Departement van Maatskaplike Ontwikkeling
Gavin Miller
Direktoraat Navorsing en Inligtingsbestuur
Gavin.Miller@westerncape.gov.za | Tel: 021 483 4168

WBPI RAAMWERK EN BELEID

Verwysingsnommer: 4/6/2 WBPI Privaatheidskennisgewing

DEPARTEMENT VAN MAATSKAPLIKE ONTWIKKELING

WBPI VOLDOENINGSRAAMWERK EN BELEID

Weergawe 02/2022

Datum van publikasie: 08/04/2022

Geskiedenis van hersiening

Datum	Weergawe	Beskrywing	Skrywer
7 Julie 2021	01/2021	Opstel van Privaatheidskennisgewing	G Miller
8 April 2022	02/2022	Jaarlikse hersiening	G Miller

Definisies

Data-onderwerp	Beteken die identifiseerbare natuurlike/regspersoon op wie persoonlike inligting betrekking het.
Inligtingsbates	Beteken 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	Beteken die persoon wat verantwoordelik is vir die omskrywing en implementering van sekuriteitsmaatreëls en kontroles vir Inligting- en Kommunikasietegnologie ("IKT") bates.
Eindgebruiker van inligting	Beteken 'n persoon wat in aanraking kom met inligtingsbates en IKT-bates met die doel om 'n gemagtigde taak uit te voer.
Inligtingsbeampte	Beteken 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	Beteken 'n persoon wat verantwoordelik is vir, of afhanklik is van die besigheidsproses wat met 'n inligtingsbate geassosieer word.
Persoonlike inligting	Beteken 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 h) 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.

Western Cape Government

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 die WKR Inligting-sekuriteit Klassifikasiestelsel ("ISCS") gelees word. Definisies verskyn aan die einde vir die betekenis van terme wat in hierdie beleid gebruik 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 privaatheidbeginsels 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
- 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 Inligting-sekuriteit 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 sekuriteitstandaarde.
- Doen gereelde kontroles en skanderings om te verseker dat sekuriteitshardeware en -sagteware behoorlik funksioneer.
- Evalueer enige derdepartydienste wat die organisasie oorweeg om te gebruik om persoonlike inligting te verwerk. Byvoorbeeld, wolkbediener rekenaardienste.

e) Die **Hoofdirekteur Sakebeplanning en -strategie** in samewerking met die **Direkteur Sakebeplanning en Monitoring** is vir die volgende verantwoordelik:

- 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.

f) Die **Rekordbestuurder** is vir die volgende verantwoordelik:

- 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.
- 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.

g) Die **Kennisbestuurder** is vir die volgende verantwoordelik:

- Voer 'n oudit uit van persoonlike inligting wat deur individue en eenhede gehou word.
- Gee opleiding aan DMO-personeel oor die veilige bewaring van elektroniese rekords.
- Skakel met die Rekordbestuurder om te verseker dat elektroniese rekords in ooreenstemming met die beskikkingstydperk weggedoen/argiveer word.

[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].

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 regsdienste in die Departement van die Premier genader kan word om 'n verduideliking te verskaf.

7.1 Versameling

Die organisasie samel inligting in om sy dienslewering mandaat 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.[2]

[2] Skep 'n hiperskakel na hierdie Privaatheidskennisgewing/ sluit besonderhede in waar dit verkry kan word.

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-sekuriteit 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 skerms 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-posteks) 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 opgelaai 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-inligtingsbeampte 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 ingesteek 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].[3]
h) Bedieners wat persoonlike inligting bevat, moet op **'n veilige plek geleë wees,** weg van algemene kantoorruimte.

[3] Skep 'n hiperskakel na waar toegang tot hierdie dokument verkry kan word.

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, rekenaars 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. Onderwerptoegangsversoeke 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[4]

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

[4] Verwys na Hoofstuk 8 vir Kennisgewingformate.

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/assets/departments/social-development/popia_dsd_privacy_notice.pdf

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 paragrawe word die Privaatheidsbeleidkennisgewing vir die Departement van Maatskaplike Ontwikkeling hiermee goedgekeur.

DEPARTEMENTSHOOF: MAATSKAPLIKE ONTWIKKELING

DR ROBERT MACDONALD

Datum: