RIGLYNE OOR DIE WET OP DIE BESKERMING VAN PERSOONLIKE INLIGTING VIR DIE DEPARTEMENT VAN BASIESE ONDERWYS

Hoofstuk 1:
Inleiding

1.1. Die Wet op die Beskerming van Persoonlike Inligting (algemeen bekend as die "POPI"-wet afgelei van die Engelse benaming *Protection of Personal Information Act)* het ten doel om die konstitusionele reg tot privaatheid ten uitvoer te bring deur ’n balans tussen die reg tot privaatheid en die reg tot toegang tot inligting te bewerkstellig. Die POPI-wet vereis dat persoonlike inligting wat op die individu betrekking het, op ’n regmatige en redelike wyse verwerk word wat nie inbreuk op daardie individu se die reg tot privaatheid maak nie.

1.2. Die konstitusionele reg tot privaatheid is vervat in artikel 14 van die Grondwet:
Elkeen het die reg op privaatheid, inbegrepe die reg dat –
a) hul persoon of woning nie deursoek word nie;
b) hul eiendom nie deursoek word nie;
c) daar nie op hul besittings beslag gelê word nie; of
d) daar nie op die privaatheid van hul kommunikasies inbreuk gemaak word nie.

1.3. Die bedoelings van die Wet op die Beskerming van Persoonlike Inligting, 2013 (POPI-wet) word in artikel 2 van dié wet uiteengesit. Die POPI-wet het ten eerste ten doel om:
Die konstitusionele reg tot privaatheid ten uitvoer te bring deur persoonlike inligting te beveilig wanneer dit deur ’n verantwoordelike party verwerk word, onderworpe aan regverdigbare beperkings wat daarop gemik is om:

a) ’n Balans tussen die reg tot privaatheid en ander regte te bewerkstellig, veral die reg op toegang tot inligting, en
b) Vername belange, ingeslote die vrye vloei van inligting binne Suid-Afrika en oor internasionale grense, te beskerm.

1.4 Die POPI-wet verleen inhoud aan die reg op privaatheid soos in die Grondwet vasgelê. Dit is nie ’n onbeperkte reg nie en kan ingevolge die beperkingsklousule,

soos vervat in die Grondwet, beperk word. Die POPI-wet poog om ’n balans te bewerkstellig tussen die reg op privaatheid en die reg van andere, met inbegrip van die reg op toegang tot inligting.

1.5 In sy aanhef erken die POPI-wet dat:

a) Artikel 14 van die Grondwet bepaal dat almal ’n reg op privaatheid het.
b) Ingeslote by die reg op privaatheid is beskerming teen die onregmatige versameling, retensie, disseminasie en gebruik van persoonlike inligting.
c) Voorts moet die staat die regte vervat in die Handves van Regte respekteer, beskerm, bevorder en gestand doen.

1.6 In wese kom die bekragtiging van die POPI-wet dus daarop neer dat die staat hiermee gestand doen aan sy verpligting om die reg op privaatheid, soos vasgelê in die Handves van Regte, te beskerm en te bevorder.

Die Beperkingsklousule

Die reg op privaatheid is nie ’n onbeperkte reg nie. Sonder om strydig met die Grondwet te wees, kan konstitusionele regte beperk word. In artikel 36 van die Grondwet (die Beperkingsklousule) word vasgelê op welke wyse konstitusionele regte beperk mag word. Geen beperkings op die reg tot privaatheid mag strydig met die Beperkingsklousule wees nie.

Die POPI-wet erken ook dat die verwydering van onnodige hindernisse tot die vrye vloei van inligting, met inbegrip van persoonlike inligting, nodig is binne die konteks van die konstitusionele waardes van ’n demokratiese, ope bestel en die behoefte aan ekonomiese en maatskaplike vooruitgang.

Wat die POPI-wet ten doel het

Soos hierbo vermeld, het die POPI-wet eerstens ten doel om die konstitusionele reg op privaatheid ten uitvoer te bring. Sodoende moet dit ook die beperkings inherent aan hierdie reg aanspreek. Die ander doeleindes wat in die POPI-wet vasgelê is, is om:

a) Die wyse waarop persoonlike inligting verwerk mag word, te reguleer;

b) Regte en remedies aan mense te verleen om hul persoonlike inligting te beskerm teen verwerking wat nie met die POPI-wet strook nie; en
c) Maatreëls, met inbegrip van ’n Inligtingsreguleerder, daar te stel ten einde te verseker dat die regte wat deur die POPI-wet beskerm word, gerespekteer, bevorder, afgedwing en nagekom word.

Die toepassing van die POPI-wet

Die POPI-wet het betrekking op die verwerking van persoonlike inligting wat deur of vir ’n verantwoordelike party opgeteken is. Om die POPI-wet te verstaan, is dit belangrik om vertroud te raak met die volgende sleutelterme soos gebruik in die POPI-wet:

Verwerking:

Verwerking word omskryf as enige handeling of aktiwiteit of stel handelinge, hetsy geoutomatiseerd of nie, wat betrekking het op persoonlike inligting, met inbegrip van —

a) die insameling, ontvangs, optekening, organisering, insortering, berging, bywerking of modifisering, herwinning, wysiging, raadpleging of gebruik;
b) disseminering by wyse van transmissie, verspreiding of beskikbaarstelling in enige ander vorm; of
c) samevoeging of koppeling van inligting sowel as die beperking, degradering, uitwissing of vernietiging van inligting.

Verwerking het, byvoorbeeld, betrekking op maar is nie beperk nie tot persoonlike inligting wat deur die DBO benodig word soos voornaam en van, geboortedatum, identiteitsnommer, paspoortnommer, adres en persoonlike/werkkontakdetails (bv. e-pos en telefoonnommers) sowel as inligting oor demografie, onderwys, beroep, gesondheid, lidmaatskap en vakbondaffiliasies.

Persoonlike inligting:

Beteken inligting wat betrekking het op ’n identifiseerbare, lewende, natuurlike persoon en, waar van toepassing, op ’n identifiseerbare, bestaande regspersoon, met inbegrip van maar nie beperk nie tot:

a) inligting wat betrekking het op die ras, geslagtelikheid, geslag, swangerskap, huwelikstaat, nasionaliteit, etniese of sosiale herkoms, kleur, seksuele

georiënteerdheid, ouderdom, fisieke of geestesgesondheid, welstand, gestremdheid, godsdiens, gewete, oortuiging, kultuur, taal en geboorte van die persoon;

b) inligting wat betrekking het op die onderwys of die mediese, finansiële, kriminele of werksgeskiedenis van die persoon;
c) enige identifiserende nommer, simbool, e-posadres, fisiese adres, telefoonnommer, liggingsinligting, aanlyn identifikasie of iets soortgelyks wat aan die persoon toegewys is;
d) die biometriese inligting van die persoon;
e) korrespondensie wat deur die persoon versend is wat voorwaardelik of onvoorwaardelik as privaat en vertroulik geag moet word.

Voorbeelde van persoonlike inligting sluit in ’n persoon se huis-, pos- en e-posadres; die persoon se vingerafdrukke; die inligting vervat in sy/haar curriculum vitae en die menings wat daardie persoon ná afloop van ’n werksessie op ’n evaluasievorm vasgelê het.

Rekord:

Beteken enige aangetekende inligting,

(a) ongeag die vorm of medium, met inbegrip van die volgende:

i. Enigiets wat neergeskryf is, ongeag waarop;
ii. Inligting wat by wyse van enige bandopnemer, rekenaartoerusting – hetsy harde- of sagteware of beide – of enige ander toestel voortgebring, opgeneem of geberg is, of enige materiaal wat daarna ontleen word uit inligting wat op hierdie wyse voortgebring, opgeneem of geberg is;
iii. ’n Plakkertjie, merkertjie of ander notatjie wat iets identifiseer of beskryf of wat deeluitmaak daarvan of op enige wyse daaraan geheg is;
iv. ’n Boek, kaart, plan, grafiek of tekening;
v. ’n Foto, film, negatief, band of ander toestel waarop een of meer visuele beeld vasgelê is en waar daardie beeld, met of sonder die hulp van ander toerusting, gereproduseer kan word;

(b) Deur ’n verantwoordelike party besit of deur daardie party beheer word;
(c) Ongeag of dit deur die verantwoordelike party geskep is, al dan nie; en
(d) Ongeag wanneer dit ontstaan het.
Persoonlike inligting omvat, byvoorbeeld, om foto's van iemand te neem, om ’n persoon se besonderhede neer te skryf en te berg, of om iemand se identiteitsnommer op ’n stukkie papier neer te skryf.
Die verantwoordelike party moet, in wese, in Suid-Afrika woonagtig wees of, indien nie woonagtig in Suid-Afrika nie, gebruik maak van ’n Suid-Afrikaanse wyse om rekord te hou – tensy daardie wyse slegs gebruik word om persoonlike inligting via Suid-Afrika te versend.

SAMEVATTING VAN SLEUTELPUNTE

- Die POPI-wet maak dit moontlik om die konstitusionele reg op privaatheid ten uitvoer te bring.
- Die reg op privaatheid word erken as ’n onafhanklike persoonlikheidsreg.
- Die POPI-wet het betrekking op die verwerking van persoonlike inligting wat deur of vir ’n verantwoordelike party opgeteken is.
- Die POPI-wet het ten doel om persoonlike inligting te beskerm wanneer dit verwerk word.
- Die reg op privaatheid is onderworpe aan regverdigbare beperkings.
- In die POPI-wet word die regte en remedies ter beskerming van persoonlike inligting vasgelê.

Hoofstuk 2:
Tersaaklikheid van die POPI-wet vir DBO

2.1 Die POPI-wet is tersaaklik vir die DBO aangesien persoonlike inligting weens die aard van die dienste wat aangebied word, in die gewone loop van sake verwerk word. Die POPI-wet lê ’n aantal verpligtinge op wanneer persoonlike inligting verwerk word.

2.2 POPI is ’n algemeen geldende wet wat van toepassing is op die verwerking van persoonlike inligting, inaggenome dat dié wet ’n persoon as ’n natuurlike of regspersoon omskryf. Gegewe hierdie omskrywing, let daarop dat die datasubjek daardie persoon is.

2.3 Die volgende is ’n paar voorbeelde van wanneer die DBO, as die verantwoordelike party, persoonlike inligting verwerk:

a) Wanneer indiensnemingskontrakte aangegaan word met werknemers,
b) diensverskaffingkonsultante, diensverskaffers,
c) kundiges;
d) Wanneer personeel gewerf en hulle aansoeke verwerk word;
e) Wanneer inligting versprei word, ingeslote deelname aan ’n webwerf;
f) Wanneer kliënte se klagtes behartig word;
g) Wanneer inligting rakende sekere datasubjekte se noodkontakte / naasverwantes verwerk word;
h) Wanneer regsdienste se kliënte bedien word.

