WET van.....,
houdende regels ter bescherming
van privacy en persoonsgegevens
(Wet Bescherming Privacy en
Persoonsgegevens)

ONTWERP

DE PRESIDENT VAN DE REPUBLIEK SURINAME,

In overweging genomen hebbende, dat - vanwege de uitdagingen die informatietechnologie met zich meebrengt in het rechtsverkeer - het noodzakelijk is regels met betrekking tot bescherming van privacy en persoonsgegevens vast te stellen;

Heeft, de Staatsraad gehoord, na goedkeuring door De Nationale Assemblée, bekrachtigd de onderstaande wet:

HOOFDSTUK I
ALGEMENE BEPALINGEN

Artikel 1
Begripsbepalingen

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

a. President : de President van de Republiek Suriname;
b. Minister : de Minister belast met de zorg voor justitiële aangelegenheden;
c. Commissaris voor persoonsgegevensbescherming: de onafhankelijke autoriteit voor gegevensbescherming, als bedoeld in HOOFDSTUK VII;
d. privacy: het recht op bescherming van alle informatie betreffende een geïdentificeerde of identificeerbare levende natuurlijke persoon;
e. persoonsgegevens : alle informatie betreffende een geïdentificeerde of identificeerbare levende natuurlijke persoon;
f. identificeerbare natuurlijke persoon : een persoon die direct of indirect geïdentificeerd kan worden, op grond van de informatie in het bezit van de verwerkingsverantwoordelijke, in het bijzonder door verwijzing naar een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificerend kenmerk of een of meer factoren die specifiek zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
g. verwerking : elke bewerking of geheel van bewerkingen met betrekking tot de persoonsgegevens of het geheel van persoonsgegevens, al dan niet verricht met behulp van geautomatiseerde procedures zoals het verzamelen, registreren, ordenen, structureren, opslaan, wijzigen, opvragen, raadplegen, gebruiken, analyseren, uitvoeren van logische en/of rekenkundige bewerkingen van gegevens, samenvoegen, aaneenschakelen, onthullen door overbrenging, verspreiding of het anderszins beschikbaar maken, groeperen of combineren, afschermen, wissen of vernietigen van gegevens;
h. profilering : elke vorm van geautomatiseerde verwerking van persoonsgegevens bestaande uit het gebruik van persoonsgegevens voor het evalueren van bepaalde aspecten van de persoonlijkheid van een natuurlijke persoon, in het bijzonder het analyseren of voorspellen van elementen betreffende zijn prestaties op het werk, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen;

i. pseudonimisering : de verwerking van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet langer kunnen worden gekoppeld aan specifieke betrokkene zonder aanvullende informatie, mits zodanige aanvullende informatie gescheiden wordt bewaard en technische en organisatorische maatregelen worden genomen om te waarborgen dat de persoonsgegevens niet worden toegekend aan een geïdentificeerde of identificeerbare natuurlijke persoon;
j. bestand: elk geheel van persoonsgegevens dat gestructureerd en toegankelijk is volgens specifieke criteria, ongeacht of het is gecentraliseerd, gedecentraliseerd of verspreid op een functionele of geografische basis;
k. betrokkene: een geïdentificeerde of identificeerbare levende natuurlijke persoon;
l. verwerkingsverantwoordelijke : een natuurlijke persoon of een rechtspersoon, een overheidsinstantie, een dienst of andere instelling die, alleen of samen met andere(n), het doel van en de middelen voor de verwerking van persoonsgegevens bepaalt;
m. verwerker : een natuurlijke persoon of een rechtspersoon, een overheidsinstantie, een dienst of andere instelling die persoonsgegevens verwerkt ten behoeve van de verwerkingsverantwoordelijke;
n. ontvanger : een natuurlijke persoon of een rechtspersoon, een overheidsinstantie, een dienst of andere instelling aan wie of waaraan persoonsgegevens worden mede gedeeld, ongeacht of het al dan niet een derde betreft;
o. derde : een natuurlijke persoon of een rechtspersoon, een overheidsinstantie, een dienst of enige andere instelling, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;
p. toestemming : elke vrijelijk gegeven, specifieke, geïnformeerde en ondubbelzinnige wilsuiting van de betrokkene waarmee hij, door middel van een verklaring of een ondubbelzinnige actieve handeling met de verwerking van de hem betreffende persoonsgegevens aanvaardt;
q. inbreuk in verband met persoonsgegevens: inbreuk op de beveiliging die leidt tot de vernietiging, verlies, wijziging, ongeoorloofde mededeling van, of toegang tot, doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens;
r. genetische gegevens : persoonsgegevens die verband houden met de overgeërfde of verkregen genetische kennerken van een natuurlijke persoon die unieke informatie verschaffen omtrent de fysiologie of de gezondheid van desbetreffende natuurlijke persoon, en die met name voortkomen uit de analyse van een biologisch monster van die natuurlijke persoon;
s. biometrische gegevens : persoonsgegevens die het resultaat zijn van specifieke, technische verwerking met betrekking tot de fysieke, fysiologische of gedragskenmerken van een natuurlijke persoon, die de unieke identificatie van die natuurlijke persoon toestaan of bevestigen, met inbegrip van gezichtsopnamen, bloedgroep, vingerafdrukken, DNA-analyse, netvliesscan en stemherkenning;
t. gegevens die de gezondheid betreffen: persoonsgegevens betreffende de fysieke of geestelijke gezondheid van een natuurlijke persoon, met inbegrip van de verleende gezondheidsdiensten, die informatie aan het licht brengen over zijn gezondheidsstatus;
u. onderneming : een natuurlijke persoon of een rechtspersoon die een economische activiteit uitoefent, ongeacht de rechtsvorm;
v. derde land : elk ander land dan de Republiek Suriname;
w. bindende bedrijfsvoorschriften : beleid inzake de bescherming van persoonsgegevens dat wordt gevolgd door een verwerkingsverantwoordelijke of verwerker over de doorgifte of een reeks van doorgiften van persoonsgegevens aan een verwerkingsverantwoordelijke of

verwerker in een of meer derde landen binnen een concern, of een concern die gezamenlijk een economische activiteit uitoefenen;

x. Instituut voor Gegevensbescherming: het Instituut bedoeld in artikel 23;

y. kind : elke natuurlijke persoon jonger dan 18 (achttien) jaar.

Artikel 2
Materieel toepassingsgebied

1. Deze wet is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens en op de niet-geautomatiseerde verwerking van persoonsgegevens die zijn opgenomen in een bestand of bestemd zijn in een bestand te worden opgenomen.
2. Deze wet is niet van toepassing op de verwerking van persoonsgegevens door een natuurlijke persoon in de context van zijn persoonlijke, gezins- of huishoudelijke aangelegenheden, zonder oogmerk van commercieel gebruik.
3. Specifieke wetten kunnen gemaakt worden voor de verdere regulering van aangelegenheden betreffende privacy en gegevensbescherming in specifieke sectoren, ter verdere versterking van de beschermingsmaatregelen voor betrokkenen, waar zulks van toepassing is; het *lex specialis derogat generali*-beginsel geldt in casu.

Artikel 3
Territoriaal toepassingsgebied

1. Deze wet is van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Republiek Suriname, ongeacht of de verwerking al dan niet plaatsvindt in de Republiek Suriname.
2. Deze wet is van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich bevinden in de Republiek Suriname door een verwerkingsverantwoordelijke of een verwerker die niet is gevestigd in de Republiek Suriname, waarbij de verwerkingsactiviteiten betrekking hebben op:
   a. het aanbod van goederen of diensten door betrokkenen in de Republiek Suriname, ongeacht of enige betaling van de betrokkene vereist is; of
   b. het monitoren van hun gedrag voor zover dit gedrag plaatsvindt in de Republiek Suriname; of
   c. het gebruik van apparaten, al dan niet geautomatiseerd, die zich bevinden op het grondgebied van de Republiek Suriname, tenzij die apparaten uitsluitend gebruikt worden voor doorgifte via het grondgebied van de Republiek Suriname.
3. Deze wet is van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke die niet is gevestigd in de Republiek Suriname, maar in een plaats waar de wetgeving van de Republiek Suriname van toepassing is krachtens het internationaal publiekrecht.

Artikel 4
Het recht op gegevensbescherming

1. Een ieder heeft recht op de bescherming van persoonsgegevens hem betreffende.
2. Persoonsgegevens worden verwerkt in overeenstemming met het bepaalde in deze wet en in het bijzonder te allen tijde met inachtneming van de beginselen als vastgesteld in artikel 5.
3. Deze wet regelt de bescherming van elke natuurlijke persoon met betrekking tot de verwerking van persoonsgegevens alsmede het vrije verkeer van persoonsgegevens, in harmonie met internationale normen.

4. De wet draagt bij aan de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen. In het bijzonder voorziet deze wet in het recht op de bescherming van persoonsgegevens en specificeert deze wet het recht op privacy, als vastgelegd in artikel 17 van de Grondwet in het kader van de verwerking van persoonsgegevens.
5. Deze wet heeft tot doel te voorzien in een rechtskader ter ondersteuning van de ontwikkeling van de cultuur en de praktijk van privacy en gegevensbescherming door middel van:
   a. bevordering van verantwoorde en transparante behandeling van persoonsgegevens;
   b. beschrijving van de algemene beginselen voor de verwerking van persoonsgegevens en van de relevante taken en verplichtingen bij de verwerking van persoonsgegevens; en
   c. de opzet van een bestuurlijk kader voor het waarborgen van transparant toezicht en onpartijdige geschillenbeslechting dat de bescherming van persoonsgegevens door zowel de publieke als de private sector zal versterken.

HOOFDSTUK II
BEGINSELEN

Artikel 5
Beginselen betreffende verwerking persoonsgegevens

Persoonsgegevens worden verwerkt overeenkomstig de volgende beginselen:

a. **rechtmatigheid en eerlijkheid:** persoonsgegevens worden in overeenstemming met deze wet, alsmede met de rechten en vrijheden van personen, verwerkt. Met name wordt iedere verwerking van persoonsgegevens die aanleiding geeft tot ongeoorloofde of willekeurige discriminatie van de betrokkene geacht oneerlijk te zijn;
b. **openheid en transparantie:** verwerking van persoonsgegevens geschiedt op een open en transparante wijze. Specifieke informatie over beleid en praktijken die verband houden met de verwerking van persoonsgegevens worden gemakkelijk beschikbaar gesteld aan natuurlijke personen in een vorm die voor iedereen begrijpelijk is. In principe worden natuurlijke personen op de hoogte gebracht van de risico's, voorschriften, waarborgen en rechten met betrekking tot de verwerking van persoonsgegevens en hoe zij hun rechten kunnen uitoefenen met betrekking tot zodanige verwerking. Natuurlijke personen moeten in staat zijn deze informatie te verkrijgen zonder onredelijke inspanning.
   De specifieke informatie die aan de betrokkene wordt verstrekt, staat aangegeven in artikel 10;
c. **doelbinding, beperking van verwerking en gegevensminimalisering (proportionaliteit):** persoonsgegevens moeten adequaat, relevant en beperkt zijn tot het nodige met betrekking tot de doeleinden waarvoor ze worden verwerkt. De doeleinden waarvoor persoonsgegevens worden verzameld, moeten gespecificeerd zijn, expliciet en legitiem. Persoonsgegevens mogen niet gebruikt worden voor verdere verwerking op een wijze die niet verenigbaar is met die doeleinden. Verdere verwerking voor archiveringsdoeleinden in het algemeen belang, voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden wordt, overeenkomstig het bepaalde in artikel 43, niet geacht onverenigbaar te zijn met het oorspronkelijke doel;
d. **kwaliteit van de gegevens:** persoonsgegevens moeten relevant zijn voor de doeleinden waarvoor ze worden verwerkt, en voor zover nodig voor die doeleinden, moeten ze nauwkeurig, volledig en geactualiseerd zijn. Alle redelijke stappen moeten worden genomen om te garanderen dat persoonsgegevens die onnauwkeurig zijn, in aanmerking nemende de doeleinden waarvoor ze worden verwerkt, onverwijld worden gewist of gecorrigeerd;
e. **beperking op de opslag:** persoonsgegevens worden niet langer bewaard in een vorm die identificatie van betrokkenen mogelijk maakt dan nodig is voor de doeleinden waarvoor de

gegevens worden verwerkt. Persoonsgegevens kunnen worden opgeslagen voor langere perioden voor zover de persoonsgegevens uitsluitend worden verwerkt voor archiveringsdoeleinden in het algemeen belang, voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden, overeenkomstig het bepaalde in artikel 43, mits de gepaste technische en organisatorische maatregelen zijn getroffen krachtens deze wet voor het waarborgen van de rechten en vrijheden van de betrokkene;

f. **veiligheidswaarborgen:** persoonsgegevens worden beschermd door passende veiligheidswaarborgen (technische of organisatorische maatregelen) tegen risico's zoals niet-geautoriseerde of onrechtmatige verwerking, toevallig verlies, vernietiging of beschadiging;
g. **deelname van de betrokkene:** betrokkenen hebben die rechten als vastgesteld in artikel 11;
h. **ethische gegevensverwerking:** persoonsgegevens worden verwerkt op verantwoorde en ethische wijze, indachtig de waardigheid, mensenrechten en vrijheden van personen;
i. **verantwoordelijkheid:** de verwerkingsverantwoordelijke en de verwerker zijn voor zover van toepassing verantwoordelijk (zijn aansprakelijk en moeten in staat zijn naleving aan te tonen) voor het nakomen van de maatregelen om uitvoering te geven aan de hoger genoemde beginselen.

Artikel 6
Rechtmatigheid verwerking

1. Verwerking is rechtmatig indien en voor zover ten minste één van de volgende omstandigheden aanwezig is:
   a. het is noodzakelijk voor het nakomen van een contract, waarbij de betrokkene partij is, of om op verzoek van betrokkene maatregelen te nemen, voordat desbetreffend contract wordt aangegaan;
   b. het is noodzakelijk om de verwerkingsverantwoordelijke in staat te stellen aan een wettelijke verplichting te voldoen;
   c. het is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
   d. het is noodzakelijk voor de uitvoering van een taak verricht in het algemeen belang, waaronder begrepen de nationale veiligheid;
   e. het is noodzakelijk voor de uitoefening van het officiële gezag toegekend aan de verwerkingsverantwoordelijke, waaronder begrepen rechtshandhavingsactiviteiten;
   f. het is noodzakelijk om de verwerkingsverantwoordelijke of derden aan wie de gegevens zijn verstrekt, in staat te stellen een legitiem belang na te streven, behalve waar de belangen of fundamentele rechten en vrijheden van de betrokkene prevaleren boven zodanig belang waarbij bijzondere aandacht zal worden besteedt aan de belangen en grondrechten en fundamentele vrijheden van een kind.
   Het bepaalde hieronder is niet van toepassing op verwerking uitgevoerd door overheidsinstanties bij de uitoefening van hun taken.
2. De verwerking is ook rechtmatig wanneer de betrokkene toestemming heeft verleend voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden. Indien de toestemming van de betrokkene is gegeven in een schriftelijke verklaring die tevens andere aangelegenheden betreft, wordt het verzoek om toestemming gepresenteerd op een wijze die duidelijk te onderscheiden is van de overige aangelegenheden, in een begrijpelijke en gemakkelijk toegankelijke vorm, gesteld in duidelijke en eenvoudige taal. Ieder deel van een zodanige verklaring dat een inbreuk vormt op deze wet, is niet bindend.
3. De betrokkene heeft het recht zijn toestemming te allen tijde in te trekken. De intrekking van de toestemming is niet van invloed op de rechtmatigheid van de verwerking gebaseerd op de desbetreffende toestemming vóór de intrekking daarvan. Alvorens toestemming te verlenen, moet de betrokkene daarover worden geïnformeerd. Het intrekken van de toestemming zal

even gemakkelijk zijn als het geven daarvan. Bij het beoordelen of de toestemming vrijelijk gegeven is, wordt er in hoge mate rekening mee gehouden of, onder meer, de uitvoering van een contract, met inbegrip de verlening van een dienst, afhankelijk is van de toestemming tot de verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van dergelijk contract.

Artikel 7
Voorwaarden inzake toestemming van kinderen

1. Wanneer de verwerking van persoonsgegevens is gebaseerd op toestemming, is de verwerking van persoonsgegevens van een kind rechtmatig, indien het kind dat de toestemming heeft gegeven ten minste 16 (zestien) jaar oud is. Wanneer het kind jonger is dan 16 (zestien) jaar, is zodanige verwerking slechts rechtsmatig indien en voor zover deze toestemming is verleend door de wettelijke vertegenwoordiger van het kind. De verwerkingsverantwoordelijke doet redelijke inspanning te verifiëren dat toestemming is verleend door de wettelijke vertegenwoordiger van het kind.
2. Persoonsgegevens betreffende kinderen mogen niet worden verwerkt op een wijze die niet strookt met het belang van het kind.

Artikel 8
Verwerking bijzondere categorieën van persoonsgegevens

1. De verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van vakvereniging blijken, alsmede de verwerking van genetische gegevens, biometrische gegevens, gegevens met het oog op de gezondheid of gegevens met betrekking tot iemands seksueel gedrag of de seksuele geaardheid, is verboden.
2. Het bepaalde in lid 1 is niet van toepassing indien er sprake is van één van de volgende situaties:
   a. de verwerking is noodzakelijk voor het nakomen van verplichtingen en het uitoefenen van specifieke rechten van de verwerkingsverantwoordelijke of van de betrokkene op het gebied van arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht voor zover dat is toegestaan bij wet of een collectieve overeenkomst die voorziet in passende waarborgen voor de grondrechten en de fundamentele belangen van de betrokkene;
   b. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
   c. de verwerking wordt door een stichting, een vereniging of een andere instantie zonder winstoogmerk, wier doel gelegen is op politiek, religie, of vakbeweging, in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen, op de voorwaarde, dat de verwerking uitsluitend betrekking heeft op de leden of de voormalige leden van de instantie of op personen die in verband met haar doeleinden regelmatig contact met haar onderhouden, en dat, de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt;
   d. de verwerking is noodzakelijk voor de instelling, de uitoefening of de onderbouwing van rechtsvorderingen of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid;
   e. de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op basis van wettelijke regelingen, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene;

f. de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor het beoordelen van de arbeidsgeschiktheid van de werknemer, medische diagnoses, het verstrekken van gezondheidszorg of sociale diensten of behandelingen, danwel het beheren van systemen en diensten voor gezondheidszorg of sociale zorg op basis van de nationale wetgeving of krachtens een contract met een gezondheidswerker;
g. de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals het beschermen tegen ernstige bedreigingen voor de gezondheid of het waarborgen van hoge kwaliteits- en veiligheidsnormen met betrekking tot gezondheidszorg en geneesmiddelen of medische hulpmiddelen, op basis van wettelijke regelingen die voorzien in geschikte en specifieke maatregelen voor het waarborgen van de rechten en vrijheden van de betrokkene, met name het beroepsgeheim;
h. de verwerking is noodzakelijk voor archiveringsdoeleinden in het algemeen belang, wetenschappelijke of historische onderzoeksdoeleinden of statistische doeleinden overeenkomstig het bepaalde in artikel 43 op basis van wettelijke regelingen, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene;
i. de betrokkene heeft uitdrukkelijke toestemming verleend voor de verwerking van die persoonsgegevens voor één of meer specifieke doeleinden, behalve waar andere wettelijke regelingen bepalen dat het verbod bedoeld in lid 1 niet door betrokkene kan worden opgeheven.

3. De verwerking van persoonsgegevens, zoals bedoeld in lid 1, vereist bijzondere zorg om geen oneerlijke discriminatie, vooroordelen of andere nadelen te veroorzaken voor de betrokkenen.

Artikel 9
Verwerking persoonsgegevens betreffende strafrechtelijke veroordelingen en overtredingen

1. De verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen mag op grond van artikel 6 uitsluitend worden uitgevoerd onder toezicht van een officiële autoriteit of wanneer de verwerking is toegestaan krachtens specifieke wettelijke regelingen die passende waarborgen bieden voor de rechten en vrijheden van betrokkenen. Omvattende registers van strafrechtelijke veroordelingen mogen alleen worden bijgehouden onder toezicht van een officiële autoriteit.
2. Onverminderd het bepaalde in lid 1, is een verwerkingsverantwoordelijke die geen officiële autoriteit is, bevoegd tot het verwerken van persoonsgegevens daarmee verband houdende strafrechtelijke veroordelingen en strafbare feiten of gerelateerde veiligheidsmaatregelen, indien de verwerking noodzakelijk is voor het uitvoeren dan wel het uitoefenen van zijn verplichtingen of rechten ofwel die van de betrokkene, ingevolge het arbeidsrecht. In dat geval heeft de verwerkingsverantwoordelijke een intern beleidsdocument, dat bij of krachtens staatsbesluit nader wordt vastgesteld waarin de door de verwerkingsverantwoordelijke te volgen procedures voor het waarborgen van de naleving van artikel 5 worden uitgelegd en het beleid van de verwerkingsverantwoordelijke met betrekking tot het bewaren en het wissen van die gegevens wordt omschreven. De verwerkingsverantwoordelijke stelt dit document op verzoek daartoe beschikbaar aan de Commissaris voor Gegevensbescherming.

HOOFDSTUK III
RECHTEN BETROKKENE

Artikel 10
Informatie te verstrekken aan betrokkene

1. De verwerkingsverantwoordelijke verstrekt de in lid 3 bedoelde informatie aan de betrokkene, hetzij schriftelijk hetzij op andere wijze, waaronder mede begrepen langs elektronische weg, in beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm, en in duidelijke en eenvoudige taal, in het bijzonder wanneer het specifiek aan een kind gerichte informatie betreft.
2. Indien persoonsgegevens bij de betrokkene worden verzameld, verstrekt de verwerkingsverantwoordelijke de in lid 3 aangegeven informatie op het moment van het verzamelen van de persoonsgegevens. Indien de persoonsgegevens niet zijn verkregen van de betrokkene, verstrekt de verwerkingsverantwoordelijke de in lid 3 aangegeven informatie:
   a. binnen een redelijke termijn na het verkrijgen van de persoonsgegevens, maar ten minste binnen 1 (één) maand, met inachtneming van de specifieke omstandigheden waaronder de persoonsgegevens worden verwerkt;
   b. indien de persoonsgegevens worden gebruikt voor communicatie met de betrokkene, tenminste op het tijdstip van de eerste mededeling aan die betrokkene; of
   c. indien mededeling aan een andere ontvanger wordt overwogen, tenminste op het moment dat de persoonsgegevens voor de eerste keer worden doorgegeven.
3. De verwerkingsverantwoordelijke verstrekt aan de betrokkene de hieronder bedoelde informatie:
   a. de identiteit en de contactgegevens van de verwerkingsverantwoordelijke en van zijn eventuele vertegenwoordiger;
   b. de contactgegevens van de functionaris voor gegevensbescherming, indien van toepassing;
   c. de doeleinden van de verwerking waarvoor de gegevens bedoeld zijn en de rechtsgrond van de verwerking; wanneer de verwerking gebaseerd is op artikel 6 lid 1 onder f, dient het rechtmatig belang dat door de verwerker of door een derde wordt nagestreefd, gespecificeerd te worden;
   d. de betreffende categorieën van persoonsgegevens;
   e. de ontvangers of categorieën ontvangers van de persoonsgegevens, zo deze er zijn; indien van toepassing, dat de verwerkingsverantwoordelijke voornemens is de persoonsgegevens door te geven aan een ontvanger in een derde land en de rechtsgrond voor de doorgifte van persoonsgegevens krachtens artikel 22;
   f. de periode gedurende welke de persoonsgegevens worden opgeslagen, of indien dat niet mogelijk is, de criteria gebruikt voor het vaststellen van deze periode;
   g. het bestaan van de rechten van de betrokkene als bedoeld in artikel 11, leden 2 tot en met 11;
   h. waar de verwerking plaatsvindt op basis van artikel 6 lid 2 of van artikel 8 lid 2 onder i, het bestaan van het recht om de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van toestemming vóór de intrekking daarvan;
   i. het recht een klacht in te dienen bij de Commissaris voor Gegevensbescherming.
4. Wanneer de verwerkingsverantwoordelijke voornemens is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor deze persoonsgegevens zijn verzameld of verkregen, dient de verwerkingsverantwoordelijke voorafgaand aan deze verdere verwerking de betrokkene te informeren omtrent dat andere doel, alsmede alle relevante verdere informatie zoals bedoeld in lid 3.

