



Verwysingsnommer: 4/6/2

DEPARTEMENT VAN MAATSKAPLIKE ONTWIKKELING

**WBPI VOLDOENINGSRAAMWERK EN PRIVAATHEIDSKENNISGEWING
2025 - 2026**

Geskiedenis van Hersiening

Datum	Weergawe	Beskrywing	Skrywer
17 Februarie 2025	Konsep W1	Jaarlike hersiening	K Marthinus
29 Februarie 2025	Konsep W2	Jaarlikse hersiening	K Marthinus
13 Maart 2025	Finaal	Goedgekeur	K Marthinus

INHOUDSOPGAWE

Definisies.....	2
1. Inleiding	4
2. Doel.....	4
3. Beleidsverklaring	4
4. Omvang.....	5
5. Risiko's	5
6. Verantwoordelikhede.....	5
7. Algemene riglyne vir personeel	7
7.1 Versameling	8
7.2 Klassifikasie	8
7.3 Gebruik	8
7.4 Bewaring	8
7.5 Akkuraatheid van data.....	9
7.6 Wegdoening.....	10
8. Data-onderwerp toegangsversoeke	10
9. Openbaarmaking (deel) van persoonlike inligting	10
9.1 Interne openbaarmaking.....	10
9.2 Eksterne openbaarmaking.....	11
10. Kennisgewing aan data-onderwerpe.....	11
11. Afdwinging van beleid	11
12. Hersiening en bywerking	11
13. Aanbeveling en goedkeuring	12
BYLAE A: DMO WBPI PRIVAATHEIDSKENNISGEWING	13

Definisies

die Departement	Departement Maatskaplike Ontwikkeling, Wes- Kaap
Data-onderwerp	Betekende die identifiseerbare natuurlike/regspersoon op wie persoonlike inligting betrekking het.
Inligtingsbates	Betekende die bates wat die organisasie gebruik om inligting te skep, stoor, oordra, uitwis en/of te vernietig om sy besigheidsaktiwiteite te ondersteun asook die inligtingstelsels waarmee daardie inligting verwerk word. Dit sluit in: • Alle elektroniese en nie-elektroniese inligting wat geskep of gebruik word om besigheidsaktiwiteite te ondersteun ongeag vorm of medium, byvoorbeeld papierdokumente, elektroniese lêers, stemkommunikasie, teksboodskappe, foto's of video's. • Alle toepassings, toestelle en ander stelsels waarmee die organisasie sy inligting verwerk, byvoorbeeld telefone, faksmasjiene, drukkers, rekenaars, netwerke, stempos, e-pos, kitsboodskappe, slimfone en ander mobiele toestelle ("IKT-bates")
Inligtingsbewaarder	Betekende die persoon wat verantwoordelik is vir die omskrywing en implementering van sekuriteitsmaatreëls en kontroles vir Inligting- en Kommunikasietegnologie ("IKT") bates.
Eindgebruiker van inligting	Betekende 'n persoon wat in aanraking kom met inligtingsbates en IKT-bates met die doel om 'n gemagtigde taak uit te voer.
Inligtingsbeampte	Betekende die Direkteur-Generaal in die geval van die Departement van die Premier en die Rekenpligtige Beampte in die geval van die ander provinsiale departemente.
Inligtingseienaar	Betekende 'n persoon wat verantwoordelik is vir, of afhanklik is van die besigheidsproses wat met 'n inligtingsbate geassosieer word.
Persoonlike inligting	Betekende inligting met betrekking tot 'n identifiseerbare, lewende, natuurlike persoon, en waar dit van toepassing is, 'n identifiseerbare, bestaande regspersoon, insluitend, maar nie beperk nie tot – a) Inligting wat verband hou met die ras, geslag, huwelikstatus, nasionaliteit, ouderdom, fisiese of geestelike gesondheid, gestremdheid, geloof, kultuur, taal en geboorte van die persoon. b) Inligting wat verband hou met die opvoeding of die mediese, finansiële, kriminele of werkgeskiedenis van die persoon. c) enige identiteitsnommer, simbool, e-posadres, fisiese adres, telefoonnommer, ligginginligting, aanlyn identifiseerder of ander spesifieke toekenning aan die persoon

	d) die biometriese inligting van die persoon. e) die persoonlike opinies, sienings of voorkeure van die persoon. f) korrespondensie gestuur deur die persoon wat implisiet of uitdruklik van 'n private of vertroulike aard is of verdere korrespondensie wat die inhoud van die oorspronklike korrespondensie sou openbaar g) die sienings of menings van 'n ander individu oor die persoon; en die naam van die persoon indien dit saam met ander persoonlike inligting wat met die persoon verband hou verskyn of as die bekendmaking van die naam self inligting oor die persoon sou openbaar.
Verwerking	Beteken enige operasie of aktiwiteit of enige stel operasies rakende persoonlike inligting, insluitend: a) die versameling, ontvangs, optekening, organisering, versameling, stoor, opdatering, wysiging, herwinning, wysiging, konsultasie of gebruik; b) verspreiding deur middel van oordrag of beskikbaarstelling in enige ander vorm; of c) samevoeging, koppeling, sowel as beperkings, agteruitgang, uitwis of vernietiging van inligting.
Spesiale persoonlike inligting	Beteken persoonlike inligting soos bedoel in artikel 26 van WBPI, insluitend. (a) Die godsdienstige of filosofiese oortuigings; ras of etniese herkoms; lidmaatskap van 'n vakbond; politieke oortuigings; gesondheid of sekslewe of biometriese inligting van 'n data-onderwerp. (b) die kriminele gedrag van 'n data-onderwerp en die mate waarin sodanige inligting verband hou met- (i) die beweerde pleging deur 'n data-onderwerp van enige misdryf; of (ii) Enige verrigtinge ten opsigte van enige misdryf wat na bewering deur 'n 'n data-onderwerp gepleeg word of die afhandeling van sodanige verrigtinge.
WBPI	Wet op die Bevordering van Toegang tot Persoonlike Inligting (POPIA, 2013)
WKR	Wes Kaapse Regering

1. Inleiding

Die Departement van Maatskaplike Ontwikkeling ("Departement") moet sekere inligting oor individue en regspersone (gesamentlik na verwys as "data-onderwerpe") insamel en gebruik. Dit kan kliënte/klante, verskaffers, besigheidskontakte, werknemers en ander mense insluit met wie die organisasie 'n verhouding het of dalk mee in verbinding moet tree. Hierdie beleid beskryf hoe hierdie inligting ingesamel, hanteer en gestoor moet word om aan die organisasie se persoonlike inligtingbeskermingstandaarde en aan die wet te voldoen.

Hierdie beleid moet saam met dié Departement se Inligting-sekuriteit Klassifikasiestelsel ("ISCS") gelees word.

2. Doel

Hierdie privaatheidsbeleid verseker dat die organisasie:

- voldoen aan die Wet op die Beskerming van Persoonlike Inligting, 2013 (Wet 4 van 2013) (WBPI).
- die regte van data-onderwerpe beskerm.
- deursigtig is wat betref die stoor en verwerking van persoonlike inligting oor data-onderwerpe, en
- homself beskerm teen die risiko's van 'n sekuriteitskending.

