes gebruik ook Gmail om hulle data in te stoor of eposse mee te doen. Daar is ook ander programme wat gebruik kan word. Daar moet geweet word waar hierdie data gestoor word en of dit veilig is. Baie gemeentes versamel inligting in word/excel. Winkerk 7 kan ook verskillende verslae uitvoer na MS Word / Excel / PDF.
   Persoonlike inligting van lidmate kan ook op ander platforms gestoor word. Bv sosial media, gemeentelike webwerwe en selfone

4. Microsoft Excel en Word

5. PDF leêrs en ander dokumente

6. Gemeentelike webwerwe
7. Sosiale media
8. Selfone
9. Harde kopieë

   Die POPI inligtingsbeampte moet ook weet waar harde kopieë geberg word, bv lessenaar laaie, liasseerkabinette of self buite die kantoor.

<u>Fisiese sekuriteit</u>

Daar moet aandag gegee aan die fisiese en elektroniese beveiliging van persoonlike inligting.

Fisiese sekuriteit: Ten opsigte van die fisiese beveiliging van die gebou waar persoonlike inligting in papier en elektroniese formaat geberg word moet verseker word dat die volgende in plek is:

- Brandkluis: Verkieslik ’n instapkluis wat groot genoeg is om registers en ook rekenaartoerusting in te berg wanneer nie in gebruik is nie.
- Diefwering en / of veiligheidshekke: voor alle vensters en deure wat na buite oopmaak.
- Alarmstelsel: verkieslik ’n alarmstelsel wat gekoppel is aan ’n reaksie-eenheid
- Sekuriteitskameras: waar moontlik ’n kamera-stelsel sodat toegang tot die terrein en gebou gemonitor kan word indien die gemeente se begroting dit toelaat.
- Van-terrein beveiliging: Maak seker dat die volgende in plek is:
  - Rekenaarhardeskywe (ekstern en geheuestokkies) veilig gestoor word
  - Skootrekenaars beveilig is en bewaar word.

<u>Beveiliging</u>

<u>Elektroniese sekuriteit</u>

Wagwoorde. Daar is verskillende soorte wagwoorde.

- Die wagwoord om in Windows aan te teken. Jy moet ‘n sterk wagwoord hê om in Windows in te kom.

- Die wagwoord om in Winkerk 7 aan te teken. Elke gebruiker moet sy of haar eie gebruikersnaam en wagwoord gebruik om in Winkerk 7 aan te teken. Die POPI beampte moet weet wie het almal toegang tot Winker online en wat is hulle sekuriteitsvlakke. Verskillende gebruikers kan verskillende

sekuriteitsvlakke hê. Dit beteken dat nie alle gebruikers alles hoef te sien wat in die data aangaan nie.

- Die wagwoord om Winkerk online te gebruik. Jy moet ook ‘n sterk wagwoord skep. Die word deur die gebruiker self opgestel. Dit kan ook verander word indien nodig op die winkerk online webwerf.

- Finkerk se wagwoorde. Daar is verskillende sekuriteitsvlakke net soos vir Winkerk. Gebruikers stel hulle eie wagwoorde op.

- Webwerwe se wagwoorde. Webwerwe vereis aanteken besonderhede. ‘n Goeie idee is om iets wat verband hou met die webwerf. Bv mybank/myabsa. 2de Idee is een baie sterk wagwoord vir alles 1q2w3e4r5t6y7u8i of iets soos asdfghijklm. 3de idee is wagwoord frases bv. ChristusOnsKoning. Hou net ingedagte moenie dieselfde rympie vir al jou webwerwe gebruik nie. ‘n Goeie idee is om ‘n wagwoordbestuurder te gebruik.

- E-pos programme wagwoorde. Dis ‘n goeie idee om ‘n wagwoord in jou epos programme in te sluit.

Goeie wagwoord praktyke:

- Verskillende wagwoorde – Moet nie dieselfde wagwoorde gebruik vir al jou programme/webwerwe nie. Moet nie vir jou “browser” die reg gee om jou gebruikersnaam / wagwoord te onthou nie. Sodoende verhoed mens dat ongemagtigde persone toegang tot jou webwerwe kry sonder dat jy beheer daaroor het.