2.4 ’n Datasubjek is die persoon op wie die persoonlike inligting betrekking het.

Persoonlike inligting beteken inligting wat betrekking het op ’n identifiseerbare, lewende, natuurlike persoon en, waar van toepassing, op ’n identifiseerbare, bestaande regspersoon.

Die data wat tot die DBO se beskikking is, is omvattend. Heelwat van daardie data word ingevolge die POPI-wet as "persoonlike inligting" geag. In die besonder kan die 13-syfer- nasionale identiteitsnommer van leerders en werknemers, sowel as hul name, gender en geboortedatum, via hierdie data

opgespoor word. Die provinsiale departemente van onderwys benodig persoonlike inligting vir operasionele doeleindes, en as die bron van baie van die DBO se data word provinsiale departemente se persoonlike data hierby ingesluit. Ingevolge die Wet op Nasionale Onderwysbeleid (algemeen bekend as NEPA afgelei van die Engelse benaming *National Education Policy Act*) word die gebruik van data deur die DBO beperk tot die monitering en evaluering van vordering ten einde voldoening aan die Grondwet en NEPA te verseker. In samewerking met provinsiale departemente van onderwys kan data óf via EMIS óf ander gepaste wyses versamel word. Die gebruik van leerkragte se selfoonnommers moet beperk word.

Van belang hier is dat die persoonlike data wat deur die DBO gehou word, nodig is vir analitiese doeleindes en om aan die moniteringsverpligtinge, soos opgedra deur NEPA, te voldoen. In die besonder is persoonlike inligting nodig wanneer verskillende databronne met mekaar verbind moet word. Byvoorbeeld, om te ontleed hoe goed kandidate wat die Graad 12-eksamen geskryf het in grade laer as Graad 12 gevaar het, moet die data van die Graad 12-eksamen gekoppel word aan afsonderlike datastelle wat die laer grade dek.

Dit is dikwels nodig om meervoudige veranderlikes te gebruik wanneer databronne met mekaar verbind word aangesien die gebruik van ’n enkele veranderlike die data kan begrens. Byvoorbeeld, die 13-syfer-identiteitsnommer sal die meeste leerders wat die Graad 12-eksamen geskryf het met die datastelle vir laer grade verbind, maar nie met almal nie omdat sommige identiteitsnommers ontbreek. In só ’n geval kan name en geboortedatums gebruik word om die gaping te oorbrug, sowel as om die akkuraatheid van die nasionale identiteitsnommer te verifieer. Hier is dit allerbelangrik om daarop te let dat die moniteringswerk waarna hier verwys word, nooit behels dat persoonlike inligting onthul word in die DBO-verslae wat as deel van die proses voortgebring word nie. Dié verslae sal slegs saamgestelde statistiek weerspieël wat, byvoorbeeld, betrekking het op die uitsakkoers.

Ingevolge die Wet op Nasionale Onderwysbeleid (Wet 27 van 1996) [hierna NEPA] word daar van die DBO verwag om beplanning, navorsing en monitering

namens die Minister van Basiese Onderwys te onderneem ter bevordering van nasionale doelwitte. Sodoende produseer die DBO elke jaar baie interne en openbare verslae wat gegrond is op die data waartoe dit toegang het. Hierdie verslae dek ŉ wye verskeidenheid aspekte soos die bywoning van skole, skole wat geopen/gesluit is, onderwysers wat in diens geneem is en hoe leerders presteer het. Ingevolge NEPA word daar ook van die DBO verwag om die gebruik van data in die breër "nasionale onderwysstelsel" te bevorder, wat daarop neerkom dat verskeie staatsentiteite aangemoedig moet word om hierdie data te gebruik waar dit kennis en ŉ beter begrip van die onderwyssektor sal verbreed.

Dit is alledaags vir die DBO om deel te neem aan oefeninge waar sy data aan dié van ander staatsentiteite gekoppel word sodat die gehalte en geldigheid van data wat tot die regering se beskikking is, getoets en gemoniteer kan word. So, byvoorbeeld, maak die DBO en die Suid-Afrikaanse Agentskap vir Maatskaplike Sekerheid (algemeen bekend as SASSA) gebruik van verskeie datavelde wat persoonlike inligting bevat om te bepaal of diegene van skoolgaande ouderdom wat maatskaplike toelaes ontvang wel skool bywoon. Eweneens is dit belangrik om, in medewerking met die Departement van Hoër Onderwys en Opleiding (DHOO), die rekords van leerders wat voorheen by skole ingeskryf was, te koppel aan daardie van studente wat tans by naskoolse instansies ingeskryf is sodat beter insig verkry kan word in die vloei tussen hierdie twee vlakke van onderwys. Artikel 57(1)(a) van die POPI-wet dui aan dat magtiging deur die Inligtingreguleerder verkry moet word voordat ŉ unieke identifikasie (soos ŉ ID-nommer) gebruik kan word vir ŉ doeleinde anders as die een waarvoor dit ten tyde van versameling bedoel is met die voorneme om daardie inligting aan ander verantwoordelike partye se inligtingsprosesse te koppel.

SAMEVATTING VAN SLEUTELPUNTE

a) Die departement verwerk persoonlike inligting in die gewone loop van sake.
b) Persoonlike inligting moet ooreenkomstig die POPI-wet verwerk word.

Hoofstuk 3:
Hoe om inligting regmatig te verwerk

3.1 Die POPI-wet het spesifieke regsaanspreeklikhede ingestel vir die bestuur en verwerking van persoonlike inligting wat deur dié wet beheer word. Nakoming van die POPI-wet sal:

a. Verseker dat die persoonlike inligting waaroor die DBO beskik, beskerm word;
b. Verhoudinge met en die vertroue van belanghebbendes versterk;
c. Blootstelling aan onnodige risiko's minimaliseer; en
d. Help om die sektor se reputasie te beskerm.

3.2 Daarteenoor kan nienakoming van die POPI-wet aanleiding gee tot:

a. Blootstelling aan onnodige finansiële en reputasierisiko's;
b. Negatiewe publisiteit;
c. Negatiewe openbare beeld;
d. Boetes wat deur die Inligtingsreguleerder opgelê word; en
e. Privaatregtelike stappe wat deur die datasubjek geneem word.

3.3 Dit is van kardinale belang dat alle inligting wat verskaf word op die regte wyse hanteer word.

3.4 Die regte van datasubjekte word in die POPI-wet omskryf. ’n Datasubjek is die persoon op wie persoonlike inligting betrekking het.

3.5 In artikel 5 van die POPI-wet word, onder andere, die volgende regte van datasubjekte vasgelê, naamlik dat hulle verwittig moet word:

a. Dat hulle persoonlike inligting versamel is;
b. Dat toegang tot hulle persoonlike inligting verkry of deur ’n ongemagtigde persoon bekom is;
c. Watter persoonlike inligting deur die DBO gehou word;
d. Hoe hulle toegang tot hul persoonlike inligting kan verkry;
e. Hoe hulle kan versoek dat hul persoonlike inligting reggestel, vernietig of geskrap moet word;

f. Hulle op redelike gronde beswaar kan aanteken teen die verwerking van hul persoonlike inligting;
g. Hoe hulle beswaar kan aanteken teen die verwerking van hul persoonlike inligting vir die doeleindes van direkte bemarking (met inbegrip van fondswerwing) via ongevraagde elektroniese kommunikasie.

3.6. Soos in Hoofstuk 2 aangedui, sluit verwerking die volgende in: die insameling, ontvangs, optekening, organisering, insortering, berging, bywerking of modifisering, herwinning, wysiging, raadpleging of gebruik van persoonlike inligting sowel as die disseminasie daarvan hetsy by wyse van transmissie of verspreiding of deur dit hoegenaamd in enige ander vorm beskikbaar te stel.
Om as wettig geag te word, moet die verwerking van inligting ooreenkomstig die bepalings van die POPI-wet geskied. In artikel 4 van die POPI-wet word die agt voorwaardes vir die wettige verwerking van persoonlike inligting gelys, naamlik:

1.1 <u>Aanspreeklikheid</u>

Die DBO moet ’n party (inligtingsbeampte) aanstel wat daarvoor verantwoordelik sal wees om te verseker dat daar voldoen word aan die beginsels vir die beskerming van inligting soos vervat in die **POPI-wet** en dat die nodige beheermaatreëls in plek is om nakoming van daardie beginsels te verseker.
Om aanspreeklikheid te aanvaar, is om die verantwoordelikhede – soos opgelê ingevolge die POPI-wet – na te kom:

a) Keur gepaste beleide en stelsels vir die bestuur en verwerking van persoonlike inligting goed;
b) Verseker dat beleide en stelsels verstaan, nagestreef en nagekom word;
c) Verseker dat personeellede behoorlik toegerus en opgelei is om aan die POPI-wet te voldoen;
d) Verseker dat tersaaklike POPI-verantwoordelikhede in kontrakte met werknemers en derde partye vervat is; en
e) Moniteer en hersien die doeltreffendheid van beleide en stelsels op ’n gereelde grondslag.

1.2 Beperkings op verwerking

Die DBO moet verseker dat die verwerking van inligting geoorloof is, dat so min as moontlik inligting versamel word en dat persoonlike inligting regstreeks van die datasubjek verkry word, welke subjek die geleentheid gegun moet word om tot geoorloofde verwerking in te stem of daarteen beswaar te maak.
Artikel 9 vereis dat die verwerking van persoonlike inligting op 'n regmatige en redelike wyse geskied wat nie inbreuk op die datasubjek se privaatheid maak nie.
Kortom, daar moet regsgeldige redes wees vir die verwerking van enige datasubjek se persoonlike inligting. Waarskynlik sal die datasubjek se instemming tot verwerking onomwonde bepaal of sulke regsgeldige redes wel bestaan.
Die DOEL MET DIE VERWERKING van persoonlike inligting moet:

a) Toereikend,
b) Relevant,
c) en nie Buitensporig wees nie.

Wanneer is die verwerking van persoonlike inligting wettig?

Persoonlike inligting mag slegs verwerk word (waarby die versameling, ontvangs, optekening, organisering, insortering, bywerking, wysiging en verspreiding daarvan ingesluit is) as:

a. Die datasubjek daartoe instem;
b. 'n Bevoegde persoon (ouer of voog) in gevalle waar die datasubjek 'n kind is
c. daartoe toestem;
d. Die verwerking nodig is om handelinge te verrig ter voldoening aan of uitvoering van 'n kontrak waaraan die datasubjek deel het;
e. Dit voldoen aan 'n plig wat volgens wet aan die verantwoordelike party opgelê is;
f. Dit 'n wettige belang van die datasubjek beskerm; of
g. Dit nodig is vir die nastrewing van die wettige belange van die verantwoordelike party of 'n derde party aan wie die inligting verskaf word.

Kan ’n datasubjek instemming tot verwerking terugtrek en daarteen beswaar maak?

Ja, ’n datasubjek (of ’n ouer of voog van ’n kind) kan op enige tydstip sy of haar instemming terugtrek in situasies waar toestemming verleen is.
’n Datasubjek kan, tensy die wet vir sodanige verwerking voorsiening maak, op redelike gronde beswaar maak teen die verwerking van persoonlike inligting deur die DBO in situasies waar die verwerking:

a. ’n Wettige belang van die datasubjek beskerm, of
b. Dit nodig is vir die nastrewing van die wettige belange van die departement of ’n derde party aan wie die inligting verskaf word.

Die beswaar moet op die voorgeskrewe wyse aangeteken word.
’n Datasubjek kan ook beswaar maak teen die verwerking van persoonlike inligting vir die doeleindes van direkte bemarking (insluitende fondswerwing).

Terugtrekking van toestemming en aantekening van beswaar

Die POPI-wet vereis dat die verwerking van persoonlike inligting van ’n datasubjek gestaak word waar die datasubjek daarteen beswaar maak. Die POPI-wet verduidelik nie uitdruklik wat sal gebeur in geval daar ’n dispuut tussen die partye is oor die gronde waarop die beswaar gebaseer word nie.

1.3 <u>Doelspesifikasie</u>

Die persoonlike inligting moet vir ’n spesifieke doel versamel word, en die datasubjek van wie die persoonlike inligting versamel word, moet ingelig word oor die doel waarvoor die persoonlike inligting versamel is. DIE POPI-WET vereis dat die DOEL MET DIE VERSAMELING van persoonlike inligting:

a) Spesifiek moet wees
b) Uitdruklik omskryf moet word
c) Verband moet hou met ’n regmatige doeleinde verwant aan die funksie of handeling.

Persoonlike inligting moet nie vir langer gehou word as wat nodig is vir die bereiking van die doel waarvoor dit versamel of verwerk is nie, tensy:

a) Die wet sodanige retensietydperk vereis,
b) Die DBO sodanige rekord vir regmatige doeleindes benodig,
c) Retensie gegrond word op ’n kontrak tussen die partye,
d) Die datasubjek ingestem het tot sodanige retensie, of
e) ’n Bevoegde persoon namens ’n minderjarige ingestem het tot sodanige retensie.

Persoonlike inligting kan vir historiese, statistiese of navorsingsdoeleindes vir langer tydperke gehou word mits gepaste beskerming daargestel is om te verhoed dat rekords vir ander doeleindes gebruik word.
Wanneer magtiging vir die retensie van persoonlike inligting nie meer gemagtig is nie, moet dit vernietig, geskrap of deïdentifiseer word.
Deïdentifisering beteken dat inligting geskrap word wat —

a) die datasubjek identifiseer;
b) volgens ’n metode wat redelikerwys te wagte kan wees, gebruik of gemanipuleer kan word om die datasubjek te identifiseer; of
c) volgens ’n metode wat redelikerwys te wagte kan wees, gekoppel kan word aan ander inligting wat die datasubjek identifiseer.

1.4 <u>Beperkings op verdere verwerking</u>

As ’n verantwoordelike party persoonlike inligting verder verwerk, moet sodanige verwerking versoenbaar wees met die doel waarvoor die inligting versamel is. Die POPI-wet vereis dat verdere verwerking van persoonlike inligting in ooreenstemming moet wees met die doel waarvoor dit versamel is. Kortom, die inligting wat vir een doel versamel is, moet nie verwerk en gebruik word vir ander doeleindes nie.
Die volgende faktore moet in aanmerking geneem word om versoenbaarheid tussen die doel waarvoor die inligting ingesamel is en die doel waarvoor dit verwerk word te bewerkstellig:

a) Die verband tussen die doel waarvoor inligting versamel is en die doel waarvoor dit verder verwerk word;
b) Die aard van die betrokke inligting;
c) Die gevolge wat verdere verwerking vir die datasubjek inhou;
d) Die wyse waarop die persoonlike inligting versamel is; en
e) Die kontraktuele regte en verpligtinge waartoe die partye ingestem het.

In sekere gevalle is verdere verwerking van persoonlike inligting toelaatbaar, ingeslote waar:

a) Die datasubjek toestemming verleen het;
b) Die persoonlike inligting van 'n openbare rekord verkry kan word; of
c) Die datasubjek willens en wetens sodanige persoonlike inligting openbaar gemaak het.

1.5 Gehalte van inligting

Die verantwoordelike party moet redelike stappe neem om te verseker dat die persoonlike inligting wat versamel is volledig, akkuraat, geldig en nie misleidend is nie. Sodoende moet die verantwoordelike party die doel waarvoor die persoonlike inligting versamel is oorweeg.

1.6 Openheid

Die verantwoordelike party moet openlik wees oor die versameling van persoonlike inligting deur die Reguleerder in te lig dat dit persoonlike inligting gaan verwerk en, indien persoonlike inligting versamel gaan word, moet die verantwoordelike party alle redelik moontlike stappe neem om te verseker dat die datasubjek daarvan bewus is dat sy of haar persoonlike inligting versamel gaan word. Die verantwoordelike party moet, byvoorbeeld, redelike stappe neem om die datasubjek in te lig oor sy naam en adres en die doel waarvoor persoonlike inligting versamel word.

Nienakoming van die voormelde word in die volgende situasies toegelaat:

a) Die datasubjek tot nienakoming ingestem het

b) Nienakoming nodig is om aan ’n regsverpligting te voldoen
c) Nienakoming nodig is om aan hofverrigtinge te voldoen
d) Nienakoming in belang van nasionale veiligheid nodig is
e) Nakoming ’n regmatige doel vir die versameling van inligting sal benadeel
f) Nakoming onder die omstandighede nie prakties haalbaar is nie
g) Die inligting nie op ’n wyse gebruik sal word wat die datasubjek identifiseer nie
h) Die inligting vir historiese, statistiese of navorsingsdoeleindes gebruik gaan word

1.7 Beveiliging

Die verantwoordelike party moet verseker dat die integriteit van die persoonlike inligting waaroor hy beskik, beveilig word deur tegniese en organisatoriese maatreëls te tref wat die volgende sal verhoed:

a) Die verlies van, skade aan of ongemagtigde vernietiging van persoonlike inligting; en
b) Ongemagtigde toegang tot of verwerking van persoonlike inligting.

Die verantwoordelike party moet:

a) Alle risiko's met betrekking tot persoonlike inligting wat redelikerwys te wagte kan wees, identifiseer;
b) Gepaste maatreëls ter beveiliging van sodanige inligting instel en handhaaf;
c) Op ’n gereëlde basis verifieer dat daardie beveiligingsmaatreëls doeltreffend geïmplementeer word; en
d) Verseker dat beveiligingsmaatreëls deurentyd bygewerk word.

1.8 Deelname deur datasubjekte

Datasubjekte het die reg om te versoek dat ’n verantwoordelike party (gratis) bevestig of daardie party oor enige persoonlike inligting van die datasubjek beskik, en hy of sy kan ook ’n beskrywing van daardie inligting versoek.
Ingevolge artikel 10 van die POPI-wet kan persoonlike inligting slegs onderworpe aan sekere voorwaardes, soos hierna gelys, verwerk word:

a) Die datasubjek of ’n bevoegde persoon (in gevalle waar die datasubjek ’n kind is) ingestem het tot die verwerking; of
b) Die verwerking nodig is om handelinge te verrig ter voldoening aan of uitvoering van ’n kontrak waaraan die datasubjek deel het;
c) Verwerking voldoen aan ’n plig wat ingevolge wetgewing aan die verantwoordelike party opgedra is; of
d) Verwerking ’n wettige belang van die datasubjek beskerm; of
e) Verwerking nodig is vir die nastrewing van die wettige belange van die verantwoordelike party of ’n derde party aan wie die inligting verskaf word.

SAMEVATTING VAN SLEUTELPUNTE

Artikel 4 van die POPI-wet lys agt voorwaardes vir die regmatige verwerking van inligting soos hierbo geïllustreer.

Hoofstuk 4:
Beveiliging van persoonlike inligting

Die integriteit en vertroulikheid van persoonlike inligting waaroor die DBO beskik of wat deur hom beheer word, sal as beveilig beskou word wanneer gepaste, redelike tegniese en organisatoriese maatreëls getref is om die verlies van, skade aan of ongemagtigde vernietiging en onregmatige toegang tot of verwerking van persoonlike inligting te verhoed.

Die DBO sal, ooreenkomstig regeringswye reëls, streng protokolle vir datasekuriteit toepas met betrekking tot die berging van oorspronklike datastelle. Data-ontleding wat benodig word om aan NEPA te voldoen, behels noodwendig dat analiste met data op hul rekenaars werk, waarop sagteware vir statistiese ontleding gelaai is. Sodanige werk moet afgestem wees op monitering en navorsing, om scenario's te skets of om die gehalte van data te verifieer.

Ter bevordering van die doelwitte vervat in NEPA, sal analiste verbonde aan staatsentiteite buite die DBO dalk ook met data moet werk wat persoonlike inligting bevat. Om die risiko van diefstal of een of ander vorm van ongemagtigde uitruiling van persoonlike inligting te verhoed, is twee dinge van kritieke belang. Eerstens, die tydperk waartydens persoonlike inligting op ’n persoonlike rekenaar gehou word, moet tot ’n minimum beperk word. Tweedens, die beheer van die betrokke persoonlike rekenaar waarop persoonlike inligting vir die duur van hierdie tydperk geberg word, moet voldoende beveilig wees.

Die POPI-wet vereis dat persoonlike inligting waaroor die DBO beskik, beveilig word. Verwerking sluit geoutomatiseerde en ongeoutomatiseerde wyses in. Die DBO moet gepaste maatreëls tref om:

a) Die verlies van, skade aan of ongemagtigde vernietiging van persoonlike inligting, en
b) Ongemagtigde toegang tot of verwerking van persoonlike inligting te verhoed.

Verskeie dinge kan aanleiding gee tot die verlies van, skade aan of ongemagtigde vernietiging van persoonlike inligting, met inbegrip van:

a) Diefstal van dokumente of elektroniese rekords,
b) Rekenaarvirusse,
c) Rekenaarstakings,
d) Kuberkrakery,
e) Toevallige skade wat deur werknemers of kontrakteurs veroorsaak word, of
f) Natuurrampe.

'n Doeltreffende IT-sekuriteitstelsel behels beveiliging van rekenaarapparatuur en die persoonlike inligting wat op die apparatuur geberg word.

Die volgende stappe word in die POPI-wet gelys:
Identifiseer alle risiko's met betrekking tot persoonlike inligting wat redelikerwys te wagte kan wees. Hier kan 'n evaluering van risiko's verbonde aan persoonlike inligting van waarde wees, en die Prokureursorde van Suid-Afrika (LSSA) beveel aan dat prokureurs dit implementeer.
Die risiko-evaluering moet basies die volgende dek:
 Identifiseer die aard van die persoonlike inligting waaroor die DBO beskik,
 Identifiseer die vernaamste risiko's wat betrokke is by die versameling, berging en verwerking van persoonlike inligting, en
 Bepaal die implikasies vir datasubjekte indien hul persoonlike inligting verlore of vernietig sou raak, of indien onregmatige toegang daartoe verkry sou word.
Sodra duidelikheid verkry is oor die risiko's wat aan persoonlike inligting verbonde is, moet die DBO uitsluitsel kry oor gepaste beveiligingsmaatreëls.

SAMEVATTING VAN SLEUTELPUNTE

a) 'n Doeltreffende IT-sekuriteitstelsel behels beveiliging van rekenaarapparatuur en die persoonlike inligting wat op die apparatuur geberg word.
b) Wolkverwerking kan verskeie vorme aanneem en sal, in die meeste gevalle, daartoe lei dat datasubjekte se persoonlike inligting verwerk word.

AANHANGSEL A: POPI-KONTROLELYS

A. AANWYSING VAN INLIGTINGSBEAMPTE

1. Dit is raadsaam om dieselfde inligtingsbeampte vir beide PAIA (Wet op Bevordering van Toegang tot Inligting) en POPIA (Wet op Beskerming van Persoonlike Inligting) aan te wys.
2. Wys dieselfde adjunkinligtingsbeampte vir beide PAIA en POPIA aan.
3. Kom formeel ooreen oor die rolle en verantwoordelikhede van die inligtingsbeampte en die adjunkinligtingsbeampte, met inbegrip van verslagdoeningstrukture en verpligte gereelde verslagdoening [die tydsverloop tussen verslae moet nie langer as ’n maand wees nie].
4. Handel die aanwysingsproses formeel af by wyse van ’n aanstellingsbrief waarin die rolle en verantwoordelikhede uitgestip word.

B. PROSES

1. Die proses wat gevolg moet word, moet soortgelyk wees aan dié wat vir basiese risikobestuur gevolg word.
2. Oorweging moet aan risiko's en geleenthede geskenk word, en hier behoort kostedoeltreffendheid die riglyn te wees.
3. Verskeie scenario's met ’n velerlei temperende handelinge moet ontwikkel word.
4. Tempering in hierdie geval sal die optrede wees wat voldoening aan die geïdentifiseerde vernaamste risiko's verseker.

C. LEEMTE-ANALISE

1. Maak seker dat vername interne belanghebbendes of ’n deursnee van personeel vanuit verskillende afdelings aan hierdie proses deelneem.
2. Evalueer en hersien bestaande proses en risiko's teen die POPI-wet.
3. Stel voorlopige en finansiële teikens vir voldoening aan die POPI-wet.
4. Maak gebruik van ’n bewysgebaseerde benadering.

D. ONTLEDING VAN DIE VERWERKING EN BERGING VAN PERSOONLIKE INLIGTING

1. Hierdie afdeling is ’n allerbelangrike deel van die beleid.
2. Maak gebruik van die omskrywings en tipe rekords wat in die POPI-wet vervat is.
3. Ooreenkomstig die POPI-wet moet rekords as ’n minimum die volgende velde bevat: stem in, doel, bron, ruil uit, vernietig.
4. Lê slegs die nodige inligting vas.
5. Maak seker dat die velde "reg tot toegang" en "reg tot vaslegging" van inligting ’n vereiste is. [Verwys na die POPI-wet waarin uiteengesit word watter toegangsregte voorgeskryf word en hoe daardie inligting met sake-inligting verbind kan word.]
6. Hou die IKT-beleid in gedagte wanneer gebruikersregte en die bestuur daarvan oorweeg word.
7. Berging van digitale data moet oorweeg word met inagneming van toegangsvergunning [wagwoorde], ’n perk op gebruikers [toeganklikheid] en die beleid oor wagwoorde [verpligte verstryking van wagwoorde wat vereis dat hulle verander word ooreenkomstig ’n voorafbepaalde struktuur – minimum lengte, gebruik van spesiale karakters, ens.].
8. Inligting in gedrukte formaat moet op ’n beveiligde wyse geberg word en wanneer inligting nie benodig word nie, voldoen aan die bepalings soos neergelê deur, onder andere, die SAID en soos uitgestip in die Wet op die Finansiële Inligtingsentrum (FICA).

