

April 2021

HOOFSTUK 7

HANDLEIDING OOR POPIA WETGEWING

BESKERMING VAN EN TOEGANG TOT PERSOONLIKE INLIGTING

INHOUDSOPGawe

1. OMSKRYWING EN OOGMERK VAN DIE WET	BL 4
1.1. INLEIDING	BL 4
1.2. DOEL VAN DIE WET	BL 4
1.3. OOGMERK VAN DIE WET	BL 5
1.4. VOORWAARDES VIR DIE UITVOERING VAN DIE WET	BL 6
2. REGMATIGE PROSESSERING VAN PERSOONLIKE INLIGTING	BL 8
2.1. POPIA INLIGTINGSBEAMpte	BL 8
2.2. WETTIGE PROSESSERING VAN INLIGTING	BL 9
2.3. WAT IS PERSOONLIKE INLIGTING	BL 10
2.4. VERPLIGTING VAN CARITAS GEMEENSKAPSFOKUS NPC /TAKKE / DIENSPUNTE ONDER POPIA	BL 12
2.5. REKORDS GEHOU DEUR CARITAS GEMEENSKAPSFOKUS NPC /TAKKE / DIENSPUNTE	BL 12
2.6. "OPT IN"EN "OPT OUT" OPSIE VIR DIREKTE BEMARKING	BL 14
2.7. PERSOONLIKE INLIGTING WAT VERWERK MAG WORD	BL 14
3. IMPAKSTUDIE VAN PERSOONLIKE INLIGTING	BL 15
3.1. OUDITS	BL 15
3.2. BERG VAN DATA	BL 15
3.3. BEVEILIGING VAN DATA	BL 16
3.4. DATA RETENSIE	BL 17
3.5. VERNIETIGING VAN DOKUMENTE	BL 17
4. KONTROLELYS VAN AKSIES VOLGENS POPIA	BL 19
4.1. ASPEKTE VAN BELANG	BL 19
4.2. KONTROLE LYS	BL 19
5. TOEGANG TOT INLIGTING	BL 22
5.1. WIE MAG TOEGANG VERSOEK	BL 22
5.2. AANSOEKVORMS	BL 22
6. REGSADVIES	BL 23
7. IMPAK VAN POPIA OP ANDER WETGEWING	BL 24

BYLAE 1: TOESTEMMING TOT HOU VAN PERSOONLIKE INLIGTING	BL 25
BYLAE 2: PERSONEEL: VERTROULIKHEIDSONDERNEMING	BL 26
BYLAE 3: KONTRAKTEURS: VERTROULIKHEIDSONDERNEMING	BL 27

ENGELSE BYLAES (OUDIT BY CARITAS ADMIN. KANTOOR GEDOE)

BYLAE 4: POPI AUDIT	BL 28
BYLAE 5: POPI POLICY, PERSONAL INFO REQUEST FORM, COMPLAINT FORM	BL 31
BYLAE 6: AUDIT REPORT	BL 51
BYLAE 7: APPOINTMENT LETTER FOR INFORMATION OFFICER	BL 53

AFDELING 1: OMSKRYWING EN OOGMERK VAN DIE WET

POPIA

<https://www.gov.za/documents/protection-personal-information-act>

1. INLEIDING

Die Wet op Beskerming van Persoonlike Inligting: Wet 4 van 2013 (Protection of Personal Information Act [POPIA]) het op 1 Julie 2020 van krag geword. Die Wet moet saamgelees word met regulasies (R 1383) wat betrekking het op die POPI Wet soos gepubliseer in die Staatskoerant op 14 Desember 2018.

Die Wet bepaal ook 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 (die persone oor wie die inligting gaan)** het die reg om 'n regsaksies teen die verantwoordelike party in te stel en dit sou selfs moontlik wees dat, onder sekere omstandighede, die Inligtingsbeamppte gevangenisstraf opgelê kan word.

2. DOEL VAN DIE WET

"Om die beskerming van persoonlike inligting wat deur openbare en private liggeme verwerk word, te bevorder;

om sekere voorwaardes in te stel ten einde minimum vereistes vir die verwerking van persoonlike inligting vas te stel;

om voorsiening te maak vir die instelling van 'n **Inligtingsreguleerder** (deur die staat) om sekere bevoegdhede uit te oefen en om sekere pligte en funksies uit te voer ingevolge hierdie Wet en die Wet op die Bevordering van Toegang tot Inligting, 2000 (PAIA) ;

om voorsiening te maak vir die uitreiking van gedragskodes;

om voorsiening te maak vir die regte van persone rakende ongevraagde elektroniese kommunikasie en outomatiese besluitneming;

om die vloei van persoonlike inligting oor die grense van die Republiek te reguleer; en om voorsiening te maak vir aangeleenthede wat daarmee verband hou".

Artikel 14 van die Grondwet van die Republiek van Suid-Afrika, 1996, bevestig elke persoon se reg op privaatheid.

'n Verantwoordelike party moet die integriteit en vertroulikheid van persoonlike inligting in sy besit of onder sy beheer verseker deur toepaslike, redelike, tegniese en organisatoriese maatreëls daar te stel.

Die POPIA is van toepassing op almal wat enige tipes rekords verwerk wat persoonlike inligting van persone bevat. Dit stel dus die minimum standaarde vir die beskerming van persoonlike inligting. Verwerking behels die insameling, ontvangs, optekening, organisering, herwinning of die gebruik van sodanige inligting. Verder sluit dit ook die verspreiding en beskikbaarstelling van sodanige inligting in (gratis of teen vergoeding).

Die POPIA word saam gelees met die Wet op die Bevordering van Toegang tot Inligting 2 van 2000 (PAIA).

3. OOGMERK VAN DIE WET

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 liggeme (bv. Binnelandse Sake, SAID) en privaat instansies (bv. finansiële instellings; gesondheidsorg instansies, besighede, direkte bemarkers, asook diensorganisasies en kerke).

Die oogmerk van hierdie Wet volgens artikel 2 is om:

- uitvoering te gee aan die grondwetlike reg op privaatheid (Grondwet Art 14), deur persoonlike inligting te beskerm wanneer dit deur 'n verantwoordelike party verwerk word, onderworpe aan regverdigbare beperkings in terme van:
 - die balans tussen die reg op privaatheid en ander regte, veral die reg op toegang tot inligting; en
 - die beskerming van persoonlike belang, insluitend die vrye vloei van inligting binne die Republiek en oor internasionale grense;
- die wyse waarop persoonlike inligting verwerk kan word, te reguleer deur voorwaardes vas te stel, in ooreenstemming met internasionale standaarde, wat die minimum drempelvereistes vir die wettige verwerking van persoonlike inligting voorskryf;
- persone regte en remedies te bied om hul persoonlike inligting te beskerm teen verwerking wat nie in ooreenstemming met hierdie wet is nie; en
- vrywillige en verpligte maatreëls in te stel, insluitend die instelling van 'n inligtingsreguleerde (deur die staat), om respek te verseker vir en om die regte wat deur hierdie wet beskerm word, te bevorder, af te dwing en te vervul.