5. Wanneer de persoonsgegevens niet zijn verkregen van de betrokkene, is het bepaalde in de leden 3 en 4 niet van toepassing voor zover:
   a. de betrokkene reeds over de informatie beschikt;
   b. de verstrekking van deze informatie onmogelijk blijkt of een onevenredige inspanning zou vergen, in het bijzonder voor verwerking voor archiveringsdoeleinden in het algemeen belang, voor doeleinden van wetenschappelijk of historisch onderzoek of voor statistische doeleinden, of voor zover de in lid 3 bedoelde verplichting de verwezenlijking van de doelstellingen van die verwerking onmogelijk zou kunnen maken of ernstig belemmeren. In die gevallen treft de verwerkingsverantwoordelijke gepaste maatregelen om de rechten en de vrijheden alsmede de rechtmatige belangen van de betrokkene te beschermen, waaronder het voor het publiek toegankelijk maken van de informatie;
   c. het verkrijgen of mededelen is uitdrukkelijk voorgeschreven in specifieke wetten waaraan de verwerkingsverantwoordelijke onderworpen is en die voorzien in geschikte maatregelen voor het beschermen van de rechtmatige belangen van de betrokkene; of,
   d. wanneer de persoonsgegevens vertrouwelijk moeten blijven krachtens een verplichting van beroepsgeheim geregeld bij wettelijke regeling, met inbegrip van een wettelijke geheimhoudingsplicht.

Artikel 11
Rechten van betrokkene

1. Iedere betrokkene maakt aanspraak op de rechten als hierna opgenomen in de leden 2 tot en met 11 en de verwerkingsverantwoordelijke dient de uitoefening van die rechten te faciliteren.
2. Iedere betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking - waaronder begrepen profilering, bedoeld om bepaalde aspecten van zijn persoonlijkheid te evalueren, zoals bijvoorbeeld zijn arbeidsprestaties, kredietwaardigheid, betrouwbaarheid, gedrag - gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft, tenzij het besluit:
   a. noodzakelijk is voor het aangaan van, of het uitvoeren van een contract tussen de betrokkene en de verwerkingsverantwoordelijke;
   b. is toegestaan bij een nationale wet waaraan de verwerkingsverantwoordelijke is onderworpen en die als zodanig voorziet in passende maatregelen ter bescherming van de rechten en de vrijheden alsmede de rechtmatige belangen van de betrokkene; of
   c. berust op de uitdrukkelijke toestemming van de betrokkene,

   terwijl de verwerkingsverantwoordelijke passende maatregelen heeft genomen om de rechten en de vrijheden alsmede de rechtmatige belangen van de betrokkene te waarborgen, waaronder niet in het minst het recht op menselijke tussenkomst vanwege de verwerkingsverantwoordelijke, zijn standpunt kenbaar maken en het besluit aan te vechten.
3. Elke betrokkene heeft het recht om, op verzoek, kennis te nemen van de onderliggende redenen voor de gegevensverwerking wanneer de resultaten van zodanige verwerking op hem worden toegepast.
4. Elke betrokkene heeft het recht om, op verzoek, met redelijke tussenpozen, bevestiging te krijgen van de verwerking van hem betreffende persoonsgegevens.
5. Elke betrokkene heeft het recht om de hem betreffende persoonsgegevens, welke hij heeft verstrekt aan een verwerkingsverantwoordelijke, in een gestructureerd, gangbaar en machine leesbaar formaat te ontvangen en om die gegevens over te dragen aan een andere verwerkingsverantwoordelijke; in dit opzicht heeft de betrokkene het recht die persoonsgegevens direct te doen doorgeven van de verwerkingsverantwoordelijke aan wie

de persoonsgegevens waren verstrekt, aan een andere verwerkingsverantwoordelijke voor zover zulks technisch uitvoerbaar is. Dit recht wordt uitsluitend toegekend aan de betrokkene indien:

a. de verwerking is gebaseerd op een contract krachtens artikel 6 lid 1 onder a of met toestemming krachtens artikel 6 lid 2 of artikel 8 lid 2 onder i; en
b. de verwerking wordt uitgevoerd langs geautomatiseerde weg. Dit recht is niet van toepassing op de verwerking die noodzakelijk is voor de uitvoering van een taak verricht in het algemeen belang of bij de uitoefening van het openbaar gezag verleend aan de verwerkingsverantwoordelijke.

6. Elke betrokkene heeft het recht op het ontvangen van alle beschikbare informatie inzake de oorsprong, inzake de termijn voor de bewaring van de gegevens alsmede alle andere informatie die de verwerkingsverantwoordelijke verplicht is te verstrekken overeenkomstig artikel 10, met het oog op het garanderen van de transparantie van verwerking.
7. Elke betrokkene heeft het recht te allen tijde bezwaar te maken, tegen de verwerking van hem betreffende persoonsgegevens op gronden verband houdend met zijn omstandigheden, tenzij de verwerkingsverantwoordelijke gerechtvaardigde gronden voor de verwerking aantoont welke zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene. Wanneer evenwel persoonsgegevens worden verwerkt voor direct marketing (inclusief de levering van reclamemateriaal, directe verkoop, uitvoering van marktonderzoeken en commerciële communicatie) en/of voor profilering in verband met dergelijke direct marketing, en de betrokkene bezwaar heeft tegen dergelijke verwerkingsactiviteiten, worden de persoonsgegevens niet langer verwerkt voor dergelijke direct marketing- en profileringsdoeleinden.
8. Elke betrokkene heeft het recht gegevens, op verzoek, te doen rectificeren of wissen, naargelang het geval, indien deze gegevens worden verwerkt of zijn verwerkt in strijd met het bepaalde in deze wet.
9. Wanneer de verwerking is gebaseerd op artikel 6 lid 2 of artikel 8 lid 2 onder i, heeft elke betrokkene het recht zijn toestemming te allen tijde in te trekken, zonder afbreuk te doen aan de rechtmatigheid van de verwerking gebaseerd op toestemming voor de intrekking daarvan.
10. Elke betrokkene heeft het recht een klacht in te dienen ingevolge artikel 33 en recht op de rechtsmiddelen en compensatie krachtens de artikelen 36, 37 en 38 wanneer zijn rechten uit hoofde van deze wet zijn geschonden.
11. De betrokkene heeft het recht om bijgestaan te worden door de Commissaris voor Gegevensbescherming bij de uitoefening van zijn rechten ingevolge deze wet.
12. De besluiten genoemd in lid 2 mogen niet gebaseerd worden op bijzondere categorieën persoonsgegevens genoemd in artikel 8 lid 1, tenzij artikel 8 lid 2 onder e of i van toepassing is en passende maatregelen zijn getroffen ter bescherming van de rechten en de vrijheden alsmede de rechtmatige belangen van de betrokkene.
13. Elk recht toegekend aan een betrokkene zelf uit hoofde van deze wet, mag door de betrokkene worden uitgeoefend of:
    a. wanneer de betrokkene is overleden, door zijn rechtsopvolgers of degene die krachtens erfrecht met het beheer van de nalatenschap is belast indien de uitoefening van het recht of de bevoegdheid, het beheer van de nalatenschap van deze persoon betreft;
    b. door de gemachtigde van de betrokkene, op grond van een volmacht;
    c. door de wettelijke vertegenwoordiger van de betrokkene;
    d. wanneer de betrokkene een kind is, door de wettelijke vertegenwoordiger van het kind.
14. De verwerkingsverantwoordelijke verstrekt informatie aan de betrokkene over een actie ondernomen op een verzoek krachtens de leden 2 tot 11, zonder onredelijke vertraging en in elk geval binnen 1 (één) maand na ontvangst van het verzoek. Die termijn kan met nog 1 (één) maand worden verlengd, waar nodig, rekening houdend met de complexiteit en het

aantal verzoeken. De verwerkingsverantwoordelijke stelt de betrokkene binnen 3 (drie) weken na ontvangst van het verzoek op de hoogte van deze verlenging, onder vermelding van de redenen voor de vertraging. Wanneer de betrokkene het verzoek langs elektronische weg indient, wordt de informatie waar mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

15. Indien de verwerkingsverantwoordelijke geen actie onderneemt op een verzoek van de betrokkene, informeert de verwerkingsverantwoordelijke de betrokkene zonder uitstel en uiterlijk binnen 1 (één) maand na ontvangst van het verzoek omtrent de redenen voor het niet ondernemen van enige actie en omtrent de mogelijkheid om een klacht in te dienen bij een Commissaris voor Gegevensbescherming en het ondernemen van gerechtelijke stappen.
16. Informatie verstrekt ingevolge artikel 10 en iedere kennisgeving alsmede iedere actie ondernomen ingevolge de leden 2 tot en met 11 en artikel 20 lid 5 zijn kosteloos. Wanneer verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, in het bijzonder vanwege hun herhaaldelijk karakter, kan de verwerkingsverantwoordelijke:
    a. een redelijke vergoeding in rekening brengen, in aanmerking nemende de administratieve kosten voor het verstrekken van de informatie of de kennisgeving of het ondernemen van de verzochte actie; of
    b. weigeren gehoor te geven aan het verzoek.

    De bewijslast met betrekking tot het kennelijk ongegronde of buitensporige karakter van het verzoek rust op de verwerkingsverantwoordelijke.
17. Wanneer de verwerkingsverantwoordelijke gegronde twijfel heeft omtrent de identiteit van de natuurlijke persoon die het in de leden 2 tot en met 11 bedoelde verzoek doet, kan de verwerkingsverantwoordelijke om verstrekking van aanvullende informatie noodzakelijk voor het bevestigen van de identiteit van de betrokkene, verzoeken.

HOOFDSTUK IV
BEPERKINGEN

Artikel 12
Beperkingen

1. Specifieke wettelijke regelingen kunnen de reikwijdte van de verplichtingen en rechten vastgelegd in artikel 5, Hoofdstuk III alsmede in artikel 20 lid 5beperken voor zover de bepalingen daarvan overeenstemmen met de rechten en verplichtingen vastgelegd in Hoofdstuk III, wanneer persoonsgegevens worden verwerkt voor de volgende doeleinden:
    a. nationale veiligheid;
    b. defensie;
    c. openbare veiligheid;
    d. de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, waaronder begrepen de bescherming tegen en de preventie van bedreigingen voor de openbare veiligheid;
    e. belangrijke doelstellingen van algemeen openbaar belang van de Republiek Suriname, zoals economische en financiële belangen, monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
    f. de bescherming van de onafhankelijkheid van de rechterlijke macht en van gerechtelijke procedures;
    g. de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;

h. een taak op het gebied van toezicht, inspectie of regelgeving met betrekking tot, zelfs incidenteel, de uitoefening van openbaar gezag in de gevallen genoemd onder a tot en met e en g;
i. de bescherming van de betrokkene of van de rechten en vrijheden van anderen;
j. de inning van civielrechtelijke vorderingen;
k. andere officiële of juridische ondervragingen, onderzoeken of procedures, in het bijzonder procedures gericht op het onderzoeken van oneerlijkheid, incompetentie of onbehoorlijke taakuitoefening door personen betrokken bij het verlenen van bancaire, verzekerings-, investerings- of andere financiële diensten, het beheer van ondernemingen of andere organisaties of het gedrag van personen die op enig moment tijdstip in staat van faillissement zijn verklaard;
l. de bescherming van de internationale betrekkingen van de Republiek Suriname.

2. Specifieke wettelijke regelingen als bedoeld in lid 1 specificeren, indien deze van belang zijn voor:
   a. de doeleinden van de verwerking of categorieën van verwerking;
   b. de categorieën van persoonsgegevens;
   c. de reikwijdte van de ingevoerde beperkingen;
   d. de waarborgen voor het voorkomen van misbruik of onrechtmatige toegang of doorgifte;
   e. de specificatie van de verwerkingsverantwoordelijke of categorieën van verwerkingsverantwoordelijke;
   f. de opslagtermijnen en de toepasselijke waarborgen, met inachtneming van de aard, de omvang en de doeleinden van de verwerking of categorieën van verwerking;
   g. de risico's voor de rechten en vrijheden van betrokkenen; en
   h. het recht van betrokkenen om geïnformeerd te worden over de beperking, tenzij zulks afbreuk kan doen aan het doel van de beperking.

Artikel 13
Uitoefening rechten door betrokkene en verificatie door Commissaris voor Gegevensbescherming

1. Wanneer persoonsgegevens worden verwerkt voor de doeleinden als bedoeld in artikel 12, kunnen de rechten van de betrokkene ook worden uitgeoefend via de Commissaris voor Gegevensbescherming.
2. De verwerkingsverantwoordelijke informeert de betrokkene over de mogelijkheid om zijn rechten uit te oefenen overeenkomstig het bepaalde in lid 1.
3. Wanneer het recht bedoeld in lid 1 wordt uitgeoefend, dient de Commissaris voor Gegevensbescherming de betrokkene tenminste te verwittigen dat alle noodzakelijke verificaties of een inspectie hebben, respectievelijk heeft, plaatsgevonden. Waar van toepassing, stelt de Commissaris voor Gegevensbescherming de betrokkene tevens op de hoogte van zijn recht om gerechtelijke stappen te ondernemen.

HOOFDSTUK V
VERPLICHTINGEN VERWERKINGSVERANTWOORDELIJKEN EN VERWERKERS

Artikel 14
Verantwoordelijkheid bij verwerking persoonsgegevens

1. Verwerkingsverantwoordelijken en, indien van toepassing, verwerkers, treffen alle passende technische en organisatorische maatregelen, met inbegrip van passend beleid en geschikte

gebruiken voor gegevensbescherming, van de Commissaris voor Gegevensbescherming om de bij deze wet gestelde verplichtingen na te leven en om deze naleving aan te kunnen tonen op verzoek.

2. Passende technische en organisatorische maatregelen als bedoeld in lid 1 worden door de verwerkingsverantwoordelijken en de verwerkers uitgevoerd met inachtneming van het volgende:
   a. hun juridische aard en indien van toepassing, de grootte van de onderneming, volgens de relevante nationale wet;
   b. de aard, de omvang, het kader en de doeleinden van de verwerking;
   c. de potentiële risico's die de verwerking zou kunnen veroorzaken voor de rechten en vrijheden van natuurlijke personen.
3. De Commissaris voor Gegevensbescherming kan nadere voorwaarden voor de uitvoering van de leden 1 en 2 vaststellen overeenkomstig het bepaalde in artikel 31 lid 1 onder j.
4. De verwerkingsverantwoordelijke en de verwerker en indien van toepassing, hun vertegenwoordigers, werken op verzoek daartoe samen met de Commissaris voor Gegevensbescherming bij de uitvoering van diens taken.
5. De verwerkingsverantwoordelijke en de verwerker dragen er zorg voor dat personen bevoegd voor het verwerken van persoonsgegevens zich verplicht hebben tot het in acht nemen van geheimhouding of dat een gepaste wettelijke geheimhoudingsplicht op hen rust. De verwerker en elke persoon handelende onder gezag van de verwerkingsverantwoordelijke of van de verwerker die toegang heeft tot persoonsgegevens, verwerken deze gegevens uitsluitend volgens de instructie van de verwerkingsverantwoordelijke, behalve indien bij wet daartoe verplicht.
6. Naast het bepaalde in dit artikel, moeten de verwerkingsverantwoordelijken en de verwerkers ook de overige verplichtingen in de andere artikelen van dit hoofdstuk nakomen.

Artikel 15
Verplichtingen verwerkingsverantwoordelijken

1. Verwerkingsverantwoordelijken geven uitvoering aan gegevensbescherming ingevolge artikel 17 'by design' [door ontwerp] en 'by default' [door standaardinstelling].
2. Wanneer de verwerkingsverantwoordelijke de doeleinden en middelen van de verwerking samen met andere verwerkingsverantwoordelijken ("gezamenlijk voor de verwerking verantwoordelijken") vaststelt, stellen zij op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze wet vast, in een contract of bij ander voor hen juridisch bindend instrument.
3. Wanneer artikel 3 lid 2 van toepassing is, wijst de verwerkingsverantwoordelijke of de verwerker schriftelijk een vertegenwoordiger (hetzij een natuurlijke persoon hetzij een rechtspersoon) in de Republiek Suriname aan, tot wie de Commissaris voor Gegevensbescherming en betrokkenen zich kunnen wenden, tenzij het betreft:
   a. een incidentele verwerking, geen verwerking van bijzondere categorieën van gegevens zoals bedoeld in artikel 8 omvat, noch verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten bedoeld in artikel 9, en waarbij de kans gering is, dat zij een risico inhouden voor de rechten en vrijheden van natuurlijke personen, met inachtneming van de aard, het kader, de reikwijdte en de doeleinden van de verwerking; of
   b. verwerking wordt uitgevoerd door een overheidsinstantie of overheidsorgaan.
4. Wanneer een verwerkingsverantwoordelijke één verwerker of meerdere verwerkers aanstelt voor het uitvoeren van de verwerking ten behoeve van de verwerkingsverantwoordelijke, worden door de verwerkingsverantwoordelijke:

a. alleen verwerkers aangesteld die voldoende waarborgen bieden voor het zodanig uitvoeren van passende technische en organisatorische maatregelen, dat de verwerking beantwoordt aan de bij deze wet gestelde eisen en de bescherming van de rechten van de betrokkene is gewaarborgd;
b. de verwerkingsactiviteiten van een verwerker geregeld in een bindende schriftelijke overeenkomst waarin worden vastgelegd het voorwerp en de duur van de verwerking, de aard en het doel van de verwerking, de soort persoonsgegevens en de categorieën van betrokkenen, de rechten en verplichtingen van de verwerkingsverantwoordelijke en de verplichtingen van de verwerker vastgesteld in artikel 16. De Commissaris voor Gegevensbescherming is bevoegd modelbepalingen voor de overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker vast te stellen.

5. Verwerkingsverantwoordelijken en indien van toepassing, de vertegenwoordigers van de verwerkingsverantwoordelijken, houden registers bij van hun verwerkingsactiviteiten en stellen de Commissaris voor Gegevensbescherming daarvan in kennis in overeenstemming met artikel 18.
6. De verwerkingsverantwoordelijke treft passende technische en organisatorische veiligheidsmaatregelen ingevolge artikel 19.
7. De verwerkingsverantwoordelijke stelt de Commissaris voor Gegevensbescherming overeenkomstig artikel 20 onverwijld in kennis van een inbreuk in verband met persoonsgegevens.
8. De verwerkingsverantwoordelijke wijst een functionaris voor gegevensbescherming aan in overeenstemming met artikel 21.
9. De verwerkingsverantwoordelijke ondemeemt stappen om ervoor te zorgen dat de verwerker en elke natuurlijke persoon handelende onder verantwoordelijkheid van de verwerkingsverantwoordelijke die toegang heeft tot persoonsgegevens, deze gegevens uitsluitend verwerken volgens de instructie van de verwerkingsverantwoordelijke, tenzij hij daartoe bij bijzondere nationale wet verplicht is.

Artikel 16
Verplichtingen van verwerkers

De verwerkers zullen:
a. handelen overeenkomstig artikel 15 lid 3;
b. de persoonsgegevens uitsluitend verwerken volgens gedocumenteerde instructies van de verwerkingsverantwoordelijke;
c. erop toezien dat personen bevoegd voor het verwerken van persoonsgegevens zich verplicht hebben tot het in acht nemen van de geheimhouding of dat een op hen gepaste wettelijke geheimhoudingsplicht rust;
d. andere verwerkers slechts aanstellen met voorafgaande bijzondere of algemene schriftelijke machtiging van de verwerkingsverantwoordelijke, daarbij aan de andere verwerker dezelfde verplichtingen inzake gegevensbescherming opleggend als vastgelegd in de bindende schriftelijke overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker als bedoeld in artikel 15 lid 4 onder b. Zij blijven daarbij ten volle verantwoording verschuldigd aan de verwerkingsverantwoordelijke voor de uitvoering van de verplichtingen van die andere verwerker wanneer die andere verwerker in gebreke blijft zijn verplichtingen inzake gegevensbescherming na te komen;
e. de verwerkingsverantwoordelijke bijstaan, voor zover mogelijk, bij de nakoming van de verplichting van de verwerkingsverantwoordelijke om te reageren op verzoeken voor de uitoefening van de rechten van de betrokkene, met betrekking tot de naleving van deze wet en bij controles, waaronder inspecties, uitgevoerd door de verwerkingsverantwoordelijke of een andere controleur in opdracht van de verwerkingsverantwoordelijke;

f. naar keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wissen of terugsturen naar de verwerkingsverantwoordelijke bij beëindiging van de dienstverlening gerelateerd aan de verwerking, en bestaande kopieën wissen tenzij andere bijzondere wetten verplichten tot de opslag van deze persoonsgegevens;
g. een register bijhouden van alle verwerkingsactiviteiten verricht ten behoeve van een verwerkingsverantwoordelijke ingevolge artikel 18 lid 2;
h. op verzoek daartoe, samenwerken met de Commissaris voor Gegevensbescherming bij de uitvoering van diens taken;
i. passende technische en organisatorische veiligheidsmaatregelen treffen ingevolge artikel 19;
j. melding doen aan de verwerkingsverantwoordelijke zonder vertraging na kennisneming van een inbreuk in verband met persoonsgegevens ingevolge artikel 20 lid 1;
k. ervoor zorgen dat iedere natuurlijke persoon die handelt onder de verantwoordelijkheid van de verwerker die toegang heeft tot persoonsgegevens, deze gegevens uitsluitend verwerkt volgens de instructie van de verwerkingsverantwoordelijke, tenzij hij daartoe bij bijzondere nationale wet verplicht is;
l. een functionaris voor gegevensbescherming overeenkomstig artikel 21 aanwijzen.

Artikel 17
Gegevensbescherming 'by design' [door ontwerp] en 'by default' [door standaardinstelling]

1. Met inachtneming van de stand van zaken van de techniek, de kosten van de implementatie, de aard, de omvang, de context, en de verwerkingsdoeleinden, alsmede de qua waarschijnlijkheid en ernst uiteenlopende risico voor de rechten en vrijheden van natuurlijke personen welke zijn verbonden aan de verwerking, treft de verwerkingsverantwoordelijke, zowel op het tijdstip van de vaststelling van de middelen voor de verwerking als op het tijdstip van de verwerking zelf, uitvoering aan passende technische en organisatorische maatregelen, zoals pseudonimisering, die afgestemd zijn op de beginselen inzake gegevensbescherming, zoals gegevensminimalisering, op effectieve wijze en voor de integratie van de noodzakelijke waarborgen in de verwerking, teneinde te voldoen aan de vereisten van deze wet en ter bescherming van de rechten van de betrokkenen.
2. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te garanderen dat, 'by default', alleen persoonsgegevens die nodig zijn voor elk specifiek doel van de verwerking worden verwerkt. Die verplichting geldt met betrekking tot de hoeveelheid verzamelde persoonsgegevens, de mate van hun verwerking, de periode gedurende welke ze worden opgeslagen en hun toegankelijkheid. In het bijzonder moeten deze maatregelen waarborgen dat persoonsgegevens 'by default' niet toegankelijk worden gemaakt voor een onbeperkt aantal natuurlijke personen zonder interventie van de natuurlijke persoon.

Artikel 18
Registers verwerkingsactiviteiten en melding aan Commissaris voor Gegevensbescherming

1. Elke verwerkingsverantwoordelijke en indien van toepassing, de vertegenwoordiger van de verwerkingsverantwoordelijke, houdt een register bij van verwerkingsactiviteiten onder hun verantwoordelijkheid. Dat register omvat de volgende informatie:
   a. de naam en de contactgegevens van de verwerkingsverantwoordelijke en indien van toepassing, de gezamenlijk voor de verwerking verantwoordelijke, de vertegenwoordiger van de verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming;
   b. de verwerkingsdoeleinden;

c. een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
d. de categorieën ontvangers aan wie de persoonsgegevens zijn of worden verstrekt, indien van toepassing, ontvangers in derde landen, waarbij de derde landen en de rechtsgrond voor de doorgifte van persoonsgegevens krachtens artikel 22 worden aangegeven;
e. indien mogelijk, de beoogde termijnen waarbinnen van de verschillende categorieën gegevens moet worden gewist;
f. een algemene beschrijving van de technische en organisatorische veiligheidsmaatregelen bedoeld in artikel 19.