3. Beleidsverklaring

Die organisasie is daartoe verbind om die privaatheid van data-onderwerpe te beskerm in ooreenstemming met die verpligtinge wat deur die WBPI opgelê word. Die WBPI beskryf hoe organisasies die persoonlike inligting van data-onderwerpe moet versamel, hanteer en stoor. Hierdie reëls geld ongeag of die inligting elektronies, op papier of op ander materiaal gestoor word. Om aan die wet te voldoen, moet persoonlike inligting regverdig ingesamel, veilig gestoor en nie onregmatig bekend gemaak word nie.

Die WBPI word ondersteun deur die volgende belangrike privaatheidsbeginsels wat bepaal dat persoonlike inligting aan die volgende vereistes moet voldoen:

- Op billike en wettige manier verwerk
- Slegs vir spesifieke, wettige doeleindes bekom
- Voldoende, tersaaklik en nie buitensporig
- Akkuraat en op datum gehou
- Hou vir nie langer as wat nodig is nie
- Verwerk in ooreenstemming met die regte van data-onderwerpe
- Op gepaste maniere beskerm, en
- Oorgeplaas buite Suid-Afrika slegs na 'n land of gebied wat ook 'n voldoende vlak van beskerming verseker

4. Omvang

Hierdie beleid is van toepassing op al die organisasie se werknemers en enige ander persoon of entiteit wat vir of namens die organisasie werk, insluitend:

- interns
- vrywilligers
- konsultante, en
- kontrakteurs, verskaffers of diensverskaffers, insluitend hul personeel of agente

Dit beheer alle besigheidsaktiwiteite wat die verwerking van persoonlike inligting, insluitend spesiale persoonlike inligting, vir of namens hierdie organisasie behels. Dit kan die volgende insluit:

- name van individue en regspersone (tesame met enige van die volgende)
- kontakinligting soos pos- en e-posadresse en telefoonnommers
- biografiese inligting soos geboortedatum, ras, geslag en huwelikstatus
- enige identifiserende nommer, ligginginligting of aanlyn identifiseerder
- biometriese inligting soos vingerafdrukke
- opvoedkundige, mediese, finansiële, kriminele of werkgeskiedenis

5. Risiko's

Hierdie beleid help om die organisasie teen 'n paar baie realistiese sekuriteitsrisiko's te beskerm, insluitend:

- **Verbreking van vertroulikheid.** Byvoorbeeld, inligting wat onvanpas verskaf word.
- **Versuim om keuses te bied.** Byvoorbeeld, alle data-onderwerpe moet vry wees om te kies hoe die organisasie inligting wat met hulle verband hou gebruik waar die persoonlike inligting nie ingevolge 'n wet of 'n ooreenkoms tussen die data-onderwerp en die organisasie versamel, gebruik of gedeel word nie.
- **Skending van reputasie.** Die organisasie kan byvoorbeeld ly indien kuberkrakers suksesvol toegang tot die persoonlike inligting van data-onderwerpe verkry.

6. Verantwoordelikhede

Almal wat vir of saam met die organisasie werk het 'n mate van verantwoordelikheid om te verseker dat die persoonlike inligting van datasubjekte ingesamel, gestoor en toepaslik hanteer word om die vertroulikheid, integriteit en beskikbaarheid daarvan te verseker. Elke Eindgebruiker van inligting, Inligtingseienaar, besigheidseenheid en span wat persoonlike inligting hanteer, moet verseker dat dit in ooreenstemming met hierdie beleid en die privaatheidbeginsels hanteer en verwerk word.

Hierdie mense het sleutelgebiede van verantwoordelikheid:

- a) Die **Inligtingsbeampte** is daarvoor verantwoordelik om te verseker dat die organisasie sy wetlike verpligtinge nakom.
- b) Die **Sekuriteitsbestuurder** is vir die volgende verantwoordelik:
 - Hou die Inligtingsbeampte op hoogte van inligtingsbates en persoonlike inligtingbeskermingsverantwoordelikhede, risiko's en kwessies.

- Hersiening van alle persoonlike inligtingbeskermingsprosedures en verwante beleide, in ooreenstemming met 'n ooreengekome skedule en maak aanbevelings aan die Inligtingsbeampte waar van toepassing.
 - Reël opleiding en advies oor persoonlike inligtingbeskerming vir die mense wat deur hierdie beleid gedek word.
 - Kontrolering en goedkeuring van enige kontrakte of ooreenkomste met derde partye wat persoonlike inligting namens die organisasie kan insamel, hanteer of stoor.
 - Klassifikasie van persoonlike inligting in ooreenstemming met die WKR Inligtingsekuriteit Klassifikasiestelsel.
 - Die handhawing van interne prosedures om die effektiewe hantering en sekuriteit van persoonlike inligting te ondersteun.
 - Verseker dat alle werknemers, konsultante en ander wat aan die Departement rapporteer bewus gemaak word van en opdrag gegee word om aan hierdie en alle ander tersaaklike beleide te voldoen.
- c) Die **Adjunk-inligtingsbeampte(s)** is verantwoordelik vir die hantering van versoeke van data-onderwerpe wat die persoonlike inligting wat die organisasie oor hulle besit wil sien (ook 'data-onderwerp toegangsversoeke' genoem). Die identiteit van enigiemand wat 'n data-onderwerp toegangsversoek rig, moet geverifieer voordat enige persoonlike inligting bekend gemaak word.
- d) Die **Adjunk-inligtingsbeampte, Kennisbestuur**¹ is daarvoor verantwoordelik om die volgende te monitor:
- Om te verseker dat alle IKT-bates wat gebruik word vir die verwerking van persoonlike inligting voldoen aan toepaslike sekuriteitsstandaarde.
 - Doen gereelde kontroles en skanderings om te verseker dat sekuriteitshardware en -sagteware behoorlik funksioneer.
 - Evalueer enige derdepartydienste wat die organisasie oorweeg om te gebruik om persoonlike inligting te verwerk. Byvoorbeeld, wolkbediener rekenaardienste.
- d) Die **Hoofdirekteur Sakebeplanning en -Strategie** in samewerking met die **Direkteur Sakebeplanning en Monitering** is verantwoordelik vir:
- Goedkeuring van enige persoonlike inligtingbeskermingsverklaring wat aan kommunikasie soos e-posse en briewe geheg is.
 - Beantwoording van enige persoonlike inligtingbeskermingsnavrae van joernaliste of media-afsetpunte.
 - Werk, waar nodig, saam met ander besigheidseenhede om te verseker dat alle kommunikasie-inisiatiewe by die privaatheidsbeskermingsbeginsels hou.
- e) Die **Rekordbestuurder** is verantwoordelik vir:
- Monitor die nakoming van personeel wat die goedgekeurde lêerplan van die Departement gebruik om die effektiewe herwinning van rekords te verseker.
 - Verseker dat slegs personeel binne en buite rekordbestuur toegang tot lêers het.