4. VOORWAARDES VIR DIE UITVOERING VAN DIE WET

Die Wet voorsien agt (8) voorwaardes waaraan voldoen moet word in terme van die bestuur van persoonlike inligting:

1. Aanspreeklikheid (*Accountability*)

Organisasies is aanspreeklik dat alle inligtingsprosesseringsbeginsels nagekom word.

2. Beperkte prosessering (*Processing Limitation*)

Die verwerking van inligting moet wettig en billik wees en nie die privaatheid van die datasubjek skend nie.

3. Doelspesifikasie (*Purpose Specification*)

Persoonlike inligting moet versamel word vir 'n spesifieke, gedefinieerde en wettige doel met betrekking tot 'n funksie of aktiwiteit van die betrokke onderneming.

4. Doelgerigte prosessering (*Further Processing Limitation*)

Die prosessering van inligting moet regmatig geskied en persoonlike inligting mag slegs verwerk word indien dit voldoende, relevant en nie oormatig is nie, gegewe die doel waarvoor dit verwerk word. Dit is waar persoonlike inligting dikwels van 'n derde party ontvang en oorgedra word aan 'n ander verantwoordelike party vir die verwerking.

Personnel moet ook 'n onderneming gee om nie inligting aan enige ongemagtigde persoon te verskaf asook om nie die inligting onregmatig te gebruik nie.

Vertroulikheid moet te alle tyde gehandhaaf word. SIEN BYLAE 2.

5. Kwaliteit van Inligting (*Information Quality*)

Verseker dat persoonlike inligting volledig, akkuraat, nie misleidend en opgedateer is

6. Openheid (*Openness*)

Sekere voorgeskrewe inligting moet aan die datasubjek verskaf word, insluitend die inligting wat versamel word, die naam en adres van die verantwoordelike party, die doel waarvoor die inligting ingesamel word en of die verskaffing van die inligting deur die datasubjek vrywillig of verpligtend is.

'n Toestemmingsbrief dat persoonlike inligting gehou mag word moet van elke direksieliid; trustee; gemeenskapsraadslid; personeellid en kliënt verkry word. Dit moet ook duidelik gestel word dat geen data aan ongemagtigde persone beskikbaar gestel sal word nie. SIEN BYLAE 1.

7. Veiligheidsvoorsorgmaatreëls (*Security Safeguards*)

Die onderneming moet die integriteit van die persoonlike inligting in sy besit en onder sy beheer beskerm deur te verseker dat maatreëls in plek is om verlies van, skade aan of ongemagtigde vernietiging van persoonlike inligting te voorkom.

8. Deelname deur “datasubjek” (*Data Subject Participation*)

’n Datasubjek het die reg om:

1. persoonlike inligting wat die organisasie hou gratis aan te vra;
2. persoonlike inligting wat nie korrek, irrelevant, oorbodig, misleidend of onregmatig verkry is, op te dateer of te vernietig; en
3. ’n rekord van persoonlike inligting te vernietig wat onnodig is vir die organisasie om te hou.

AFDELING 2: REGMATIGE PROSESSERING VAN PERSOONLIKE INLIGTING

1. POPIA INLIGTINGSBEAMPTE

Ingevolge die regulasies (artikel 4) onder POPIA is die uitvoerende hoof van 'n private liggaam (organisasie) die verantwoordelike inligtingsbeamppte, tensy dit gedelegeer is. Die eerste stap tot nakoming sal dus wees om 'n inligtingsbeamppte, hetsy die uitvoerende hoof of 'n ander inligtingsbeamppte, aan te stel, of om die rol van die bestaande inligtingsbeamppte te herevalueer in ooreenstemming met die vereistes uiteengesit in POPIA.

Die verantwoordelikhede van 'n inligtingsbeamppte volgens die wet is:

- Ontwikkeling, implementering, monitering en onderhoud van 'n nakomingsraamwerk; (hierdie handleiding geld as "nakomingsraamwerk" vir die organisasie);
- Impakbeoordeling van persoonlike inligting moet gedoen word om te verseker dat voldoende maatreëls en standarde bestaan om aan die voorwaardes vir die wettige verwerking van persoonlike inligting te voldoen;
- Ontwikkeling, monitering en onderhoud van 'n handleiding;
- Ontwikkeling van interne maatreëls om versoek om inligting of toegang daartoe te verwerk; en
- Die aanbied van interne bewusmakingsessies oor die bepalings van die Wet.

KONTAK BESONDERHEDE VAN INLIGTINGSBEAMPTE

INLIGTINGSBEAMPTE:

FISIESE ADRES:

TELEFOON NR:

EPOS ADRES:

2.2 WETTIGE PROSESSERING VAN INLIGATION

Prosessering behels enigets wat met persoonlike inligting gedoen word en sluit in die insameling, gebruik, bewaring, verspreiding, aanpassing of vernietiging van persoonlike inligting, ongeag of die prosessering outomaties gebeur al dan nie.

- **Hou van rekords:** Enige persoon se inligting mag nie langer gehou word as wat dit nodig is om die doel waarvoor dit ingesamel is te bereik nie. **Uitsonderings sluit in die hou van dokumente vir historiese-en navorsingsdoeleindes.**
- **Impak op persoonlike inligting van kinders:** Volgens artikel 11.3 en artikel 34 en 35 van die Wet is die prosessering van inligting van 'n kind verbode tensy die bepalings van artikel 35 van toepassings is, wat soos volg lees:

“Die verbod op prosessering van persoonlike inligting van kinders is nie van toepassing nie indien die prosessering –

 - Met die vooraf toestemming van 'n bevoegde persoon uitgevoer word;
 - Noodsaaklik is vir die vestiging van, uitoefening of beskerming van 'n reg of 'n regspil;
 - Noodsaaklik is vir voldoening aan 'n verpligting van internasionale publieke reg;
 - Vir historiese, statistiese of navorsingsoogmerke is vir sover die oogmerk 'n openbare belang dien
 - Persoonlike inligting behels wat opsetlik, met die toestemming van 'n bevoegde persoon, deur die kind openbaar gemaak is”.
- **Kontrakteurs:** Oor die algemeen ontvang 'n kontrakteur nie persoonlike inligting nie. Die grootste risiko is egter dat hierdie kontrakteurs steeds potensiële toegang tot die persoonlike inligting van 'n organisasie het. Voorbeeldsluit die volgende in:
 - 'n IT-verskaffer wat toegang het tot die organisasie se rekenaarstelsel.
 - 'n Skoonmaakdiens wat toegang het tot personeelkantore of ander gebiede waarin persoonlike inligting mag voorkom.
 - 'n Konsultant wat beperkte toegang kry tot gehalte-, nakomings- of ander interne verslae.