2. Elke verwerker en indien van toepassing, de vertegenwoordiger van de verwerker, houdt een register bij van alle categorieën verwerkingsactiviteiten verricht ten behoeve van een verwerkingsverantwoordelijke. Dit register bevat:
   a. de naam en de contactgegevens van de verwerker of verwerkers en van elke verwerkingsverantwoordelijke ten behoeve van wie de verwerker handelt en, indien van toepassing, van de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker, en de functionaris voor gegevensbescherming;
   b. de categorieën verwerking uitgevoerd ten behoeve van elke verwerkingsverantwoordelijke;
   c. indien van toepassing, de doorgifte van persoonsgegevens aan een derde land, inclusief de identificatie van dat derde land en de rechtsgrond voor de doorgifte van persoonsgegevens krachtens het bepaalde in artikel 22;
   d. een algemene beschrijving van de technische en organisatorische veiligheidsmaatregelen bedoeld in artikel 19.
3. De registers bedoeld in de leden 1 en 2 worden schriftelijk, waaronder begrepen in elektronische vorm, bijgehouden.
4. De registers bedoeld in de leden 1 en 2 worden ter kennis gebracht van de Commissaris voor Gegevensbescherming. Deze melding wordt bijgewerkt wanneer nodig en tenminste eens per jaar.
5. De Commissaris voor Gegevensbescherming kan nadere voorwaarden stellen en richtlijnen geven voor de uitvoering van dit artikel overeenkomstig het bepaalde in artikel 31 lid 1 onder j.

Artikel 19
Beveiliging verwerking

1. De verwerkingsverantwoordelijke en de verwerker treffen passende technische en organisatorische veiligheidsmaatregelen in verband met risico's zoals accidentele of ongeoorloofde toegang tot, vernietiging, verlies, gebruik, wijziging of verstrekking van persoonsgegevens. Het niveau van gegevensbeveiliging dient in overeenstemming te zijn met het betrokken risico en rekening moet worden gehouden met de technologische ontwikkeling, de potentiële consequenties voor de betrokkenen, de kosten van uitvoering en de aard, de omvang, het kader en de doeleinden van de verwerking.
2. Indien van toepassing volgens lid 1, en voor zover van toepassing, worden de eisen inzake gegevensbeveiliging vastgesteld in Bijlage 1 bij deze wet.

Artikel 20
Inbreuk in verband met persoonsgegevens

1. De verwerkingsverantwoordelijke stelt de Commissaris voor Gegevensbescherming zonder vertraging en indien mogelijk, uiterlijk 72 (tweeënzeventig) uur na kennisneming, op de hoogte van een inbreuk in verband met persoonsgegevens, tenzij het niet waarschijnlijk is

dat deze inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging na kennisneming van een inbreuk in verband met persoonsgegevens. Wanneer de melding aan de Commissaris voor Gegevensbescherming niet is gedaan binnen 72 (tweeënzeventig) uur, moeten ook de redenen voor het oponthoud worden meegedeeld.

2. De melding zoals bedoeld in lid 1 moet ten minste:
   a. de aard van de inbreuk in verband met persoonsgegevens beschrijven, alsmede, als mogelijk, de categorieën en bij benadering het betreffende aantal betrokkenen en de categorieën en het geschatte aantal persoonsgegevensregisters in kwestie;
   b. de naam en de contactgegevens van de functionaris voor gegevensbescherming vermelden, of ander contactpunt waar meer informatie kan worden verkregen;
   c. de mogelijke consequenties van de inbreuk in verband met persoonsgegevens schetsen;
   d. de door de verwerkingsverantwoordelijke genomen of voorgestelde maatregelen voor de aanpak van de inbreuk in verband met persoonsgegevens beschrijven, alsmede, waar van toepassing, de maatregelen voor het verlichten van de mogelijke negatieve gevolgen.
3. Indien het niet mogelijk is de informatie op hetzelfde tijdstip te verstrekken, kan de informatie worden verstrekt in opeenvolgende stadia zonder onredelijke vertraging.
4. De verwerkingsverantwoordelijke documenteert elke inbreuk in verband met persoonsgegevens, met inbegrip van de feiten betreffende de inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de Commissaris voor Gegevensbescherming in staat de naleving van dit artikel te controleren.
5. Na overweging van de aard, mogelijke consequenties en maatregelen ter verzachting van de inbreuk in verband met persoonsgegevens, kan de Commissaris voor Gegevensbescherming de verwerkingsverantwoordelijke verplichten de inbreuk mee te delen aan de betrokkenen en de nodige mededelingen en te gebruiken communicatiemiddelen specificeren.
6. De Commissaris voor Gegevensbescherming houdt een register bij van ontvangen meldingen van inbreuken in verband met persoonsgegevens. Dit register is niet openbaar. Informatie over de gerapporteerde inbreuken in verband met persoonsgegevens kan alleen gebruikt worden in geanonimiseerde of samengevoegde vorm in jaarverslagen en andere publicaties van de Commissaris voor Gegevensbescherming.

Artikel 21
Aanwijzing en taken functionaris voor gegevensbescherming

1. De verwerkingsverantwoordelijke en de verwerker wijzen een functionaris voor gegevensbescherming aan die verantwoordelijk is voor:
   a. het informeren en adviseren van de verwerkingsverantwoordelijke of verwerker en de werknemers die de verwerking van persoonsgegevens uitvoeren, omtrent hun verplichtingen volgens de wet;
   b. het samenwerken met de Commissaris voor Gegevensbescherming;
   c. het fungeren als een contactpunt voor betrokkenen en het verwerken van hun verzoeken voor de uitoefening van de rechten bedoeld in deze wet.
2. De Commissaris voor Gegevensbescherming is bevoegd nadere voorwaarden te stellen en richtlijnen te geven voor de uitvoering van dit artikel overeenkomstig artikel 31 lid 1 onder j.

HOOFDSTUK VI
INTERNATIONALE DOORGIFTE VAN GEGEVENS

Artikel 22

Doorgifte persoonsgegevens buiten de Republiek Suriname

1. De verwerkingsverantwoordelijke of de verwerker geeft geen persoonsgegevens door aan een ontvanger die zich in een derde land bevindt, tenzij:
   a. de ontvanger van de gegevens onderworpen is aan een wet, bindende bedrijfsvoorschriften of een bindende overeenkomst die een adequaat beschermingsniveau biedt welke:
      (i) effectief de beginselen voor verwerking van de persoonsgegevens handhaaft die substantieel vergelijkbaar zijn met de voorwaarden voor de rechtmatige verwerking als vastgesteld in artikel 5; en
      (ii) bepalingen omvat die substantieel vergelijkbaar zijn met dit hoofdstuk, betreffende de verdere doorgifte van persoonsgegevens van de ontvanger aan andere ontvangers die zich bevinden in een derde land;
   b. één van de voorwaarden voor rechtmatige gegevensverwerking als vastgesteld in artikel 6 van toepassing is;
   c. de Commissaris voor Gegevensbescherming toestemming heeft gegeven voor deze specifieke doorgifte van gegevens.
2. Bijzondere categorieën persoonsgegevens (artikel 8) en van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (artikel 9) worden slechts doorgegeven in overeenstemming met punt a of punt c van lid 1.
3. De Commissaris voor Gegevensbescherming kan specifieke wetten, bindende bedrijfsvoorschriften of bindende overeenkomsten die een goed niveau van bescherming verschaffen ingevolge punt a van lid 1 in overeenstemming met artikel 31 lid 1 onder j identificeren.

HOOFDSTUK VII
COMMISSARIS VOOR GEGEVENSBESCHERMING.

Artikel 23
Onafhankelijke status van de Commissaris voor Gegevensbescherming

1. Een onafhankelijke autoriteit voor gegevensbescherming wordt hierbij opgericht. Deze Commissaris voor Gegevensbescherming is verantwoordelijk voor het toezicht op en de handhaving van de toepassing van deze wet en de uitoefening van elke andere taak als vastgesteld in deze wet.
2. De Commissaris voor Gegevensbescherming en zijn personeel, bij de uitoefening van de taken krachtens deze wet:
   a. zijn onafhankelijk, vrij van elke directe of indirecte beïnvloeding van buitenaf;
   b. zijn onpartijdig en oefenen hun taken en bevoegdheden uit zonder vrees, voorkeur of vooroordeel;
   c. handelen in overeenstemming met de Grondwet, deze wet en andere toepasselijke wettelijke regelingen;
3. De Commissaris voor Gegevensbescherming legt verantwoording af aan De Nationale Assemblée.

Artikel 24
Benoeming Commissaris voor Gegevensbescherming

1. De Commissaris voor Gegevensbescherming:
   a. wordt benoemd, geschorst en ontslagen door de President, op voordracht van de Minister, gehoord De Nationale Assemblée;

b. geeft leiding aan het personeel dat de Commissaris voor Gegevensbescherming ondersteunt bij de uitoefening van zijn taken ("Bureau van de Commissaris voor Gegevensbescherming");
c. heeft de kwalificaties en ervaring genoemd in lid 4.

2. Een persoon kan niet fungeren als Commissaris voor Gegevensbescherming, indien hij:
   a. ambtenaar of Minister of griffier van of lid van De Nationale Assemblée is; of
   b. rechter of rechterlijk ambtenaar is; of
   c. lid is van een regionaal of lokaal orgaan (ressortraad of districtsraad); of
   d. enig financieel of ander belang heeft in een onderneming of activiteit dat zijn taken als Commissaris voor Gegevensbescherming kan beïnvloeden; of
   e. failliet of insolvabel is verklaard en niet heeft aangezuiverd; of
   f. ooit is veroordeeld voor een strafbaar feit inzake oneerlijkheid; of
   g. door een rechter geestesziek of psychisch ongeschikt is verklaard.
3. De Commissaris voor Gegevensbescherming wordt voorzien van de personele, technische en financiële hulpmiddelen, het gebouw en de infrastructuur benodigd voor de effectieve uitvoering van zijn taken en de uitoefening van zijn bevoegdheden. De Commissaris voor Gegevensbescherming heeft personeel dat onder het administratieve toezicht van de Commissaris voor Gegevensbescherming staan.
4. Een persoon die is benoemd tot Commissaris voor Gegevensbescherming ingevolge lid 1 is jurist of hoogleraar recht aan een universiteit met ten minste 10 jaar werkervaring en beschikt over een opleiding of bewezen kennis op het gebied van informatiebeveiliging, technologie en audits.
5. Een persoon benoemd overeenkomstig lid 1, legt voordat hij overgaat tot de uitoefening van de taken van de Commissaris voor Gegevensbescherming, de ambtseed af die is vastgesteld in Bijlage 2 bij deze wet, ten overstaan van de President.
6. De Commissaris voor Gegevensbescherming wordt op voltijdse basis aangesteld en mag gedurende zijn ambtsperiode geen ander bezoldigde functie uitoefenen of aannemen, tenzij het wetenschappelijke of academische werkzaamheden betreft.
7. Een persoon benoemd tot Commissaris voor Gegevensbescherming bekleedt dit ambt gedurende vijf jaar en mag worden herbenoemd voor een periode van 5 (vijf) jaar.

Artikel 25
Rechtspersoonlijkheid en vertegenwoordiging Commissaris voor Gegevensbescherming

1. De Commissaris voor Gegevensbescherming heeft rechtspersoonlijkheid en is bevoegd om, behoudens het bepaalde in deze wet, overeenkomsten te sluiten, roerende en onroerende goederen te kopen, te bezitten en te verkopen ten behoeve van de uitoefening van zijn taken, in rechte te laten vervolgen en kan vervolgd worden, en alle handelingen te verrichten die verband houden met of bevorderlijk zijn voor de uitoefening van zijn taken ingevolge deze wet.
2. Elk document opgesteld of afgegeven namens of voor de Commissaris voor Gegevensbescherming en door hem ondertekend, wordt aanvaard als bewijsstuk en wordt geacht, tot het tegendeel is bewezen, een instrument te zijn dat door de Commissaris voor Gegevensbescherming is opgesteld of afgegeven.

Artikel 26
Stafleden Bureau van de Commissaris voor Gegevensbescherming

1. De stafleden van de Commissaris voor Gegevensbescherming beschikken over de kwalificaties, ervaring en professionele vaardigheden, in het bijzonder op het gebied van

privacy en de bescherming van persoonsgegevens, die vereist zijn voor de uitoefening van hun taken en bevoegdheden.

2. De Commissaris voor Gegevensbescherming en zijn stafleden, zijn overeenkomstig deze wet en andere wettelijke regelingen, onderworpen aan het beroepsgeheim zowel tijdens als na hun ambtstermijn, ten aanzien van vertrouwelijke informatie waarvan zij kennis hebben gekregen tijdens de uitoefening van hun taken of bevoegdheden. Tijdens hun ambtstermijn is de plicht tot het bewaren van het beroepsgeheim in het bijzonder van toepassing op meldingen door natuurlijke personen van inbreuken met betrekking tot deze wet.
3. De Commissaris voor Gegevensbescherming en zijn stafleden maken geen gebruik van, noch verstrekken zij, direct of indirect, gegevens die zijn verkregen naar aanleiding van de uitoefening van een bevoegdheid of tijdens de uitoefening van een taak ingevolge deze wet, tenzij:
   a. in overeenstemming met deze wet of andere wettelijke regelingen; of
   b. daartoe gemachtigd krachtens gerechtelijk bevel.

Artikel 27
Financiële middelen Commissaris voor Gegevensbescherming

1. De middelen van de Commissaris voor Gegevensbescherming bestaan uit de jaarlijkse begroting toegewezen door het Ministerie van Justitie en Politie, boeten en vergoedingen die geïnd mogen worden ingevolge deze wet.
2. Het boekjaar van de Commissaris voor Gegevensbescherming loopt vanaf 1 (één) januari tot en met 31 (eenendertig) december. Het eerste boekjaar begint op de datum waarop deze wet van kracht wordt en eindigt op 31 (eenendertig) december van dat jaar.
3. Binnen 6 (zes) maanden na afloop van elk boekjaar moet de Commissaris voor Gegevensbescherming een jaarrekening opstellen in overeenstemming met gevestigde boekhoudkundige praktijken, beginselen en procedures, bestaande uit:
   a. een verslag waaruit voldoende en gedetailleerd het inkomen en de uitgaven van de Commissaris voor Gegevensbescherming over het voorgaande boekjaar blijken; en
   b. een balans van de activa en passiva en de financiële positie aan het einde van het financiële jaar.
4. De Nationale Assemblée controleert jaarlijks het financieel rapport van de Commissaris voor Gegevensbescherming.

Artikel 28
Bescherming Commissaris voor Gegevensbescherming en Bureau van de Commissaris voor Gegevensbescherming

Er worden geen acties of andere procedures voor schadevergoeding ingesteld tegen de Commissaris voor Gegevensbescherming en zijn stafleden voor een handeling te goeder trouw verricht bij de uitoefening van een taak of krachtens bevoegdheid of beoordelingsvrijheid ingevolge deze wet.

Artikel 29
Ontslag of ontheffing Commissaris voor Gegevensbescherming

1. De Commissaris voor Gegevensbescherming kan slechts ontslagen worden op grond van ernstig wangedrag, fysiek of psychisch onvermogen, incompetentie om de verantwoordelijkheden te vervullen, of indien hij niet langer voldoet aan de voorwaarden voor de uitvoering van zijn taken, na een bevinding van die strekking door een Parlementaire

commissie en de goedkeuring door De Nationale Assemblée van een besluit waarin wordt verzocht om deze persoon uit het ambt te ontzetten.

2. Een besluit van De Nationale Assemblée inzake beëindiging van het mandaat van de Commissaris voor Gegevensbescherming moet worden aangenomen door een gewone meerderheid van de leden van De Nationale Assemblée.
3. De President mag de Commissaris voor Gegevensbescherming te allen tijde na de aanvang van de procedure van een Parlementaire commissie vóór ontheffing schorsen; en ontheft de Commissaris voor Gegevensbescherming uit het ambt na goedkeuring door De Nationale Assemblée.
4. De Commissaris voor Gegevensbescherming mag zijn ontslag middels een met redenen omkleed schriftelijke kennisgeving aan de President aanbieden.
5. Wanneer de ambtstermijn van de Commissaris voor Gegevensbescherming is verstreken, blijft hij bevoegd de taken vervullen totdat een opvolger is benoemd.

Artikel 30
Competentie Commissaris voor Gegevensbescherming

1. De Commissaris voor Gegevensbescherming is bevoegd om de taken uit te voeren die zijn toegewezen en de bevoegdheden uit te oefenen die zijn toegekend aan hem overeenkomstig deze wet op het grondgebied van de Republiek Suriname.
2. De Commissaris voor Gegevensbescherming is niet bevoegd om toezicht uit te oefenen op verwerkingen door gerechten bij de uitoefening van hun rechtsbevoegdheid.

Artikel 31
Taken Commissaris voor Gegevensbescherming

1. De Commissaris voor Gegevensbescherming:
   a. monitoort en handhaaft de toepassing van deze wet;
   b. bevordert het publieke bewustzijn en het begrip van de risico's, voorschriften, waarborgen en rechten met betrekking tot gegevensverwerking en verhoogt het besef onder verwerkingsverantwoordelijken en verwerkers van hun plichten in het kader van deze wet; bijzondere aandacht wordt gewijd aan de bewustmaking en het begrip omtrent de risico's, de voorschriften, de waarborgen en de rechten met betrekking tot de verwerking van de persoonsgegevens van kinderen;
   c. brengt, op eigen initiatief of op verzoek, adviezen uit aan de President, De Nationale Assemblée, alsmede aan andere overheidsinstanties en organisaties over wetgevende en bestuurlijke maatregelen inzake de bescherming van de rechten en vrijheden van natuurlijke personen met betrekking tot privacy en de verwerking van persoonsgegevens;
   d. verschaft, op verzoek, informatie en bijstand aan elke betrokkene bij de uitoefening van zijn rechten overeenkomstig deze wet;
   e. behandelt klachten voorgelegd door een betrokkene, of door een instelling, organisatie of associatie krachtens artikel 40 en onderzoekt de inhoud van de klacht in de mate waarin het gepast is, en houdt de indiener van de klacht op de hoogte van de voortgang en het resultaat van het onderzoek zoals bepaald in artikel 34;
   f. voert proactief onderzoek uit naar de toepassing van deze wet;
   g. zorgt voor het aanleggen en het bijhouden van de registers van meldingen ingevolge artikel 18 leden 1 en 2 en artikel 20 lid 6;
   h. werkt samen, zowel op nationaal als op internationaal niveau, met andere instanties betrokken bij de bescherming van privacy en persoonsgegevens, en vergemakkelijkt grensoverschrijdende samenwerking bij de tenuitvoerlegging van wetten inzake privacy en gegevensbescherming door te participeren in initiatieven die gericht zijn op dergelijke

samenwerking;

i. volgt relevant ontwikkelingen, voor zover deze van invloed zijn op de privacy en de bescherming van persoonsgegevens, in het bijzonder de ontwikkeling van informatie- en communicatietechnologieën en handelspraktijken;
j. verleent autorisaties en stelt vast modelformulieren, richtlijnen, aanbevelingen en andere documenten gericht op het nader aangeven of uitvoeren van deze wet;
k. oefent iedere andere taak uit die verband houdt met de bescherming van privacy en persoonsgegevens;
l. stelt het jaarverslag op inzake de activiteiten van zijn Bureau, dient dit verslag in bij de President en De Nationale Assemblée en stelt het beschikbaar aan het publiek.

2. Deze wet verleent de Commissaris voor Gegevensbescherming alle bevoegdheden die nodig zijn om zijn taken uit te oefenen.
3. De Commissaris voor Gegevensbescherming vergemakkelijkt de indiening van de onder lid 1 sub e bedoelde klachten door maatregelen zoals een klachtenformulier dat ook elektronisch kan worden ingevuld, zonder uitsluiting van andere communicatiemiddelen.
4. De uitvoering van de taken van de Commissaris voor Gegevensbescherming is kosteloos voor de betrokkene.
5. Wanneer verzoeken kennelijk ongegrond of buitensporig zijn, in het bijzonder vanwege hun herhaaldelijk karakter, kan de verwerkingsverantwoordelijke een redelijke vergoeding op basis van de administratieve kosten in rekening brengen, of weigeren gehoor te geven aan het verzoek.

Artikel 32
Bevoegdheden Commissaris voor Gegevensbescherming

1. De Commissaris voor Gegevensbescherming heeft de volgende bevoegdheden:
   a. het opdragen van de verwerkingsverantwoordelijke en de verwerker en waar van toepassing, de vertegenwoordiger van de verwerkingsverantwoordelijke of van de verwerker, om de informatie te verschaffen welke hij nodig heeft voor het uitvoeren van zijn taken;
   b. het verrichten van onderzoek in de vorm van controles op gegevensbescherming;
   c. het in kennis stellen van de verwerkingsverantwoordelijke of de verwerker van een vermeende inbreuk op deze wet;
   d. het verkrijgen van toegang tot alle persoonsgegevens en de informatie noodzakelijk voor het uitvoeren van zijn taken van de verwerkingsverantwoordelijke en de verwerker;
   e. het verkrijgen van toegang van de verwerkingsverantwoordelijke en de verwerker tot alle gebouwen, met inbegrip van de apparaten en middelen voor gegevensverwerking, overeenkomstig het toepasselijke procesrecht;
   f. het waarschuwen van een verwerkingsverantwoordelijke of verwerker wiens voorgenomen verwerkingen mogelijk inbreuk zullen maken op het in deze wet bepaalde;
   g. het verstrekken van handhavingskennisgevingen aan een verwerkings-verantwoordelijke of verwerker wanneer verwerkingshandelingen inbreuk hebben gemaakt op het in deze wet bepaalde;
   h. het gelasten van de verwerkingsverantwoordelijke of de verwerker om te voldoen aan het verzoek van de betrokkene om zijn rechten uit te oefenen overeenkomstig artikel 11;
   i. het gelasten van de verwerkingsverantwoordelijke of verwerker om de verwerkingen te laten beantwoorden aan het in deze wet bepaalde, waar van toepassing, op een welbepaalde wijze en binnen een welbepaalde termijn;
   j. het gelasten van de verwerkingsverantwoordelijke om een betrokkene omtrent een inbreuk in verband met persoonsgegevens te informeren overeenkomstig artikel 20 lid 5;
   k. het opleggen van een tijdelijke of definitieve beperking met inbegrip van een verbod op

verwerking;

l. het gelasten tot rectificatie of wissen van persoonsgegevens overeenkomstig artikel 11;
m. het opleggen van een administratieve boete overeenkomstig artikel 35, afhankelijk van de omstandigheden van elk afzonderlijk geval;
n. het gelasten van de opschorting van gegevensstromen naar een ontvanger in een derde land;
o. het onder de aandacht van de gerechtelijke autoriteiten brengen van inbreuken op deze wet en waar van toepassing, aanvangen van of anderszins optreden in gerechtelijke procedures met het oog op het uitvoeren van het in deze wet bepaalde;
p. het trachten een klacht op te lossen door ze te verwijzen naar beschikbare mechanismen voor geschillenbeslechting zoals bemiddeling. het uitvoeren van verificatie overeenkomstig artikel 13.

2. Op de uitoefening van bevoegdheden verleend aan de Commissaris voor Gegevensbescherming overeenkomstig dit artikel zijn passende waarborgen van toepassing, met inbegrip van doeltreffende rechterlijke voorzieningen en eerlijke rechtsgang, overeenkomstig de Grondwet.

HOOFDSTUK VIII
RECHTSMIDDELEN, AANSPRAKELIJKHEID EN ADMINISTRATIEVE BOETEN

Artikel 33
Indiening klacht bij Commissaris voor Gegevensbescherming

1. Onverminderd andere mogelijkheden van administratief beroep of rechterlijke voorzieningen, heeft iedere betrokkene of zijn wettelijke vertegenwoordiger het recht een klacht in te dienen bij de Commissaris voor Gegevensbescherming, indien de betrokkene van mening is dat de verwerking van de hem betreffende persoonsgegevens inbreuk maakt op de onderhavige wet.
2. Een klacht gericht aan de Commissaris voor Gegevensbescherming wordt schriftelijk ingediend of met gebruikmaking van de elektronische formulieren die voor dit doel door de Commissaris voor Gegevensbescherming beschikbaar zijn gesteld. De Commissaris voor Gegevensbescherming verleent zodanige redelijke bijstand als nodig is om een persoon die een klacht wenst in te dienen, in staat te stellen de klacht op schrift te stellen.
3. Een klacht omvat de volgende informatie:
   a. de naam en de contactgegevens van de betrokkene of waar van toepassing, zijn wettelijke vertegenwoordiger;
   b. de naam en het adres van de verwerkingsverantwoordelijke;
   c. omschrijving van het handelen en/of het nalaten dat tot de klacht heeft geleid;
   d. een kopie van het verzoek om toegang tot persoonsgegevens, rectificatie, annulering of bezwaar gezonden naar de verwerkingsverantwoordelijke;
   e. een kopie van het antwoord ontvangen van de verwerkingsverantwoordelijke;
   f. ander beschikbaar bewijs of beschikbare informatie die geschikt wordt geacht om onder de aandacht van de Commissaris voor Gegevensbescherming te brengen;
   g. de datum van de klacht en handtekening.
4. Afwijken van het formaat van een klacht zoals bedoeld in lid 3 mag geen grond zijn voor weigering de klacht te onderzoeken.
5. Anonieme klachten worden niet onderzocht, tenzij de Commissaris voor Gegevensbescherming anders besluit.

6. De Commissaris voor Gegevensbescherming kan, op eigen initiatief, een onderzoek beginnen naar het handelen of het nalaten dat een schending kan zijn van de wet en de rechten van een betrokkene of een groep betrokkenen.

Artikel 34
Klachtenprocedure

1. Na ontvangst van een klacht, wordt door de Commissaris voor Gegevensbescherming:
   a. een onderzoek ingesteld naar de klacht en een besluit genomen overeenkomstig zijn relevante bevoegdheden genoemd in artikel 32; of
   b. de klacht verworpen, overeenkomstig lid 7.
2. De Commissaris voor Gegevensbescherming informeert de indiener van de klacht over de voortgang en het resultaat van de behandeling van de klacht, met inbegrip van de mogelijkheid van rechtsmiddelen overeenkomstig de artikelen 36 en 37.
3. De Commissaris voor Gegevensbescherming onderzoekt de klacht en neemt een besluit binnen 3 (drie) maanden na de datum van ontvangst van de klacht. Indien het onderzoek een langere periode beslaat vanwege de complexiteit van de omstandigheden aangegeven in de klacht, wordt de termijn voor het nemen van een besluit verlengd met ten hoogste 3 (drie) maanden. De Commissaris voor Gegevensbescherming informeert de indiener van de klacht over de verlenging van de termijn voor het nemen van een besluit binnen 2 (twee) maanden na de datum van ontvangst van de klacht. Het onderzoeken van klachten en het nemen van relevante besluiten geschiedt binnen de kortst mogelijke tijd.
4. De Commissaris voor Gegevensbescherming, of een aangewezen functionaris van het Bureau van de Commissaris voor Gegevensbescherming, kan een onderzoek of inspectie verrichten in het kader van het klachtenonderzoek, indien vergezeld van een politiefunctionaris en met een bevel afgegeven door een hulpofficier van justitie, elk gebouw betreden, de noodzakelijke onderzoekingen doen om na te gaan of deze wet wordt nageleefd, elk goed, document, apparaat of ander materiaal voor korte tijd in zijn bezit te hebben en vasthouden zo lang als zulks nodig mocht zijn.
5. De bij bevel verleende bevoegdheden bedoeld in lid 4 kunnen beperkt worden overeenkomstig wettelijke regelingen, wanneer persoonsgegevens worden verwerkt voor doeleinden gespecificeerd in artikel 12.
6. De bij bevel verleende bevoegdheden bedoeld in lid 4 kunnen niet worden uitgeoefend met betrekking tot:
   a. een communicatie tussen een professioneel juridisch adviseur en zijn cliënt in verband met het geven van juridisch advies aan de cliënt met betrekking tot zijn verplichtingen, aansprakelijkheden of rechten krachtens deze wet; of
   b. elke communicatie tussen een professioneel juridisch adviseur en zijn cliënt, of tussen die adviseur of zijn cliënt en een andere persoon, gedaan in verband met of met het oog op enige procedure krachtens of naar aanleiding van deze wet.
7. De Commissaris voor Gegevensbescherming kan een klacht afwijzen, binnen 1 (één) maand na de datum van ontvangst van de klacht en dit schriftelijk ter kennis brengen van de indiener en met vermelding van de redenen voor de afwijzing, indien:
   a. het onderzoek naar de omstandigheden genoemd in de klacht buiten de competentie van de Commissaris voor Gegevensbescherming vallen;
   b. een klacht voor hetzelfde handelen of nalaten reeds is onderzocht door de Commissaris voor Gegevensbescherming en een definitief besluit met betrekking tot dezelfde betrokkene is genomen, tenzij nieuwe feiten worden ingediend;
   c. een juridische procedure in verband met hetzelfde handelen of nalaten aanhangig gemaakt door de betrokkene in behandeling is bij de bevoegde gerechtelijke instanties;
   d. de klacht aanstootgevend, onbeduidend of niet te goeder trouw is;

e. de tijd verstreken tussen de datum van het handelen of nalaten dat aanleiding gaf tot de klacht en de datum waarop de klacht is ingediend zodanig is dat een onderzoek naar de klacht niet langer uitvoerbaar of wenselijk is.

8. Alle besluiten van de Commissaris voor Gegevensbescherming worden openbaar gemaakt in het Advertentieblad van de Republiek Suriname en in ten minste één in Suriname verschijnend dagblad, waarbij alle verwijzingen naar de betrokkenen die hen identificeren of identificeerbaar maken, worden verwijderd.

Artikel 35
Administratieve boete

1. De Commissaris voor Gegevensbescherming kan de verwerkingsverantwoordelijke en de verwerker die een inbreuk maken op de bepalingen als bedoeld in de Hoofdstukken II, III, V en VI een geldboete opleggen.
2. De hoogte van de boete wordt afgestemd op de ernst van het feit, de omstandigheden waarin de betrokkene verkeert en de mate van verwijtbaarheid.
3. De boete kan voorwaardelijk of onvoorwaardelijk worden opgelegd.
4. Het opleggen van een voorwaardelijke boete geschiedt steeds onder de algemene voorwaarde dat de betrokkene zich voor het einde van de proeftijd, die op ten hoogste twee jaar gesteld kan worden, niet gedraagt op de in het lid 1 bedoelde wijze.
5. Bij het opleggen van een boete alsmede bij de vaststelling van de hoogte ervan wordt in ieder geval rekening gehouden met de ernst en de duur van de overtreding.
6. De hoogte van de geldboete, bedoeld in lid 1, bedraagt:
   a. bij inbreuk op de bepalingen als bedoeld in Hoofdstuk V ten hoogste 5000,- SRD (vijfduizend) of in het geval van een onderneming, tot 2 (twee) % van de totale wereldwijde jaarlijkse omzet over het voorgaande boekjaar, als dit laatste bedrag hoger is.
   b. bij inbreuk op de bepalingen als bedoeld in de Hoofdstukken II, III en VI en bij niet-nakoming van een besluit, een bevel, een uitvoeringskennisgeving of een tijdelijke of definitieve beperking inzake de verwerking of de opschorting van de gegevensstromen door de Commissaris voor Gegevensbescherming of het niet-verlenen van toegang tot alle persoonsgegevens, informatie en gebouwen noodzakelijk voor het onderzoek van klachten overeenkomstig a artikel 32 ten hoogste SRD. 10.000,- (tienduizend Surinaamse Dollar) tot 4 (vier) % van de totale wereldwijde jaarlijkse omzet over het voorgaande boekjaar, als dit laatste bedrag hoger is.
7. De Commissaris voor Gegevensbescherming is bevoegd een dwangbevel uit te doen vaardigen ten einde de ingevolge deze wet verschuldigde geldsommen in te vorderen, indien de volledige betaling door een overtreder niet binnen de in lid 11 gestelde aanmaningstermijn heeft plaatsgevonden. Het dwangbevel kan evenwel zonder aanmaning en voor het verstrijken van bij wettelijk voorschrift gestelde of eerder gegunde betalings- of aanmaningstermijnen worden uitgevaardigd of ten uitvoer worden gelegd, indien het op voorhand duidelijk is dat de overtreder niet aan diens geldelijke verplichtingen zal voldoen.
8. Het dwangbevel vermeldt in ieder geval:
   a. aan het hoofd het woord "dwangbevel";
   b. het bedrag van de invorderbare hoofdsom;
   c. de beschikking of het wettelijk voorschrift waaruit de geldschuld voortvloeit;
   d. de kosten van het dwangbevel;
   e. dat het op kosten van de schuldenaar ten uitvoer kan worden gelegd; en voorts indien van toepassing
   f. het bedrag van de aanmaningsvergoeding; en
   g. de ingangsdatum van de wettelijke rente.

9. Alvorens een dwangbevel uit te vaardigen wordt de overtreder aangemaand tot betaling, binnen een termijn van vier weken. De aanmaning vermeldt dat bij niet tijdige betaling deze kan worden afgedwongen door op kosten van de schuldenaar uit te voeren invorderingsmaatregelen.
10. Voor de aanmaning wordt een vergoeding in rekening gebracht. De hoogte van de vergoeding wordt bij of krachtens staatsbesluit vastgesteld. De aanmaning vermeldt de vergoeding die in rekening wordt gebracht.
11. Het dwangbevel wordt op kosten van de overtreder bij deurwaardersexploot betekend en levert een executoriale titel op in de zin van het Tweede Boek van het Wetboek van Burgerlijke Rechtsvordering.

Artikel 36

1. Indien de Commissaris voor Gegevensbescherming voornemens is een geldboete op te leggen, geeft hij daarvan kennis aan de betrokkene, onder vermelding van het feit ter zake waarvan het voornemen bestaat en van de gronden waarop het voornemen berust.
2. Voordat de boete wordt opgelegd, stelt de Commissaris voor Gegevensbescherming de betrokkene in de gelegenheid om naar keuze schriftelijk of mondeling zijn zienswijze naar voren te brengen. Hij kan zich daarbij doen bijstaan door een raadspersoon.

Artikel 37

1. Bij het vaststellen of een administratieve boete moet worden opgelegd en het bepalen van het bedrag van de administratieve boete in elk afzonderlijk geval, houdt de Commissaris voor Gegevensbescherming naar behoren rekening met het volgende:
   a. de aard, ernst en duur van de inbreuk, met inachtneming van de aard, omvang of het doel van de desbetreffende verwerking alsmede het aantal getroffen betrokkenen en de mate waarin zij schade hebben ondervonden;
   b. het feit of de inbreuk opzettelijk of uit nalatigheid is gepleegd;
   c. elke maatregel genomen door de verwerkingsverantwoordelijke of de verwerker om de schade geleden door de betrokkenen te beperken;
   d. de mate van aansprakelijkheid van de verwerkingsverantwoordelijke of de verwerker, met inachtneming van de technische en organisatorische maatregelen die door hen zijn geïmplementeerd;
   e. elke relevante eerdere inbreuken door verwerkingsverantwoordelijke of de verwerker;
   f. de mate van samenwerking met de Commissaris voor Gegevensbescherming bij het opheffen van de inbreuk en het verlichten van de mogelijke nadelige gevolgen van de inbreuk;
   g. de categorieën van persoonsgegevens getroffen door de inbreuk;
   h. de wijze waarop de inbreuk ter kennis is gekomen van de Commissaris voor Gegevensbescherming, in het bijzonder of en zo ja, in hoeverre de verwerkingsverantwoordelijke of de verwerker melding hebben gemaakt van de inbreuk;
   i. indien eerder besluiten zijn genomen tegen de desbetreffende verwerkingsverantwoordelijke of verwerker ten aanzien van hetzelfde onderwerp, de nakoming van die besluiten;
   j. eventuele andere verzwarende of verzachtende factoren van toepassing op de omstandigheden van het geval, zoals financiële voordelen behaald, of verliezen vermeden, direct of indirect, door de inbreuk.

Artikel 38

Recht effectieve rechterlijke voorzieningen tegen Commissaris voor Gegevensbescherming

1. Onverminderd enig ander administratief of buitengerechtelijk beroep, heeft elke natuurlijke persoon of rechtspersoon doeltreffende voorzieningen van rechtswege tegen een juridisch bindend besluit van de Commissaris voor Gegevensbescherming.
2. Onverminderd enig ander administratief of buitengerechtelijk beroep, heeft elke natuurlijke persoon of rechtspersoon doeltreffende voorzieningen van rechtswege indien de Commissaris voor Gegevensbescherming een klacht niet afhandelt overeenkomstig artikel 34.
3. Gerechtelijke stappen tegen de Commissaris voor Gegevensbescherming worden ingesteld bij de kantonrechter.

Artikel 39
Recht effectieve rechterlijke voorzieningen tegen verwerkingsverantwoordelijke of verwerker

尊1. Onverminderd enig ander beschikbaar administratief of buitengerechtelijk beroep,
1. Onverminderd enig ander beschikbaar administratief of buitengerechtelijk beroep, inclusief het recht een klacht in te dienen bij de Commissaris voor Gegevensbescherming krachtens artikel 33, heeft elke betrokkene doeltreffende voorzieningen van rechtswege indien hij van mening is dat zijn rechten krachtens deze wet zijn geschonden als gevolg van een verwerking van zijn persoonsgegevens die niet overeenkomstig deze wet is uitgevoerd.
2. Gerechtelijke stappen tegen een verwerkingsverantwoordelijke of verwerker worden ingesteld bij de kantonrechter.

Artikel 40
Recht op schadevergoeding en aansprakelijkheid

1. Elke persoon die materiële of niet-materiële schade heeft geleden als gevolg van een inbreuk op deze wet heeft het recht van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade.
2. Elke verwerkingsverantwoordelijke betrokken bij de verwerking is aansprakelijk voor de schade veroorzaakt door verwerking die niet overeenkomstig deze wet is uitgevoerd. Een verwerker is slechts aansprakelijk voor de schade veroorzaakt door verwerking, indien de verwerker de specifiek op verwerkers gerichte verplichtingen uit hoofde van deze wet niet is nagekomen of indien de verwerker heeft gehandeld buiten of in strijd met rechtmatige instructies van de verwerkingsverantwoordelijke.
3. Verwerkingsverantwoordelijken of verwerkers zijn niet aansprakelijk ingevolge lid 2, indien zij aantonen dat zij in generlei opzicht verantwoordelijk zijn voor de gebeurtenis waardoor de schade is ontstaan.
4. Wanneer meer dan één verwerkingsverantwoordelijke of verwerker, of zowel een verwerkingsverantwoordelijke als een verwerker, betrokken zijn bij dezelfde verwerking en wanneer zij, ingevolge de leden 2 en 3, verantwoordelijk zijn voor eventuele schade veroorzaakt door verwerking, wordt elke verwerkingsverantwoordelijke of verwerker aansprakelijk gehouden voor de volledige schade teneinde doeltreffende vergoeding van de betrokkene te garanderen.
5. Wanneer een verwerkingsverantwoordelijke of verwerker, overeenkomstig lid 4 de volledige vergoeding heeft betaald voor de geleden schade, is die verwerkingsverantwoordelijke of verwerker gerechtigd van de overige verwerkings-verantwoordelijken of verwerkers betrokken bij die verwerking dat deel van de vergoeding dat overeenkomt met hun deel van de aansprakelijkheid voor de schade terug te vorderen, overeenkomstig de voorwaarden opgenomen in lid 2.

6. Gerechtelijke procedure voor de uitoefening van het recht op het ontvangen van vergoeden wordt ingesteld bij de kantonrechter.

Artikel 41
Bescherming klokkenluiders

Een werkgever, al dan niet een overheidsinstantie, ontslaat een werknemer niet, schorsen, degraderen, disciplineren, beboeten, intimideren of anderszins benadelen of een voordeel ontzeggen, omdat:

a. de werknemer, handelend te goeder trouw en op de basis van redelijke overtuiging, de Commissaris voor Gegevensbescherming heeft gemeld dat de werkgever of enige andere persoon op de werkplek deze wet heeft of zal overtreden;
b. de werkgever meent dat de werknemer de Commissaris voor Gegevensbescherming in kennis zal stellen krachtens sub a;
c. de werknemer iets heeft gedaan of te kennen heeft gegeven iets te zullen doen dat gedaan moet worden om te voorkomen dat een persoon deze wet overtreedt; of
d. de werknemer geweigerd heeft of te kennen heeft gegeven te zullen weigeren iets te doen dat in strijd is met deze wet.

Artikel 42
Vertegenwoordiging betrokkenen

De betrokkene heeft het recht een instelling, organisatie of vereniging zonder winstoogmerk welke rechtsgeldig is opgericht overeenkomstig specifieke wettelijke regelingen, met een statutair doel dat in het algemeen belang is en die actief is op het gebied van de bescherming van de rechten en vrijheden van betrokkene met betrekking tot de bescherming van zijn privacy en persoonsgegevens, last te verlenen om namens hem een klacht in te dienen overeenkomstig artikel 33 en rechten uit te oefenen overeenkomstig de artikelen 38, 39 en 40.

HOOFDSTUK IX
UITZONDERINGEN VOOR SPECIFIEKE VERWERKINGSSITUATIES

Artikel 43
Uitzonderingen voor journalistieke, literaire of artistieke doeleinden

Deze wet is niet van toepassing op de verwerking van persoonsgegevens uitsluitend voor journalistieke, literaire of artistieke uitingen voor zover zodanige uitsluiting in het algemeen belang noodzakelijk is overeenkomstig deze wet.

Artikel 44
Verwerking en toegang publiek tot officiële documenten

Persoonsgegevens in officiële documenten in het bezit van een overheidsinstantie of een openbare instelling of een particuliere instelling ter uitvoering van een taak verricht van algemeen belang mogen door de instantie of de instelling worden bekendgemaakt in overeenstemming met specifieke wettelijke regelingen waaraan die overheidsinstantie of die instelling onderworpen is teneinde de toegang van het publiek tot officiële documenten overeen te stemmen met het recht op privacy en het recht op gegevensbescherming overeenkomstig deze wet.

Artikel 45
Waarborgen en afwijkingen inzake verwerking voor archiveringsdoeleinden in het algemeen belang, doeleinden van wetenschappelijk of historisch onderzoek of statistische doeleinden

Indien persoonsgegevens worden verwerkt voor doeleinden van wetenschappelijk of historisch onderzoek, statistische doeleinden en archiveringsdoeleinden, kunnen de rechten van de betrokkene inzake toegang, rectificatie en om bezwaar te maken overeenkomstig artikel 11 beperkt worden voor zover deze rechten het verwezenlijken van de specifieke doelen onmogelijk zouden maken of ernstig belemmeren en voor zover zodanige afwijkingen noodzakelijk zijn voor het bereiken van deze doeleinden.

HOOFDSTUK X
Intrekking en Slotbepalingen

Artikel 46
Intrekking

Eventuele bepalingen in enige andere nationale wet worden ingetrokken voor zover deze resulteren in een eventuele vermindering van de bescherming verleend aan betrokkenen door deze wet.

Artikel 47
Slotbepaling

1. Deze wet wordt aangehaald als: Wet Bescherming Privacy en Persoonsgegevens.

2. Zij wordt in het Staatsblad van de Republiek Suriname afgekondigd en treedt in werking met ingang van de dag volgende op die van haar afkondiging.

3. De Minister van Justitie en Politie is belast met de uitvoering van deze wet.

Gegeven te Paramaribo, de .....

CHANDRIKAPERSAD SANTOKHI

WET van.....,
houdende regels ter bescherming
van privacy en persoonsgegevens
(Wet Bescherming Privacy en Persoonsgegevens)

MEMORIE VAN TOELICHTING

A. Algemeen

De toenemende zorg over privacy in Suriname heeft te maken met het toegenomen gebruik van ICT. Daardoor is de wereld kleiner geworden met andere woorden dat we meer en vaker en sneller met elkaar te maken hebben, maar ook door het commerciële belang dat is ontstaan bij het verkrijgen van persoonsgegevens.
We zijn ons nog onvoldoende bewust van de gevaren die kleven aan computerprogramma's zoals Facebook en Instagram.

Er zijn wettelijke mogelijkheden in Suriname om bescherming van persoonsgegevens te eisen, te weten:
- artikel 17 van de Grondwet;
- artikel 11 van het Inter-Amerikaans Verdrag voor de Rechten van de Mens;
- artikel 17 van het Verdrag inzake Burgerlijke en Politieke Rechten.

Echter, in Suriname willen we dat onze privacy verantwoord en duurzaam gewaarborgd wordt.
Deze wet benadrukt hoe belangrijk de verantwoordelijkheid is voor iedereen die met persoonsgegevens te maken heeft.
Op het moment dat een persoon, een bedrijf, een organisatie (sportclub, kerkgenootschap, school) over persoonsgegevens beschikt, heeft die persoon, dat bedrijf, die organisatie de wettelijke verplichting om op verantwoorde wijze met die gegevens om te gaan.

B. Artikelsgewijze toelichting

Artikel 1
In artikel 1 zijn de definitiebepalingen opgenomen.
Deze wet geeft een brede definitie aan persoonsgegevens, namelijk, alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, om alle informatie te beslaan die verband kan houden met een individu. De aard van de informatie omvat objectieve informatie, d.w.z. naam, familienaam, telefoonnummer, bankrekeningnummer, leeftijd, geslacht, adres, biometrische gegevens, vingerafdrukken, DNA; alsmede subjectieve informatie, opinies of beoordelingen, namelijk de beoordeling van de betrouwbaarheid van een individu in het verzekerings- of bankwezen [geld] of van de geschiktheid voor een baan. Het is niet noodzakelijk dat informatie waar of bewezen is, om beschouwd te worden als persoonsgegevens. Het formaat of het medium waarop de informatie is vastgelegd kan van elk type zijn, bijv. alfabetisch, numeriek, grafisch, fotografisch of akoestisch (bijv. een tekening op papier, informatie opgeslagen in een computergeheugen met behulp van binaire code, een opgenomen beeld of geluidsgegevens). Persoonsgegevens bestaan uit informatie die rechtstreeks van individuen is verkregen, bijv. wanneer zij een formulier invullen, maar gegevens kunnen ook worden verkregen door observatie (bijv. aankoopvoorkeuren, bezochte websites verkregen door individuele personen online te volgen), of ontleend (bijv. het combineren van verzamelingen gegevens), of afgeleid (bijv. door gebruik te maken van algoritmen voor het analyseren van sociale media, locatiegegevens en registraties van aankopen met als doel individuele personen te profileren.)

Informatie kan geacht worden "verband te houden" met een individu wanneer het dat individu betreft, of wanneer die informatie wordt gebruikt voor het bepalen of beïnvloeden van de status of het gedrag van een individu of, anderzijds, wanneer het gebruik van die informatie invloed zou kunnen hebben op de rechten en belangen van een bepaalde persoon (bijv. het individu kan anders dan andere personen worden behandeld als gevolg van de verwerking van die gegevens), daarbij rekening houdend met de omstandigheden van een specifiek geval.

Een individu kan worden beschouwd als "geïdentificeerd" wanneer hij kan worden onderscheiden van andere leden van de groep en als "identificeerbaar" wanneer de mogelijkheid daartoe bestaat. Identificatie van een individu kan geschieden aan de hand van bepaalde stukjes informatie ("identificatiemiddelen") die nauw verband houden met die bepaalde persoon, zoals naam, fysiek voorkomen zoals lengte, haarkleur, kleding, culturele of sociale identiteit, zoals beroep, functie, enz. De mate waarin bepaalde identificatiemiddelen toereikend zijn voor het identificeren van een individu hangt af van de omstandigheden van het concrete geval.

Een individu kan direct geïdentificeerd worden of identificeerbaar zijn, bijv., aan de hand van de naam van een persoon, soms in combinatie met andere stukjes informatie (geboortedatum, namen van de ouders, adres of een foto van het gezicht) om zijn identiteit vast te stellen. Een individu kan ook indirect geïdentificeerd worden, bijv. door beschikbare identificatiemiddelen te combineren met andere stukjes informatie. Bijvoorbeeld: natuurlijke personen kunnen geassocieerd worden met online identificatiemiddelen die worden verstrekt door hun apparaten, applicaties, instrumenten en protocollen, zoals internetprotocoladressen, Mac-adres, IMEI, IDFA, identificatiecookies of andere identificatiemiddelen, bijv. radiofrequentie-identificatie-tags. Dit kan sporen achterlaten die, in het bijzonder in combinatie met unieke identificatiemiddelen en andere informatie ontvangen door de servers, gebruikt kunnen worden om een profiel op te stellen van die personen en om hen te identificeren.