- Sterk wagwoorde – Gebruik wagwoorde wat moeilik geraai kan word. Vermy wagwoorde waarin name, vanne, geboortedatums bevat. Vermy ook woorde wat die woord “password, wagwoord, admin, info, 123, abc” bevat. Moet nie jou wagwoorde op ‘n stukkie papier hou nie. ‘n Goeie metode is om ‘n dokument op jou rekenaar te stoor wat altyd beskikbaar is wanneer jy jou wagwoorde benodig. Indien jou rekenaar gesteel word kan jy wel die dokument verloor. Daar is verskillende maniere om sodanige dokument te beskerm. Tik al jou sterk wagwoorde in ‘n Word dokument en dan kan jy die word dokument met ‘n wagwoord beskerm. Daar is ook ander beter metodes wat gebruik kan word. Dit word genoem ‘n wagwoord bestuurderprogram.

Wagwoordbestuurders

Wat is dit?

Dit is ‘n program wat op jou rekenaar gelaai word waarin jou wagwoorde gelaai word en wat jy ontsluit met ‘n meesterwagwoord.

Het almal ‘n wagwoordbestuurder nodig?

Ja, die wagwoordbestuurder onthou en beskerm jou wagwoorde.

Is dit veilig?

Ja, die meeste wagwoordbestuurder programme se data word in geïnkripteerde formaat op jou hardeskyf gestoor en sou iets met jou hardeskyf gebeur gaan niemand toegang tot daardie wagwoorde kan kry nie, behalwe as hy / sy die meesterwagwoord ken. Dit word ook gesinkroniseer met jou verskillende toestelle gewoonlik via die 'wolk'. Al die vervaardigers van wagwoordbestuurders programme maak gebruik van 'n tegniek genaamd "Zero Knowledge Security". "Zero Knowledge Security" beveiliging beteken dat alhoewel die wagwoordbestuurder program jou wagwoorde ken is die instansie wat die wagwoordbestuurder gemaak het nie self in staat om jou wagwoorde te kan lees of vir iemand te kan gee nie.

Daar is verskeie wagwoord programme:

Gratis programme

Dashlane; LastPass; 1Password; en Kaspersky

Die meeste van hierdie gratis programme het beperkinge. Party werk net vir beperkte tyd terwyl ander se funksionaliteit beperk word, bv Kaspersky laat jou net toe om 10 wagwoorde te stoor.

Betaalde programme

Dashlane; LastPass; 1Password

As jy een van hierdie 3 koop het jy beter funksionaliteite.

Kaspersky word aanbeveel – dit vorm deel van Kaspersky total security pakket. Jy kan ook ID, paspoort, bestuurslisensies, koopkontrakte ens. skandeer en die geskandeerde dokumente veilig in jou 'passwordmanager' bêre. Jy kan dan die oorspronklike dokument van jou harde skyf af verwyder. Kaspersky se password manager gee jou die vermoeë om webwerwe se adresse se inligting te kan voltooi, maw die gebruikersnaam en wagwoord kan outomaties ingevul word. Dit bied dan vir jou vinnige toegang tot jou webwerwe sonder dat jy die gevaar het dat jy jou 'browser' moet toelaat om die wagwoorde te onthou. Kaspersky se password manager sal slegs en alleenlik die invul outomaties op die webwerwe doen indien jy jou meesterwagwoord ingesit het. As jy dit nie ingesit het nie sal hy nie die webwerwe vir jou oopsluit nie. Dit kan ook vir jou baie sterk wagwoorde genereer en toets of die wagwoorde wat op jou bestaande webwerwe in werking is sterk genoeg is en indien nie kan jy hulle verbeter. Mens kan ook met Kaspersky se password manager vasstel of van die webwerwe waar jy 'n gebuirker is al gekuberkraak ("gehack") was.

Enkripsie van hardeskywe

Indien ‘n rekenaar gesteel word en die hardeskryf uit die rekenaar gehaal word kan dit op in ‘n ander rekenaar gekoppel word en dan is die hardeskyf se inhoud nie meer deur Windows se wagwoord beskerm nie en is alle inligting bloot sigbaar vir enige persoon.

Die volgende is oplossings vir hierdie probleem:

1. Enkripteer die hardeskyf van die rekenaar

   Wat is enkripsie van hardeskywe: ‘n mens gebruik ‘n program op jou rekenaar om inligting oop en toe te sluit. Die gebruiker voorsien ‘n wagwoord vir die program. Die program gebruik dan hierdie sleutel op data oop en toe te sluit.

2. Hoe word dit gedoen

   Daar word ‘n program op die rekenaar geinstalleer en hierdie program het die vermoeë om elke lêer op die hardeskyf te ontvorm deur ‘n sleutel aan elke lêer te voorsien. Hierdie program kan nie oopgesluit word sonder die sleutel nie - selfs al plaas jy die hardskyf in ‘n ander rekenaar.