¹ Indien hierdie funksies/sommige van hierdie funksies deur 'n derde party (bv. Ce-I of hul diensverskaffers) verskaf word, is die bestuur en toesig oor die ooreenkoms tussen die Departement en Ce-I die verantwoordelikheid van die [Sekuriteitsbestuurder/Adjunk-inligtingsbeampte/Ander].

- Rangskik rekords op so 'n manier dat dit die behoefte om die volledige lêer te ondersoek wanneer 'n lêer gebruik word, minimaliseer, bv. deur inligting oor die lêers te segmenteer.
 - Verseker dat personeel by die bewaringstydperke van lêers hou sodat rekords weggedoen kan word volgens die goedgekeurde wegdoeningskedule.
 - Gee opleiding aan DMO personeel rakende die veilige bewaring van elektroniese rekords
 - Verseker dat elektroniese rekords in lyn met die wegdoeningstydperk weggedoen/ argiveer word.
- f) Die Adjunk-Direkteur Rekords and Kennisbestuur (**Kennisbestuurder**) is vir die volgende verantwoordelik:
- Voer 'n oudit uit van persoonlike inligting wat deur individue en eenhede gehou word.
 - Stel 'n Persoonlike Inligtingsregister vir die Departement op, werk dit by en hou dit in stand

7. Algemene riglyne vir personeel

- a) Die enigste mense wat toegang kan verkry tot enige persoonlike inligting wat deur hierdie beleid gedek word, moet diegene wees wat **dit vir hul werk nodig het**.
- b) Persoonlike inligting **moet nie informeel gedeel word nie** en moet nooit via sosiale media-rekeninge soos Facebook, LinkedIn, Google Plus ens. gedeel word nie.
- c) Wanneer toegang tot hul vertroulike inligting vereis word, kan werknemers dit van hul lynbestuurders aanvra.
- d) Die organisasie **sal opleiding** aan alle werknemers verskaf om hulle te help om hul verantwoordelikhede te verstaan wanneer persoonlike inligting hanteer word.
- e) Werknemers moet alle persoonlike inligting **veilig** hou deur verstandige voorsorgmaatreëls te tref en die riglyne wat hierin uiteengesit word, te volg.
- f) Dit is uiters belangrik dat **sterk wagwoorde gebruik word** en dit moet nooit met ander gedeel word nie.
- g) Persoonlike inligting **moet nie** aan ongemagtigde persone bekend gemaak word nie, hetsy binne die organisasie of ekstern.
- h) Persoonlike inligting moet **gereeld hersien en bygewerk** word indien daar bevind word dat dit verouderd is. Indien dit nie meer nodig is nie, moet dit uitgewis en weggedoen word in ooreenstemming met die wegdoeningsinstruksies.
- i) Werknemers **moet hulp** van hul lynbestuurder versoek indien hulle onseker is oor enige aspek van die beskerming van persoonlike inligting.
- j) Lynbestuurders moet die hulp van die Adjunk-inligtingsbeamptes versoek indien hulle onseker is oor enige aspek van die beskerming van persoonlike inligting. Die Adjunk-inligtingsbeampte kan met die Sekuriteitsbestuurder en/of ander Adjunk-inligtingsbeamptes in 'n Departementele WBPI-forum konsulteer.
- k) **Let daarop** dat regsdiens in die Departement van die Premier genader kan word om 'n verduideliking te verskaf.

7.1 Versameling

Die organisasie samel inligting in om sy diensleweringmandaat te ondersteun. Persoonlike inligting word direk van data-onderwerpe ingesamel waar prakties en altyd in ooreenstemming met WBPI. Die soort inligting en die doeleindes waarvoor persoonlike inligting ingesamel word, word in die organisasie se Privaatheidskennisgewing uiteengesit. <https://www.westerncape.gov.za/site-page/dsd-paia-popia-2023>. Sien **Bylae A** vir die gewysigde Privaatheidskennisgewing vir die Departement.

7.2 Klassifikasie

Die Inligtingsbeampte klassifiseer inligting in ooreenstemming met die toepaslike wetlike vereistes, waarde, kritiek en sensitiwiteit vir ongemagtigde openbaarmaking, wysiging of verlies met betrekking tot die WKR Inligting-sekureiteits Klassifikasiestelsel ("ISCS").

- Persoonlike inligting word gewoonlik as **VERTROULIK** geklassifiseer.
- Spesiale persoonlike inligting en kinders se inligting word gewoonlik as **GEHEIME INLIGTING** geklassifiseer.

7.3 Gebruik

Wanneer toegang tot persoonlike inligting verkry en gebruik word, skep dit die grootste risiko vir verlies, korrupsie of diefstal. Daarom:

- a) moet werknemers wanneer hulle met persoonlike inligting werk, verseker dat **die skerm van hul rekenaars gesluit is** wanneer hulle onbewaak gelaat word.
- b) Persoonlike inligting moet **nie informeel gedeel word nie**.
- c) Alle persoonlike inligting wat per **e-pos gestuur word** (as 'n aanhangsel of in 'n e-postteks) moet as sensitief en as sodanig beskerm word. Dit moet nie aan iemand buite die organisasie gestuur word nie, tensy dit deur die lynbestuurder goedgekeur is. Dit sluit die aanstuur van sulke e-posse na 'n werknemer se eie persoonlike e-posrekening in.
- d) Voordat e-pos aan 'n mede-werknemer gestuur word, bevestig met die lynbestuurder dat die ontvanger toegelaat word om toegang daartoe te hê aangesien nie alle gebruikers binne die organisasie toegang tot dieselfde inligting het nie.
- e) Data moet **geënkripteer voordat dit elektronies oorgedra word**. Die [Sekuriteitsbestuurder/IT-bestuurder/Ander] kan verduidelik hoe om data na gemagtigde eksterne kontakte te stuur.
- f) Persoonlike inligting moet **nooit buite Suid-Afrika oorgedra word** sonder bevestiging deur die Sekuriteitsbestuurder dat die land waarheen dit oorgedra word 'n voldoende vlak van beskerming van persoonlike inligting verseker nie.
- g) Werknemers **moet nie kopieë van persoonlike inligting op hul eie rekenaars stoor nie**. Verkry altyd toegang tot die sentrale kopie van enige persoonlike inligting en werk dit by

7.4 Bewaring

Hierdie reëls beskryf hoe en waar persoonlike inligting veilig gestoor moet word. Vrae oor die veilige bewaring van persoonlike inligting kan aan die betrokke Adjunk-inligtingsbeampte gerig word.

Wanneer persoonlike inligting **op papier gestoor word**, moet dit op 'n veilige plek gehou word waar ongemagtigde mense dit nie kan sien nie. Hierdie riglyne is ook van toepassing op persoonlike inligting wat gewoonlik elektronies gestoor word, maar om een of ander rede uitgedruk is:

- a) Wanneer toegang nie nodig is nie, moet die papier of lêers **in 'n geslote laai of liasseerkas gehou word**. Waar die inligting as **GEHEIM geklassifiseer word**, moet **toegang** tot die omgewing **beperk** en aangeteken word.
- b) Werknemers moet seker maak dat papier en drukstukke nie op 'n drukker of fotostaatmasjien **waar ongemagtigde mense dit kan sien gelaat word nie**.
- c) **Drukstukke wat persoonlike inligting bevat, moet onmiddellik versnipper word** en veilig vernietig word wanneer dit nie meer benodig word nie.