'n Kontrakteur moet 'n dokument onderteken waar onderneem word dat persoonlike inligting nie gedeel mag word nie. SIEN BYLAE 3

3. WAT IS PERSOONLIKE INLIGTING

2.3.1 Die CARITAS GEMEENSKAPSFOKUS NPC /TAKKE /DIENSPUNTE is in besit van sensitiewe inligting van personeel; inwoners en kinders. Daar moet met sorg omgegaan word met die volgende persoonlike inligting:

- Identiteitsnommer / Paspoortnommer.
- Geboortedatum / Ouderdom.
- Telefoonnummers.
- E-posadresse.
- Fisiese adres.
- Geslag, ras en etniese oorsprong.
- Foto's, stemopnames, video-opnames (ook CCTV) en biometriese data.
- Huwelikstatus en familieverwantskap.
- Kriminele rekord.
- Private korrespondensie.
- Godsdienstige en filosofiese oortuiging asook politieke opinies.
- Indiensnemingsrekord en vergoeding.
- Opvoedkundige inligting.
- Fisiese en psigiese gesondheidsinligting, mediese geskiedenis, bloedgroep en sekualiteit.
- Lidmaatskap van verenigings en organisasies.

2.3.2 Geloofs- en filosofiese oortuigings

Alhoewel artikel 28 van die Wet dit verbied om 'n datasubjek se geloofs- en filosofiese oortuigings, in te samel, laat artikel 26 wel ruimte vir kerke om dit te doen. Artikel 28 lees soos volg:

“(1) Die verbod op die prosessering van persoonlike inligting met betrekking tot ‘n datasubjek se geloofs- of filosofiese oortuiginge, soos in artikel 26 bedoel, is nie van toepassing nie indien die prosessering uitgevoer word deur –

- (a) geestelike of geloofsorganisasie, of onafhanklike afdeling daarvan, indien –
 - (i) die inligting betrekking het op datasubjekte wat aan daardie organisasie behoort; of
 - (ii) dit noodsaaklik is om hul oogmerke en beginsels te bereik;
- (b) instellings gegrond op geloofs- of filosofiese beginsels ten opsigte van hul lede of werknemers of ander persone wat aan die instelling behoort, indien dit noodsaaklik is vir die bereiking van die instelling se oogmerke en beginsels; of
- (c) ander instellings, met die voorbehoud dat die prosessering van inligting noodsaaklik is vir die beskerming van die datasubjekte se geestelike welsyn, tensy hul teen die prosessering daarvan beswaar gemaak het.

2.3.3 Mediese Rekords

Die definisie van persoonlike inligting sluit in:

- inligting rakende die fisiese of geestelike gesondheid, welstand, gestremdheid ... van die persoon; en
- inligting rakende die mediese geskiedenis van die persoon.
- Spesiale persoonlike inligting sluit inligting rakende die gesondheid van die betrokkene in.

Artikel 26 van die POPI-wet verbied die verwerking van persoonlike inligting rakende die persoon se gesondheid. Maar ingevolge artikel 32(1) is die verbod nie van toepassing nie op byvoorbeeld:

- mediese fondse,
- gesondheidsorginstellings of –fasiliteite, of maatskaplike dienste;
- versekeringsmaatskappye, administrateurs van mediese skemas en gesondheidsorgorganisasies;
- skole; en enige openbare of private liggaam wat die versorging van ‘n kind bestuur.

Artikel 32 moet noukeurig gelees word. Dit bevestig ook die gemeenregtelike vertroulikheidsplig of skep dit waar dit nie bestaan nie. Jy kan persoonlike inligting rakende die persoon se gesondheid verwerk as jy:

- die voorwaardes en reëls in artikel 32 volg;
- die persoonlike inligting vertroulik hou; en
- aan die res van die voorwaardes van die POPIA voldoen.

4. DIE VERPLIGTINGE VAN DIE ORGANISASIE ONDER POPIA

Van die verpligtinge sluit in:

- Om slegs inligting vir 'n **spesifieke doel** in te samel;
- Om te verseker dat inligting **relevant en op datum** is;
- Om redelike sekuriteitsmaatreëls in plek te hê om die inligting **te beskerm**;
- Om **net die nodige** inligting te hou; en
- Om toe te laat dat die datasubjek sy of haar **inligting op aanvraag** mag sien of bekom.

5. REKORDS GEHOU DEUR CARITAS GEMEENSKAPSFOKUS NPC /TAKKE/DIENSPUNTE

Persoonlike inligting kan in die volgende dokumente voorkom:

2.5.1 MAATSKAPPY DOKUMENTE

- Nuusbriewe en publikasies
- Toepaslike statutêre dokumente
- Jaarverslae
- Konstitusies
- Gedragskodes
- Sakelyste en Notules
- Regsnakomingsrekords
- Akte van oprigting
- Groepsbeleid en prosedures
- Strategiese dokumente
- Ooreenkomste met Diensorganisasies

2. FINANSIELLE DOKUMENTE

- Beleide en prosedures
- Rekeningkundige rekords
- Finansiële Jaarstate
- Auditverslae
- Rekords van kapitaaluitgawes
- Fakture en state
- Bestuursverslae
- Aankope rekords
- Belastingrekords en opbrengste
- Versekeringsdokumente

3. MENSELIKE HULPBRONNE

- Werknemersvoordeelrekords
- Dienskontrakte
- Inligting oor werknemers
- Personeelbeleid- en prosedures
- Verlofrekords
- Pensioenrekords
- Belastingopgawes van werknemers
- WVF-opbrengste

4. INLIGTINGSTECHNOLOGIE

- Ooreenkomste

- Hardware- en sagtewarepakkette
- Beleid en prosedures
- Ondersteuning en programmering van interne stelsels
- Lisensies

5. BEMARKING EN KOMMUNIKASIE

- Nuusbriewe en advertensiemateriaal
- Kliëntinligting
- Bemarkingsbrosjures
- Bemarkingsstrategieë

6. “OPT-IN” OF “OPT-UIT” OPSIE VIR DIREKTE BEMARKING?

Elke onderneming moet gebruik maak van ’n “opt-in” en “opt-uit” opsie wanneer hulle ’n datasubjek vir bemarkingsdoeleindes kontak. Baie maatskappye bied reeds die opsie wanneer hulle boodskappe per SMS stuur en baie e-posse wat vir bemarkingsdoeleindes aan datasubjekte gestuur word bied die opsie om die datasubjek se e-posadres te verwyder. Die opsie moet aangebied word sodat die datasubjek verstaan waarvoor hy of sy toestemming gee of beswaar teen maak.

7. PERSOONLIKE INLIGTING WAT VERWERK MAG WORD

- Direkteure / trustees, gemeenskapsraadslede en personeel
- Inwonersinligting
- Inligting van kinders (**volgens art 35**).
- Posaanvraers
- Bestaande en voormalige werknemers

- Dienverskaffers en kontrakteurs
- Besoekersinligting
- Korrespondensie en navrae
- Dokumente van navorsingsbelang

AFDELING 3: IMPAKSTUDIE VAN PERSOONLIKE INLIGTING

3.1 OUDITS

Sodra alle werknemers ingelig is, moet selfbeoordelings en -oudits in die maatskappy / takke en dienspunte begin. Dit is belangrik om te verstaan watter inligting versamel word, hoe dit versamel word, deur wie dit versamel word, waarvoor dit gebruik word, hoe dit gestoor en verwerk word, hoe dit bewaar en vernietig word en of dit met die nodige toestemming versamel is.

Sodra selfoudits deur die organisasie voltooi is, moet daar 'n duidelike begrip wees van hoe data in die organisasie verwerk word, watter leemtes en gapings, sowel as risiko's geïdentifiseer is.

