

NHKA

NEDERDUITSCH HERVORMDE KERK VAN AFRIKA



POPIA-BELEID

VAN

NEDERDUITSCH HERVORMDE KERK VAN AFRIKA

Mei 2025



**BELEIDSDOKUMENT VIR DIE TOEPASSING VAN
DIE WET OP DIE BESKERMING VAN PERSOONLIKE INLIGTING, NO 4 VAN 2013**

Saamgestel deur: Gerhard Pieters
Inligtingsbeampte van die Sinodale Dienssentrum

INLIGTING

Dokumentverwysing:	POPIA-beleid
Verantwoordelike persoon (vir beleid):	Gerhard Pieters
Afdeling verantwoordelik:	Argief en Inligtingsbestuur
Outeur(s):	Gerhard Pieters Dr Wouter van Wyk
Datum van hierdie weergawe:	27 Mei 2025
Weergawe nommer:	3
Hersieningsdatum:	27 Mei 2025
Konsultasie met:	Nándor Sarkady Dr Wouter van Wyk

WEERGAWEREKORD

	Nr	Datum	Veranderinge
Huidige weergawe	3	27 Mei 2025	
Vorige weergawe:	2	31 Augustus 2023	

INHOUDSOPGAWE

1. INLEIDING EN DOEL VAN DIE HANDLEIDING.....	4
2. POPIA: INLIGTINGSBEAMPTE	4
3. DATA-INSAMELING	5
3.1. Tipe data	5
3.2. Doel waarvoor die data ingesamel word	7
3.3. Toestemming van datasubjek.....	7
3.4. Berging van data.....	8
3.5. Deursigtigheid	8
3.6. Toegang tot data	8
4. DATAGEBRUIK EN BEPERKINGS	8
4.1. Datagebruik.....	8
4.2. Databeperkings	9
5. DATABERGING	9
6. DATABEVEILIGING.....	9
7. DATARETENSIE.....	10
8. DATAVERNIETIGING	11

1. INLEIDING EN DOEL VAN DIE HANDLEIDING

Die Wet op die Beskerming van Persoonlike Inligting (“POPIA”) het ten doel om uitvoering te gee aan die grondwetlike reg op privaatheid deur dit te balanseer met dié van toegang tot inligting. POPIA vereis dat persoonlike inligting wat op individue betrekking het, wettig en op ’n redelike wyse verwerk moet word wat nie inbreuk maak op die reg op privaatheid nie.

Hierdie dokument hou dus verband met en verduidelik hoe die Sinodale Dienssentrum van die NHKA persoonlike inligting verkry, verwerk, gebruik, berg, openbaar maak en vernietig in ooreenstemming met die vereistes van POPIA.

2. POPIA: INLIGTINGSBEAMPTE

Die Sinodale Dienssentrum het ’n hoof inligtingsbeampte en adjunk inligtingsbeampte aangestel soos uiteengesit in die Wet volgens artikel 55, en die aanstelling geregistreer by die Reguleerder. Die registrasie sertifikaat van die inligtingsbeampte(s) aan die Reguleerder is aangeheg as **BYLAAG A**.

Die verantwoordelikhede van die inligtingsbeampte(s) behels die volgende:

- Aanmoediging tot voldoening, deur die NHKA, aan die voorwaardes vir die regmatige prosessering van persoonlike inligting.
- Die hantering van versoeke wat ooreenkomstig hierdie Wet aan die NHKA gerig word.
- Samewerking met die Reguleerder rakende ondersoeke in ooreenstemming met hoofstuk 6 met betrekking tot die NHKA.
- Om andersins die NHKA se voldoening aan die bepalings van hierdie Wet te verseker.

Besonderhede van die inligtingsbeampte(s)

Hoofinligtingsbeampte	Mnr Johan Hattingh	Swaanstraat 129, East Lynne, Pretoria Posbus 2368 Pretoria 0001 johan@nhk.co.za +27 72 244 0490
-----------------------	--------------------	---

		(012) 322 8885 x 3008
Adjunkinligtingsbeamppte	Mnr Gerhard Pieters	Swaanstraat 129, East Lynne, Pretoria Posbus 2368 Pretoria 0001 Erfenisentrum Monumentheuwel, Eufeesstraat Groenkloof, Pretoria Posbus 2368 Pretoria 0001 data@nhk.co.za +27 84 438 6052 (012) 322 8885 x 3

3. DATA-INSAMELING

3.1. Tipe data

Die tipe data wat versamel word deur die Sinodale Dienssentrum is van toepassing op gemeentes, predikante en personeellede in hul diens. Die volgende is 'n lys van die soort inligting wat die Sinodale Dienssentrum versamel en bewaar:

- Identiteitsnommer/paspoortnommer.
- Geboortedatum/ouderdom.
- Telefoonnommers.
- E-posadresse.
- Fisiese adres.
- Geslag, ras en etniese oorsprong.
- Foto's, stemopnames, video-opnames, biometriese data.
- Huwelikstatus en familieverwantskappe.
- Kriminele rekord.
- Private korrespondensie.