Wanneer persoonlike inligting **elektronies gestoor word**, moet dit teen ongemagtigde toegang, toevallige uitwissing en kwaadwillige inbraakpogings beskerm word:

- a) Alle elektroniese berging vereis toegangskontroles en lêerbeskermingsmeganismes soos **enkripsie**.
- b) Alle elektroniese toegang moet **aangeteken word**.
- c) Persoonlike inligting moet slegs op **aangewese drywers en bedieners gestoor word** en moet slegs na **goedgekeurde wolkbediener rekenaardienste opgelaaai word**.
- d) Die stoor van persoonlike inligting op enige ander fisiese toestelle, insluitend maar nie beperk nie tot USB-aandrywers (geheuestokkies), eksterne hardeskyf, CD of DVD moet **vooraf** deur die betrokke Adjunk-inligtingsbeamppte goedgekeur word.
- e) Indien persoonlike inligting **op verwyderbare media** (soos 'n geheuestokkie, eksterne hardeskyf, CD of DVD) gestoor word, moet die lêers geïnkripteer, wagwoordbeskerm wees en die media moet veilig weggesluit word wanneer dit nie gebruik word nie.
- f) Waar daar gevind word dat USB-aandrywers (geheuestokkies) as 'n promosie-item uitgedeel is, moet dit nie by enige rekenaar ingesteeek word nie, aangesien hierdie toestelle versteekte wanware of virusse kan bevat.
- g) Alle verlore of gesteelde toestelle (insluitend verwyderbare media) moet onmiddellik by die lynbestuurder aangemeld [en die Sekuriteitsvoorvalkennisgewingdokument moet voltooi word]. <https://inforegulator.org.za/wp-content/uploads/2020/07/FORM-SCN1-Security-Compromises-Notification-Fillable-Formpdf.pdf>
- h) Bedieners wat persoonlike inligting bevat, moet op **'n veilige plek geleë wees**, weg van algemene kantoorruimte.
- i) Elektroniese lêers wat persoonlike inligting bevat, moet gereeld **gerugsteun word**. Daardie rugsteun moet gereeld getoets word in ooreenstemming met die organisasie se standaard rugsteunprosedures.
- j) Alle bedieners, rekenars en ander elektroniese toestelle wat persoonlike inligting bevat, moet deur **goedgekeurde sekuriteitsagteware en 'n brandmuur beskerm word**.

7.5 Akkuraatheid van data

Die wet vereis dat die organisasie redelike stappe moet neem om te verseker dat persoonlike inligting akkuraat en op datum gehou word. Hoe belangriker dit is dat persoonlike inligting akkuraat is, hoe meer moeite moet die besigheidseenheid doen om die akkuraatheid daarvan te

verseker. Dit is die verantwoordelikheid van alle werknemers wat met persoonlike inligting werk om redelike stappe te neem om te verseker dat dit so akkuraat en op datum as moontlik gehou word.

- a) Elektroniese lêers wat persoonlike inligting bevat, sal op **so min plekke as wat nodig is gehou word**. Personeel moenie enige onnodige bykomende datastelle skep nie.
- b) Personeel moet **elke geleentheid gebruik om te verseker dat persoonlike inligting bygewerk word**. Byvoorbeeld, deur 'n kliënt se besonderhede te bevestig wanneer hulle bel.
- c) Die organisasie sal dit **vir data-onderwerpe maklik maak om hul persoonlike inligting wat** die organisasie oor hulle het, by te werk. Byvoorbeeld, via sy webtuiste.
- d) Persoonlike inligting moet **opgedateer word soos onakkuraathede ontdek word**. Byvoorbeeld, indien 'n kliënt nie meer op hul gestoorde telefoonnommer bereik kan word nie, moet dit van die databasis verwyder word.

7.6 Wegdoening

Werkspapiere en kopieë wat ingevolge 'n algemene wegdoeningsinstruksie mee weggedoen mag word, moet weggedoen word deur 'n veilige wegdoeningshouer of versnipperaar te gebruik. Afskrifte van persoonlike inligting, insluitend spesiale persoonlike inligting, geklassifiseer as **GEHEIM** wat **elektronies gestoor word**, moet óf permanent vernietig óf oorskryf word. Die wegdoening van alle oorspronklike lêers en elektroniese lêers moet in ooreenstemming met die organisasie se **Rekordbestuurbeleid uitgevoer word**.

8. Data-onderwerp toegangsversoeke

Alle data-onderwerpe wie se persoonlike inligting deur die organisasie gestoor word, is daarop geregtig om:

- te vra **watter inligting** die organisasie oor hulle het, hoekom hulle dit stoor en met wie dit gedeel word.
- te vra **hoe om toegang** daartoe te kry.
- ingelig te wees oor **hoe om dit op datum te hou**.
- ingelig te wees oor hoe die organisasie **sy verpligtinge ingevolge die WBPI nakom**.

Indien 'n data-onderwerp met die organisasie in verbinding tree en hierdie inligting aanvra, word dit 'n data-onderwerp toegangsversoek genoem. Onderwerptogangsversoeke van data-onderwerpe moet na die betrokke Adjunk-inligtingsbeampte verwys word.

9. Openbaarmaking (deel) van persoonlike inligting

Persoonlike inligting kan intern en met eksterne diensverskaffers gedeel word, byvoorbeeld vir opleidingsdoeleindes.

9.1 Interne openbaarmaking

Oor die algemeen word persoonlike inligting binne die organisasie gedeel waar dit wetlik toegelaat word vir redelike en toepaslike besigheidsdoeleindes. Selfs binne die organisasie is toegang egter beperk tot daardie werknemers of derde partye wat toegang benodig om hul toegewysde funksies uit te voer.

9.2 Eksterne openbaarmaking

Eksterne openbaarmaking van die organisasie geskied slegs ingevolge 'n ooreenkoms, soos toegelaat of vereis deur die wet of wetlike proses, of met die toestemming van die data-onderwerp. Die WBPI maak daarvoor voorsiening dat persoonlike inligting gedeel word indien dit **nasionale veiligheid raak of kriminele aktiwiteite sonder die toestemming** van die data-onderwerp behels. Onder hierdie omstandighede sal die versoekte persoonlike inligting bekend gemaak word. Die Adjunk-inligtingsbeampte sal egter in oorleg met die Sekuriteitsbestuurder verseker dat die versoek wettig en in ooreenstemming met die WBPI is, en, waar nodig, die hulp van Regsdienste aanvra.

10. Kennisgewing aan data-onderwerpe

Die organisasie poog om te verseker dat data-onderwerpe daarvan bewus is dat hul persoonlike inligting verwerk word, en dat hulle verstaan hoe die persoonlike inligting gebruik word, wat hul regte ingevolge die WBPI is en hoe om hul regte uit te oefen. Vir hierdie doeleindes het die organisasie 'n privaatheidskennisgewing wat uiteensit hoe persoonlike inligting met betrekking tot 'n data-onderwerp deur die organisasie ingesamel en gebruik word. Dit is op aanvraag beskikbaar. 'n Weergawe van hierdie kennisgewing is ook beskikbaar by <https://www.westerncape.gov.za/social-development/service/dsd-paiapopia>

11. Afdwinging van beleid

Versuiming om die beleid na te kom deur die organisasie se werknemers sal in ooreenstemming met die [Dissiplinêre Kode/Regulasies] van die organisasie hanteer word. Gevolge kan dissiplinêre stappe en diensbeëindiging, en/of regstappe om enige verlies of skade aan die organisasie te verhaal insluit, insluitend die verhaling van enige boetes of administratiewe strawwe wat deur die Inligtingsreguleerder aan die organisasie ingevolge die WBPI opgelê is.

Versuiming om die beleid na te kom deur enige ander derdeparty wat persoonlike inligting namens die organisasie verwerk, sal hanteer word in ooreenstemming met die ooreenkoms wat tussen die organisasie en sodanige derde party aangegaan is. Gevolge kan die verhaling van enige boetes of administratiewe strawwe insluit wat deur die Inligtingsreguleerder aan die organisasie ingevolge die WBPI opgelê is.

12. Hersiening en bywerking

Hierdie beleid sal ten minste jaarliks hersien en bygewerk word. Indien enige regulatoriese of besigheidsveranderinge lei tot 'n beduidende toevoeging of verandering aan die aard of hantering van persoonlike inligting wat 'n hersiening van hierdie beleid mag vereis, sal die veranderinge gelei word deur die Sekuriteitsbestuurder/Adjunkinligtingsbeamptes en deur die Inligtingsbeampte goedgekeur word.

Enige vrae en versoeke om die beleid by te werk, moet aan die Direkteur Navorsing en Inligtingsbestuur gerig word.

13. Aanbeveling en goedkeuring

In ooreenstemming met die bogenoemde paragrafe word dit aanbeveel dat die:

- 13.1 die gewysigde WBPI Voldoeningsraamwerk 2025-26 en
- 13.2 die gewysigde Privaatheidsbeleidkennisgewing 2025-26 aangeheg as Bylae A, hiermee goedgekeur word

Oorspronlike dokument geteken op 11 April 2025

DEPARTEMENTSHOOF: MAATSKAPLIKE ONTWIKKELING

DR R Macdonald

Verwysingsnommer: 4/6/2

DEPARTEMENT VAN MAATSKAPLIKE ONTWIKKELING: WBPI PRIVAATHEIDSKENNISGEWING: 1 APRIL 2025 – 31 MAART 2026**BYLAE A: DMO WBPI PRIVAATHEIDSKENNISGEWING*****Die Departement van Maatskaplike Ontwikkeling respekteer en beskerm jou privaatheid*****Wat is hierdie kennisgewing en op wie is dit van toepassing?**

Dit is 'n algemene kennisgewing wat die volgende verduidelik:

- Van wie ons persoonlike inligting insamel;
- Watter persoonlike inligting ons insamel;
- Waarom ons jou persoonlike inligting insamel;
- Hoe ons jou persoonlike inligting gebruik; en
- Watter regte jy met betrekking tot jou persoonlike inligting het.

Hierdie kennisgewing verduidelik ook:

- Hoe jy toegang kan verkry tot die inligting wat ons oor jou besit en kan vra dat daardie inligting gekorrigeer word; en
- Hoe jy 'n klag kan indien oor die manier waarop ons jou persoonlike inligting hanteer het.

Hierdie algemene kennisgewing is van toepassing op alle persone (beide natuurlike persone en regspersone, soos maatskappye en beslote korporasies) wie se persoonlike inligting ons insamel, ongeag vorm en medium. Dit sluit ons werknemers, konsultante, agente en diensverskaffers in.

Dit is van toepassing op al ons dienste en verwante webtuistes.

Jy moet hierdie privaatheidskennisgewing saam met die [reëls vir die gebruik van ons webtuiste](#) (insluitend ons vrywaring), ons [kopiereglisensie en](#) enige ander kennisgewings en beleide wat op jou van toepassing is, lees. (Byvoorbeeld, die WKR IT Eindgebruikersbeleid).

Benewens hierdie algemene kennisgewing sal ons dalk spesifieke privaatheidspraktyke in meer besonderhede moet verduidelik. In sulke omstandighede ontwikkel en verskaf ons aparte privaatheidskennisgewings om te beskryf hoe ons die persoonlike inligting wat ons insamel sal hanteer.

Byvoorbeeld, waar ons jou vra om persoonlike inligting met betrekking tot jou indiensneming of in 'n openbare voorlegging tot 'n beleidsvoorstel te verskaf, sal ons jou van 'n privaatheidskennisgewing voorsien ten tyde van insameling of so gou moontlik daarna. Hierdie privaatheidskennisgewings

verduidelik ons persoonlike inligtinghanteringspraktyke met betrekking tot daardie spesifieke doel of aktiwiteit.

Die kontakbesonderhede en adresse van die Departement se kantore verskyn onderaan hierdie kennisgewing.

Die Wet op die Beskerming van Persoonlike Inligting, 2013 (WBPI)

Die Wet op die Beskerming van Persoonlike Inligting, 2013 (WBPI) beskerm persoonlike inligting van natuurlike- en regspersone en vereis van die Departement van Maatskaplike Ontwikkeling om te voldoen aan die agt minimum voorwaardes wat in die Wet uiteengesit word.

“Persoonlike inligting” is inligting of 'n mening oor 'n geïdentifiseerde persoon, of 'n individu wat redelik identificeerbaar is.

Persoonlike inligting sluit **“spesiale** persoonlike inligting” in, wat 'n spesifieke kategorie van persoonlike inligting is. Alhoewel ons erken dat die beskerming van alle persoonlike inligting belangrik is om jou vertroue te verkry en te behou, word spesiale persoonlike inligting dikwels 'n hoër vlak van beskerming gebied.

Insameling van persoonlike inligting van burgers, werknemers, OSW's en verskaffers

Ons versamel en stoor 'n wye reeks persoonlike inligting in rekords wat verband hou met:

- Korrespondensie van lede van die publiek of organisasies wat aan ons of ons Provinsiale Minister gerig is;
- Korrespondensie van ander Provinsiale Ministers en staatsorgane;
- Indiensneming en personeelaangeleenthede met betrekking tot personeel en kontrakteurs;
- Fasilitering van afsprake;
- Fasilitering van vergaderings;
- Administrasie van programme waarvoor die Departement verantwoordelik is;
- Navorsing wat ons uitgekонтрактеer het;
- Kontrakbestuur (insluitend Oordragbetalingsooreenkomste en Sakeplanne);
- Klagtes (insluitend privaatheidsklagtes) en terugvoering aan ons verskaf;
- Versoeke kragtens die Wet op die Bevordering van Toegang tot Inligting, 2000 (WBTI);
- Regsadvies verskaf deur interne staatsregsadviseurs en eksterne prokureurs; en
- Die uitvoering van wetgewende en administratiewe funksies.

Ons gebruik verskillende metodes om inligting in te samel. Dit sluit die volgende in:

- Korrespondensie en voorleggings;
- Papiervorms;
- Aanlyn (vorms wat van die internet afgelaai kan word en e-pos); en
- Telefoonoproepe, fakse en aangesig tot aangesig vergaderings.

Ons samel dikwels persoonlike inligting direk van jou af in. In sommige omstandighede kan ons egter ook inligting oor jou van 'n ander staatsorgaan of organisasie insamel.

- Sekere derdeparty-diensverskaffers kan inligting van of oor jou namens ons insamel of nagaan. Byvoorbeeld, waar ons gebruik maak van eksterne indiensnemingsagentskappe, keuringsagentskappe, kredietburo's, prokureurs, rekenmeesters, konsultante, professionele liggame, banke, reisagentskappe, nie-regeringsorganisasies en sekuriteitsmaatskappye.
- Ons werk saam met openbare liggame of staatsorgane soos plaaslike, provinsiale en nasionale regeringsdepartemente, munisipaliteite, openbare universiteite en maatskappye in staatsbesit, wat inligting van of oor jou namens ons kan insamel of nagaan.
- Ons samel slegs persoonlike inligting in waar daardie inligting redelikerwys nodig is vir, of direk verband hou met, een of meer van ons funksies of aktiwiteite.

Ons versamel persoonlike inligting van en oor:

- **Mense wat ons webtuiste besoek:**
 - Ons samel inligting in wat jy direk aan ons verskaf via ons webtuiste-kontakvorms.
 - Ons gebruik ook algemene tegnologieë (insluitend "koekies") om webtuistegebruik anoniem en outomaties na te spoor en gebruikerservaring te verbeter. Jy kan dit gewoonlik deaktiveer indien jy dit sou verkies. Ons webtuiste se privaatheids- kennisgewing bevat bykomende inligting.
- **Ons werkaansoekers, beursansoekers, internansoekers en werknemers:**
 - Ons samel jou inligting in wanneer jy vir 'n werk, internskap of beurs aansoek doen, en indien jy suksesvol is en ons jou aanstel of vir jou 'n internskap of beurs aanbied.
 - Ons kan ook inligting oor jou van derde partye, soos opvoedkundige liggame of vorige werkgevers, insamel.
 - Ons samel ook inligting in oor werknemers en interns se gebruik van e-pos en die internet om e-pos en internetaktiwiteit te monitor en na te gaan, waar ons glo dat dit redelik en nodig is om misbruik of onwettige aktiwiteite met betrekking tot die Departement se hulpbronne op te spoor. Jy kan nie privaatheid in hierdie verband verwag nie.
- **Ons verskaffers, diensverskaffers, kontrakteurs, konsultante en OSW's:**
 - Ons samel inligting van jou in wanneer jy aansoek doen om op ons verskafferdatabasis gelys te word en bly om goedere of dienste aan ons te verskaf.
 - Ons kan ook inligting oor jou van verskeie private of openbare liggame, soos banke of belastingowerhede, insamel of nagaan.
- **Ons burgers en gebruikers van die Departement se openbare dienste en geriewe:**
 - Ons samel inligting in wat jy vir ons gee wanneer jy vir ons 'n brief, 'n e-pos of teksboodskap stuur, of wanneer jy sosiale media of ons inbelsentrum gebruik om met ons in verbinding te tree.
 - Ons samel ook persoonlike inligting in wanneer dit direk tersaaklik is vir die spesifieke openbare dienste wat ons aan jou verskaf.
 - Ons samel ook inligting in van besoekers aan ons geboue en fasiliteite ingevolge die Wet op Beheer van Toegang tot Openbare Persele en Voertuie, 1985.

Soorte persoonlike inligting wat ons insamel en gebruik

Die persoonlike inligting wat ons insamel en stoor, wissel na gelang van wat ons nodig het om ons funksies en verantwoordelikhede uit te voer. Dit kan die volgende insluit:

- Jou naam, adres en kontakbesonderhede (byvoorbeeld jou telefoonnommer of e-posadres);

- Inligting oor jou identiteit (soos geboortedatum, geboorteland, paspoortbesonderhede, visumbesonderhede en bestuurslisensie);
- Inligting oor jou persoonlike omstandighede (byvoorbeeld ouderdom, geslag, huwelikstatus en beroep);
- Inligting oor jou finansiële sake (byvoorbeeld betalingsbesonderhede, bankrekeningbesonderhede en sake- en finansiële belange);
- Inligting oor jou Indiensneming (byvoorbeeld aansoeke om indiensneming, werkgeskiedenis, kommentaar van referente en vergoeding); en
- Staatsidentifiseerders.

Ons versamel nie noodwendig al hierdie inligting van elke persoon nie, maar slegs waar dit van toepassing is.

Spesiale persoonlike inligting

Ons kan ook "spesiale persoonlike inligting" insamel wat as 'n subkategorie van persoonlike inligting ingevolge die WBPI geklassifiseer word.

Spesiale persoonlike inligting sluit inligting oor die volgende in:

- Jou gesondheid;
- Jou lidmaatskap van 'n professionele of vakvereniging, of 'n vakbond;
- Jou ras of etniese herkoms;
- Jou gestremdheidstatus;
- Kriminele aktiwiteite waarby jy dalk betrokke was; en
- Jou biometrie (insluitend foto's en stem- of video-opnames van jouself).

Oor die algemeen sal ons slegs spesiale persoonlike inligting insamel indien die versameling daarvan redelikerwys nodig is vir, of direk verband hou met, een of meer van ons funksies of aktiwiteite of die versameling deur die wet vereis of gemagtig word.

Ons samel byvoorbeeld spesiale persoonlike inligting soos ras en gestremdheid in om die ontwikkeling van 'n arbeidsmagplan te struktureer. Ons vereis dat werknemers die WGI 1-vorm voltooi wat deur die Wet op Gelyke Indiensneming, 1998, voorgeskryf word. Ons verseker dat die inhoud vertroulik bly en dat die inligting slegs gebruik word om aan bovermelde wet te voldoen.

Ons versamel algemene persoonlike en kontakbesonderhede oor ons werknemers, verskaffers, kliënte, OSW's en gebruikers van ons openbare dienste en geriewe.