2. BERGING VAN DATA

Wanneer daar besin word oor die bering van persoonlike inligting moet besluit word watter tipe data versamel word en wie toegang daartoe moet verkry. Dit is bepalend in die wyse waarop data geberg en beskikbaar gemaak word. Die formaat, hetsy elektroniese of papierkopie, bepaal ook die bering van die inligting.

Persoonlike inligting word hoofsaaklik op die volgende wyses geberg:

- Papier weergawes van inligting: Wanneer daar papier weergawes van persoonlike inligting gehou word moet dit weggesluit wees.
- Elektroniese dokumente: Dokumente met persoonlike inligting word dikwels versprei in Microsoft Word, Excel formaat en PDF lêers. Die nodige voorsorg moet getref word om ongemagtigde toegang en lees daarvan te voorkom.
- E-posadresse: Daar moet toegesien word dat dit beveilig is teen ongemagtigde toegang.
- Webwerf: Webwerwe verskaf dikwels persoonlike inligting oor personeel. Sien toe dat skriftelike toestemming ontvang is om die inligting te publiseer.
- Kinders: Wanneer inligting oor kinders geplaas word is die skriftelike toestemming van beide ouers/voogde nodig.
- Sosiale media: Soos met webwerwe geld dieselfde reëls vir die plaas van persoonlike inligting op Facebook, Twitter en Instagram.
- Selfone: WhatsApp groepe: Daar moet verseker word dat skriftelike toestemming ontvang is dat die persoonlike inligting (selnommers) op 'n toestel geberg mag word

en dat dit sigbaar sal wees vir ander groepslede. Daar moet 'n opsie wees om die groep te kan verlaat.

3. BEVEILIGING VAN DATA

Aandag moet gegee word aan die fisiese en elektroniese beveiligung van persoonlike inligting.

3.1. FISIESE SEKURITEIT:

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

- Kluis: Verkieslik 'n instapkluis / toegewysde kantoor wat groot genoeg is om registers en ook rekenaartoerusting in te berg.
- Diefwering: Voor alle vensters en deure wat na buite oopmaak.
- Alarmstelsel: Verkieslik 'n alarmstelsel wat gekoppel is aan 'n reaksieeenheid
- Sekuriteitskameras: Waar moontlik 'n kamera-stelsel sodat toegang tot die terrein en gebou gemonitor kan word.
- Terreinbeveiliging: Maak seker dat die volgende in plek is:
 - Rekenaarhardeskywe (ekstern en geheuestokkies) veilig gestoor word.
 - Skootrekenaars beveilig is en bewaar word.

3.2. ELEKTRONIESE SEKURITEIT:

Ten opsigte van die elektroniese sekuriteit is daar drie belangrike sake wat deurlopende aandag vereis, nl. rugsteun, wagwoorde en enkripsie.

- Rugsteun: As 'n sekerheidsmaatreël maak seker dat
 - Rugsteun gereeld gemaak word van data op rekenaarstelsels
 - Bewaar hierdie eksterne rugsteun op 'n veilige plek. Dit word aangeraai dat dit op 'n ander terrein sal wees.
 - Indien dit op internet geberg word, dat dit beveilig is met die nodige sterk wagwoorde.
- Wagwoorde: Maak seker dat:
 - Sterk wagwoorde gebruik word
 - Gereelde verandering van wagwoorde plaasvind
 - 'n Wagwoordbestuursprogram gebruik word om al die verskillende wagwoorde van databasisse, webwerwe en stelsels te bestuur.

- **Enkripsie:** Maak seker dat die volgende in plek is
 - Antivirusprogramme
 - Enkripsieprogramme wat moontlik gebruik word om dokumente te beskerm teen ongemagtigde toegang.

4. DATA RETENSIE

Die Wet vereis dat inligting van datasubjekte nie langer geberg mag word as die oorspronklike oogmerk daarvan nie (artikel 14 (1) en (2)). Die Wet bepaal egter dat dit wel gebêre mag word in sekere gevalle vir:

- Historiese, statistiese en navorsings doeleindes, en
- Finansiële inligting

Die Wet bepaal ook dat inligting gehou mag word as dit benodig word vir die funksionering van die organisasie.

5. VERNIETIGING VAN DATA

Dit is die Inligtingsbeampte se verantwoordelikheid om toe te sien dat die volgende vernietig word:

- Oorbodige duplikaat dokumente.
- Duplikaatuitdrukke wat as werkskopieë gebruik is.
- Lyste met inligting wat nie meer benodig word nie, ens.

Vernietiging van Elektroniese data (rekenaars, dataskywe en geheue stokkies) moet met sorg gedoen word.

- Vernietig elektroniese kopieë van inligting wat saamgestel is vir 'n ander doel, maar waarvan die oorspronklike inligting reeds in databasisse vasgevang is.
- Vernietig ou hardeskywe wat in onbruik is.

Moenie ongebruikte of ou inligtingstukke in die snippermandjie goo nie. Sien toe dat dit verbrand, versnipper of verpulp word.

DIEFSTAL:

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

AFDELING 4: POPIA: KONTROLELYS VAN AKSIES

1. ASPEKTE VAN BELANG

Die volgende aspekte van belang moet aandag kry:

- Die hersiening en opdatering van alle kliënt-, verskaffer- en derdeparty-ooreenkomste. **Caritas/Takke en Dienspunte dra die bewyslas vir die datasubjek se toestemming.**
- Implementering van tegniese en organisatoriese maatreëls om ongemagtigde toegang tot en verkryging van persoonlike inligting te beskerm en te voorkom
- Voorbereiding van toestemmingsdokumentasie en privaatheidskennisgewings
- Heroorweging en/of maatreëls in plek stel vir die oor landsgrense vloei van persoonlike inligting – soek vooraf toestemming van die Inligtingsreguleerder en implementering van data-oordragooreenkomste
- Die ontwikkeling van 'n kultuur van privaatheid deur die opleiding van personeel, die opdatering en implementering van beleide en prosedures en die implementering van bewusmakingsveldtogte
- Implementering van 'n data-oortreding en voorval-reaksieplan en -beleid
- Implementering van 'n stelsel vir die bestuur van toegangsregte vir die betrokkene ingevolge die POPIA- en PAIA-wetgewing

4.2 KONTROLELYS

AKTIWITEIT	DATUM VOLTOOI	REMEDIE
Aanstel van inligtingsbeampte		
Opstel van Handleiding		
Bewusmaking van POPIA		
Interne Opleiding		
Herbevestiging van bestaande inligting van Direksie; Beheerraadslede; Personeel en Inwoners		

Ondertekening van toestemmingsbrief om persoonlike data te hou.		
Nuwe intrekkers: Ondertekening van toestemmingsbrief om persoonlike data te hou.		
Elektroniese kommunikasie: “Opt out” funksies		
Skriftelike toestemming verkry vir publikasie van persoonlike inligting op webblad; inligtingsbrosjure; Facebook; deelname aan 'n WhatsApp groep		
Maak lys van alle tipes inligting wat ingesamel word. By voltooiing word dit as Bylae tot die Handleiding gevoeg.		
Lys van ALLE persone wat toegang tot inligting het en waarvoor benodig. Vertroulikheidsdokument moet geteken word. By voltooiing word lys van personeel as Bylae tot Handleiding gevoeg.		
Maak seker alle papier korrespondensie / dokumente word toegesluit.		
Maak lys van rekenaartoerusting. By voltooiing word as Bylae tot Handleiding gevoeg.		

Bevestig elke rekenaar is met 'n wagwoord beskerm.		
Bevestig daar is antivirusprogramme op rekenaars.		
Nagaan van Fisiese Sekuriteitsmaatreëls		
Dokumente van historiese / navorsingsbelang: Oudit alle dokumente en vernietig oorbodige dokumente.		
Dokumente moet korrek vernietig / gesnipper word.		
Byhou van data-oortreding en voorval insidente.		
Kontrakteurs: Ondertekening van onderneming vir die beskerming van persoonlike inligting		

AFDELING 5: TOEGANG TOT INLIGATION

1. WIE MAG TOEGANG TOT INLIGATION VERSOEK

Die Wet bepaal dat 'n aanvraer slegs geregtig is op toegang tot 'n rekord as die rekord benodig word vir die uitoefening of beskerming van 'n reg. Slegs versoeke om toegang tot 'n rekord, waar die versoeker die inligtingsbeampte oortuig het dat die rekord nodig is om 'n reg uit te oefen of te beskerm, sal oorweeg word. Indien 'n data oortreding plaasgevind het, word die betrokke datasubjek dadelik in kennis gestel.

Toegang tot persoonlike Inligting geskied skriftelik onder die volgende omstandighede:

- 'n Persoonlike aanvraer wat 'n rekord van hom- / haarself versoek;
- 'n Derde Party wat 'n rekord versoek namens iemand anders met die persoon se toestemming en waar dit nodig is vir die beskerming van die reg van daardie persoon;
- 'n Openbare liggaam wat 'n rekord kan aanvraa indien die rekord nodig is vir die uitoefening of beskerming van 'n reg.

5.2 AANSOEKVORMS

Die volgende aansoekvorms is beskikbaar by:

https://www.popiact-compliance.co.za/images/Documents/POPIA_Regulations_- Dec_2018.pdf

- Beswaar teen verwerking van persoonlike inligting (vorm 1).
- Versoek om registrelling of skrapping van persoonlike inligting of vernietiging of skrapping van rekord van persoonlike inligting (vorm 2).
- Aansoek om die toestemming van 'n datasubjek vir die verwerking van persoonlike inligting vir die doel van direkte bemarking (vorm 4).

AFDELING 6: REGSIMPLIKASIES

Artikel 86 van die Wet bepaal dat kommunikasie tussen 'n kliënt en 'n professioneleregsadviseur (sogenaamde "geprivilegerde inligting") uitgesluit is van die bepalings van die Wet en lees as volg: "Kommunikasie tussen regsadviseur en kliënt vrygestel".

Die bevoegdhede van deursoeking en beslaglegging deur 'n lasbrief moet eerbiedig word, behoudens die bepalings van artikel 82, uitgesluit -

- (a) enige kommunikasie tussen 'n professioneleregsadviseur en sy of haar kliënt in verband met die verlening van regadvies aan die kliënt met betrekking tot sy of haar verpligtinge, aanspreeklikhede of regte; of
- (b) enige kommunikasie tussen 'n professioneleregsadviseur en sy of haar kliënt, of tussen sodanige adviseur of sy of haar kliënt en 'n ander persoon, in verband met, of in afwagting van verrigtinge kragtens of voortvloeiend uit hierdie Wet, met inbegrip van verrigtinge voor 'n hof.

AFDELING 7: IMPAK VAN POPIA OP ANDER WETTE

Volgens die Suid-Afrikaanse Regskommissie, wat die POPIA-wet opgestel het, is die grootste veranderinge ten opsigte van ander wette soos volg: (Lees dit saam met Hoofstuk 12 van die POPIA en BYLAE:

- Die privaatheidsbepalings van die Wet op Elektroniese Kommunikasie en Transaksies: Dele van hierdie Wet sal wegval waar daar duplisering met POPIA is.
- Die Wet op die Bevordering van Toegang tot Inligting: Alle afdelings wat handel oor 'n persoon se persoonlike inligting sal wegval en in POPIA behandel word.
- Die Nasionale Kredietwet en die Wet op Verbruikersbeskerming: Hierdie Wet sal gewysig word sodat alle afdelings oor privaatheid verwyder en in POPIA behandel word.

BYLAE 1

(Plaas op briefhoof)

POPIA: TOESTEMMING TOT HOU VAN PERSOONLIKE INLIGTING

Toestemming verleen in terme van die Wet op Beskerming van Persoonlike Inligting: Wet 4 van 2013 (Protection of Personal Information Act [POPIA]).

TOESTEMMING

Hiermee gee ek, ID: toestemming dat my persoonlike inligting aangewend gaan word vir die interne funksionering van die maatskappy / organisasie en dat geen data aan ongemagtigde persone beskikbaar gestel sal word nie.

DATUM: _____

DIREKTEUR

UITVOERENDE HOOF

BYLAE 2

(Plaas op briefhoof)

POPIA: PERSONEEL**VERKLARING TOT DIE BEWARING VAN PERSOONLIKE INLIGTING**

Verklaring in terme van die Wet op Beskerming van Persoonlike Inligting: Wet 4 van 2013 (Protection of Personal Information Act [POPIA]).

VERKLARING

Hiermee onderneem ek,; ID: dat ek met omsigtigheid met die persoonlike inligting van direkteure/beheerraadslede, kliënte, familie van kliënte, personeel, en/of kontrakteurs sal handel en dat geen data aan ongemagtigde persone beskikbaar gestel sal word nie.

DATUM: _____

PERSONEELLID

UITVOERENDE HOOF/BESTUURDER

BYLAE 3

(Plaas op briefhoof)

POPIA: KONTRAKTEURS**VERKLARING TOT DIE BEWARING VAN PERSOONLIKE INLIGTING**

Verklaring in terme van die Wet op Beskerming van Persoonlike Inligting: Wet 4 van 2013 (Protection of Personal Information Act [POPIA]).

VERKLARING

Hiermee onderneem ek,; ID: van (maatskappy) dat ek met omsigtigheid met die persoonlike inligting van direkteure/beheerraadslede, kliënte, familie van kliënte, personeel, en/of ander kontrakteurs sal handel en dat geen data aan ongemagtigde persone beskikbaar gestel sal word nie.

DATUM: _____

KONTRAKTEUR

UITVOERENDE HOOF/BESTUURDER

Bylae 4

PROTECTION OF PERSONAL INFORMATION AUDIT

COMPANY _____ CARITAS GEMEENSKAPFOKUS NPC

Date ...1 MARCH 2021

PROTECTION OF PERSONAL INFORMATION AUDIT

COMPANY _____ CARITAS GEMEENSKAPFOKUS NPC

Date ...1 MARCH 2021

SN	OFFICE	INCUMBENT	DOCS KEPT	STORAGE	REMARKS
3	Reception/ admin and filing	Sandra Walles	<ul style="list-style-type: none"> • Employees personal file • Pay sheets of employees • Sick Notes • Leave forms • Irp3 information • Registration documents of staff members • Disciplinary Information • CV's • Minutes and Agendas of meetings • Business Plans • Data on Computers 	Secure Walk-in safe Password protected on server	All documents not in use are shred. Archives are kept at Eagle Transport Safe keeping facilities. Offices are lock afterhours and alarm system activated
SN	OFFICE	INCUMBENT	DOCS KEPT	STORAGE	REMARKS

1	ADMINISTRATION	C DU PLOOY	<ul style="list-style-type: none"> • Employees personal file • Pay sheets of employees • Sick Notes • Leave forms • Irp3 information • Registration documents of staff members • Disciplinary Information • CV's • Minutes and Agendas of meetings • Business Plans • Data on Computers 	<p>Secure Walk-in safe</p> <p>Password protected on server</p>	<p>Pay sheets secure</p> <p>All documents not in use are shred. Archives are kept at Eagle Transport Safe keeping facilities.</p> <p>Offices are lock afterhours and alarm system activated</p>
2	MARKETING	ESTE V/D MERWE	<p>DATABASE INFORMATION ON COMPUTER</p> <p>Clients and sponsors info</p> <p>Marketing of Caritas</p>	<p>Server secure password protected</p>	

CARITAS GEMEENSKAPFOKUS NPC**PROTECTION OF PERSONAL INFORMATION POLICY**

Version	001
Publishing Date	MARCH 2021
Review Date	MARCH 2022
Policy Owner	CARITAS GEMEENSKAPFOKUS NPC

POLICY STATEMENT

- This policy forms part of the policy owner's internal business processes and procedures.
- Any reference to the "organisation" shall be interpreted to include the "policy owner".
- The organisation's governing body, its employees, volunteers, contractors, suppliers and any other persons acting on behalf of the organisation are required to familiarise themselves with the policy's requirements and undertake to comply with the stated processes and procedures.
- Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities.

POLICY ADOPTION

By signing this document, I authorise the policy owner's adoption of the processes and procedures outlined herein:

Name and Surname	
Capacity	
Signature	
Date	

TABLE OF CONTENTS

1. INTRODUCTION.....	Page 4
2. DEFINITIONS.....	Page 4
2.1 Personal Information.....	Page 4
2.2 Data Subject.....	Page 4
2.3 Responsible Party.....	Page 4
2.4 Operator.....	Page 5
2.5 Information Officer.....	Page 5
2.6 Processing.....	Page 5
2.7 Record.....	Page 5
2.8 Filing System.....	Page 5
2.9 Unique Identifier.....	Page 5
2.10 De-Identify.....	Page 6
2.11 Re-Identify.....	Page 6
2.12 Consent.....	Page 6
2.13 Direct Marketing.....	Page 6
2.14 Biometrics.....	Page 6
3. POLICY PURPOSE.....	Page 6
4. POLICY APPLICATION.....	Page 7
5. RIGHTS OF DATA SUBJECTS.....	Page 7
5.1 The Right to Access Personal Information.....	Page 7
5.2 The Right to have Personal Information Corrected or Deleted.....	Page 7
5.3 The Right to Object to the Processing of Personal Information.....	Page 8
5.4 The Right to Object to Direct Marketing.....	Page 8
5.5 The Right to Complain to the Information Regulator.....	Page 8
5.6 The Right to be Informed.....	Page 8
6. GENERAL GUIDING PRINCIPLES.....	Page 8
6.1 Accountability.....	Page 8
6.2 Processing Limitation.....	Page 8
6.3 Purpose Specification.....	Page 9
6.4 Further Processing Limitation.....	Page 9
6.5 Information Quality.....	Page 9
6.6 Open Communication.....	Page 9
6.7 Security Safeguards.....	Page 10
6.8 Data Subject Participation.....	Page 10
7. INFORMATION OFFICERS.....	Page 10

8. SPECIFIC DUTIES AND RESPONSIBILITIES.....	Page 11
8.1 Governing Body.....	Page 11
8.2 Information Officer.....	Page 11
8.3 IT Manager.....	Page 12
8.4 Marketing & Communication Manager.....	Page 12
8.5 Employees and other Persons acting on behalf of the Organisation.....	Page 13
9. POPI AUDIT.....	Page 15
10. REQUEST TO ACCESS PERSONAL INFORMATION.....	Page 15
11. POPI COMPLAINTS PROCEDURE.....	Page 16
12. DISCIPLINARY ACTION.....	Page 16
13. ANNEXURE A: PERSONAL INFORMATION REQUEST FORM.....	Page 18
14. ANNEXURE B: POPI COMPLAINT FORM.....	Page 19
15. ANNEXURE C: POPI NOTICE AND CONSENT FORM.....	Page 20
16. ANNEXURE D: EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE.....	Page 21
17. ANNEXURE E: SLA CONFIDENTIALITY CLAUSE.....	Page 22
18. ANNEXURE F: INFORMATION OFFICER APPOINTMENT LETTER.....	Page 23

1. INTRODUCTION

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 (“POPIA”).

POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

Through the provision of quality goods and services, the organisation is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

Given the importance of privacy, the organisation is committed to effectively managing personal information in accordance with POPIA's provisions.

2. DEFINITIONS

2.1 Personal Information

Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

- race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person;
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

2.2 Data Subject

This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies the organisation with products or other goods.

2.3 Responsible Party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the organisation is the responsible party.

2.4 Operator

An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third-party service provider that has contracted with the organisation to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

2.5 Information Officer

The Information Officer is responsible for ensuring the organisation's compliance with POPIA.

Where no Information Officer is appointed, the head of the organisation will be responsible for performing the Information Officer's duties.

Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

2.6 Processing

The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

- the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, as well as any restriction, degradation, erasure or destruction of information.

2.7 Record

Means any recorded information, regardless of form or medium, including:

- Writing on any material;
- Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph or drawing;
- Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

2.8 Filing System

Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of
Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or
geographical basis, which is accessible according to specific criteria.

2.9 Unique Identifier

that responsible party and that uniquely identifies that data subject in relation to that responsible party.

2.10 De-Identify

This means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

2.11 Re-Identify

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.12 Consent

Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

2.13 Direct Marketing

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
- Requesting the data subject to make a donation of any kind for any reason.

2.14 Biometrics

Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

3. POLICY PURPOSE

This purpose of this policy is to protect the organisation from the compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality. For instance, the organisation could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose the organisation uses information relating to them.
- Reputational damage. For instance, the organisation could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the organisation.

This policy demonstrates the organisation's commitment to protecting the privacy rights of data subjects in the following manner:

- Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
- By cultivating an organisational culture that recognises privacy as a valuable human right.
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
- By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the organisation.

- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of the organisation and data subjects.
- By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4. POLICY APPLICATION

This policy and its guiding principles applies to:

- The organisation's governing body
- All branches, business units and divisions of the organisation
- All employees and volunteers
- All contractors, suppliers and other persons acting on behalf of the organisation

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the organisation's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with POPIA's provisions is activated in any situation where there is:

- A processing of.....
-personal information.....
-entered into a record.....
-by or for a responsible person.....
-who is domiciled in South Africa.

