WET van .....,
houdende regels inzake
Elektronische Transacties
(Elektronische Transacties
Wet)

ONTWERP

DE PRESIDENT VAN DE REPUBLIEK SURINAME,

In overweging genomen hebbende, dat het wenselijk is in het kader van de herziening van het Burgerlijk Wetboek regels te stellen inzake Elektronische Transacties;

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

Hoofdstuk I
Algemene bepalingen

Artikel 1. Deze wet wordt aangehaald als Elektronische Transacties Wet, 2012.

Artikel 2. In deze wet en de daarop berustende bepalingen wordt verstaan onder:

a.	computerbemiddelende netwerken (“computer-mediated networks”)	netwerken die opgezet worden door de logische of fysieke aansluiting van meerdere informatiesystemen, welke behoren tot dezelfde meerdere personen, gefaciliteerd door de overheid of particuliere telecommunicatie netwerken;
b.	consument	elke persoon die in een elektronische transactie met een leverancier aangaat als de eindgebruiker die goederen of diensten aanbiedt door de leverancier;
c.	data	de inhoud (‘content’) inclusief maar niet gelimiteerd tot de tekst, beeldmateriaal of geluidsmateriaal dat een data bericht vormt;
d.	data bericht (“data message”)	elk document, correspondentie, memorandum, boek, plannen, plattegrond, tekening, diagram, geïllustreerd blad of grafische werk, foto, audio of video opname, machine-leesbare symbolen gegenereerd, verzonden, ontvangen of opgeslagen door elke elektronisch middel door of namens de persoon die het vertegenwoordigt;
e.	e-commerce	alle vormen van aanbieden en aanprijzen van goederen, diensten, bedrijven en personen, waaronder reclame en direct marketing, gebruikmakend van internet vanuit of gericht op Suriname, direct of indirect gericht op het tot stand brengen van overeenkomsten;

f.	elektronisch	digitale of immateriële vorm met de mogelijkheid tot creatie, opslag, transmissie of ontvangst door elektronisch, magnetisch, draadloos, optisch, biometrisch of elke andere vergelijkbaar middel;
g.	elektronische agent	een programma of andere elektronisch of geautomatiseerd middel geconfigureerd en ingeschakeld door een persoon die is ingezet om data berichten te initiëren of te reageren of te presteren in zijn geheel of deel daarvan zonder beoordeling of interventie door een persoon op het moment van initiatie of response;
h.	Elektronische Authenticatie Dienstverlener	een persoon die elektronische authenticatie producten en diensten die daaraan gerelateerd zijn aanbiedt;
i.	elektronische authenticatie product	een product ontworpen voor de identificatie van de houder van een elektronische handtekening van een ander persoon;
j.	elektronische handtekening	informatie in elektronische vorm aangebracht of logisch geassocieerd met een data bericht dat gebruikt kan worden om - (a) ter identificatie van de ondertekenaar in relatie tot het data bericht; of (b) ter indicatie van de ondertekenaars goedkeuring van de informatie dat opgenomen is in de data bericht;
k.	elektronische transactie	transactie bij de verkoop of aankoop van goederen en diensten die worden bestuurd door computergestuurde netwerken van informatiesystemen, waar de goederen en diensten kunnen worden besteld via zulke netwerken van systemen, maar de betaling en uiteindelijke levering van de goederen en diensten kunnen geschieden zonder het gebruik van zulke netwerken van systemen;
l.	elektronische vastlegging	een vastlegging gecreëerd, opgeslagen, gegenereerd, ontvangen of gecommuniceerd door een elektronisch middel;
m.	encryptie	technieken voor het versleutelen van elektronisch opgeslagen gegevens met het oogmerk dat die gegevens slechts door bepaalde personen te ontsleutelen zijn;
n.	geadresseerde	een persoon die de data bericht ontvangt, maar dat niet een persoon betreft die als tussenpersoon van telecommunicatie dienstverlener fungeert met betrekking tot data berichten;
o.	gerechtshof	het Gerechtshof van Suriname;
p.	individu	een natuurlijke persoon;
q.	informatie	data, codes, computer programma's, software en databases;
r.	informatiesysteem	een apparaat of combinatie van apparaten inclusief input en output apparaten, die in staat zijn om in conjunctie met externe bestanden gebruikt kunnen worden, die computer programma's

		bevatten, elektronisch instructies, input data en output data die logische, rekenkundig, data opslag en ontvangst, communicatiebeheer en andere functies vervullen.
s.	intermediair	een persoon die namens een andere persoon data berichten verzend, transporteert, ontvangt of andere diensten met betrekking tot die data berichten bevattende 'content', e-mail, 'caching' en 'hosting services';
t.	Minister	de Minister die verantwoordelijk is gesteld voor Informatie en Communicatie Technologie;
u.	onderneming	een samenwerking of lichaam, met of zonder rechtspersoonlijkheid, zakelijk is betrokken;
v.	ondertekenaar	een persoon die al dan niet een handtekening creërende apparaat heeft en optreedt namens zichzelf of namens een andere persoon door een elektronische handtekening te plaatsen;
w.	Persoonsgegevens	gegevens betreffende een bepaalde natuurlijke persoon of rechtspersoon, daaronder zowel begrepen informatie die de identiteit bepaalt, met inbegrip van adresgegevens, telefoonnummer, faxnummer en elektronisch postadres, alsook bijzonderheden met betrekking tot die persoon zoals koopgedrag en preferenties.
x.	Producten	hierbij worden tevens goederen, diensten en werken bedoeld in deze wet;
y.	telecommunicatie dienstverlener	aanbieder van telecommunicatie diensten;
z.	Vastlegging	het vastleggen van informatie dat verzameld, gecreëerd of ontvangen is bij de initiatie, uitvoering of afronding van een activiteit en die bestaat uit voldoende inhoud ('content'), context en structuur om als bewijs te dienen van die activiteit of transactie;
aa.	Verzender	een persoon door wie of namens wie een data bericht wordt verzonden of gegenereerd voorafgaand aan de opslag, maar niet de persoon die handelt als intermediair of telecommunicatie dienstverlener met betrekking tot dat data bericht.