3. Die volgende programme kan gebruik word om die hardeskyf te enkripteer:

   Windows10 professional se Bitlocker program.

   Hierdie program kan egter slegs gebruik word op Windows 10 professional en nie die gewone intreëvlak weergawe nie. Dis ook baie duur. Dis moeilik om te installeer, kan slegs deur professionele persone geinstalleer word en maak die rekenaar stadig. Indien jou wagwoord verlore raak is daar geen manier om dit weer oop te kry nie.

   Ander enkripsie programme:

   Gratis programme – nie aanbeveelbaar nie.

   Hulle bestaan gewoonlik na 2 jaar nie meer nie, of die webwerf bestaan nie meer nie.

   Betaalde programme – Koop die programme van maatskappye wat al jare bestaan.

Enkripsie van lêers

Daar is 2 opsies:

Bitlocker kan die hele hardeskyf enkripteer of jy kan aparte lêers enkripteer. Die laaste opsie is die voorkeur opsie, as gebruikers nie Bitlocker kan gebruik nie.

Individuele enkripsie van lêers of houers (folders) word gedoen deur ‘n program wat jy op jou rekenaar installeer wat vir jou die enkripsie behartig. Jy kan gratis programme gebruik, maar dit is nie veilig nie.

Programme wat veilig is:

AxCrypt – hierdie weergawe werk vir 30 dae.

Microsoft OneDrive – Meeste gemeentes gebruik dit. Microsoft het in Oktober 2019 ‘n persoonlike kluis (vault)l by die bestaande funksionaliteite van OneDrive gevoeg. Die persoonlike kluis is ‘n area binne OneDrive wat jy kan enkripteer. Dit kan 1 of meer houers binne OneDrive wees. Al sou jy ingeteken wees in OneDrive en jy al jou lêers kan sien in OneDrive, moet jy ‘n ekstra wagwoord insit om die persoonlike kluis mee te kan oopmaak.

Kaspersky se total security – Voorkeur opsie. Jy kan jou hardeskyf se houers hiermee enkripteer. Jy kan kies watter houers jy wil hê, grootte, ens.

Watter leêrs moet ge-enkripteer word.

Nie alle leêrs hoef ge-enkripteer te word nie. Slegs leêrs met geidentifiseerbare persoonlike inligting (eposse, selfoonnrs, ID) moet ge-enkripteer word.

Winkerk 7 data is reeds ge-inkripteer en sal onleesbaar wees vir iemand wat jou rekenaar steel.

Winkerk 7 verslae – Hierdie verslae wat wel persoonlike inligting bevat wat jy voorberei om vir iemand elektronies aan te stuur moet ge-enkripteer of met ‘n wagwoord beskerm word. Hier kan jy Kaspersky gebruik om vir jou ‘n ge-enkripteerde houer te skep wat ‘n groot area is sodat jy dit in Windows Explorer kan oopmaak en verskillende verslae daarin kan sit. Maw die verslag self is nie ge-enkripteer nie, maar Kaspersky gaan met 1 knoppie die hele houer vir jou enkripteer. Die nadeel is dat as jy een van hierdie leêrs vir iemand per epos stuur moet jy onthou dat daardie leêr eers met ‘n wagwoord beskerm moet word alvorens jy dit uitstuur.

RETENSIE VAN DATA

Die Wet vereis dat inligting van datasubjekte nie langer geberg mag word as die oorspronklike oogmerk waarvoor dit ingesamel was nie. Daar is egter sekere uitsonderings. Die wet noem in art 14 1(B) dat indien die verantwoordelike party die rekord redelikerwys benodig vir regmatige oogmerke wat met daardie verantwoordelike party se werksaamhede of aktiwiteite verband hou dan mag dit langer bewaar word.

Indien ‘n gemeente lidmate se inligting benodig, al is hulle nie meer in die gemeente nie en dit hou direk verband met die gemeente se werksaamhede dan mag die data behoue bly.

In art 14 (2) spesifiseer dit dat as rekords van persoonlike inligting vir historiese statistiese of navorsingsoogmerke benodig word dit vir langer tydperke waarvoor dit oorspronklik ingesamel was gehou mag word, indien die verantwoordelike party die geskikte voorsorgmaatreëls het teen die gebruik van die rekords vir ander oogmerke as waarvoor dit dan nou bewaar word.