- Godsdienstige en wêreldbeskoulige oortuigings.
- Indiensnemingsrekords en vergoedingsinligting.
- Finansiële inligting.
- Opvoedkundige inligting.
- Fisiese en psigiese gesondheidsinligting, mediese geskiedenis en bloedgroep.
- Lidmaatskap van verenigings en organisasies.
- Personeelinligting – pensioen, medies.

Die Sinodale Dienssentrum versamel persoonlike inligting van die volgende groepe: personeellede en predikante.

Predikante	Volle name en van ID-nommer Kontakbesonderhede Huis- en posadres Persoonlike e-posadresse Pensioen- en mediese inligting Opvoedkundige inligting Huwelikstatus en familieverwantskappe Private korrespondensie
Personeel	Volle name en van ID-nommer Kontakbesonderhede Huis- en posadres Persoonlike e-posadresse Geslag, ras en etniese oorsprong Kriminele rekord Pensioen- en mediese inligting Opvoedkundige inligting Huwelikstatus
Lidmate	Die Sinodale Dienssentrum versamel nie lidmate se persoonlike data nie. Die taak om sodanige inligting te bekom, rus by die gemeente self. Dit beteken dat elke gemeente moet verseker dat hul POPIA-beleid duidelik aandui watter data hulle bymekaarmaak.

3.2. Doel waarvoor die data ingesamel word

Die Sinodale Dienssentrum dien as 'n skakel tussen die gemeentes van die Nederduitsch Hervormde Kerk van Afrika (NHKA) en is die sentrum wat gedeelde dienste aan al die gemeentes van die Kerk lewer. Hierdie dienste sluit onder meer kommunikasie, publikasies en kerklike skryfbehoeftes, IT, finansies, en ouditering in. Die Sinodale Dienssentrum dien ook as skakel met ringskommissies, kerklike rade en werkgroepe, ander kerke en ekumeniese vennote, die staat, die pensioenfonds, die mediese fonds, en ander instansies.

Die Sinodale Dienssentrum versamel en bewaar daarom die kontakinligting van predikante en gemeentes se funksionariese (skribas, skribas vir registrasie, kassiere, administratiewe beampptes en ander) ter wille van effektiewe kommunikasie. Hierdie inligting word veilig in die Kerk se inligtingstelsel bewaar en aan geen buite-instansie verskaf nie. Die inligting word met die medewete en instemming van die betrokkenes jaarliks in die NHKA se Almanak gepubliseer, wat slegs via gemeentes verkoop en versprei word. Die inligting is nie in elektroniese formaat in die openbare domein beskikbaar nie.

3.3. Toestemming van datasubjek

Die Sinodale Dienssentrum verkry toestemming van gemeentes, predikante en personeel deur hulle 'n vorm te laat invul. Die vorm bevat al die inligting wat benodig word vir die toestemming om persoonlike inligting te verkry, te verwerk en te berg. Daar word ook rekord gehou van hierdie vorms, wat op 'n veilige plek gestoor word. Die doel van die vorms is ook om rekord te hou van wie toestemming gegee het en om te verseker dat nuwe ampsdraers en personeellede toestemming gee dat hul persoonlike inligting versamel mag word.

Die Sinodale Dienssentrum bevestig ook dat alle nuwe ampsdraers en personeellede (van die Kerk, gemeentes en die Sinodale Dienssentrum) hierdie vorm sal invul om te verseker dat die Sinodale Dienssentrum voldoen aan die Wet. Die toestemmingsvorm is aangeheg as **BYLAAG B**. Indien iemand beswaar wil maak teen die verwerking van sy/haar persoonlike inligting, kan die vorm wat as **BYLAAG C** aangeheg is, ingevul word.

Indien 'n persoon minderjarig is, moet toestemming verkry word van die minderjarige se ouer of voog. Dit is van uiterste belang dat hierdie toestemming verkry moet word wanneer 'n minderjarige se persoonlike inligting versamel word, en dat dit vertroulik geberg moet word. Persoonlike inligting sal nooit gebruik word vir direkte bemerking nie.

3.4. Berging van data

Die data word geberg op personeellede se rekenaars wat gekoppel is aan 'n aanlyn platform. Hierdie platform het streng maatreëls in plek wat verseker dat nie almal toegang het tot die persoonlike inligting nie, maar net personeellede wat nodig het om hierdie persoonlike inligting te verwerk. Streng vertroulike inligting word ook geberg en gestoor op 'n aanlyn platform, wat verhoed dat enige personeellid toegang het tot die inligting.