POPIA does not apply in situations where the processing of personal information:

- is concluded in the course of purely personal or household activities, or
- where the personal information has been de-identified.

5. RIGHTS OF DATA SUBJECTS

Where appropriate, the organisation will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects.

The organisation will ensure that it gives effect to the following seven rights.

5.1 The Right to Access Personal Information

The organisation recognises that a data subject has the right to establish whether the organisation holds personal information related to him, her or it including the right to request access to that personal information.

An example of a "Personal Information Request Form" can be found under Annexure A.

5.2 The Right to have Personal Information Corrected or Deleted

The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where the organisation is no longer authorised to retain the personal information.

5.3 The Right to Object to the Processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.

In such circumstances, the organisation will give due consideration to the request and the requirements of POPIA. The organisation may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

5.4 The Right to Object to Direct Marketing

The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

5.5 The Right to Complain to the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

An example of a "POPI Complaint Form" can be found under Annexure B.

5.6 The Right to be Informed

The data subject has the right to be notified that his, her or its personal information is being collected by the organisation.

The data subject also has the right to be notified in any situation where the organisation has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

6. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of the organisation will at all times be subject to, and act in accordance with, the following guiding principles:

6.1 Accountability

For damages. The protection of personal information is therefore everybody's responsibility. Isation to a civil claim

The organisation will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the organisation will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

6.2 Processing Limitation

The organisation will ensure that personal information under its control is processed:

- in a fair, lawful and non-excessive manner, and
- only with the informed consent of the data subject, and
- only for a specifically defined purpose.

The organisation will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.

Alternatively, where services or transactions are concluded over the telephone or electronic video feed, the organisation will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

The organisation will under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the organisation's business and be provided with the reasons for doing so.

An example of a "POPI Notice and Consent Form" can be found under Annexure C.

6.3 Purpose Specification

All of the organisation's business units and operations must be informed by the principle of transparency.

The organisation will process personal information only for specific, explicitly defined and legitimate reasons. The organisation will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

6.4 Further Processing Limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

Therefore, where the organisation seeks to process personal information it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, the organisation will first obtain additional consent from the data subject.

6.5 Information Quality

The organisation will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

The more important it is that the personal information be accurate (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort the organisation will put into ensuring its accuracy.

Where personal information is collected or received from third parties, the organisation will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

6.6 Open Communication

The organisation will take reasonable steps to ensure that data subjects are notified (are at all times aware) that their personal information is being collected including the purpose for which it is being collected and processed.

The organisation will ensure that it establishes and maintains a "contact us" facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

- Enquire whether the organisation holds related personal information, or

- Request access to related personal information, or
- Request the organisation to update or correct related personal information, or
- Make a complaint concerning the processing of personal information.

6.7 Security Safeguards

The organisation will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.

The organisation will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the organisation's IT network.

The organisation will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the organisation is responsible.

All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

The organisation's operators and third-party service providers will be required to enter into service level agreements with the organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

An example of "Employee Consent and Confidentiality Clause" for inclusion in the organisation's employment contracts can be found under Annexure D.

An example of an "SLA Confidentiality Clause" for inclusion in the organisation's service level agreements can be found under Annexure E.

6.8 Data Subject Participation

A data subject may request the correction or deletion of his, her or its personal information held by the organisation.

The organisation will ensure that it provides a facility for data subjects who want to request the correction or deletion of their personal information.

Where applicable, the organisation will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. INFORMATION OFFICERS

The organisation will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.

The organisation's Information Officer is responsible for ensuring compliance with POPIA.

There are no legal requirements under POPIA for an organisation to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within larger organisations.

Where no Information Officer is appointed, the head of the organisation will assume the role of the Information Officer. Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.

Once appointed, the organisation will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties.

An example of an "Information Officer Appointment Letter" can be found under Annexure F.

8. SPECIFIC DUTIES AND RESPONSIBILITIES

8.1 Governing Body

The organisation's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the organisation meets its legal obligations in terms of POPIA.

The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The governing body is responsible for ensuring that:

- The organisation appoints an Information Officer, and where necessary, a Deputy Information Officer.
- All persons responsible for the processing of personal information on behalf of the organisation:
 - are appropriately trained and supervised to do so,
 - understand that they are contractually obligated to protect the personal information they come into contact with, and
 - are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
- Data subjects who want to make enquiries about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
- The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which the organisation collects, holds, uses, shares, discloses, destroys and processes personal information.

8.2 Information Officer

The organisation's Information Officer is responsible for:

- Taking steps to ensure the organisation's reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about the organisation's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures. This will include reviewing the organisation's information protection procedures and related policies.
- Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- Ensuring that the organisation makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the organisation. For instance, maintaining a "contact us" facility on the organisation's website.

- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of the organisation's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the organisation's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organisation.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by the organisation's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

The Deputy Information Officer will assist the Information Officer in performing his or her duties.

8.3 IT Manager

The organisation's IT Manager is responsible for:

- Ensuring that the organisation's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
- Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Ensuring that personal information being transferred electronically is encrypted.
- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- Performing regular IT audits to ensure that the security of the organisation's hardware and software systems are functioning properly.
- Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the organisation's behalf. For instance, cloud computing services.

8.4 Marketing & Communication Manager

The organisation's Marketing & Communication Manager is responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the organisation's website, including those attached to communications such as emails and electronic newsletters.
- Addressing any personal information protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with persons acting on behalf of the organisation to ensure that any outsourced marketing initiatives comply with POPIA.

8.5 Employees and other Persons acting on behalf of the Organisation

Employees and other persons acting on behalf of the organisation will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

Employees and other persons acting on behalf of the organisation are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of the organisation may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the organisation or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of the organisation must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of the organisation will only process personal information where:

- The data subject, or a competent person where the data subject is a child, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing protects a legitimate interest of the data subject; or
- The processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:

- Clearly understands why and for what purpose his, her or its personal information is being collected; and
- Has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of the organisation will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the organisation will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- the personal information has been made public, or
- where valid consent has been given to a third party, or
- the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of the organisation will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the organisation's central database or a dedicated server.
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
- Transfer personal information outside of South Africa without the express permission from the Information Officer.

Employees and other persons acting on behalf of the organisation are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the organisation, with the sending or sharing of personal information to or with authorised external persons.
- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.
- Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first

be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.

- Undergoing POPI Awareness training from time to time.

Where an employee, or a person acting on behalf of the organisation, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

9. POPI AUDIT

The organisation's Information Officer will schedule periodic POPI Audits.

The purpose of a POPI audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy personal information.
- Determine the flow of personal information throughout the organisation. For instance, the organisation's various business units, divisions, branches and other associated organisations.
- Redefine the purpose for gathering and processing personal information.
- Ensure that the processing parameters are still adequately limited.
- Ensure that new data subjects are made aware of the processing of their personal information.
- Re-establish the rationale for any further processing where information is received via a third party.
- Verify the quality and security of personal information.
- Monitor the extend of compliance with POPIA and this policy.
- Monitor the effectiveness of internal controls established to manage the organisation's POPI related compliance risk.