Om te bepalen of een natuurlijke persoon identificeerbaar is, moeten alle middelen in aanmerking worden genomen die redelijkerwijs kunnen worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijv. om een individu af te scheiden. Om na te gaan of middelen redelijkerwijs kunnen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, gezien de technologie beschikbaar op het moment van de verwerking.
Deze wet is niet van toepassing op anonieme gegevens, d.w.z. gegevens die geen geïdentificeerde of identificeerbare natuurlijke persoon betreffen, of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet langer identificeerbaar is. Als vuistregel, om na te gaan of gegevens anoniem zijn, moeten de volgende drie vragen negatief worden beantwoord: a) is het nog mogelijk een individu af te scheiden? b) is het nog mogelijk om registraties die verband houden met een individu te koppelen? en c) kan informatie betreffende een individu worden afgeleid? Verder moet er rekening mee worden gehouden dat een geanonimiseerde verzameling gegevens nog steeds restrisico's kan inhouden voor betrokkenen. Enerzijds zijn anonimisering en re-identificatie inderdaad actieve gebieden van onderzoek en regelmatig worden nieuwe ontdekkingen gepubliceerd. Aan de andere kant kunnen zelfs geanonimiseerde gegevens, zoals statistieken, gebruikt worden om bestaande profielen van individuen te verrijken, waardoor nieuwe vraagstukken van gegevensbescherming zich voordoen. Anonimisering moet derhalve niet gezien worden als een eenmalige oefening en de inherente risico's zouden regelmatig opnieuw beoordeeld moeten worden. Persoonsgegevens die pseudonimisering hebben ondergaan, maar met behulp van additionele informatie zouden

kunnen worden toegeschreven aan een natuurlijke persoon, moeten beschouwd worden als informatie betreffende een identificeerbare natuurlijke persoon en vallen onder deze wet.
De verantwoordelijke voor de verwerking is een natuurlijke persoon of een rechtspersoon, een overheidsinstantie, een dienst of andere instelling die het doel en de middelen voor de verwerking van persoonsgegevens bepaalt, d.w.z. effectieve controle heeft over de verwerking. De verwerkingsverantwoordelijke kan besluiten de persoonsgegevens binnen zijn organisatie te verwerken of de verwerkingsactiviteiten in hun geheel of gedeeltelijk te delegeren aan een externe organisatie (een verwerker).
Voorbeeld 1: Onderneming A gaat een overeenkomst aan met Onderneming B om haar betaalstaat te verwerken. Onderneming A geeft duidelijke instructies aan Onderneming B (bijv. wie betaald moet worden, welke bedragen, op welke datum, enz.). Hoewel Onderneming B enige vrijheid van oordelen heeft (ook over welke software te gebruiken), zijn haar taken duidelijk en scherp afgebakend. Onderneming A is de verwerkingsverantwoordelijke en Onderneming B is de verwerker.
Voorbeeld 2: Onderneming B verleent directmarketingdiensten aan diverse ondernemingen. Onderneming A sluit een contract af met Onderneming B, waaronder Onderneming A (een kopie van) haar klantenbestand deelt met Onderneming B en Onderneming B e-mailberichten voor direct marketing zendt naar klanten van Onderneming A. Aan het eind van de dienst, wist Onderneming B het klantenbestand van Onderneming A uit. Onderneming A is de verwerkingsverantwoordelijke en Onderneming B is de verwerker. Voorbeeld 3: Een district gaat een contract aan met Onderneming B (gespecialiseerd in informatietechnologie) voor het installeren van videocamera's in het centrum in verband met de openbare veiligheid. De beelden van de videocamera worden veilig opgeslagen in de server van Onderneming B. Geselecteerde districtsfunctionarissen hebben toegang tot de videocamerabeelden voor doeleinden van openbare veiligheid en melden wetsovertredingen aan de bevoegde rechtshandhavers (bijv. de politie). Het district is de verwerkingsverantwoordelijke en Onderneming B is de verwerker. Om in aanmerking te komen als verwerker, moet een organisatie een afzonderlijke rechtspersoon zijn ten opzichte van de verwerkingsverantwoordelijke en persoonsgegevens verwerken ten behoeve van de verwerkingsverantwoordelijke.

Begrijpen wie verwerkingsverantwoordelijke is en wie de verwerker is in een concreet gegevensverwerkingsscenario is essentieel voor de toepassing van deze wet en haar naleving in de praktijk, omdat dit aangeeft aan wie verantwoordelijkheid wordt toegewezen voor de nakoming van de verplichtingen inzake gegevensbescherming, hoe betrokkenen hun rechten kunnen uitoefenen, wanneer deze wet van toepassing is, wie aansprakelijk zal worden gehouden voor eventuele schade voortvloeiende uit onrechtmatige verwerking. Het vermogen om de doeleinden en middelen te bepalen, vloeit voort uit een wet of een contract waarin een verwerkingsverantwoordelijke uitdrukkelijk wordt aangewezen maar kan ook voortkomen uit een analyse van de feitelijke omstandigheden van het geval. Aanwijzing van een verwerkingsverantwoordelijke bij contract is niet bepalend bij de vaststelling van de werkelijke status van een persoon of een instelling, wat gebaseerd moet zijn op concrete omstandigheden. De analyse van specifieke verwerkingen in kwestie kan aangeven wie daadwerkelijk bepaalt welke gegevens verwerkt zullen worden voor het beoogde doel. De vaststelling van het doel van de verwerking zou in alle gevallen de kwalificatie als verwerkingsverantwoordelijke bepalen, maar de vaststelling van de middelen zou zeggenschap alleen impliceren wanneer de vaststelling de essentiële elementen van de middelen betrof (bijv. de categorieën gegevens, opslagperioden, derde partijen aan wie de gegevens zouden worden medegedeeld, enz.). Puur technische beslissingen verband houdend met de verwerking (bijv. te gebruiken hardware of software) zouden uitsluitend worden genomen door de verwerkingsverantwoordelijke. In dit verband is het nuttig om te denken aan het voorbeeld van Onderneming A die een overeenkomst aangaat met Onderneming B om haar betaalstaat te verwerken en duidelijke instructies geeft aan

Onderneming B (bijv. wie betaald moet worden, welke bedragen, op welke datum, enz.). Onderneming A moet hierbij beschouwd worden als een verwerkingsverantwoordelijke. Hoewel Onderneming B enige beoordelingsvrijheid heeft (ook over welke software te gebruiken), zijn haar taken duidelijk en nauwkeurig afgebakend.

De toenemende complexiteiten in de realiteit van gegevensverwerking demonstreren dat er verschillende modaliteiten van 'pluralistische controle' kunnen zijn en dat meer dan een verwerkingsverantwoordelijke de doeleinden en middelen van gegevensverwerking kan bepalen. Verwerkingsverantwoordelijken kunnen afzonderlijk controle uitoefenen, d.w.z. elke verwerkingsverantwoordelijke is verantwoordelijk voor slechts een deel van de verwerking (zie onderstaand voorbeeld), of gezamenlijk, d.w.z. de verwerkingsverantwoordelijken stellen gezamenlijk de doeleinden of de essentiële middelen vast voor specifieke verwerkingsoperaties (zie voorbeeld twee hieronder).
Voorbeeld 1: Een e-overheidsportaal fungeert als een intermedium tussen de burgers en de overheidsdiensten door de verzoeken van de burgers door te geleiden en de documenten van de overheidsdiensten op te slaan om ze beschikbaar te maken voor de burger. Elke overheidsdienst blijft de verwerkingsverantwoordelijke voor de data verwerkt voor haar eigen doeleinden. Het portaal kan echter ook beschouwd worden als verwerkingsverantwoordelijke aangezien het de verwerking verricht van de verzoeken van de burger (d.w.z. het verzamelt en geeft door aan de bevoegde instantie) alsmede van de overheidsdocumenten (d.w.z. het slaat deze op en reguleert de toegang daartoe, zoals het downloaden door de burgers) voor verdere doeleinden (faciliteren van e-overheidsdiensten) behalve die waarvoor de gegevens oorspronkelijk werden verwerkt door elke overheidsdienst.
Voorbeeld 2: een reisbureau, een hotelketen en een luchtvaartmaatschappij besluiten een gemeenschappelijk platform op te zetten op het intemet voor het verbeteren van hun samenwerking wat betreft het beheren van reisreserveringen. Ze maken afspraken over belangrijke aspecten van de te gebruiken middelen, zoals welke gegevens worden bewaard, hoe reserveringen worden toegekend en bevestigd, en wie toegang kan hebben tot de opgeslagen informatie. Verder komen ze overeen de gegevens van hun klanten aan elkaar door te geven met het oog op geïntegreerde marketing. In dit geval hebben het reisbureau, de luchtvaartmaatschappij en de hotelketen gezamenlijk controle over de wijze waarop de persoonsgegevens van hun respectieve klanten worden verwerkt en derhalve zijn ze gezamenlijk voor de verwerking verantwoordelijk met betrekking tot de verwerkingsoperaties waarbij het gemeenschappelijk boekingsplatform op het internet betrokken is. In de context van gezamenlijke controle, kan de participatie van de partijen aan de gezamenlijke vaststelling verschillende vormen aannemen en hoeft die niet gelijkelijk gedeeld te worden. In geval van pluraliteit van actoren, kunnen deze een zeer nauwe relatie onderhouden (delen, bijv., alle doeleinden en middelen van een verwerking) of een lossere relatie (bijv. delen alle doeleinden of middelen, of een deel daarvan). Een brede verscheidenheid van vormen van gezamenlijke controle moet mogelijk zijn, waarbij ruimte wordt gelaten voor de nodige mate van flexibiliteit teneinde de ontwikkeling van steeds meer datacentrische vormen van de maatschappij, de overheid en de economie aan te kunnen.
"Derde" betekent een natuurlijke persoon of een rechtspersoon, een overheidsinstantie, een dienst of andere instelling andere dan de betrokkene, de verwerkingsverantwoordelijke, de verwerker en personen die, op direct gezag van de verwerkingsverantwoordelijke of de verwerker, bevoegd zijn persoonsgegevens te verwerken. Verwerkingsverantwoordelijke en verwerker en hun personeel worden beschouwd als de 'binnencirkel van gegevensverwerking' en worden niet gedekt door bijzondere bepalingen inzake derden.

Overheidsinstanties waaraan persoonsgegevens worden verstrekt overeenkomstig een wettelijke verplichting voor de uitoefening van hun officiële taak, zoals, belasting-, douane-, financiële,

bestuurlijke autoriteiten, moeten niet beschouwd worden als ontvangers, indien zij persoonsgegevens ontvangen die noodzakelijk zijn voor het uitvoeren van een bepaald onderzoek in het algemeen belang, in overeenstemming met de wet. De verzoeken voor mededeling verstuurd door de overheidsinstanties moeten altijd schriftelijk, met redenen omkleed en incidenteel zijn en dienen niet een bestand in zijn geheel te betreffen of te leiden tot de koppeling van bestanden.

Toestemming wordt gegeven door middel van een duidelijke, positieve actie, die blijk geeft van een vrijelijk gegeven, specifieke, op informatie berustende en ondubbelzinnige indicatie van de instemming van de betrokkene met de verwerking van de hem betreffende persoonsgegevens. Dit zou kunnen inhouden een vakje afhaken bij het bezoeken van een website of andere verklaring die of ander gedrag dat in deze context duidelijk aangeeft dat de betrokkene instemt met de voorgenomen verwerking van zijn persoonsgegevens, zoals een overeenkomst met verwerking tot uitdrukking gebracht door een schriftelijke verklaring, elektronisch middel of door een mondelinge verklaring. Bijvoorbeeld, toestemming verkregen middels een vooraf afgehaakt vakje (of een 'opt-out'-mechanisme) zou niet worden geacht geldig te zijn. Zo ook, naar beneden scrollen langs voorwaarden die toestemmingsverklaringen omvatten, waarbij een verklaring op het scherm verschijnt om de betrokkene te waarschuwen dat verder scrollen toestemming inhoudt, zou niet moeten worden beschouwd als een ondubbelzinnige indicatie van een wens middels een verklaring of door duidelijke positieve actie. Daarentegen, wanneer duidelijke informatie wordt verstrekt, kunnen vegen over een scherm, zwaaien voor een smartcamera, een smartphone met de klok mee draaien, geschikte opties zijn om instemming aan te geven (bijv. als u deze balk naar links veegt, gaat u akkoord met het gebruik van persoonsgegevens X voor doel Y. Herhaal de beweging om dit te bevestigen). Het moet duidelijk zijn voor de betrokkene dat de beweging in kwestie instemming met een specifiek verzoek aanduidt.

Toestemming moet vrijelijk gegeven worden en is alleen geldig indien de betrokkene in staat is een echte keuze te maken (bijv. wanneer het niet mogelijk is apart toestemming te geven voor verschillende verwerkingsoperaties inzake persoonsgegevens, of indien de uitvoering van een contract, inclusief de verlening van een dienst, afhankelijk is van toestemming ook al is die toestemming niet noodzakelijk voor de uitvoering). Indien een betrokkene weigert toe te stemmen in de gegevensverwerking, mag er geen risico van misleiding, intimidatie, dwang of ander negatieve consequentie zijn. Toestemming is niet vrij in gevallen waarin sprake is van een element van dwang, druk of onmogelijkheid tot vrije wilsuiting. Een ongelijke machtsverhouding in de relatie tussen de betrokkene en de verwerkingsverantwoordelijke (die zou bijvoorbeeld kunnen bestaan tussen een werkgever en een werknemer, of burger en overheidsinstantie) zou één van deze gevallen kunnen zijn. In deze situatie zou gegevensverwerking gebaseerd moeten zijn op andere legitieme gronden dan de toestemming van de betrokkene. Bijvoorbeeld, door de afhankelijkheid die ontstaat naar aanleiding van de relatie tussen werkgever en werknemer is het onwaarschijnlijk dat een werknemer in staat zou zijn vrijelijk te reageren op een verzoek om toestemming van zijn werkgever om monitoringssytemen te activeren op een werkplek, of om beoordelingsformulieren in te vullen, zonder enige druk om toe te stemmen te ervaren.
Echter, in bepaalde situaties kan de werkgever in staat zijn vrijelijk gegeven toestemming te verkrijgen. Indien, bijvoorbeeld, voordat een filmcrew begint te filmen in een bepaald deel van een kantoor, de werkgever alle werknemers die in dat gedeelte zitten om hun toestemming vraagt om ze te filmen en er zijn geen negatieve consequenties of sancties voor hen die weigeren toestemming te geven (bijv. er wordt gezorgd voor soortgelijke bureaus elders in het gebouw voor de duur van de opnames).

In bepaalde situaties waarin er meer controle over persoonsgegevens van een individu gepast wordt geacht (voor de verwerking van bijzondere categorieën van gegevens en voor geautomatiseerde individuele besluitvorming, inclusief profilering), eist de wet dat de toestemming van een betrokkene uitdrukkelijk wordt gegeven. Uitdrukkelijke toestemming betekent dat de betrokkene een expliciete verklaring van toestemming moet geven. De meest gebruikelijke manier om toestemming expliciet aan te geven, is een schriftelijke verklaring, zoals een verzoek om een formulier te ondertekenen, maar uitdrukkelijke toestemming kan eveneens in de digitale context worden verkregen door een elektronisch formulier in te vullen, een gescand document met een handtekening te uploaden, enz. of door mondeling geuite verklaringen te verkrijgen.
Bijvoorbeeld, een gezondheidswerker, optredend als verwerkingsverantwoordelijke, kan de betrokkenen tijdens een telefoongesprek uitdrukkelijke toestemming vragen voor het gebruik van hun gegevens betreffende de gezondheid door een mondelinge verklaring, waarin de betrokkenen bevestigen dat zij toestemmen in het gebruik van hun gegevens voor het opgegeven doel van het doen van onderzoek, op te nemen.
De verwerkingsverantwoordelijke kan ook een verificatie in twee fasen gebruiken voor het toestemmingsproces om een geldige uitdrukkelijke toestemming te verkrijgen.
Bijvoorbeeld, betrokkenen kunnen een e-mail ontvangen waarin zij in kennis worden gesteld van het voornemen van de verwerkingsverantwoordelijke, met uitleg en het verzoek om toestemming voor het gebruik van een specifieke reeks gegevens inzake gezondheid, voor een specifiek doel. Indien de betrokkene toestemt in het gebruik van deze gegevens, vraagt de verwerkingsverantwoordelijke hem een antwoord per e-mail waarin de verklaring "Ik stem toe" wordt gebruikt. Nadat het antwoord is opgestuurd, ontvangt de betrokkene een verificatielink die moet worden aangeklikt, of een sms-bericht met een verificatiecode, om de toestemming te bevestigen.

Genetische gegevens worden omschreven als persoonsgegevens betreffende de overgeërfde of verkregen genetische kenmerken van een natuurlijke persoon die resulteren uit de analyse van een biologisch monster van de natuurlijke persoon in kwestie, in het bijzonder de analyse van chromosomaal desoxyribonucleïne zuur (DNA) of ribonucleïne zuur (RNA), of uit de analyse van een ander element dat het mogelijk maakt soortgelijke informatie te verkrijgen.

Persoonsgegevens met betrekking tot gezondheid moeten bestaan uit alle gegevens betreffende de gezondheidsstatus van een betrokkene, die informatie verband houdende met voorbije, huidige of toekomstige fysieke of mentale gezondheidsstatus van de betrokkene onthullen. Hieronder valt informatie over de natuurlijke persoon verzameld tijdens de registratie voor of de verlening van gezondheidszorgdiensten; een nummer, een symbool of een bijzonderheid toegewezen aan een natuurlijke persoon voor de unieke identificatie van die persoon voor gezondheidsdoeleinden; informatie ontleend aan het testen of onderzoeken van een lichaamsdeel of lichaamsmateriaal, inclusief van genetische gegevens en biologische monster; en informatie omtrent, bijvoorbeeld, een ziekte, een handicap, een ziekterisico, medische geschiedenis, klinische behandeling of fysiologische of biomedische staat van de betrokkene onafhankelijk van de bron ervan, bijvoorbeeld van een arts of andere gezondheidswerker, een ziekenhuis, een medisch instrument of een in-vitro diagnostische test.

Een groep ondernemingen bestaat uit een zeggenschap uitoefenende onderneming en de ondernemingen waarover ze zeggenschap uitoefent, waarbij de onderneming die zeggenschap uitoefent de onderneming moet zijn die een dominante invloed kan uitoefenen over de andere ondernemingen krachtens, bijvoorbeeld, eigendom, financiële deelneming of de voorschriften waardoor ze wordt beheerst of de bevoegdheid om voorschriften inzake gegevens-bescherming te doen implementeren. Een onderneming die controle uitoefent over de verwerking van

persoonsgegevens in ondernemingen gelieerd aan de eerstgenoemde moet samen met die ondernemingen worden beschouwd als een groep ondernemingen.

De Commissaris voor Gegevensbescherming is een onafhankelijke autoriteit ingesteld bij deze wet en bezit rechtspersoonlijkheid. De bevoegdheden van dit gezag berusten uiteindelijk bij een enkele persoon die, tijdens de uitvoering van de relevante taken, wordt bijgestaan door zijn staf, d.w.z. het Bureau van de Commissaris voor Gegevensbescherming.

Overeenkomstig de wereldwijd geaccepteerde definitie van het VN-Verdrag inzake de Rechten van het Kind, wordt een kind beschreven als een individu jonger dan 18 jaar. Deze definitie is relevant voor alle artikelen van deze wet die betrekking hebben op kinderen. Verder, de definitie is onverminderd van toepassing op het feit dat artikel 7, dat een specifiek artikel is dat beschrijft wanneer de toestemming van een kind geldig is, voorziet dat wanneer persoonsgegevens worden verwerkt op basis van toestemming, kinderen die tenminste 16 jaar zijn, geacht worden in staat te zijn toestemming te verlenen.

Artikel 2

Bijna alle internationale en nationale instrumenten voor gegevensbescherming zijn in deze wet van toepassing op natuurlijke personen. Deze beperking in toepassingsgebied vloeit voort uit het doel de fundamentele rechten en vrijheden te waarborgen, met name het recht op privacy en bescherming van persoonsgegevens, die zijn toegekend aan natuurlijke personen. Bijgevolg betreft deze wet niet de verwerking van persoonsgegevens die betrekking hebben op rechtspersonen, waaronder begrepen de naam en de vorm van de rechtspersoon en de contactgegevens van de rechtspersoon alsmede overleden natuurlijke personen. Informatie omtrent rechtspersonen dient beschermd te worden door andere juridische instrumenten met betrekking tot, bijv. handelsgeheimen, intellectueel eigendom en geheimhouding.

De bescherming van individuele natuurlijke personen moet net zozeer van toepassing zijn op de automatische verwerking van gegevens als op de handmatige verwerking, en de reikwijdte van de bescherming moet niet afhangen van de gebruikte technieken. Het gebruik van nieuwe technologie in de vorm van elektronische gegevensverwerking maakt evenwel een gemakkelijkere en ruimere toegang tot persoonsgegevens mogelijk, dan de traditionele manieren voor het bewerken van gegevens. Deze wet is van toepassing op de verwerking van persoonsgegevens langs geautomatiseerde weg, en op de handmatige verwerking. In het geval van handmatige verwerking is de wet alleen van toepassing indien de persoonsgegevens zijn vervat of bedoeld zijn vervat te worden in een bestand (gestructureerde dossiers); daarentegen, dossiers of verzamelingen van dossiers die niet gestructureerd zijn overeenkomstig specifieke criteria, vallen niet binnen de werkingssfeer van deze wet.

Deze wet is niet van toepassing op de verwerking van persoonsgegevens door een natuurlijke persoon in de context van zijn persoonlijke, gezins- of huishoudelijke aangelegenheden, die geen verband houden met een beroeps- of commerciële activiteit. Zodanige uitzondering is niet van toepassing op verwerkingsverantwoordelijken of verwerkers die de middelen verschaffen voor de verwerking van persoonsgegevens voor dergelijke persoonlijke of huishoudelijke activiteiten (bijv. exploitanten van sociale netwerken die online communicatieplatformen aanbieden aan individuele personen voor het publiceren en uitwisselen van informatie met andere gebruikers voor persoonlijke doeleinden).
Persoonlijke of huishoudelijke activiteiten kunnen omvatten correspondentie en het bewaren van adressen, bijv. wanneer een individu telefoonnummers en namen opslaat in zijn mobiele telefoon, of online-activiteiten ondernomen om persoonlijke redenen (bijv. berichten uitwisselen met vrienden). In gevallen waarin er twijfel ontstaat of persoonsgegevens al dan niet verwerkt

worden in het kader van persoonlijke, gezins- of huishoudelijke aangelegenheden of in verband met beroeps- of handelsactiviteiten, dienen de volgende criteria in aanmerking genomen te worden: schaal en frequentie (incidentele of voltijdse activiteit) van de gegevensverwerking, de relatie tussen personen (persoonlijk of commercieel, enkele of collectieve actie) die gegevens verwerken en wier gegevens worden verwerkt, en negatieve gevolgen voor personen wier gegevens worden verwerkt.

Wettelijke regelingen kunnen gemaakt worden voor de verdere regulering van aangelegenheden betreffende privacy en gegevensbescherming in specifieke sectoren. Specifieke wetten kunnen meer gedetailleerde voorschriften geven, maar mogen niet resulteren in een verlaging van de bescherming die zij bieden aan betrokkenen in bepaalde sectoren, gegeven dat deze wet beoogt te dienen als de basis voor privacy- en gegevensbescherming.

Artikel 3
Deze wet is van toepassing op de verwerking van persoonsgegevens in de context van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Republiek Suriname, ongeacht of de verwerking al dan niet plaatsvindt in de Republiek Suriname. Vestiging heeft betrekking op een stabiele regeling, zoals een filiaal of een dochteronderneming met rechtspersoonlijkheid, via welke de verwerkingsverantwoordelijke of de verwerker effectief en werkelijk zijn activiteiten in verband met gegevensverwerking ontplooit.

Teneinde de betrokkenen die zich bevinden in de Republiek Suriname, ten volle te beschermen, dient de verwerking van hun persoonsgegevens door een verwerkingsverantwoordelijke of een verwerker die niet gevestigd is in de Republiek Suriname ook overeenkomstig deze wet te geschieden wanneer de verwerkingsactiviteiten verband houden met het aanbieden van (gratis of betaalde) goederen of diensten aan de betrokkenen in de Republiek Suriname of wanneer ze verband houden met het monitoren van het gedrag van die betrokkenen, d.w.z. ze worden gevolgd op het internet of er worden profielen gemaakt met het oog op het nemen van besluiten, het analyseren of voorspellen van persoonlijke voorkeuren, gedragingen en attitudes. Een voorbeeld zou zijn een onderneming die haar hoofdzetel in een derde land heeft en een e-handelswebsite beheert waarop zij producten en diensten aanbiedt aan gebruikers in de Republiek Suriname. Het oogmerk goederen en diensten aan te bieden aan betrokkenen in de Republiek Suriname zou moeten worden vastgesteld, gebaseerd op specifieke feiten, zoals het gebruik van het Nederlands, Sranan, Javaans, Samami of Saramaccaans voor het beschrijven van goederen, diensten (en meer in het algemeen voor het verschaffen van informatie, inclusief bijv. advertenties en juridische kennisgevingen), de Surinaamse dollar als betaalmiddel bij de aankoop van goederen en diensten, de levering van diensten of producten aan de Republiek Suriname of de toegankelijkheid van de dienst afhankelijk van het gebruik van een Surinaams betalingsinstrument (bijv. locale credit-/debitkaarten). De toegankelijkheid van de website van een verwerkingsverantwoordelijke, een verwerker of een intermedium in de Republiek Suriname alleen mag niet beschouwd worden als een aantoning van dat oogmerk.