3.5. Deursigtigheid

Elke predikant, gemeente en personeellid moet verstaan hoekom hul persoonlike inligting versamel, verwerk en gestoor word. Die Sinodale Dienssentrum sal nooit inligting versamel of bewaar vir enige ander doel as om kerklike werksaamhede te ondersteun nie, en onderneem om te alle tye deursigtig te wees oor die doel en wyse waarop predikante, gemeentes en personeellede se persoonlike inligting versamel en bewaar word.

3.6. Toegang tot data

Persone wat daarop geregtig is, kan toegang kry tot hul persoonlike inligting wat die Sinodale Dienssentrum oor hulle berg en bewaar. Dit is elke persoon se reg om toegang te kry tot hierdie inligting.

Hoe kan jy toegang kry tot jou persoonlike inligting?

'n Vorm wat hierby aangeheg is as **BYLAAG D**, kan ingevul word om toegang te verkry tot jou persoonlike inligting.

4. DATAGEBRUIK EN BEPERKINGS

4.1. Datagebruik

Persoonlike inligting word gebruik om daaglikse take binne die Sinodale Dienssentrum te verrig. Spesifiek word persoonlike inligting gebruik om die volgende te doen:

- **Kommunikasie.** Kontakbesonderhede word gebruik om predikante, gemeentes se funksionaris (skribas, skribas vir registrasie, kassiere, administratiewe beamptes en ander) te kontak.
- **Personeelfunksies.** Personeelle se persoonlike inligting word versamel en word gebruik deur die afdelings Finansies en Menslike Hulpbronne vir administratiewe doeleindes.
- **Jaarlikse Almanak.** Persoonlike inligting word versamel om 'n jaarlikse Almanak te publiseer wat verkoop word aan predikante en gemeentes. Die inligting is nie in elektroniese formaat in die openbare domein beskikbaar nie.

4.2. Databeperkings

Net sekere personeelle en predikante het toegang tot bepaalde persoonlike inligting.

- Predikante het die minimum toegang tot persoonlike inligting, maar het wel toegang tot sekere inligting om hul ampswerk te verrig.
- 'n Beperkte aantal personeelle het toegang tot persoonlike inligting. Net sekere personeelle kan hierdie persoonlike inligting wysig en verander. Hierdie persoonlike inligting kan net verander as die betrokke predikante, gemeentes en kerkrade dit versoek of daartoe instem.

5. DATABERGING

Data word geberg op die volgende maniere:

- Op personeelle se skootrekenaars wat gekoppel is aan 'n aanlyn bediener (*server*) en platforms soos Microsoft OneDrive en Microsoft SharePoint.
- Persoonlike kontaknommer(s) en ander persoonlike inligting word aanlyn geberg en 'n rugsteun word na 'n bediener gemaak sodat geen inligting per abuis vernietig word of verlore gaan nie.
- Verouderde persoonlike inligting (harde kopieë) word gehou vir argiefdoeleindes en bewaring van die geskiedenis, en word bewaar in die Kerkargief wat toegesluit word. Toegang tot hierdie Argief word met opgaaf van redes verkry van die personeelle verantwoordelik vir inligtingsbestuur en die Kerkargief.

6. DATABEVEILIGING

Die Sinodale Dienssentrum beveilig persoonlike inligting op die volgende maniere:

- **Aanlyn bediener.** Die aanlyn bediener is beveilig deur sterk wagwoorde sodat net sekere personeellede toegang daartoe kan kry. Kommunikasiedata word bewaar deur data-enkripsie. Data word ook gereeld gerugsteun om te verseker dat persoonlike inligting nie verlore gaan nie. Die IT-funksie hou bedryfstelsels op datum en pas sekuriteitsmaatreëls toe soos dit vrygestel word.
- **Toegangsbeheer.** Net sekere personeel het toegang tot sekere platforms en lêers waar persoonlike inligting gestoor word in lyn met hul verantwoordelikhede en onderhewig aan die ondertekening van 'n onderneming om die inligting vertroulik te hou.
- **Wagwoorde.** Wagwoorde is die eerste lyn van verdediging teen ongemagtigde toegang tot aanlyn rekeninge, toestelle en lêers. Die Sinodale Dienssentrum gebruik sterk wagwoorde wat help om data teen kwaadwillige persone en sagteware te beskerm, asook om die toegang van personeellede te beheer en te monitor. Personeel moet hul wagwoorde elke 12 maande verander en mag ook onder geen omstandighede mekaar se wagwoorde gebruik nie.
- **Gebruik van twee-faktor-verifikasie (Microsoft Authenticator).** Twee-faktor-verifikasie (2FA) is 'n sekuriteitsproses wat die waarskynlikheid verhoog dat 'n persoon is wie hy sê hy is. Die proses versoek gebruikers om twee verskillende stawingsfaktore te verskaf voordat hulle toegang tot 'n toepassing of stelsel kan kry, eerder as bloot hul gebruikersnaam en wagwoord.
- **Antivirus en brandmure.** Rekenaars en stelsels word beveilig deur antivirusprogramme en brandmure wat geïnstalleer is regoor die netwerk van die Sinodale Dienssentrum.