Winkerk7 program help ons met hierdie vereiste van die wet. Die program is sodanig ontwerp dat die hele argiveringsproses waardeur die gebruiker moet gaan wanneer ‘n lidmaat verwyder word seker maak dat slegs die persoon wat as lidmaat geklassifiseer is oorgeplaas kan word na ‘n ander gemeente. Persone wat nie as lidmate geklassifiseer word nie, bv mense wat as besoekers op jou databasis ingevul het. Hulle inligting gaan heeltemal van die stelsel verwyder word tydens die argiveringsproses. Die inligting word dus onherroepelik verwyder. Winkerk 7 se argiveringsproses is 100% in lyn met artikel 14 (2) van die wet.

Winkerk online se data

Winkerk online se data is ook 100% in lyn met die Wet omdat dit nie ou data in Winkerk Online bêre nie. Die “backup buddy” inligting word weekliks opgelaai na die wolk bediener (‘cloud server’) toe. Elke 3de week se ou data word outomaties op die plaaslike rekenaar sowel as in Winkerk Online verwyder.

Rugsteun kopieë

Die POPI inligtingsbeampte moet ‘n skedule hou waarvolgens alle ou rugsteen kopieë - waar dit ookal geberg word - van tyd tot tyd deurgegaan moet word om seker te maak dat die inligting wat daarop is nie verouderd is nie en verwyder moet word.

Elektroniese dokumente

Hierdie is dokumente wat gewoonlik aan amptenare / derde partye voorsien is. Dit is belangrik dat daardie partye ook kennis moet neem dat as die data in hulle besit verouderd raak hulle dit ook moet verwyder. Ou hardeskywe moet dus skoongemaak word wat aan amptenare / predikante / personeel gegee was om in lyn te wees met die Wet.

Harde kopieë

Dit moet ook op ‘n gereelde basis nagegaan word om te verseker dat daar nie verouderde inligiting op harde kopieë is nie.

- Harde kopieë (papier rekords)
    - Vermy onnodige papier-uitdrukke van persoonlike data
    - Moenie ongebruikte of ou inligtingstukke in die snippermandjie gooi nie

- Sien toe dat dit verbrand, versnipper of verpulp word.

Kerk argief

Verskillende kerke se data argiewe het voorskrifte van hoe lank data gebêre mag word. Sien argief webwerf

DIE VERNIETIGING VAN DATA

Die vernietiging van data is baie belangrik net soos die beveiliging van data.

Wanneer jy inligting uitwis op jou rekenaar, onthou om altyd die herwinningsmandjie ('recycle-bin') ook uit te vee.

Daar is verskillende metodes van vernietiging van ou toerusting (rekenaars, skootrekenaars, hardeskywe.)

1. Formatering

   Met formatering kan die inligting soms wel weer herwin word

2. Digitale sanitasie

   Digitale sanitasie word aanbeveel. Dit is die proses om data fisies uit te wis deur harde skywe met spesifieke elektroniese patrone of willekeurige data oor te skryf sodat die herstel van die oorspronklike data onmoontlik is. Vir die normale rekenaar gebruiker is dit nie so eenvoudig nie, maar alhoewel dit nogsteeds moeilik is, word hierdie proses aanbeveel. Die digitale sanitasie module is beskikbaar in Kaspersky Total Security (waar dit bekend staan as die "file shredder").

3. Fisiese vernietiging

   Dit kan ook fisies vernietig word. Gee dit liewer vir vakmanne wat daarmee werk.

Persone met wie ons elektroniese data gedeel het moet ingelig word dat die elektroniese data wat hulle nie meer gebruik nie, vernietig moet word.

<u>DIEFSTAL:</u>

Indien 'n rekenaar en/of hardeskyf gesteel word, meld dit onmiddellik aan by SAPD. Bewaar die SAPD Saaknommer vir verwysing dat data onregmatig bekom is deur diefstal.

VOORWAARDE 8: DEELNAME DEUR DATASUBJEK

Die datasubjek (lidmaat) het die reg om:

- Toegang te hê tot sy / haar persoonlike inligting wat oor hom / haar gehou word en mag ook vra vir toegang daartoe;

- Te versoek dat regstellings / skrappings gemaak word;

- Beswaar te maak teen die verwerking van persoonlike inligting

<u>Die volgende vorms is beskikbaar op die webblad:</u>

- Vorm 1: Beswaar teen verwerking van persoonlike inligting

  Vorm 2: Versoek om regstelling / skrapping van persoonlike inligting of vernietiging of skrapping van rekord van persoonlike inligting
-
- Vorm 3: Aansoek om toestemming van ‘n datasubjek (lidmaat) vir die verwerking van persoonlike inligting vir die doel van direkte bemarking.