Ter voorkoming van situaties waarin de Republiek Suriname wordt gebruikt als een 'personal data haven', bijvoorbeeld wanneer een verwerkingsactiviteit ontoelaatbare ethische kwesties met zich meebrengt, is deze wet van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich bevinden in de Republiek Suriname door een verwerkingsverantwoordelijke of een verwerker die niet is gevestigd in de Republiek Suriname, die gebruik maakt van geautomatiseerde of andere apparatuur, geplaatst op het grondgebied van de Republiek Suriname.

Deze wet dient ook van toepassing te zijn op een verwerkingsverantwoordelijke die niet is gevestigd in de Republiek Suriname, maar waar het Surinaams recht van toepassing is krachtens het internationaal publiekrecht. Bijvoorbeeld, een ambassade van de Republiek Suriname in het buitenland zou onderworpen zijn aan deze wet.

Artikel 4

Gezien de snelle technologische evolutie, de ontwikkeling van data-gestuurde ondernemingsmodellen en de toenemende globalisering van persoonsgegevensstromen, is het noodzakelijk elke natuurlijke persoon te beschermen met betrekking tot de verwerking van zijn persoonsgegevens alsmede om voorschriften te geven voor het vrije verkeer van persoonsgegevens, in harmonie met internationale normen.

Deze wet legt het fundamentele recht op bescherming van persoonsgegevens vast. Meer nog, ze specificeert het recht op privacy, vastgelegd in artikel 17 van de Grondwet en in internationale verdragen, onder andere in artikel 11 van het Amerikaanse Verdrag inzake de rechten van de mens, artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten, artikel 16 van het VN-Verdrag inzake de Rechten van het Kind, die bepalen dat een ieder recht heeft op de eerbiediging van zijn privacy, gezinsleven, huis en eer en reputatie, en dat de wet bescherming dient te bieden tegen wederrechtelijke daden tegen dit recht. Bescherming van natuurlijke personen met betrekking tot de verwerking van hun persoonsgegevens draagt ook bij aan de bescherming van andere mensenrechten en fundamentele vrijheden, alsmede menselijke waardigheid en persoonlijke autonomie op basis van het recht van een persoon om controle uit te oefenen over zijn persoonsgegevens.

De relatie tussen het recht op privacy en het recht op bescherming van persoonsgegevens kan worden geformuleerd als volgt. Het concept 'privacy' omvat de verwerking van persoonsgegevens. Echter, verwerking van persoonsgegevens moet niet altijd gezien worden als bemoeienis met privacy, d.w.z. het is niet vereist dat wordt vastgesteld dat er inmenging is in de persoonlijke levenssfeer om deze wet te schenden. Verwerking van persoonsgegevens moet altijd voldoen aan de in deze wet opgenomen voorwaarden; alleen dan kan de bescherming van de fundamentele rechten en vrijheden van een ieder, en met name hun recht op privacy, worden gerealiseerd. Het recht op gegevensbescherming is derhalve van wezenlijk belang voor het recht op privacy, maar het is ruimer in toepassingsgebied en anders verwoord dan het recht op privacy en dient het specifieke doel van vergroting van de transparantie en bescherming van privacy, autonomie, non-discriminatie en integriteit van individuen in het digitale tijdperk, wat het mogelijk maakt situaties aan te pakken die het recht op privacy alleen niet kan aanpakken. In feite, de voorschriften betreffende de bescherming van persoonsgegevens in deze wet gaan verder dan de bescherming van het privéleven en het gezinsleven.

De noodzaak van economische en sociale vooruitgang, in het kader van de informatiemaatschappij, de versterking van de digitale economie en het welzijn van natuurlijke personen eisen het wegnemen van onnodige belemmeringen voor de vrije stroom van informatie, waaronder begrepen persoonsgegevens. Dergelijke vrije stromen moeten evenwel gebaseerd zijn op de verantwoordelijke en transparante bewerking van persoonsgegevens, eerbiediging van de algemene beginselen en verplichtingen inzake gegevensbescherming, en mechanismen inhouden voor transparant toezicht en onpartijdige geschillenbeslechting.

Het recht op bescherming van persoonsgegevens is geen absoluut recht. Het moet verzoend worden met andere mensenrechten en fundamentele vrijheden, inclusief vrijheid van meningsuiting, toegang tot documenten, vrijheid van kunst en wetenschap, bescherming van eigendom, en samengaan met collectieve belangen, zoals nationale veiligheid. In dit verband

staat de wet de noodzakelijke mate van flexibiliteit toe, zodoende in de gelegenheid stellend het gepaste evenwicht te bereiken tussen bescherming van de rechten van betrokkenen enerzijds en anderzijds de legitieme belangen van verwerkingsverantwoordelijken of derden en publieke belangen.

Artikel 5
Persoonsgegevens moeten rechtmatig verwerkt worden, d.w.z. overeenkomstig deze wet, de rechten en vrijheden van personen erkend in de internationale mensenrechten verdragen zoals het Amerikaanse Verdrag inzake de rechten van de mens, het Internationaal Verdrag inzake burgerrechten en politieke rechten, het VN-Verdrag inzake de rechten van het kind en andere relevante mensenrechteninstrumenten waar de Republiek Suriname partij bij is. In het streven deze doelen van gegevensverwerking te bereiken, moeten verwerkingsverantwoordelijken en verwerkers ook eerlijk handelen, d.w.z. rekening houden met de redelijke verwachtingen van de betrokkenen, te goeder trouw handelen bij het verwerken van persoonsgegevens, en persoonsgegevens niet gebruiken op manieren die ongerechtvaardigd negatieve gevolgen voor personen veroorzaken en in het bijzonder leiden tot onrechtmatige discriminatie.

Openheid en transparantie stellen betrokkenen in staat controle uit te oefenen over hun eigen persoonsgegevens. Deze kunnen worden bereikt door het verstrekken van de relevante informatie over de verwerking van persoonsgegevens, bijv. publicatie van privacybeleid op websites. Betrokkenen moeten op de hoogte zijn van de verwerking van hun gegevens – inclusief de bijzonderheden van de verantwoordelijke voor de verwerking en van de verwerkingsactiviteiten, of en hoe hun gegevens worden gedeeld met andere lichamen of doorgegeven aan andere landen – en van hun rechten. Betrokkenen moeten geïnformeerd worden voordat begonnen wordt met de verwerking van hun gegevens. Tenzij specifiek bij wet toegestaan, mag er geen geheime en verborgen verwerking van persoonsgegevens plaatsvinden. Verwerkingen moeten worden uitgelegd aan de betrokkenen op een duidelijke en eenvoudige wijze die garandeert dat zij begrijpen wat er zal gebeuren met hun gegevens en welke de belangrijkste feitelijke gevolgen en effecten van de verwerking zijn.

Het doel waarvoor persoonsgegevens worden verwerkt, dient gespecificeerd te worden en de verwerking moet worden beperkt tot wat nodig is voor dat specifieke doel. Het doelbindingsbeginsel is nauw verbonden aan het beginsel van de kwaliteit van gegevens, de beperking van de verwerking en het beginsel van gegevensminimalisering. Persoonsgegevens moeten alleen verwerkt worden indien het doel van de verwerking niet redelijkerwijs met andere middelen kan worden bereikt. De categorieën van gegevens gekozen voor verwerking zijn nodig voor het bereiken van het aangegeven algemene doel van de verwerking, en een voor de verwerking verantwoordelijke moet het verzamelen van data strikt beperken tot die informatie welke direct van relevantie is voor het specifieke doel beoogd door de verwerking. Verwerking voor een doel dat niet gedefinieerd en/of niet beperkt is, is niet in overeenstemming met het doelbindingsbeginsel. Het doel moet zijn aangegeven en duidelijk zijn gemaakt door de verantwoordelijke voor de verwerking nog voordat een aanvang wordt gemaakt met de gegevensverwerking. Elk nieuw doel voor de verwerking van gegevens moet zijn eigen specifieke rechtsgrondslag hebben en kan niet berusten op het feit dat de gegevens aanvankelijk waren verkregen of verwerkt voor een ander legitiem doel, tenzij het tweede doel waarvoor de gegevens verder worden verwerkt verenigbaar is met het oorspronkelijke.

Bij het beoordelen of een doel van gegevensverwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, moeten de volgende criteria in aanmerking worden genomen, onder andere: elk verband tussen die doeleinden en de doeleinden van de voorgenomen verdere verwerking; het kader waarbinnen de persoonsgegevens zijn verzameld,

in het bijzonder de redelijke verwachtingen van betrokkenen op basis van hun relatie met de verwerkingsverantwoordelijke wat betreft het verdere gebruik; de aard van de persoonsgegevens; de gevolgen van de voorgenomen verdere verwerking voor betrokkenen; en het bestaan van passende waarborgen in zowel de oorspronkelijke en voorgenomen verdere verwerkingsoperaties.

Persoonsgegevens moeten relevant zijn voor de doeleinden waarvoor ze gebruikt zullen worden en moeten nauwkeurig, volledig en bijgewerkt zijn. De verplichting om de nauwkeurigheid van gegevens te garanderen, moet worden gezien in de context van het doel van de gegevensverwerking. In feite kunnen er ook gevallen zijn waarin het bijwerken van opgeslagen gegevens wettelijk verboden kan zijn, omdat het doel van het opslaan van gegevens voornamelijk is het documenteren van gebeurtenissen (bijv. een medisch protocol voor operaties); in die omstandigheden mogen alleen aanvullingen op het protocol worden gemaakt mits duidelijk wordt aangegeven dat dit bijdragen zijn die in een later stadium zijn toegevoegd. Verder, historische gegevens, gegevens betreffende maatschappelijk onderzoek en de activiteiten van archieven kunnen vallen onder specifieke regelingen die in samenhang de toepassing van het beginsel van de kwaliteit van gegevens specificeren en/of beperken. Bijgevolg zijn er situaties waarin het regelmatig controleren van de nauwkeurigheid van gegevens, met inbegrip van bijwerking, een absolute noodzakelijkheid is vanwege de potentiële schade die kan worden veroorzaakt aan de betrokkene ingeval de gegevens onjuist zouden blijven (bijv. relaties met bankinstellingen).

Persoonsgegevens moeten worden bewaard in een vorm die de identificatie van betrokkenen mogelijk maakt zolang dat nodig is voor de doeleinden waarvoor de gegevens werden verzameld of verder worden verwerkt. In beginsel moeten de gegevens derhalve worden gewist of geanonimiseerd wanneer die doeleinden zijn gediend, tenzij anders bepaald in toepasselijke wettelijke regelingen. De bewaring van gegevens moet in verhouding staan tot het doel van het verzamelen en voor een beperkte tijdsduur zijn. De tijdsbeperking voor de opslag van persoonsgegevens is echter slechts van toepassing op gegevens bewaard in een vorm die de identificatie van betrokkenen mogelijk maakt (in dit opzicht zijn geanonimiseerde gegevens derhalve hiervan uitgesloten). Teneinde te garanderen dat de persoonsgegevens niet langer dan noodzakelijk worden bewaard, moeten termijnen worden vastgesteld door de verwerkingsverantwoordelijke voor het wissen of voor een periodieke evaluatie.

Persoonsgegevens moeten beschermd worden door passende veiligheidswaarborgen tegen risico's zoals verlies of ongeoorloofde toegang tot, vernietiging, gebruik, wijziging of bekendmaking van gegevens. Veiligheidswaarborgen omvatten fysieke maatregelen (bijv. afgesloten deuren, identificatiekaarten), organisatorische maatregelen (bijv. machtiging voor toegang tot persoonsgegevens, geheimhoudingsplicht opgelegd aan personeel dat persoonsgegevens verwerkt), technologische maatregelen (bijv. versleuteling en pseudonimisering van persoonsgegevens, streng identiteitsbeheer en toegangsbewaking om de vertrouwelijkheid van gegevens te bewaren, andere technische maatregelen voor het garanderen van de integriteit, beschikbaarheid en veerkracht van gegevensverwerkingssystemen). Specifieke technische en organisatorische maatregelen inzake gegevensbeveiliging zijn aangegeven in Bijlage 1 van deze wet, waar van toepassing volgens artikel 19 lid 1 en voor zover van toepassing, moeten ze worden uitgevoerd door verwerkingsverantwoordelijken en verwerkers.

De verwerkingsverantwoordelijken moeten de uitoefening van de rechten die door deze wet worden toegekend aan de betrokkenen, daadwerkelijk garanderen. Bovendien moet er een ethische dimensie zijn die verder gaat dan de toepassing van de voorschriften inzake

gegevensbescherming. Persoonsgegevens worden verwerkt op verantwoorde en ethische wijze, indachtig de waardigheid, mensenrechten en vrijheden van personen. Er dient serieus rekening gehouden te worden met de ethische implicaties van de wijze waarop persoonsgegevens worden gedefinieerd en gebruikt in de grote, door data en kunstmatige intelligentie aangestuurde wereld. De Commissaris voor Gegevensbescherming moet de ontwikkeling bevorderen van technologieën, engineering-technieken, instrumenten en methodologieën die verantwoorde en ethische gegevensbescherming die de volledige eerbiediging van de waardigheid, mensenrechten en vrijheden van betrokkenen mogelijk maken en die personen weerbaar maken, ook overeenkomstig de beginselen van gegevensbescherming by design en by default [door ontwerp en door standaardinstellingen].

Het beginsel van verantwoordingsplicht legt de verantwoordelijkheid bij verwerkingsverantwoordelijken voor het naleven van maatregelen die uitvoering geven aan alle beginselen die in deze wet zijn opgenomen. Om de beginselen en vereisten van gegevensbescherming die in deze wet zijn opgenomen te vertalen in effectieve mechanismen die zorgen voor echte bescherming, moeten de verwerkingsverantwoordelijken passende en doelmatige maatregelen treffen om uitvoering te geven aan deze wet, alsmede om naleving op verzoek van betrokkenen en de Commissaris voor Gegevensbescherming, autonoom of met de hulp van verwerkers, aan te tonen.
De essentie van de verantwoordingsplicht is de verplichting van de verwerkingsverantwoordelijke om: (i) maatregelen in te stellen die - onder normale omstandigheden - zouden garanderen dat voorschriften inzake gegevensbescherming worden nageleefd in de context van verwerking; en (ii) documentatie gereed te hebben waarmee aan betrokkenen en de Commissaris voor Gegevensbescherming wordt aangetoond welke maatregelen zijn genomen om naleving van de voorschriften inzake gegevensbescherming te bewerkstelligen.

Artikel 6
Voor rechtmatige verwerking dienen persoonsgegevens verwerkt te worden op basis van één van de wettelijke gronden die genoemd worden in deze wet. Deze wet benadrukt dat de toestemming van de betrokkenen niet de enige wettelijke grondslag is voor de verwerking van persoonsgegevens. Alternatieve juridische gronden, gespecificeerd in artikel 6 en artikel 8, kunnen afhankelijk van de context beter geschikt zijn zowel vanuit het perspectief van de verwerkingsverantwoordelijke als vanuit het perspectief van de betrokkene. Theoretisch is de toestemming van de betrokkene de beste manier voor personen om zelfbeschikking uit te oefenen en te controleren welke soort van verwerkingsactiviteiten worden uitgevoerd met betrekking tot hun persoonsgegevens Echter, toestemming in de praktijk is niet altijd de meest effectieve waarborg voor betrokkenen. In feite geven betrokkenen vaak toestemming voor gegevensverwerking zonder echt aandacht te besteden aan, of inzicht te hebben in de gevolgen van hun daad. Bovendien, in bepaalde situaties kan het zijn dat de toestemming niet vrijwillig is gegeven, bijv. in het werkmilieu waarin werknemers bang zijn voor repercussies van de werkgever.

Verwerking moet rechtmatig zijn waar het noodzakelijk is in het kader van een contract of het aangaan van een contract waarbij de betrokkene partij is. Dit kan bijvoorbeeld omvatten de contactgegevens van de betrokkene zodat online gekochte goederen geleverd kunnen worden, verwerking van betalingsgegevens van de betrokkene zodat de relevante transactie kan worden uitgevoerd, verwerking van salaris- en bankgegevens van employés zodat salarissen kunnen worden uitbetaald, of verwerking van basisinformatie omtrent de betrokkene, zoals naam, adres en verwijzing naar uitstaande contractuele verplichtingen zodat formele herinneringen kunnen worden verzonden. Ook, bijvoorbeeld, indien een individu een offerte aanvraagt bij een

verzekeraar voor zijn voertuig, kan de verzekeraar de noodzakelijke gegevens van de persoon, zoals naam, familienaam, adres, leeftijd, aantal eerdere ongevallen en andere relevante en aan het doel evenredige persoonsgegevens verwerken, zodat de offerte kan worden gemaakt.

Gegevensverwerking is toegestaan wanneer het noodzakelijk is om de verwerkingsverantwoordelijke in staat te stellen aan een wettelijke verplichting te voldoen. De verplichting moet bindend zijn, duidelijk en specifiek de verwerking van persoonsgegevens eisen. Ze moet de verwerkingsverantwoordelijke veeleer bij wet zijn opgelegd dan bij contract of vrijwillige eenzijdige handeling. Voorbeelden van de toepassing van die rechtsgrond kunnen zijn, gegevensverwerking uitgevoerd door werkgevers in verband met het melden van salarisgegevens van hun werknemers aan sociale zekerheids- of belastingautoriteiten; door financiële instellingen voor het melden van bepaalde verdachte transacties aan het bevoegde gezag in het kader van anti-moneylaunderingregelingen.

Persoonsgegevens mogen verwerkt worden wanneer de verwerking noodzakelijk is voor de uitoefening van het officiële gezag toegekend aan de verwerkingsverantwoordelijke, waaronder begrepen rechtshandhavingsactiviteiten. Voorbeelden van de toepassing van die rechtsgrond kunnen betrekking hebben op: een belastinginstantie die de belastingaangifte van een persoon in ontvangst neemt en verwerkt om het te betalen bedrag aan belastingen vast te stellen en te verifiëren; een locale overheidsinstantie, zoals een districtsbestuur, voor de instandhouding van een bibliotheek, een school, of een plaatselijk zwembad; door een locale instantie voor het afhandelen van geldboeten voor foutparkeren (dit laatste kan ook een voorbeeld zijn van een verwerking die noodzakelijk is om de verwerkingsverantwoordelijke in staat te stellen aan een wettelijke verplichting te voldoen). Vanwege een potentieel zeer breed toepassingsgebied, vereist deze grond een strakke interpretatie en een duidelijke onderkenning, per geval, van de officiële bevoegdheid toegekend aan de verwerkingsverantwoordelijke die de verwerking rechtvaardigt.

Persoonsgegevens mogen ook verwerkt worden wanneer de verwerking noodzakelijk is voor de uitvoering van een taak verricht in het algemeen belang (bijv. openbare gezondheid, sociale bescherming, nationale veiligheid). Voorbeelden van de toepassing van die rechtsgrond kunnen betrekking hebben op: een beroepsvereniging, bijv. een orde van advocaten of een vereniging van medici, die disciplinaire maatregelen treft tegen enkele van de leden; een verwerkingsverantwoordelijke die opmerkt dat een strafbaar feit is gepleegd en op eigen initiatief deze informatie doorspeelt aan de bevoegde wetshandhavingsautoriteiten. Vanwege een potentieel zeer breed toepassingsgebied, vereist deze grond een strakke interpretatie en een duidelijke onderkenning, per geval, van het algemeen belang dat op het spel staat en zodoende deze verwerking rechtvaardigt.

Verwerking moet ook rechtmatig zijn wanneer het nodig is ter bescherming van een belang dat essentieel is voor het leven van de betrokkene of van een andere natuurlijke persoon, bijv., voor een ziekenhuis om een bewusteloze persoon die de Spoedeisende Hulp wordt binnengebracht, te kunnen behandelen; voor humanitaire doeleinden, voor het monitoren van epidemieën en hun verspreiding, humanitaire noodgevallen, natuurrampen en door de mens veroorzaakte rampen. Sommige soorten verwerking kunnen in feite zowel belangrijke gronden van algemeen belang en de vitale belangen van de betrokkene (of van een andere natuurlijke persoon) dienen.

De rechtmatige belangen van een verwerkingsverantwoordelijke, of die van derden waaraan de persoonsgegevens worden verstrekt, bieden een rechtsgrond voor de verwerking, indien de belangen of de fundamentele rechten en vrijheden van de betrokkene niet terzijde worden geschoven. Voor deze afweging is het van belang de aard en de bron van de rechtmatig belangen

in aanmerking te nemen, en ook of de verwerking noodzakelijk is voor de behartiging van die belangen, enerzijds, en de gevolgen voor de betrokkenen anderzijds. Het rechtmatige belang als rechtsgrond voor verwerking is erop gericht de verwerkingsverantwoordelijken de noodzakelijke flexibiliteit te garanderen wanneer er geen oneigenlijke gevolgen zijn voor de betrokkenen, terwijl tegelijkertijd voldoende rechtszekerheid en garanties worden geboden aan de betrokkenen dat deze open-eindbepaling niet zal worden misbruikt. Derhalve wordt ook aanbevolen dat de Commissaris voor Gegevensbescherming de richtlijnen voor het uitvoeren van een dergelijke 'afweging' publiceert.Voorlopig is het uiterst belangrijk te begrijpen dat het bestaan van een rechtmatig belang zorgvuldig beoordeeld moet worden, waarbij ook moet worden overwogen of een betrokkene redelijkerwijs mag verwachten op het moment en in het kader van de verzameling van de persoonsgegevens, dat verwerking voor dat doel kan plaatsvinden, bijv., waar er tussen de betrokkene en de verwerkingsverantwoordelijke een relatie bestaat die relevant en evenredig tot het doel is, in situaties zoals die waarin de betrokkene een klant is of in dienst is van de verwerkingsverantwoordelijke.
De volgende doelstellingen kunnen onder andere beschouwd worden als rechtmatige belangen van de verwerkingsverantwoordelijke voor het verwerken van persoonsgegevens: tenuitvoerlegging van juridische vorderingen, inclusief inning van schulden via buitengerechtelijke procedures; preventie door particuliere verwerkingsverantwoordelijke van fraude of misbruik van diensten; beheer van klokkenluidersregelingen; duurzame fysieke beveiliging, IT- en netwerkbeveiliging; verwerking voor historische, wetenschappelijke of statistische doeleinden; direct marketing en andere vormen van marketing of reclame, mits de betrokkene het recht heeft te allen tijde bezwaar te maken tegen dergelijke verwerkingsactiviteiten.
Wat betreft verwerking op basis van toestemming van de betrokkene, kan worden verwezen naar wat reeds is behandeld in artikel 1. Daamaast is het in deze vermeldenswaard dat de verwerkingsverantwoordelijke in staat moet zijn om aan te tonen dat de betrokkene toestemming heeft gegeven welke zinvol is voor de desbetreffende verwerkingsoperatie (krachtens het beginsel inzake de verantwoordingsplicht). Verder, bepalingen inzake toestemming voor verwerking van persoonsgegevens zijn niet van invloed op de voorschriften inzake toestemming voor medische behandeling en toestemming ingevolge het verbintenissenrecht.

Artikel 7
Kinderen zijn zich minder bewust van de consequenties, waarborgen en rechten in verband met de verwerking van persoonsgegevens, worden gemakkelijker beïnvloed en misleid, of missen de bevoegdheid om geldig toestemming te geven voor de verwerking van hun persoonsgegevens. Daarom moet aan kinderen, als betrokkenen, een grotere bescherming van hun persoonsgegevens worden toegekend. De verwerking van gegevens van kinderen vereist extra zorg, in het bijzonder, bij het verzamelen van persoonsgegevens voor commerciële doeleinden (bijv. voor marketing, het creëren van persoonlijkheids- of gebruikersprofielen) of bij de planning om persoonsgegevens van kinderen aan derden te verstrekken. In alle gevallen dient het belang van het kind in aanmerking te worden genomen en verwerkingsverantwoordelijken moeten zich onthouden van handelen in strijd met die belangen (bijv. van het verwerken van gegevens van kinderen op een wijze die nadelige gevolgen veroorzaakt inzake de rechten en vrijheden van het kind of die hun gedrag manipuleert).

