WET OP BESKERMING VAN PERSOONLIKE INLIGTING, WET NO. 4 VAN 2013

Hierdie beleid is van toepassing op inligting rakende geïdentifiseerde individue in terme van die Wet op Beskerming van Persoonlike Inligting, 2013.

Oorsig van die Wet

Die Wet is in November 2013 onderteken en net gedeeltes daarvan het in werking getree gedurende April 2014. In Desember 2016 is die Inligtingsreguleerder aangestel. Die res van die regulasies het op 1 Julie 2020 in werking getree en organisasies moes teen 30 Junie 2021 aan alle wetlike vereistes voldoen. *In omgangstaal word verwys na die Wet as POPI en daar sal in hierdie dokument deurgaans van die afkorting gebruik gemaak word.*

Wie moet aan die POPI-Wet voldoen?

Die POPI-wet is van toepassing op enige instansie, maatskappy of organisasie wat op een of ander wyse persoonlike inligting verwerk. Die Wet geld dus vir openbare liggame (bv. Binnelandse Sake) en private instansies soos finansiële instellings, direkte bemarkers, kerke, asook kultuurorganisasies. Hierdie wetgewing is dus van toepassing op Die Dameskring wat persoonlike inligting van lede hanteer, (hierin verwys na as “die organisasie” en haar lede) in soverre hul werksaamhede uitgevoer word.

Die beskerming van persoonlike inligting is nou meer as ooit noodsaaklik, omdat die ontwikkeling van elektronika die risiko dat dit misbruik en mense se privaatheid geskend kan word, nog groter maak.

Doel van die beleid is om die volgende te bereik:

1. Die bevordering van die beskerming van persoonlike inligting wat deur openbare en privaat liggame verwerk word.
2. Om te voldoen aan die Wet op Persoonlike Inligting t.o.v. spesifieke inligting wat dit inhou.
3. Beskerming van die organisasie se lede en ander individue betrokke.
4. Beskerming van die organisasie van gevolge by verbreking van sy verantwoordelikhede.

Die beleid bepaal dat die organisasie en sy lede:

1. Sal voldoen aan die wetgewing van die POPI-Wet;
2. Persoonlike inligting van lede, geaffilieerde lede en diensverskaffers sal beskerm en respekteer;
3. Die nodige opleiding aanbied waar van toepassing in terme van die Wet; en
4. Alle inligting sal bewaar soos vereis deur die POPI-Wet.

Geïdentifiseerde risiko's

1. Verbreking van vertroulikheid binne die organisasie rakende enige persoonlike inligting aan 'n derde party;
2. Gebrek aan kommunikasie met lede, geaffilieerdes of diensverskaffers rakende toestemming of beveiliging met die gebruik van persoonlike inligting;
3. Gebrek aan voorsorgmaatreëls dat programme en elektroniese stelsels nie opgedateer en geldig is nie;
4. Gebrek aan beveiliging van fisiese dokumentasie wat persoonlike inligting bevat;
5. Gebrek aan die aanstelling van 'n inligtingsbeampte waar nodig; en
6. Onvoldoende toegangskontrole tot areas waar persoonlike inligting gestoor word.

Aanstelling van inligtingsbeampte

Die organisasie se administratiewe beampte is formeel aangewys as inligtingsbeampte wat die nodige registrasie gedoen het. Die inligtingsbeampte sal slegs verslag doen aan die Uitvoerende Bestuur rakende die POPI-Wet. Slegs die inligtingsbeampte sal versoeke rakende bekendmaking van persoonlike inligting met die nodige toestemming hanteer.

Verkryging van toestemming, waar van toepassing in terme van die POPI-Wet

Die organisasie sal skriftelike toestemming verkry vanaf lede en diensverskaffers waar van toepassing, rakende die hantering van persoonlike inligting in terme van die POPI-Wet.

Verwerking en berging van persoonlike inligting

1. Alle persoonlike inligting sal tydens verwerking vertroulik hanteer word.
2. Alle inligting sal in 'n veilige area geliasseer word.
3. Rekenaars en selfone wat gebruik word om inligting te verwerk, sal toegerus wees met 'n geldige anti-virusprogram en gereeld opgedateer word.
4. Die vernietiging van dokumentasie wat persoonlike inligting bevat, sal na behore geskied ten einde te verhoed dat inligting versprei word.

Hersiening van prosesse en prosedures

Die organisasie sal op gereelde basis prosedures en stelsels hersien om te verseker dat alle inligting korrek is en reg hanteer word. Elektroniese programme word voortdurend opgedateer om behoorlike funksionering te verseker.

Sekuriteitsisteme

Die organisasie sal verseker dat:

1. Toegangskontrole in plek is in areas waar persoonlike inligting gestoor word;
2. Alle elektroniese toerusting toegerus is met geldige en opgegradeerde anti-virusprogramme; en
3. Slegs gemagtigde werknemers betrokke sal wees in die evaluering en implementering van sekuriteitstelsels, ten einde te verseker dat stelsels behoorlik funksioneer.

Wat word beskou as persoonlike inligting?

Die organisasie het die reg om die volgende persoonlike inligting met toestemming te verkry ten einde effektief te kan funksioneer:

a) Volle name van ‘n lid
b) Identiteitsnommer
c) Fisiese woon- en/of werkadres
d) Kontakbesonderhede (telefoonnommers, e-posadres)
e) Enige ander persoonlike inligting wat benodig word wat van toepassing is op die organisasie.

Opleiding aan lede rakende die POPI-WET

Die organisasie sal verseker dat:

1. Alle lede ingelig word rakende die POPI-Wet;
2. Lede die gevolge/risiko’s ten volle verstaan wanneer persoonlike inligting geopenbaar word sonder die nodige toestemming;
3. Wanneer van toepassing, opgedateerde inligting aan lede gegee sal word; en
4. Die inligtingsbeampte sal verantwoordelikheid neem om lede, geaffilieerdes of diensverskaffers wat direkte toegang het tot persoonlike inligting, volledig in te lig rakende die POPI-Wet se vereistes (parameters/grense).

Verbreking van datasekuriteit

Die organisasie onderneem om enige betrokke party, hetsy lede, geaffilieerdes, of diensverskaffers, in te lig indien daar enige verbreking van persoonlike inligting plaasvind. Waar van toepassing sal die inligtingsreguleerder ook in kennis gestel word van sodanige verbreking.

MAART 2023