E. IMPLEMENTERING VAN BELEID TER NAKOMING VAN DIE POPI-WET

1. Hersien alle geldende beleide wat deur die POPI-wet geraak word.
2. Maak seker dat beleide en prosedures geskik en toereikend is.
3. Beleide is niksseggend as hulle nie gemoniteer en afgedwing word nie. Versuim om aan beleide te voldoen, kom neer op nalatigheid aan die kant van bestuur.
4. Maak seker dat die beleid uitgereik word en by alle personeellede se beleidshandleiding ingesluit is.

5. Gebruik ’n rasionele metode om via ’n gedefinieerde en sistematiese proses betroubare en reproduseerbare gevolgtrekkings af te lei. Die benadering se uitkomste of raming moet relevant, toereikend en verifieerbaar wees.
6. Die voormelde moet volledig wees soos per die vereistes wat in die POPI-wet gestel word.
7. Maak seker dat die beleid aan alle personeel verduidelik word en dat elke personeellid by wyse van sy/haar handtekening bevestig dat hy/sy die beleid ten volle verstaan, veral ten opsigte van die doelwitte en die prosesse wat gevolg moet word oor wanneer en hoe data vasgelê en geberg moet word.
8. Die raamwerk moet ten minste kwartaalliks met personeel bespreek word om te verseker dat die maatreëls vir die beskerming van data en tempering van risiko's steeds geld en relevant is.
9. Belanghebbergroepe moet ’n gepaste kennisgewing ontvang wat spesifiek vir verskillende teikengroepe ontwerp is.
10. Derdepartyrisiko's moet in die besonder bestuur word.

F. WEBWERWE EN ANDER BEVEILIGDE WEB- EN AANLYN BERGINGSWERWE

1. Vestig ’n proses vaarvolgens webwerwe hersien word.
2. Maak seker dat vrywarings toereikend is.
3. Maak seker dat geen persoonlike inligting uitwaarts sigbaar is nie [d.w.s. deur gebruikers bekyk kan word].
4. Maak seker dat gebergde inligting en persoonlike inligting beskerm word teen indringerware sowel as kuber- en ander digitale krakers.
5. Ontwikkel ’n skematiese benadering om teen hoërisiko- en geprioritiseerde inligting te waarsku.
6. Maak seker dat standaardnorme vir IKT gebruik word en verkry formele bevestiging in hierdie verband van gasheerwebwerwe en die verskaffers van ander webdienste wat gebruik word.
7. ’n Krisisplan is nodig om enige risiko te temper. Maak seker dat sulke planne vir POPI ontwikkel word. Oor die algemeen is sulke planne gestandaardiseer en

behels dat daar ’n kommunikasieplan in die geval van ’n skending in plek moet wees.

G. GIDS TOT DIE GEBRUIK VAN DIE POPI-WET

1. Maak seker dat jou POPI-gids gereed is en dat personeel teen 1 Julie 2021 opgelei is.
2. As dit reeds in plek is, hersien jou POPI-gids.
3. Maak seker dat jou gids die voorgeskrewe formaat soos per die POPI-wet volg en aan die minimumstandaarde voldoen.
4. Dit het betrekking op uitbesteding aan verskaffers van goedere en dienste wat opsigself unieke risiko's tot gevolg het aangesien hulle toegang het tot persoonlike inligting en, in baie gevalle, ook tot digitale lêers en inligting. Die risiko verbonde aan die berging van dokumentasie wat met uitbestede dienste verband hou, moet op ’n unieke wyse getemper word.

I. OPLEIDING IN NAKOMING VAN DIE POPI-WET

1. Opleiding moet volgens behoefte en vereistes aangepas word.
2. Ongeag waarop dit betrekking het, moet opleiding in die tempering van risiko's [ingeslote kuberkrakery, IKT, ens.] deurlopend wees en by die veranderende omgewing en die ontvouing van risiko's aanpas.
3. Deesdae is aanlyn en differensiële opleiding die norm; daar is dus geen verskoning vir ’n gebrek aan opleiding nie.
4. Gebruik die meegaande voorbeeld van ’n "Business Excellence Model" om alle personeel wat met data en persoonlike inligting te make het, te betrek.
5. Resultate of statistiek wat abnormaal is, vergeleke met die meerderheid resultate [standaard], moet teen daardie standaard vergelyk word.

J. NAKOMING VAN DIE POPI-WET MOET ‘N INTEGRALE DEEL VAN DIE SAKEPROSES WEES

1. Die POPI-wet moet dieselfde behandel word as die bestuur van enige ander risiko in die DBO en moet ’n integrale deel van alle relevante sakeprosesse wees.

2. Prosesse en stelsels verbonde aan nakoming van die POPI-wet moet naatloos by alle sakeprosesse geïntegreer word.
3. Soos met die bestuur van enige risiko verg dit waaksaamheid en die konstante hersiening van tendense, regulasies en wetgewing wat op beide risiko's en geleenthede betrekking het.
4. Wanneer risiko's hersien word, moet dit geskied in die lig van hoe daardie risiko's beide ŉ negatiewe en positiewe impak op bereiking van die praktyk se doelwitte kan hê.
5. Die potensiële negatiewe impak mag dalk verg dat risiko's getemper word, maar daar is ook geleenthede wat weens risiko's verken kan word. Op die lange duur kom alles daarop neer dat die korrekte sakebesluit geneem moet word.