Deze wet legt een leeftijdsgrens van 16 jaar vast; tot dan moet de wettelijke vertegenwoordiger toestemming verlenen namens het kind. Maar indien een kind in staat is zijn eigen besluiten te nemen wat de persoonsgegevens betreft, moet de vertegenwoordiger rekening houden met de zienswijze van het kind. De vereiste van ouderlijke toestemming mag het kind dat rijp genoeg is om zijn rechten als betrokkene uit te oefenen zonder de betrokkenheid van een wettelijke vertegenwoordiger, niet uitsluiten. De toestemming van de wettelijke vertegenwoordiger van

het kind dient nimmer noodzakelijk te zijn in een context waarbij de betrokkenheid van een specifieke wettelijke vertegenwoordiger mogelijk tegen de belangen van het kind in zou gaan, zoals in het kader van preventieve diensten of hulpverleningsdiensten die aan een kind worden aangeboden. Mechanismen voor het controleren van leeftijd en toestemming mogen niet leiden tot bovenmatige gegevensverwerking door verwerkingsverantwoordelijken en moeten gebruikt worden wanneer nodig, om redelijke zekerheid te verkrijgen dat een kind ouder is dan 16 jaar of dat de persoon die toestemming verleent inderdaad de wettelijke vertegenwoordiger van het kind is.

Artikel 8

Bepaalde persoonsgegevens (speciale categorieën persoonsgegevens) zijn, door hun aard, bijzonder gevoelig omdat hun verwerking kan leiden tot discriminatie, vooroordeel of ander significant nadelig gevolg voor de rechten en vrijheden van de betrokkenen. Speciale categorieën van persoonsgegevens moeten in de regel niet worden verwerkt, maar afwijking van dit verbod is toegestaan in specifieke gevallen vastgesteld in deze wet of andere wettelijke regelingen. Afwijkingen van het verbod dienen over het algemeen betrekking te hebben op het verkrijgen van de uitdrukkelijke toestemming van de betrokkene of gegevensverwerking uitgevoerd ten behoeve van natuurlijke personen (in het kader van, bijv., werkgelegenheid, sociale bescherming, gewichtige belangen) en de samenleving in haar geheel (bijv. de volksgezondheid of het beheer van gezondheidsdiensten, wetenschappelijk of historisch onderzoek, statistieken en archieven) en onderworpen te zijn aan specifieke en passende waarborgen (bijv. de verwerking voor gezondheidsgerelateerde doeleinden uitgevoerd door personen vallende onder een wettelijke verplichting van beroepsgeheim, technische en organisatorische maatregelen, inclusief gegevensminimalisering en pseudonimisering). Verwerking van bijzondere categorieën van persoonsgegevens moet ook worden toegestaan voor de vaststelling, de uitoefening of de verdediging van een recht in rechte. Stichtingen, verenigingen of andere instanties zonder winstoogmerk wier doel gelegen is op politiek, levensbeschouwelijk of religieus gebied of binnen de gezondheidszorg of de vakvereniging, zullen ook toestemming krijgen speciale categorieën persoonsgegevens te verwerken op voorwaarde dat de verwerking uitsluitend betrekking heeft op de leden (of de voormalige leden) van de organisatie of op personen die regelmatig contact met haar onderhouden in verband met haar legitieme doelen. Naast de vereisten van deze wet, is de geheimhoudingsplicht, indien vastgesteld in andere specifiekewettelijke regelingen, van toepassing op de verwerking van persoonsgegevens. Verwerking van gegevens betreffende de gezondheid om redenen van algemeen belang mag niet resulteren in de verwerking van persoonsgegevens voor andere doeleinden door derden zoals bijvoorbeeld werkgevers of verzekeringsmaatschappijen of banken.

Artikel 9

Persoonsgegevens betreffende strafrechtelijke veroordelingen en overtredingen moeten uitsluitend onder toezicht van de officiële autoriteit worden verwerkt of wanneer de verwerking is toegestaan krachtens een specifieke wettelijke regelingen die in passende waarborgen voorziet. Een uitzondering voor verwerkingsverantwoordelijken die geen officiële autoriteiten zijn, is voorzien in het kader van werkgelegenheid, bijvoorbeeld voor werkgevers of toekomstige werkgevers in de mate noodzakelijk voor de beoordeling van de geschiktheid van personeel voor bepaalde rollen, teneinde de veiligheid en de integriteit van hun zakelijke activiteiten als rechtmatige belangen te garanderen. In dat geval moet de verwerkingsverantwoordelijke passende waarborgen voor de rechten en vrijheden van de betrokkenen garanderen, d.w.z. beschikken over een intern beleidsdocument waarin de procedures van de verwerkingsverantwoordelijke voor het waarborgen van de naleving van artikel 5 worden uitgelegd en het beleid van de verwerkingsverantwoordelijke met betrekking

tot het bewaren en het wissen van die gegevens wordt omschreven. De verwerkingsverantwoordelijke stelt dit document op verzoek daartoe beschikbaar aan de Commissaris voor Gegevensbescherming.

Artikel 10
De vereiste voor de verwerkingsverantwoordelijke inzake het verstrekken van informatie aan het publiek of aan de betrokkene vloeit voort uit het beginsel van openheid en transparantie. Het helpt vertrouwen tot stand te brengen tussen de verwerkingsverantwoordelijken en de betrokkenen, biedt de gelegenheid de verantwoordingsplicht voor verwerkingsverantwoordelijken aan te tonen en stelt betrokkenen in staat om de verzameling van hun gegevens te begrijpen en indien nodig, in discussie te brengen (bijv. verlenen of intrekken van met kennis van zaken gegeven toestemming en uitoefening van de rechten van de betrokkene).
Om transparantie te bewerkstelligen, moeten de verwerkingsverantwoordelijken allereerst de praktische (informatie)vereisten aangegeven in artikel 10 volgen en de kwaliteit, de toegankelijkheid en de begrijpelijkheid van de informatie verstrekt aan betrokkenen garanderen, ook wanneer gecommuniceerd wordt met betrokkenen over de uitoefening van hun rechten en over inbreuken met betrekking tot gegevens.
De informatieverschaffing aan en de communicatie met betrokkenen moet beknopt en transparant zijn (bijv. verwerkingsverantwoordelijken moeten de informatie/communicatie efficiënt en bondig presenteren om informatiemoeheid te vermijden). Informatie moet schriftelijk worden gesteld in begrijpelijke taal voor het gemiddelde lid van het beoogde publiek. Bijzondere aandacht moet worden besteed aan de begrijpelijkheid van informatie verstrekt aan een kind (bijv. iconen en cartoons kunnen gebruikt worden zodat kinderen zaken beter kunnen begrijpen) of aan een persoon met een zintuiglijke beperking (bijv. voor slechtziende betrokkenen kan schriftelijke informatie mondeling of via audiomethodes worden gegeven, zoals een voorafopgenomen audiobericht.

Aan de hand van de informatie zou de betrokkene in staat moeten zijn vooraf te bepalen wat de reikwijdte en de gevolgen van de verwerking kunnen zijn (welke consequenties de specifieke verwerking werkelijk zal hebben voor de betrokkene), in het bijzonder wanneer de gegevensverwerking complex, technisch en onverwacht is.

Informatie moet gemakkelijk toegankelijk zijn, bijvoorbeeld verstrekt aan betrokkenen in een privacyverklaring of -bericht op een website (de link daarnaartoe moet steeds zichtbaar en duidelijk zijn tijdens het navigeren), door middel van contextgebonden pop-ups die geactiveerd worden wanneer een betrokkene een online-formulier invult, of in een interactieve digitale context via een chatbot (gespreksinterface). Verwerkingsverantwoordelijken kunnen betrokkenen geen kosten in rekening brengen voor het verstrekken van informatie en het kan niet afhankelijk van financiële transacties worden gesteld, bijvoorbeeld de betaling voor, of aankoop van, diensten of goederen.

De verwerkingsverantwoordelijke dient de betrokkene te voorzien van de informatie vastgesteld in artikel 10 en afhankelijk van de specifieke omstandigheden van de verwerking, alle aanvullende informatie noodzakelijk om een eerlijke en transparante verwerking te garanderen.

Artikel 11
Het recht niet onderworpen te worden aan uitsluitend geautomatiseerde besluiten is erop gericht te garanderen dat betrokkenen controle uitoefenen over hun persoonsgegevens en mogelijke discriminatie te voorkomen. Van een besluit uitsluitend op basis van geautomatiseerde verwerking zou, bijvoorbeeld, sprake zijn indien iemand routinematig automatisch gegenereerde

(bijv. middels analysesoftware, kunstmatige intelligentie) profielen toepast op personen zonder enig menselijk toezicht. Het recht is van toepassing onder specifieke omstandigheden wanneer een besluit, uitsluitend gebaseerd op geautomatiseerde verwerking, inclusief profilering, rechtsgevolgen heeft voor of vergelijkbare significante invloed uitoefent op iemand. Rechtsgevolg wil zeggen van invloed op de wettelijke rechten van een persoon (bijv. de vrijheid van vereniging, om te stemmen tijdens een verkiezing, of om gerechtelijke stappen te ondernemen), juridische status of rechten ingevolge een contract (bijv. annulering van een contract, ontzegging van een sociale voorziening toegekend bij wet, toelating tot een land weigeren of ontzegging van het staatsburgerschap).
Criteria om te beoordelen of een besluit ingrijpende invloed uitoefent op een persoon, bijv. dat zodanig besluit mogelijk: (i) ingrijpende invloed uitoefent op de omstandigheden, gedrag of keuzes van de betrokken persoon; (ii) een langdurige of blijvende invloed heeft op de betrokken; of (iii) leidt tot de uitsluiting of discriminatie van personen. De volgende besluiten kunnen worden beschouwd als besluiten met voldoende ingrijpende gevolgen: besluiten die de financiële omstandigheden van een persoon beïnvloeden, zoals de kredietwaardigheid, besluiten die van invloed zijn op de toegang van een persoon tot gezondheidszorg, besluiten die een persoon een werkgelegenheidskans ontzeggen of die persoon ernstig benadelen, besluiten die van invloed zijn op de toegang van een persoon tot onderwijs, bijvoorbeeld toelating tot de universiteit.

Elke persoon moet in staat zijn informatie te ontvangen over de hem betreffende gegevens die worden verwerkt, om deze te kunnen verifiëren, met name de nauwkeurigheid van de gegevens en de rechtmatigheid van de verwerking. Om deze redenen heeft elke betrokkene het recht om informatie te verkrijgen over de onderliggende redenen voor de gegevensverwerking wanneer de resultaten van zodanige verwerking op hem worden toegepast, in het bijzonder in het geval van geautomatiseerde besluiten. Bovendien heeft elke betrokkene recht op het ontvangen van alle beschikbare informatie inzake de oorsprong, inzake de termijn voor de bewaring van de gegevens alsmede alle andere informatie die de verwerkingsverantwoordelijke verplicht is te verstrekken met het oog op het garanderen van de transparantie van verwerking overeenkomstig artikel 10. Geen enkele informatie verstrekt aan de betrokkenen overeenkomstig hun rechten mag enige nadelige invloed uitoefenen op andere juridische instrumenten die gemaakt zijn ter bescherming van speciale categorieën van informatie, bijvoorbeeld, handelsgeheimen, intellectuele eigendomsrechten, eigendomsrechten verband houdende met softwareprogramma's (bijv. de broncode), geclassificeerde informatie. Daarnaast heeft elke betrokkene het recht zijn gegevens te doen rectificeren of wissen indien deze gegevens worden verwerkt of zijn verwerkt in strijd met het bepaalde in deze wet.

Het recht op overdraagbaarheid van gegevens staat elke betrokkene toe de persoonsgegevens die hij heeft verstrekt aan een verwerkingsverantwoordelijke, te ontvangen in een gestructureerd, gangbaar en machineleesbaar formaat en om die gegevens over te dragen aan een andere verwerkingsverantwoordelijke. Dit recht is erop gericht de betrokkenen te machtigen met betrekking tot hun eigen persoonsgegevens, omdat het hen in staat stelt persoonsgegevens gemakkelijk van de ene IT-omgeving naar de andere te verplaatsen, te kopiëren of over te brengen. Bijvoorbeeld, een betrokkene kan erin geïnteresseerd zijn om zijn huidige afspeellijst (of een geschiedenis van beluisterde tracks) op te vragen bij een dienst voor muziekstreaming, om uit te zoeken hoe vaak hij naar bepaalde tracks heeft geluisterd, of na te gaan welke muziek hij wil kopen of beluisteren op een ander platform. Zo ook kan hij zijn contactlijst van zijn webmailapplicatie willen opvragen, bijvoorbeeld, voor het opstellen van een bruiloftsgastenlijst, of om informatie te verkrijgen over aankopen waarbij verschillende klantenkaarten worden gebruikt. In samenhang daarmee, mits de verwerking wordt uitgevoerd langs geautomatiseerde weg en gebaseerd is op ofwel een contract krachtens artikel 6 lid 1onder a of op toestemming,

heeft elke betrokkene het recht om de hem betreffende persoonsgegevens, welke hij heeft verstrekt aan een verwerkingsverantwoordelijke, in een gestructureerd, gangbaar en machineleesbaar formaat te ontvangen en voor zover technisch uitvoerbaar, om die gegevens door te geven aan een andere verwerkingsverantwoordelijke (uitoefening van gegevensoverdraagbaarheid). Een voorbeeld hiervan: de boeken gekocht door een persoon bij een online boekhandel, of de songs beluisterd via de muziekstreamingdienst zijn voorbeelden van persoonsgegevens die in het algemeen vallen binnen het toepassingsgebied van gegevensoverdraagbaarheid, omdat ze worden verwerkt op basis van de uitvoering van een contract waarbij de betrokkene partij is. Het recht van de betrokkene hem betreffende persoonsgegevens door te geven of te ontvangen, mag geen verplichting scheppen voor de verwerkingsverantwoordelijken om verwerkingssystemen over te nemen of te onderhouden die technisch compatibel zijn. Het recht op gegevensoverdraagbaarheid gaat gemoeid met complexe juridische, technische en zakelijke aspecten die diepgaand geëvalueerd moeten worden.

Elke betrokkene heeft het recht te allen tijde bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens, tenzij de verwerkingsverantwoordelijke legitieme gronden aantoont voor de verwerking welke zwaarder wegen dan zijn belangen of rechten en fundamentele vrijheden. Dit recht is met name relevant wanneer persoonsgegevens worden verwerkt op basis van de gronden genoemd in artikel 6 lid 1 onder d, e, en f, maar kan evenwel in alle gevallen worden uitgeoefend door een betrokkene. Wanneer persoonsgegevens worden verwerkt voor directmarketingdoeleinden of voor profilering met betrekking tot direct marketing en de betrokkene bezwaar maakt tegen deze verwerkingsactiviteiten, dient de verwerkingsverantwoordelijke deze persoonsgegevens niet langer te verwerken voor die doeleinden. Betrokkenen kunnen ook hun toestemming voor gegevensverwerking te allen tijde intrekken.

Artikel 12
Beperkingen op de beginselen verband houdende met de verwerking van persoonsgegevens en de rechten van betrokkenen kunnen worden opgelegd bij specifieke wettelijke regelingen voor zover deze noodzakelijk zijn voor het waarborgen, bijvoorbeeld, van nationale veiligheid, defensie, openbare veiligheid, of belangrijke economische of financiële belangen, alsmede strafrechtelijk onderzoek en vervolging en actie met betrekking tot schending van de gedragscode van gereglementeerde beroepen. Echter moeten deze wetten de relevante elementen specificeren om de beperkingen op het recht van gegevensbescherming zoveel mogelijk te reduceren.

Artikel 13
Zelfs wanneer het recht op gegevensbescherming is beperkt vanwege de redenen aangegeven in artikel 12, kunnen betrokkenen toch gerechtigd zijn hun rechten uit te oefenen via de Commissaris voor Gegevensbescherming die de betrokkene ten minste zal verwittigen dat alle noodzakelijke verificaties of een evaluatie hebben, respectievelijk heeft, plaatsgevonden.

Artikelen 14 tot en met 21
Deze wet stelt de verplichtingen van verwerkingsverantwoordelijken en verwerkers in detail vast (zie hoofdstuk V) en legt de verantwoordelijkheid en aansprakelijkheid voornamelijk bij de verwerkingsverantwoordelijke (en een restdeel bij de verwerker - zie artikel 40 lid 2: "verwerker is slechts aansprakelijk voor de schade veroorzaakt door verwerking indien de verwerker de specifiek op verwerkers gerichte verplichtingen uit hoofde van deze wet niet is nagekomen of indien de verwerker heeft gehandeld buiten of in strijd met rechtmatige instructies van de verwerkingsverantwoordelijke") voor enige verwerking van persoonsgegevens uitgevoerd door de verwerkingsverantwoordelijke of namens de verwerkingsverantwoordelijke.

Met name zijn de verwerkingsverantwoordelijke en de verwerker verplicht passende en effectieve technische en organisatorische maatregelen ten uitvoer te leggen om ervoor te zorgen dat hun respectieve verwerkingsactiviteiten voldoen aan deze wet. Deze maatregelen moeten in aanmerking nemen: (i) de juridische aard van de verwerkingsverantwoordelijke en waar van toepassing, de grootte van de onderneming (bijvoorbeeld, micro, kleine, middelgrote of grote ondememing, volgens de relevante wettelijke regeling); (ii) de aard, , de omvang, het kader en de doeleinden van de verwerking; en (iii) de potentiële risico's die de verwerking zou kunnen veroorzaken voor de rechten en vrijheden van natuurlijke personen.

Tot de organisatorische maatregelen die noodzakelijk zijn voor verwerkingsverantwoordelijken en verwerkers om te voldoen aan deze wet, kan ook de aanwijzing van een functionaris voor gegevensbescherming worden gerekend. De werkingssfeer van deze bepaling is ervoor te zorgen dat verwerkingsverantwoordelijken, verwerkers en hun werknemers de functionaris voor gegevensbescherming kunnen raadplegen om inzicht te krijgen in hoe deze wet en de gerelateerde verplichtingen na te komen. De functionaris voor gegevensbescherming zal bovendien ook fungeren als contactpunt voor betrokkenen (die hun rechten mogen uitoefenen) en de Commissaris voor Gegevensbescherming. Gezien het feit dat de functionaris voor gegevensbescherming een nieuwe rol zal zijn in de Surinaamse gegevensmaatschappij, is de Commissaris voor Gegevensbescherming bevoegd de vereisten voor deze rol nader aan te geven en richtlijnen verstrekt omtrent de correcte ontplooiing van de gerelateerde activiteiten aangeven in artikel 21.

Om naleving van deze wet te kunnen aantonen, moet de verwerkingsverantwoordelijke intern beleid aannemen en maatregelen ten uitvoer leggen die met name voldoen aan de beginselen van gegevensbescherming by design (door ontwerp) en gegevensbescherming by default (door standaardinstellingen). Dergelijke maatregelen kunnen onder andere bestaan uit het tot een minimum beperken van de verwerking van persoonsgegevens, pseudonimisering van persoonsgegevens, transparantie met betrekking tot de functies en verwerking van persoonsgegevens, de betrokkene in staat stellend de gegevensverwerking te monitoren, de verwerkingsverantwoordelijke in staat stellend veiligheidsvoorzieningen te creëren en te verbeteren. Bij het ontwikkelen, ontwerpen, selecteren en gebruiken van applicaties, diensten en producten die gebaseerd zijn op de verwerking van persoonsgegevens of het verwerken van persoonsgegevens om hun taak te vervullen, moeten makers van de producten, diensten en applicaties aangemoedigd worden om rekening te houden met het recht op gegevensbescherming en met inachtneming van de staat van de techniek, ervoor te zorgen dat verwerkingsverantwoordelijken en verwerkers in staat zijn hun verplichtingen inzake gegevensbescherming na te komen.

Indien een verwerkingsverantwoordelijke of een verwerker valt onder de werkingssfeer van artikel 3(2), moet hij/zij een vertegenwoordiger (een natuurlijke persoon of een rechtspersoon gevestigd in de Republiek Suriname die de verwerkingsverantwoordelijke of de verwerker vertegenwoordigt met betrekking tot hun respectieve verplichtingen ingevolge deze wet) aanwijzen, tenzij de verwerking incidenteel is, geen verwerking inhoudt, op grote schaal, van bijzondere categorieën van persoonsgegevens of de verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en overtredingen, en waarschijnlijk niet zal resulteren in een risico voor de rechten en vrijheden van natuurlijke personen, met inachtneming van de aard, het kader, de reikwijdte en de doeleinden van de verwerking of indien de verwerkingsverantwoordelijke een overheidsinstantie of instelling is. De vertegenwoordiger dient op te treden namens de verwerkingsverantwoordelijke of de verwerker en mag worden aangesproken door de Commissaris voor Gegevensbescherming. De aanwijzing van die

vertegenwoordiger is niet van invloed op de verantwoordelijkheid of de aansprakelijkheid van de verwerkingsverantwoordelijke of de verwerker krachtens deze wet.

Om naleving van de vereisten van deze wet ten aanzien van de door de verwerker uit te voeren verwerking ten behoeve van de verwerkingsverantwoordelijke te garanderen, dient bij het toevertrouwen van de verwerkingsactiviteiten aan een verwerker, de verwerkingsverantwoordelijke alleen gebruik te maken van verwerkers die voldoende garanties bieden, in het bijzonder in termen van expertise, betrouwbaarheid en middelen, voor het implementeren van technische en organisatorische maatregelen die voldoen aan de eisen van deze wet, in het bijzonder voor de beveiliging van de verwerking. De uitvoering van verwerkingsactiviteiten door een verwerker moet beheerst worden door een bindende schriftelijke overeenkomst waarin zijn vastgelegd het voorwerp en de duur van de verwerking, de aard en het doel van de verwerking, de soort persoonsgegevens en de categorieën van betrokkenen, de rechten en verplichtingen van de verwerkingsverantwoordelijke en de verplichtingen van de verwerker. De Commissaris voor Gegevensbescherming is derhalve bevoegd een modelcontract vast te stellen en te publiceren om de relatie tussen een verwerkingsverantwoordelijke en een verwerker wat gegevensbescherming betreft, correct te regelen.

Verwerkingsverantwoordelijken en verwerkers moeten een register bijhouden van de verwerkingsactiviteiten onder hun verantwoordelijkheid. Bovendien moeten elke verwerkingsverantwoordelijke en elke verwerker de geregistreerde verwerkingsactiviteiten melden bij de Commissaris voor Gegevensbescherming en de melding ten minste eens per jaar bijwerken. De Commissaris voor Gegevensbescherming verstrekt richtlijnen inzake de uitvoering van de verplichtingen inzake de registers van verwerkingsactiviteiten en de desbetreffende melding (bijv. een online standaardmeldingsformulier maken en praktische instructies geven omtrent het invullen van de registers van verwerkingsactiviteiten).

Inbreuk in verband met persoonsgegevens kan bestaan uit één of een combinatie van het volgende: inbreuk in verband met geheimhouding (een ongeoorloofde of accidentele mededeling van, of toegang tot, persoonsgegevens), inbreuk in verband met beschikbaarheid (een accidenteel of ongeoorloofd verlies van toegang tot of vernietiging van persoonsgegevens) en inbreuk in verband met integriteit (een ongeoorloofde of accidentele wijziging van persoonsgegevens). Indien een inbreuk in verband met persoonsgegevens niet goed en tijdig wordt aangepakt, kan het leiden tot fysieke, materiële of niet-materiële schade voor natuurlijke personen zoals verlies van controle over hun persoonsgegevens of beperking van hun rechten, discriminatie, identiteitsdiefstal of -fraude, financieel verlies, ongeoorloofd terugdraaien van pseudonimisering, reputatieschade, verlies van geheimhouding van persoonsgegevens beschermd door beroepsgeheim of enig ander significant economisch of sociaal nadeel.
De verwerkingsverantwoordelijke stelt daarom de Commissaris voor Gegevensbescherming zonder vertraging en waar mogelijk, ten laatste 72 uur na kennisneming, op de hoogte van een inbreuk in verband met persoonsgegevens. Een uitzondering op de meldingsplicht wordt gevormd door de inbreuken die geen risico inhouden voor de rechten en vrijheden van een persoon, bijv. een verwerkingsverantwoordelijke heeft een back-up van een archief met persoonsgegevens versleuteld opgeslagen op een USB-stick, de stick wordt gestolen tijdens een inbraak; maar, zolang de gegevens versleuteld zijn met de modernste algoritmes, er back-ups zijn van de gegevens, de unieke code niet in gevaar is, en de gegevens te gelegener tijd kunnen worden hersteld, is dit geen inbreuk die gemeld moet worden.
Bovendien, in geval van een inbreuk op persoonsgegevens die bijzondere risico's inhoudt voor de betrokkene in kwestie, kan de Commissaris voor Gegevensbescherming van de verwerkingsverantwoordelijke eisen dat deze de betrokkenen informeert over zodanige inbreuk.