- **Werk aansoekers en werknemers:** Ons samel gewoonlik gedetailleerde persoonlike inligting in oor jou opvoedkundige, indiensnemings-, finansiële en kriminele agtergrond, en enige ander tersaaklike inligting soos foto's van jou, vingerafdrukke, bestuurslisensiebesonderhede, voertuigregistrasienommer, belastingnommer en bankrekeningbesonderhede. Indien ons jou aanstel, sal ons ook 'n unieke identifiseerder aan jou toeken wat 'n PERSAL-nommer genoem word. Ons kan ook bykomende inligting benodig oor sake soos gesondheidskwessies en familieleden, waar van toepassing op die diensverhouding.
- **Verskaffers, diensverskaffers, kontrakteurs en konsultante:** Ons samel dikwels gedetailleerde persoonlike inligting in oor jou kwalifikasies, ondervinding of geskiktheid as 'n verskaffer, en ander tersaaklike inligting soos bankrekeningbesonderhede en BTW-nommer. Ons mag ook dalk

bykomende inligting benodig wat van toepassing is op die besigheidsverhouding, soos byvoorbeeld finansiële state of inligting oor solvensie.

- **Besoekers aan ons geboue en geriewe:** Ons versamel gewoonlik kringtelevisiemateriaal (byvoorbeeld foto's en klankopnames, waar van toepassing) sowel as name, identiteitsnommers en kontakbesonderhede van besoekers aan die departement se geboue en fasiliteite.
- **OSW's:** Ons versamel die name en besonderhede van burgers wat gebruik maak van die OSW-dienste wat deur die Departement befonds word vir monitering, evaluering en om ons dienste aan diegene wat sorg en beskerming die meeste benodig te verbeter.

Waarom verskillende afdelings van die Departement spesifieke inligting versamel

Kantoor van die Minister

- Verskaf politieke en wetgewende skakeling tussen die regering, die burgerlike samelewing en alle ander tersaaklike belanghebbendes.
- Beantwoord parlementêre vrae

Korporatiewe Bestuursdienste

- Kapasiteitsbou van maatskaplike werk en verwante beroepe.
- Bestuur DMO-infrastruktuursake
- Koördineer die voorsiening van menslike hulpbronaangeleenthede soos werwing en opleiding tussen DMO en die Departement van die Premier
- Doen iets omtrent WBTI/WBPI-versoeke

Finansiële Bestuur

- Tydige betaling (betaling binne 30 dae) van diensverskaffer-fakture
- Verskaffing van rekeningkundige dienste
- Lewer 'n interne beheer-funksie
- Monitering en evaluering van Voorsieningskanaalbestuur (VKB) en nakoming van batebestuur-regulasies

Sakebeplanning- en Monitering

- Lewer 'n strategiese kommunikasiediens aan afdelings/streke en fasiliteite

Navorsing en Inligtingsbestuur

- Doen navorsing en lewer daarvoor verslag
- Voer bevolkingsbestuursopnames uit en doen navorsing
- Lewer rekordbestuursdienste
- Lewer 'n biblioteekdiens aan personeel
- Takel WBTI/WBPI-versoeke

Maatskaplike Welsyns- en Herstel Programme

- Verskaf welsyns- en hesteldienstediens direk of deur die OWS Sektor aan burgers insluitend slagofferbemagtiging, misdaadvoorkoming en ondersteuning vir Geslagsgebaseerde Geweld.
- Verskaf eie dienste soos sorgfasiliteite vir kinders en jeugdiges en fasiliteite wat dwelmverslaafdes rehabiliteer

- Kapasiteer organisasies om veerkragtige gemeenskappe te bou

Kinders, Gesinne en Kwesbare Groepe

- Verskaf direkte dienslewering, of via die OSW-sektor, dienste aan burgers insluitend kinderbeskerming en dienste aan families
- Verskaf dienste direk of via die OWS Sektor aan kwesbare groepe soos mense met gestremdhede en ouer persone
- Kapasiteer organisasies om veerkragtige gemeenskappe te bou

Gemeenskap- en Vennootskapsontwikkeling

- Verskaf gemeenskapsontwikkelingsdienste soos voedingsondersteuningsprogramme, dienste aan die jeug en maatskaplike verligting van nood aan burgers via die OSW-sektor.
- Skep en onderhou strategiese vennootskappe en bestuur Institusionele Kapasiteitsbou.

Diensleweringbestuur en Koördinerings

- Bestuur die implementering en gehalte van ontwikkeling- en maatskaplike welsyn en gemeenskapsontwikkelingsintervensies in die ses (6) streeks- en vyf-en-veertig (45) diensleweringssakekantore
- Lewer 'n na-uurse kinderbeskerming-blitslyndiens
- Hanteer klagtes van burgers

Gebruik en openbaarmaking van persoonlike inligting

Ons gebruik gereeld jou persoonlike inligting:

- Om ons verhouding met jou te kommunikeer en te bestuur;
- Om jou van openbare dienste te voorsien, soos vereis of toegelaat deur die wet;
- Om sekuriteit en toegangsbeheer tot ons geboue en fasiliteite te bestuur; en
- Vir rekordhouding en ander administratiewe doeleindes, soos deur die wet vereis.

Ons sal nie jou persoonlike inligting aan enigiemand anders verskaf nie, tensy jy daartoe instem of een van die volgende uitsonderings van toepassing is:

- Jy sal redelikerwys van ons verwag om die inligting vir daardie doel te gebruik;
- Dit word wetlik vereis of gemagtig, byvoorbeeld deur 'n wet, of 'n hof- of tribunaalbevel;
- Dit is redelikerwys nodig vir 'n wetstoepassingsverwante aktiwiteit;
- Ons glo redelikerwys dat dit nodig is om 'n ernstige bedreiging vir die lewe, gesondheid of veiligheid van enige individu, of vir openbare gesondheid of veiligheid te verminder of te voorkom;
- Ons het rede om te vermoed dat onwettige aktiwiteit, of wangedrag van 'n ernstige aard, wat verband hou met ons funksies of aktiwiteite plaasgevind het, plaasvind of gaan plaasvind, en ons glo redelikerwys dat dit vir ons nodig is om toepaslike stappe te neem t.o.v. die saak;
- Dit is redelikerwys nodig vir die vestiging, uitoefening of verdediging van 'n wettige of billike eis; of
- Die inligting word slegs vir historiese, statistiese of navorsingsdoeleindes gebruik en word nie in 'n identifiseerbare vorm gepubliseer nie.

- Wanneer ons jou persoonlike inligting met geselekteerde diensverskaffers deel wat namens ons werk, sal ons vir spesifieke omskrewe doeleindes wat verband hou met openbare dienste wat ons

verskaf, verseker dat toepaslike beskerming van jou persoonlike inligting by hierdie derde partye plaasvind, in ooreenstemming met ons verpligtinge kragtens die WBPI.

- Ons is baie versigtig met spesiale persoonlike inligting, en waar prakties, groepeer ons gewoonlik persoonlike inligting saam as saamgevoegde data sodat individue nie maklik geïdentifiseer kan word nie.

Tensy ons u duidelike ingeligte toestemming het of die wet ons duidelik toelaat in sekere beperkte omstandighede, sal ons nie:

- Jou persoonlike inligting verkoop of huur nie;
- Jou persoonlike inligting vir doeleindes gebruik wat anders, ongewoon of onverwags is met betrekking tot die rede vir die insameling daarvan in die eerste plek; of
- Jou persoonlike inligting met derde partye deel in ander omstandighede as dié waarna ons hierbo verwys het.