In performing the POPI Audit, Information Officers will liaise with line managers in order to identify areas within in the organisation's operation that are most vulnerable or susceptible to the unlawful processing of personal information.

Information Officers will be permitted direct access to and have demonstrable support from line managers and the organisation's governing body in performing their duties.

10. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Data subjects have the right to:

- Request what personal information the organisation holds about them and why.
- Request access to their personal information.
- Be informed how to keep their personal information up to date.

Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a "Personal Information Request Form".

Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against the organisation's PAIA Policy.

The Information Officer will process all requests within a reasonable time.

11. POPI COMPLAINTS PROCEDURE

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The organisation takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

- POPI complaints must be submitted to the organisation in writing. Where so required, the Information Officer will provide the data subject with a "POPI Complaint Form".
- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
- The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the organisation's data subjects.
- Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with the organisation's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.
- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the organisation's governing body within 7 working days of receipt of the complaint. In all instances, the organisation will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
- The Information Officer's response to the data subject may comprise any of the following:
 - A suggested remedy for the complaint,
 - A dismissal of the complaint and the reasons as to why it was dismissed,
 - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
- The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

12. DISCIPLINARY ACTION

Where a POPI complaint or a POPI infringement investigation has been finalised, the organisation may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In the case of ignorance or minor negligence, the organisation will undertake to provide further awareness training to the employee.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the organisation may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action.
- A referral to appropriate law enforcement agencies for criminal investigation.
- Recovery of funds and assets in order to limit any prejudice or damages caused.

ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer:

Name

Contact Number

Email Address:

Please be aware that we may require you to provide proof of identification prior to processing your request.

There may also be a reasonable charge for providing copies of the information requested.

A. Particulars of Data Subject

Name & Surname

Identity Number:

Postal Address:

Contact Number:

Email Address:

B. Request

I request the organisation to:

- (a) Inform me whether it holds any of my personal information
- (b) Provide me with a record or description of my personal information
- (c) Correct or update my personal information
- (d) Destroy or delete a record of my personal information

C. Instructions

<div data-bbox="26 6268 144 6281" data

ANNEXURE B: POPI COMPLAINT FORM

**PROTECTION OF PERSONAL
INFORMATION ACT 4 OF 2013**
AUDIT: 1 MARCH 2021

Bylae 6

PERSONAL INFORMATION KEPT:

1. OFFICE **CARITAS GEMEENSKAPFOKUS NPC** HEAD OFFICE INCUMBENT CHRISTELLE DU PLOOY
2.
 - a. PURPOSE OF THE OFFICE TO DELIVER AN ADMINISTRATION AND HR SERVICE TO CARITAS BUSINESS ORGANISATION
 - b. **Store** SECURE OFFICE AND WALK-IN SAFE FACILITY
 - c. **Personal Information:** race, gender, pregnancy, marital status, national, ethnic, colour, age, physical health, disability, religion, belief, culture, language and birth of the person;
 - d. education, criminal or employment history of the person
 - e. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person
 - f. the biometric information of the person;
3. OFFICE RECEPTION ADMINISTRATION INCUMBENT - SANDRA WALLES
4. PURPOSE OF THE OFFICE TO DELIVER A RECEPTION AND FILING/ADMIN SERVICE TO CARITAS
 - a. **Store** SECURE OFFICE AND WALK-IN SAFE FACILITY
 - b. **Personal Information:** race, gender, pregnancy, marital status, national, ethnic or social origin, colour, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
 - c. education or the medical, financial, criminal or employment history of the person
 - d. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person
 - e. the biometric information of the person;
5. OFFICE MARKETING INCUMBENT - ESTE VAN DER MERWE
6. PURPOSE OF THE OFFICE TO DELIVERD A MARKETING SERVICE TO CARITAS

- a. **Store On computer which are password protected and link to the server**
- b. **Personal Information:** race, gender, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- c. education or the medical, financial, criminal or employment history of the person
- d. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person
- e. the biometric information of the person;

Recruitment

Normal recruitment processes were followed. All CV's received and unsuccessful - shred after 3 days if it is not required by the applicant

Software Security

All laptops are locked in secure safe after hours. Data is stored on the server and all computers are protected by pass word and

Antivirus software

Database Storage

Data is stored on the server and all computers are protected by password and antivirus software

LETTER FOR

APPOINTMENT

BYLAE 7

INFORMATION OFFICER CARITAS

The Information Officer role is by default that of the Designated Head of a Private Body in terms of the provisions of both the Promotion of Access to Information (PAI) Act, 2000 (see Appendix A of this document) and the Protection of Personal Information (POPI) Act, 2013 (see

Appendix B of this document). The responsibilities defined for these roles in Quiver HR, a private body in terms of the POPI Act and PAI Act, are:

POPI Act Section 55(1): An information officer's responsibilities include—

- (a) the encouragement of compliance, by the body, with the conditions for the lawful processing of personal information;
- (b) dealing with requests made to the body pursuant to this Act;
- (c) working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the body;
- (d) otherwise ensuring compliance by the body with the provisions of this Act; and
- (e) as may be prescribed.

Regulations relating to the Protection of Personal Information, 2018: Responsibilities of Information Officers

4. (1) An information officer must, in addition to the responsibilities referred to in section 55(1) of the Act, ensure that-

- (a) a compliance framework is developed, implemented, monitored and maintained
 - (b) a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
 - (c) a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);
 - (d) internal measures are developed together with adequate systems to process requests for information or access thereto; and
 - (e) internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.
- (2) The information officer shall upon request by any person, provide copies of the manual to that person upon the payment of a fee to be determined by the Regulator from time to time.

POPI Act, 2013 Part B: Designation and delegation of deputy information officers

56. Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of—

- (a) such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of this Act; and

(b) any power or duty conferred or imposed on an information officer by this Act to a deputy information officer of that public or private body.

CARITAS Information Officer role appointment acceptance:

SANDRA WALLES

SIGNATURE _____

DATE OF APPOINTMENT ACCEPTANCE

Deputy Information Officer Role appointment acceptance:

SIGNATURE _____

DATE OF APPOINTMENT ACCEPTANCE

Examples of specific duties for the information officer which could be included in the appointment letter:

POPI Act Information Officer / Deputy Role Responsibilities:

- Complete initial and ongoing compliance assessments
- Developing, publishing and maintaining a POPI Policy which addresses all relevant provisions of the POPI Act
- Reviewing the POPI Act and periodic updates as published

- Ensuring that POPI Act induction training takes place for all staff
 - Ensuring that periodic communication awareness on POPI Act responsibilities takes place
 - Ensuring that Privacy Notices for internal and external purposes are developed and published
 - Handling data subject access requests
 - Approving unusual or controversial disclosures of personal data
 - Approving contracts with operators as defined in the POPI Act
 - Ensuring that appropriate policies and controls are in place for ensuring the acceptable quality of personal information in line with the POPI Act are in place
 - Ensuring that appropriate security safeguards in line with the POPI Act for personal information are in place
 - Handling all aspects of relationship with the Information Regulator as foreseen in the POPI Act
 - Provide direction to any Deputy Information Officer if and when appointed
-
-