7. DATARETENSIE

Persoonlike inligting word gehou wanneer 'n predikant, gemeente en personeellid in diens is by die Sinodale Dienssentrum en daarna. Die Wet stipuleer dat inligting oor datasubjekte nie langer bewaar mag word as wat die oorspronklike doel daarvoor was nie, soos uiteengesit in artikel 14 (1) en (2). Daar is egter uitsonderings in die Wet wat toelaat dat die inligting wel vir 'n langer tydperk bewaar kan word, soos vir historiese, statistiese en navorsingsdoeleindes en finansiële rekords. Die Wet bepaal ook dat inligting gehou mag word as dit benodig word vir die funksionering van die organisasie.

Raadpleeg hiervoor die Riglyne vir Bewaring soos deur die Argief: <https://nhka.org/wp-content/uploads/2022/11/2022-Riglyne-vir-die-bewaring-van-argiewe-2.pdf>

8. DATAVERNIETIGING

Wanneer persoonlike inligting vernietig word, sal die Sinodale Dienssentrum seker maak dat alle rekords van die hele netwerk, asook van alle bergingstoestelle en aanlyn platforms soos OneDrive en SharePoint, verwyder word. Dit is noodsaaklik om te verseker dat die persoonlike inligting van predikante en ander personeellede geskrap word volgens die onderstaande riglyne:

Volgens die wetgewing, sodra 'n werksverhouding beëindig is, of wanneer 'n predikant of personeellid aftree of bedank, moet die betrokke persoonlike inligting vernietig word. Nietemin behou die Sinodale Dienssentrum sekere rekords vir langer tydperke ter wille van historiese doeleindes of die vereistes van wetgewing soos:

- Werkskontrak (3 jaar).
- Arbitrasietoekennings (3 jaar).
- SAID-werknemersrekords (5 jaar).
- OHSa-voorvalrekords (3 jaar).
- Werknemers se dissiplinêre rekords (onbepaalde tyd).

Die Sinodale Dienssentrum het die volgende beleid ten opsigte van die vernietiging van dokumente:

- Alle dokumente mag slegs vernietig word na goedkeuring van die argivaris en/of inligtingsbeampte.

Die Inligtingsbeampte dra die verantwoordelikheid om die volgende tipes dokumente en data te vernietig:

- Onnodige duplikaatdokumente.
- Kopieë wat as werkskopieë gedien het.
- Lyste of rekords wat nie meer relevant of benodig is nie.

Aangaande die vernietiging van elektroniese rekords en data:

- Slegs die nuutste rugsteundata word behou, terwyl vorige weergawes vernietig word. Gesonde praktyke word gevolg om historiese weergawes (*version control*) te bestuur.

- Elektroniese kopieë van data wat vir ander doeleindes saamgestel is, maar waarvan die oorspronklike reeds in databasisse opgeneem is, word vernietig.
- Ongebruikte ou hardeskywe word vernietig.
- Digitale sanitasie word gebruik om ou rekenaartoerusting skoon te maak. Enkele uitwissings is dikwels onvoldoende, omdat dit slegs die toegang tot rekords verwyder. In sekere gevalle kan toerusting ook fisies verniet word.

Wat papierdokumente betref:

- Die onnodige druk van elektroniese weergawes van persoonlike data word vermy.
- Ou of oorbodige papierdokumente word nie sommer in die snippermandjie gegooi nie, maar word eerder verbrand, versnipper, of verpulp vir maksimum sekuriteit.
- Alle vernietigingsprosesse word weldeurdag uitgevoer.

Indien 'n personeellid, gemeente of predikant persoonlike inligting wil skrap of vernietig, kan die toepaslike vorm onder **BYLAAG E** ingevul en ingedien word. As alternatief vir die voltooiing van **BYLAAG E**, kan die versoek ook ingedien word deur een van die volgende kommunikasiekanale:

- Persoonlike oorhandiging
- Pos
- E-pos
- SMS
- WhatsApp

Alle versoeke sal binne 30 (dertig) dae na ontvangs van die versoek **gratis** verwerk word, en die betrokke party sal van die uitkoms in kennis gestel word.