Bewaring en datasekuriteit

Ons respekteer en beskerm jou privaatheid en stoor jou persoonlike inligting volgens algemeen aanvaarde inligtingsekuriteitspraktyke. Ons neem alle redelike stappe om die persoonlike inligting wat in ons besit gehou word te beskerm teen verlies, ongemagtigde toegang, gebruik, wysiging, openbaarmaking of misbruik. Die Departement sal dadelik optree indien enige toevallige of ongemagtigde openbaarmaking van persoonlike inligting plaasvind.

Bewaring van persoonlike inligting (en die wegdoen van inligting wanneer dit nie meer benodig word nie) word bestuur in ooreenstemming met die Wes-Kaapse Regering se rekordbestuurstelsel soos voorsien in die Wet op die Provinsiale Argief- en Rekorddiens van die Wes-Kaap, 2005. Wanneer die persoonlike inligting wat ons versamel nie meer benodig word nie, wis ons dit uit of vernietig dit op 'n veilige manier, tensy ons verplig word om dit te bewaar as gevolg van 'n wet of hof- of tribunaalbevel.

Waar 'n skending van persoonlike inligting plaasvind, sal ons die Inligtingsreguleerder en geaffekteerde individue in kennis stel soos vereis. Ons sal poog om jou tydig advies te gee om te verseker dat jy enige verlies, finansiële of andersins, wat uit die oortreding kan voortspruit, kan bestuur.

Jou keuses en toestemming in verband met jou persoonlike inligting

- Ons probeer om jou toestemming te verkry om jou persoonlike inligting in te samel en te gebruik, waar prakties.
- Jy hoef gewoonlik nie vir ons persoonlike inligting te gee nie, maar as jy dit nie doen nie, kan ons dalk nie met jou kommunikeer of regeringsdienste aan jou verskaf nie. Jy kan ons ook vra om nie vir jou ongevraagde boodskappe te stuur nie (opt-out), maar dan kan ons jou nie van openbare dienste vertel wat vir jou belangrik mag wees nie.
- Jy mag toegang verkry tot persoonlike inligting wat ons oor jou bewaar en ons vra om enige iets wat verkeerd, irrelevant, verouderd, misleidend ensovoorts is reg te stel of uit te wis. Ons mag egter jou identiteit nagaan voordat ons aan jou toegang verleen. Vir meer inligting, lees asseblief ons handleiding soos vereis deur die Wet op die Bevordering van Toegang tot Inligting 2000 (ons WBTI/WBPI-handleiding is [hier](#) beskikbaar).

<https://www.westerncape.gov.za/social-development/service/dsd-paiapopia>

Jy het ook sekere regte om toestemming terug te trek of ingevolge die WBPI daarteen beswaar te maak indien ons jou persoonlike inligting gebruik, maar hierdie regte is beperk. Byvoorbeeld, indien die doel

waarvoor jou persoonlike inligting aanvanklik aangevra is nie meer bestaan nie, kan jy versoek dat die inligting nie meer gebruik mag word nie. Ons kan jou versoek om die inligting van ons rekords uit te wis, weier indien ander wetgewing vereis dat ons die inligting behou.

Privaatheidsklagtes

- Indien jy voel dat ons nie regverdig en wettig met jou persoonlike inligting omgaan nie, kan jy by die [Inligtingsreguleerder](#) by **JD House, Stiemensstraat 27, Braamfontein, Johannesburg, 2001, kla.** Jy kan ook klagtes rig aan: **Posbus 31533, Braamfontein, Johannesburg, 2017**, tel: +27 (0) 10 023 52441/42, e-pos: POPIAComplaints@inforegulator.org.za of enquiries@inforegulator.org.za
- Gee ons asseblief eers 'n kans om enige klagte op te los deur met ons by die onderstaande kontakbesonderhede in verbinding te tree.
- Jou klagte moet 'n kort beskrywing insluit van wat gebeur het, wanneer dit gebeur het en watter persoonlike inligting geaffekteer is.

Hoe om met ons in verbinding te tree om te kla of vrae te vra oor die Privaatheidskennisgewing of jou persoonlike inligting

E-pos: HOD.DSD@westerncape.gov.za
Tel: 021 483 3083
Verantwoordelikheid: Departementshoof
Pos: Inligtingsbeampte, Departement van Maatskaplike Ontwikkeling, Wes-Kaapse Regering, Queen Victoriastraat 14, Kaapstad, Privaat Sak X9112, Kaapstad, 8001
Besoek ons persoonlik: Queen Victoriastraat 14, Unie Huis, Kaapstad, 8001

E-pos: Gavin.Miller@westerncape.gov.za
Tel: 021 483 4168
Verantwoordelikheid: Kennisbestuur
Pos: Die Adjunk-inligtingsbeampte, Departement van Maatskaplike Ontwikkeling, Wes-Kaapse regering, Queen Victoriastraat 14, Kaapstad, Privaat Sak X9112, Kaapstad, 8001
Besoek ons persoonlik: Queen Victoriastraat 14, Unie Huis, Kaapstad, 8001

E-pos: Petronell.vanWyk@westerncape.gov.za
Tel: 021 483 6741
Verantwoordelikheid: Bedryfsbestuursondersteuning
Pos: Die Adjunk-inligtingsbeampte, Departement van Maatskaplike Ontwikkeling, Wes-Kaapse regering, Unie Huis 14, Privaat Sak X9112, Kaapstad, 8001
Besoek ons persoonlik: Queen Victoriastraat 14, Unie Huis, Kaapstad, 8001

E-pos: Marshionette.Jonkerman@westerncape.gov.za
Tel: 2721-8266040
Verantwoordelikheid: Direktoraat Fasiliteitsbestuur
Pos: Die Adjunk-inligtingsbeampte, Departement van Maatskaplike Ontwikkeling, Wes-Kaapse regering, R101, De Novo-Behandelingsentrum, Kraaifontein

Besoek ons persoonlik:	R101, Ou Paarlweg, De Novo HUB, Kraaifontein, 7570
E-pos:	Annemie.vanReenen@westerncape.gov.za
Tel:	021 483 9392
Verantwoordelikheid:	Streekkantore x 6
Pos:	Die Adjunk-inligtingsbeampte, Departement van Maatskaplike Ontwikkeling, Wes-Kaapse regering, Unie Huis 14, Privaat Sak X9112, Kaapstad, 8001
Besoek ons persoonlik:	Queen Victoriastraat 14, Unie Huis, Kaapstad, 8001
<u>DMO Kliëntedienshulplyn</u> Telefoon: 021 483 5045 of 0800-250-220 E-pos: SD.CustomerCare@westerncape.gov.za Jy kan ook papierafskrifte van hierdie privaatheidskennisgewing of enige van die dokumente waarna in hierdie dokument verwys word, by enige van die kantore hierbo aanvra.	
<u>WKR Kontaksentrum</u> Telefoon: 0860 142 142 E-pos: services@westerncape.gov.za	