De Commissaris voor Gegevensbescherming vaardigt richtlijnen uit betreffende het beheer van inbreuken op persoonsgegevens (in het bijzonder ten aanzien van hoe een inbreuk op de persoonsgegevens te voorkomen, hoe een inbreuk op de persoonsgegevens te herkennen, hoe het risico voor betrokkenen te verminderen, hoe lering te trekken uit een inbreuk op persoonsgegeven en hoe gegevensbeveiliging te verbeteren), alsmede een (online) standaardformulier voor het melden van de inbreuk op de persoonsgegevens.

Artikel 22
Grensoverschrijdende persoonsgegevensstromen zijn noodzakelijk voor de uitbreiding van internationale handel en de ontwikkeling van datagestuurde economieën en maatschappijen. Deze wet beoogt deze gegevensstromen mogelijk te maken en daarbij tegelijkertijd adequate bescherming voor de desbetreffende betrokkenen te garanderen. Daarom kunnen volgens deze wet persoonsgegevens worden doorgegeven aan een ontvanger die gevestigd is in een derde land, op basis van adequate waarborgen die worden aangegeven in artikel 22.
Doorgiften van gegevens kunnen worden uitgevoerd indien de wet die van toepassing is op de ontvanger in het derde land, voorziet in een adequaat beschermingsniveau. Anderzijds kan een zodanig beschermingsniveau worden geboden door bindende bedrijfsvoorschriften of een bindende overeenkomst die door de ontvanger in een derde land wordt nagekomen. De Commissaris voor Gegevensbescherming kan bindende bedrijfsvoorschriften of bindende overeenkomsten die een goed niveau van bescherming verschaffen specifiek identificeren. Doorgiften van persoonsgegevens aan andere landen zijn eveneens toegestaan indien één van de voorwaarden voor rechtmatige gegevensverwerking vastgesteld in artikel 6 van toepassing is, bijv. de betrokkene heeft zijn toestemming voor de doorgifte gegeven, indien de doorgifte noodzakelijk is voor de nakoming van een contract waarbij de betrokkene partij is, enz.

Verder behoudt de Commissaris voor Gegevensbescherming altijd de bevoegdheid om toestemming te geven voor de doorgifte van gegevens. Daarnaast valt het op, dat een betere bescherming wordt gevraagd voor speciale categorieën van persoonsgegevens (artikel 8) en persoonsgegevens die betrekking hebben op strafrechtelijke veroordelingen en overtredingen (artikel 9) die alleen kunnen worden doorgegeven aan derde landen indien de ontvanger van de gegevens onderworpen is aan een wet, bindende bedrijfsvoorschriften of een bindende overeenkomst die een adequaat beschermingsniveau biedt of indien de Commissaris voor Gegevensbescherming toestemming heeft gegevev voor de specifieke gegevensoverdracht. In de praktijk komt het erop neer dat speciale categorieën van persoonsgegevens en persoonsgegevens die betrekking hebben op strafrechtelijke veroordelingen en overtredingen verwerkt moeten worden overeenkomstig de voorschriften opgenomen in de artikelen 8 en 9. Daarnaast dienen voor het doorgeven van deze gegevens aan derde landen de waarborgen vastgesteld in artikel 22 toegepast te worden.

Artikelen 23 tot en met 32
Een onafhankelijk overheidsorgaan dat verantwoordelijk is voor het toezicht op en de tenuitvoerlegging van deze wet, alsmede voor de bewustmaking omtrent deze wet en voor het geven van richtlijnen over hoe persoonsgegevens te verwerken met volledige eerbiediging van de rechten op privacy en gegevensbescherming, is een essentieel element van de bescherming van personen in een democratische samenleving.
In dit opzicht wordt door de wet [het ambt van] de Commissaris voor Gegevensbescherming ingesteld, een naar behoren gekwalificeerde en onafhankelijke fysieke persoon - benoemd krachtens artikel 24 - die leiding geeft aan en optreedt als vertegenwoordiger van de onafhankelijke autoriteit (artikel 23) met een eigen rechtspersoonlijkheid (krachtens artikel 25), ondersteund in zijn activiteiten door een deskundige en ervaren staf (het Bureau van de

Commissaris voor Gegevensbescherming ingevolge artikel 26) in overeenstemming met de bevoegdheid toegekend in artikel 30 van deze wet.
De wet geeft de taken aan die door de Commissaris voor Gegevensbescherming moeten worden uitgevoerd (artikel 31), verleent de noodzakelijke bevoegdheden (artikel 32) voor de uitoefening van de desbetreffende taken en verplichtingen, inclusief de bevoegdheid tot onderzoek en interventie, met name bij klachten van personen.
De onafhankelijkheid van de Commissaris in de uitoefening van zijn taken wordt geacht fundamenteel te zijn voor de correcte functionering van de autoriteit en dient gewaarborgd te worden door de methode van zijn benoeming en van de staf in zijn Bureau, de duur van de uitoefening en omstandigheden van beëindiging van zijn taken (artikel 29), de toewijzing van voldoende middelen (artikel 27) en het nemen van besluiten zonder onderworpen te zijn aan externe opdrachten of rechterlijke bevelen. In dit verband valt ook op dat geen acties of andere procedures voor schadevergoeding kunnen worden ingesteld tegen de Commissaris voor Gegevensbescherming en de stafleden van het Bureau van de Commissaris voor Gegevensbescherming voor een handeling verricht te goeder trouw bij de uitoefening van een taak of bevoegdheid of beoordelingsvrijheid ingevolge deze wet (artikel 28).

Artikelen 33 tot en met 42
Aan elke betrokkene of zijn wettelijke vertegenwoordiger is toegekend het recht een klacht in te dienen bij de Commissaris voor Gegevensbescherming indien de betrokkene van mening is, dat de verwerking van de hem betreffende persoonsgegevens inbreuk maakt op de onderhavige wet (artikelen 33 en 34), en toegang te hebben tot een effectief rechtsmiddel tegen de Commissaris voor Gegevensbescherming, een verwerkingsverantwoordelijke of een verwerker (artikelen 38 en 39). Elke persoon die materiële of niet-materiële schade heeft geleden als gevolg van een inbreuk op deze wet heeft het recht van de verwerkingsverantwoordelijke of de verwerker vergoeding te ontvangen voor die schade (artikel40). Dit recht moet verleend worden in overeenstemming met het recht op een eerlijk proces vastgesteld in artikel 10 van de Grondwet, dat garandeert dat in geval van een aantasting van de rechten en vrijheden van een persoon, deze persoon aanspraak heeft op een eerlijke en openbare behandeling van zijn klacht binnen een redelijke termijn door een onafhankelijke en onpartijdige rechter.
Bovendien, krachtens artikel 42, kunnen de betrokkenen last geven aan een instelling, organisatie of vereniging zonder winstoogmerk, welke naar behoren is opgericht en met samenhangende statutaire doelstellingen, voor de uitoefening namens hen, van hun rechten toegekend overeenkomstig artikelen 33, 38, 39 en 40 (m.n. indienen van een klacht bij de Commissaris voor Gegevensbescherming, uitoefening van het recht op rechtsmiddel tegen de Commissaris voor Gegevensbescherming of een verwerkingsverantwoordelijke of een verwerker, alsmede uitoefening van het recht op het ontvangen van een vergoeding). Vermeldenswaard is dat ook rechtspersonen recht hebben op een effectief rechtsmiddel tegen een juridisch bindend besluit van de Commissaris voor Gegevensbescherming (bijv. een verwerkingsverantwoordelijke-rechtspersoon die in beroep wil gaan tegen een besluit genomen door de Commissaris voor Gegevensbescherming, waarbij een boete wordt opgelegd aan die verwerkingsverantwoordelijke).
De wet geeft de inbreuken en het plafond alsmede de criteria aan voor het bepalen van de desbetreffende administratieve boetes, die in elk afzonderlijk geval zouden moeten worden vastgesteld door de Commissaris voor Gegevensbescherming, rekening houdend met alle relevante omstandigheden van de specifieke situatie, met inachtneming van met name de aard, de ernst en de duur van de inbreuk en van de consequenties daarvan en de maatregelen genomen om nakoming van de verplichtingen ingevolge deze wet te garanderen en om de gevolgen van de inbreuk te voorkomen of te beperken (artikel 37).
In aanmerking genomen de Surinaamse samenleving, wordt specifieke bescherming verleend aan werknemers die mogelijk onrechtmatige gedragingen van werkgevers kunnen melden bij de

Commissaris voor Gegevensbescherming; hebben gedaan of te kennen hebben gegeven iets te zullen doen dat gedaan moet worden om te voorkomen dat een persoon deze wet overtreedt; of weigeren iets te doen dat in strijd is met deze wet (zie artikel 41 inzake de bescherming voor klokkenluiders).

Artikel 43
Artikel 19 van de Grondwet waarborgt het recht op de vrijheid van meningsuiting, verklarende dat een ieder het recht heeft om middels de drukpers of andere communicatiemiddelen zijn gedachten of gevoelens te openbaren en zijn mening te uiten, behoudens ieders verantwoordelijkheid volgens de wet.
De wet erkent de behoefte om het recht op privacy en het recht op gegevensbescherming in evenwicht te brengen met het recht op vrijheid van meningsuiting (journalistieke, literaire of artistieke uiting), bijv. gevallen verband houdende met de publicatie van persoonsgegevens bij het bekendmaken van informatie, meningen of ideeën aan het publiek in het kader van journalistieke activiteiten.
Enige aanwijzingen omtrent het vinden van een goed evenwicht tussen de rechten op vrijheid van meningsuiting en de rechten op privacy en gegevensbescherming kunnen gevonden worden in de bestaande rechtspraak van het Europees Hof voor de Rechten van de Mens (bijv. Von Hannover v. Germany [Duitsland], no. 59320/00, ECHR 2004-VI) en het Inter-Amerikaans Hof voor de Rechten van de Mens (bijv. de zaak Fontevecchia en d'Amico *v.* Argentina [Argentinië], 29 november 2011).

Artikel 44
Om het recht inzake toegang van het publiek tot officiële documenten te verzoenen met het recht op privacy en het recht op gegevensbescherming, staat deze wet toe dat specifieke wettelijke regelingen worden gemaakt om te voorzien voor omstandigheden, waaronder persoonsgegevens in officiële documenten in handen van een overheidsinstantie of een openbare of particuliere instelling mogen worden openbaard voor de uitvoering van een taak verricht in het algemeen belang.

Artikel 45
De rechten van de betrokkene inzake toegang, rectificatie en om bezwaar te maken, kunnen het verwezenlijken van de specifieke doelen onmogelijk maken of ernstig belemmeren wanneer persoonsgegevens worden verwerkt voor doeleinden van wetenschappelijk of historisch onderzoek, statistische doeleinden en archiveringsdoeleinden, en daarom staat deze wet toe dat ze beperkt worden.

Artikel 46
Vanaf de datum van toepassing van deze wet worden eventuele bepalingen in enige andere wettelijke regeling ingetrokken voor zover deze strijdig zijn met het bepaalde in deze wet. Vermeldenswaard in dit verband is dat deze wet het algemeen kader biedt voor de bescherming van persoonsgegevens. Bij specifieke wettelijke regelingen kunnen aangelegenheden van privacy en gegevensbescherming in specifieke sectoren nader worden geregeld, overeenkomstig het 'lex specialis derogat generali'-beginsel, maar die mogen niet resulteren in een eventuele vermindering van de bescherming verleend aan betrokkenen door deze wet die beoogt een referentiekader voor privacy en gegevensbescherming te zijn.

Paramaribo, de.....

CHANDRIKAPERSAD SANTOKHI

BIJLAGE behorende bij Wet houdende regels ter bescherming van privacy en persoonsgegevens(Wet Bescherming Privacy en Persoonsgegevens)

TECHNISCHE EN ORGANISATORISCHE MAATREGELEN VOOR GEGEVENSBEVEILIGING

Waar van toepassing overeenkomstig artikel 19 lid 1 en voor zover van toepassing:

A. - BELEID INZAKE GEGEVENSBEVEILIGING

A.1 De aansturing van verwerkingsverantwoordelijke en verwerker inzake gegevensbeveiliging

Verwerkingsverantwoordelijken en verwerkers stellen beleid vast om de richting van en ondersteuning voor gegevensbeveiliging duidelijk te maken.

B. - ORGANISATIE VAN GEGEVENSBEVEILIGING

B.1 Interne organisatie

Verwerkingsverantwoordelijken en verwerkers zetten de rollen en verantwoordelijkheden voor gegevensbeveiliging uiteen en wijzen ze toe aan individuele personen. Indien relevant, moeten de taken worden verdeeld over rollen en individuele personen om belangenconflicten te vermijden en ongepaste activiteiten te voorkomen.

B.2 Mobiele apparaten en werken op afstand

Verwerkingsverantwoordelijken en verwerkers hebben een beveiligingsbeleid en controles voor mobiele apparaten (zoals laptops, tablet PC's, draagbare ICT-apparaten, smartphones, USB gadgets, enz.) en werken op afstand (zoals telewerken, thuiswerken en afgelegen/virtuele werkplekken).

C. - PERSONELE BEVEILIGING

C.1 Voorafgaand aan indiensttreding

Verwerkingsverantwoordelijken en verwerkers houden rekening met verantwoordelijkheden voor gegevensbeveiliging bij het werven van vaste medewerkers, aannemers en tijdelijk personeel (bijv. door goede functiebeschrijvingen, screening voor indiensttreding) en nemen die op in contracten (bijv. arbeidsvoorwaarden en andere ondertekende overeenkomsten waarin rollen en verantwoordelijkheden met betrekking tot gegevensbeveiliging worden beschreven, nalevingsverplichtingen, enz.).

C.2 Tijdens dienstverband

Verwerkingsverantwoordelijken en verwerkers zien erop toe dat werknemers en aannemers bewust worden gemaakt van en gemotiveerd worden tot het naleven van hun verplichtingen ten aanzien van gegevensbeveiliging. Een formeel disciplinair proces is noodzakelijk voor het afhandelen van incidenten in verband met gegevensbeveiliging die vermoedelijk door werkers zijn veroorzaakt.

C.3 Beëindiging en verandering van baan

Verwerkingsverantwoordelijken en verwerkers beheren de aspecten inzake gegevensbeveiliging rondom het vertrek van een persoon uit de organisatie, of ingrijpende veranderingen in rollen binnen de organisatie, zoals teruggaan naar de verwerkingsverantwoordelijke of de verwerker en vervolgens het verwijderen van persoonsgegevens verwerkt in het kader van hun activiteiten

binnen de organisatie van verwerkingsverantwoordelijke of verwerker en apparaten in hun bezit, bijwerken van hun toegangsrechten, en hen herinneren aan hun doorgaande verplichtingen krachtens de wet, contractvoorwaarden en ethische verwachtingen.

D. - ACTIVABEHEER

D.1 Verantwoordelijkheid voor activa

Verwerkingsverantwoordelijken en verwerkers inventariseren alle gegevensactiva en verantwoordelijke personen binnen de organisatie worden geïdentificeerd die verantwoordelijk zullen zijn voor hun gegevensbeveiliging. Beleid inzake 'aanvaarbaar gebruik' wordt vastgesteld door verwerkingsverantwoordelijken en verwerkers en activa moeten worden teruggegeven wanneer mensen de organisatie verlaten.

D.2 Gegevensclassificatie

Verwerkingsverantwoordelijken en verwerkers classificeren gegevens (bijv. 'persoonsgegevens', overeenkomstig artikel 1 lid 1; 'speciale categorieën van persoonsgegevens", overeenkomstig artikel 8; 'gegevens inzake strafrechtelijke veroordeling en strafbare feiten', overeenkomstig artikel 9, bestempelen ze in overeenstemming met de benodigde bescherming voor gegevensbeveiliging en gaan er dienovereenkomstig mee om.

D.3 Omgaan met media

Verwerkingsverantwoordelijken en verwerkers beheren, controleren, verplaatsen en verwijderen gegevensopslagmedia op zodanige wijze dat de gegevens worden gecompromitteerd.

E. - TOEGANGSCONTROLE

E.1 Eisen aan de organisatie betreffende toegangscontrole

Verwerkingsverantwoordelijken en verwerkers documenteren duidelijk de vereisten van de organisatie inzake het beheren van de toegang tot informatieactiva in relevante beleidsdocumenten en procedures betreffende toegangscontrole. Netwerktoegang en -verbindingen zijn beperkt.

E.2 Beheer van gebruikerstoegang

Verwerkingsverantwoordelijken en verwerkers beheren de toewijzing van toegangsrechten aan gebruikers vanaf de eerste gebruikersregistratie tot de opheffing van toegangsrechten wanneer deze niet langer vereist zijn, waaronder begrepen bijzondere beperkingen bij bevoorrechte toegangsrechten en het beheer van wachtwoorden. Toegangsrechten worden regelmatig herzien en bijgewerkt.

E.3 Gebruikersverantwoordelijkheden

Verwerkingsverantwoordelijken en verwerkers wijzen gebruikers op hun verantwoordelijkheid om te zorgen voor effectieve toegangscontroles, bijv. het kiezen van sterke wachtwoorden en het geheimhouden daarvan.

E.4 Systeem en toepassing toegangscontrole

Verwerkingsverantwoordelijken en verwerkers beperken de toegang tot gegevens overeenkomstig het beleid inzake toegangscontrole, bijv. door middel van veilige aanmelding, wachtwoordbeheer, controle over bevoorrechte voorzieningen en beperkte toegang tot de broncode van programma's.

F. -CRYPTOGRAFIE

F.1 Cryptografische controles

Verwerkingsverantwoordelijken en verwerkers voeren een beleid betreffende het gebruik van encryptie, alsmede cryptografische authentificatie en integriteitscontroles zoals digitale handtekeningen en echtheidscodes voor berichten en beheer van cryptografische sleutels.

G. FYSIEKE EN OMGEVINGSBEVEILIGING VOOR GEGEVENS

G.1 Veilige zones

Met betrekking tot afgebakende fysieke perimeters en barrières, met fysieke toegangscontroles en werkprocedures, beschermen verwerkingsverantwoordelijken en verwerkers de gebouwen, kantoren, ruimtes, aflever-/laadzones, enz. tegen ongeoorloofde toegang. Deskundig advies wordt ingeschakeld betreffende bescherming tegen brand, overstromingen, aardbevingen, bommen, enz.

G.2 Apparatuur

Verwerkingsverantwoordelijken en verwerkers beveiligen en onderhouden de "apparaten" (dat wil zeggen voornamelijk ICT-apparatuur), alsmede de ondersteunende voorzieningen (zoals elektriciteit en airconditioning) en de bekabeling. Apparaten en informatie mogen niet van de locatie worden verwijderd, tenzij met toestemming. Ze moeten zowel op als buiten de locatie adequaat beschermd zijn. Gegevens moeten vernietigd worden voordat de opslagmedia worden weggedaan of hergebruikt. Onbeheerde apparatuur moet beveiligd zijn en er moet een beleid van een leeg bureau en leeg scherm worden gevoerd.

H. - OPERATIONELE GEGEVENSBEVEILIGING

H.1 Operationele procedures en verantwoordelijkheden

Verwerkingsverantwoordelijken en verwerkers documenteren operationele verantwoordelijkheden en procedures met betrekking tot IT. Veranderingen in IT-faciliteiten en -systemen worden beheerd. Capaciteit en prestaties worden beheerd. Ontwikkelings-, test- en operationele systemen zijn gescheiden.

H.2 Bescherming tegen malware

Verwerkingsverantwoordelijken en verwerkers voeren regelmatig controles op schadelijke software uit en leggen zich toe op bewustmaking van de gebruiker.

H.3 Gegevensback-up

Goede gegevensback-ups moeten gemaakt en bewaard worden door verwerkingsverantwoordelijken en verwerkers overeenkomstig een back-upbeleid.

H.4 Registreren en monitoren

Verwerkingsverantwoordelijken en verwerkers registreren en beschermen activiteiten van systeemgebruikers en -administrateur/-beheerder, uitzonderingen, gebreken en incidenten inzake gegevensbeveiliging. Klokken moeten gesynchroniseerd worden.

H.5 Controle van besturingssoftware

Verwerkingsverantwoordelijken en verwerkers beheren de installatie van software op besturingssystemen.

H.6 Beheer van technische kwetsbaarheid

Verwerkingsverantwoordelijken en verwerkers corrigeren technische kwetsbaarheden en er dienen voorschriften te zijn voor het installeren van software door gebruikers.

H.7 Overwegingen inzake audits van gegevenssystemen

Verwerkingsverantwoordelijken en verwerkers verrichten IT-audits om de nadelige effecten op productiesystemen of ongeoorloofde toegang tot gegevens tot een minimum te beperken.

I. - COMMUNICATIEBEVEILIGING

I.1 Beheer netwerkbeveiliging

Verwerkingsverantwoordelijken en verwerkers beveiligen netwerken en netwerkdiensten, bijvoorbeeld door middel van afscheiding.

I.2 Gegevenscommunicatie/doorgifte

Verwerkingsverantwoordelijken en verwerkers zorgen voor het gereedhouden van beleid, procedures en overeenkomsten (bijv. geheimhoudingsovereenkomsten) met betrekking tot de doorgifte van gegevens aan/van derden, met inbegrip van elektronisch berichtenverkeer.

J. - AANSCHAF, ONTWIKKELING EN ONDERHOUD VAN SYSTEEM

J.1 Beveiligingseisen van gegevenssystemen

Eisen inzake het beheer van Gegevensbeveiliging worden geanalyseerd en gespecificeerd door verwerkingsverantwoordelijken en verwerkers, waaronder begrepen webtoepassingen en transacties via het web.

J.2 Beveiliging bij ontwikkelings- en ondersteuningsprocessen

Verwerkingsverantwoordelijken en verwerkers definiëren als beleid, voorschriften die de ontwikkeling van veilige software/systemen beheersen. Veranderingen in systemen (zowel toepassingen als besturingssystemen) worden beheerd. Softwarepakketten zullen idealiter niet worden gewijzigd, en engineering-beginselen voor veilige systemen dienen gevolgd te worden. De ontwikkelomgeving moet beveiligd zijn en uitbestede ontwikkeling moet gecontroleerd worden. Systeembeveiliging wordt getest en acceptatiecriteria worden zo gedefinieerd dat ze beveiligingaspecten omvatten.

J.3 Testgegevens

Testgegevens moeten zorgvuldig worden geselecteerd/gegenereerd en beheerd door verwerkingsverantwoordelijken en verwerkers.

K. - LEVERANCIERRELATIES

K.1 Gegevensbeveiliging in leverancierrelaties

Verwerkingsverantwoordelijken en verwerkers zorgen ervoor afspraken voor beleid, procedures, bewustmaking, enz. ter bescherming van persoonsgegevens die toegankelijk zijn voor externe IT-dienstverleners en overige externe leveranciers langs de toeleveringsketen, vast te leggen in de contracten of overeenkomsten.

K.2 Beheer dienstverlening leverancier

Verwerkingsverantwoordelijken en verwerkers houden toezicht op en evalueren/controleren de dienstverlening door externe leveranciers aan de hand van de contracten/overeenkomsten. Veranderingen in diensten worden gecontroleerd.

L. - Beheer incidenten in verband met gegevensbeveiliging

L.1 Beheer van incidenten in verband met gegevensbeveiliging en verbeteringen

Verwerkingsverantwoordelijken en verwerkers stellen verantwoordelijkheden en procedures vast voor het consistent en effectief beheren van (rapporteren van, beoordelen van, reageren op en leren uit) voorvallen, incidenten en zwakke plekken in verband met gegevensbeveiliging en om forensisch bewijs te vergaren.

M. - ASPECTEN VAN GEGEVENSBEVEILIGING IN HET KADER VAN BEDRIJFSCONTINUÏTEITSBEHEER

M.1 Continuïteit van gegevensbeveiliging

De continuïteit van gegevensbeveiliging moet gepland, uitgevoerd en opnieuw bekeken worden als een integraal deel van de systemen voor bedrijfscontinuïteitsbeheer van de verwerkingsverantwoordelijken en de verwerkers.

M.2 Redundanties

Verwerkingsverantwoordelijken en verwerkers zien erop toe dat IT-faciliteiten over voldoende redundantie beschikken om aan de beschikbaarheidseisen te voldoen.

N. - NALEVING

N.1 Evaluatie gegevensbeveiliging

De regelingen voor gegevensbeveiliging getroffen door verwerkingsverantwoordelijken en verwerkers worden onafhankelijk geëvalueerd (gecontroleerd) en gerapporteerd aan de leiding. Verwerkingsverantwoordelijken en verwerkers evalueren ook routinematig of de medewerkers en de systemen voldoen aan het beleid, de procedures enz. inzake gegevensbeveiliging en initiëren corrigerende maatregelen waar nodig.