Bindende werking
Artikel 3. Deze Wet bindt de Staat.

Geen verplichting om een document of informatie in elektronische vorm te accepteren of te verzenden

Artikel 4. Ondanks artikel 3, zal niets in deze Wet op zichzelf afdwingen dat een overheidslichaam elk document of informatie in een elektronische vastlegging accepteert of publiceert.

Artikel 5. Deze Wet is consistent geconstrueerd conform haar doelstellingen en is commercieel aanvaardbaar geacht conform de omstandigheden bij het opstellen van de wet. De Wet geeft inhoud aan de volgende doelen:

1. faciliteren van elektronische transacties;

2. faciliteren van elektronische handelsactiviteiten (e-commerce), elimineren van barrières bij e-commerce als gevolg van onzekerheden omtrent schriftelijke en handtekening vereisten en om de ontwikkeling van de wettelijke en zakelijke infrastructuur te promoten dat nodig is voor de implementatie van een veilige e-commerce omgeving;

3. faciliteren van elektronisch bewaren en opslaan van document bij overheidsinstanties en het promoten van een efficiënte dienstverlening van overheidslichamen door middel van betrouwbare elektronische vastleggingen;

4. helpen bij het tot stand brengen van uniforme regels, regelgeving en standaarden met betrekking tot authenticatie en integriteit van elektronische vastleggingen; en

5. promoten van het vertrouwen van de overheid in de integriteit en betrouwbaarheid van elektronische vastleggingen en e-commerce, en het aanmoedigen van de ontwikkeling van e-commerce door het gebruik van elektronische handtekeningen bij het verschaffen van authenticiteit en integriteit bij het corresponderen van elke elektronisch medium.

Ontoepasselijkheid van de Wet

Artikel 6. De hoofdstukken II, III en IV van deze Wet zal niet van toepassing zijn bij de hieronder beschreven situaties, waar bij wet een uitgeschreven handtekening van de originele documenten nodig is:

(a) het maken, uitvoering geven aan of herroepen van een testament of testamentaire instrument;
(b) de overdrachtsakte van onroerend of roerende goederen bij de overdracht van elk belang in onroerend of roerende goederen;
(c) de creatie, uitvoering of bekrachtiging van een gezegeld contract, trustakte of machtigingsverklaring;
(d) de creatie van documenten met betrekking tot immigratie, burgerschap of zaken die de paspoorten betreffen; of
(e) de erkenning of bekrachtiging van handelspapieren.

Vrijwillig gebruik van elektronische transacties

Artikel 7.
(1) Deze Wet vereist niet dat een persoon die gebruik maakt van, voorziet, accepteert of het volgende bewaart:

(a) documenten;

(b) vastleggingen; of

(c) informatie,

te gebruiken, voorzien in, accepteren of bewaren in deze elektronische vorm.

(2) Ondanks lid (1), met betrekking tot partijen rond een transactie, mag de acceptatie van elke partij worden geconcludeerd uit historisch gebruik ('past conduct') voor het gebruikmaken, voorzien, accepteren of bewaren van documenten, vastleggingen van informatie in elektronische vorm in het proces van de transactie.

Hoofdstuk II
Vereisten voor juridische erkenning

Juridische erkenning van elektronische transacties

Artikel 8. Informatie uit een vastlegging in een elektronische vorm of een data bericht zal niet worden genegeerd voor juridische voltrekking, aanvaardbaarheid of bekrachtiging uitsluitend op de volgende gronden, waarbij:

(a) het overhandigen of beschikbaar maken in elektronische vorm; of
(b) het niet opgenomen in de informatie, data bericht of vastlegging in elektronische vorm met de bedoeling om juridisch invloed te hebben, maar dat refereert naar die informatie, data bericht of vastlegging.

Op schrift

Artikel 9. Het wettelijke vereiste dat informatie, een vastlegging van een data bericht op schrift moet zijn, daar waar de informatie, vastlegging of data bericht wordt gepresenteerd in elektronische vorm, of dat de informatie, vastlegging of data bericht toegankelijk is of in staat is voor behoud als mogelijke referentie.

Voorziening omtrent informatie

Artikel 10.
(1) Het wettelijke vereiste is voldaan indien informatie, een vastlegging of een data bericht is geleverd of verzonden naar een persoon door middel van het leveren of verzenden van de informatie, vastlegging of data bericht op een elektronisch wijze.

(2) Voor het doel van deze wet, wordt informatie of een vastlegging in elektronische vorm of een data bericht geacht niet zijn verschaft of verzonden naar een persoon indien het slechts beschikbaar en toegankelijk is gemaakt aan die persoon, maar welke niet in staat is om de informatie op te slaan.

Specifieke niet-elektronische vorm

Artikel 11.
Indien een wet informatie, een vastlegging of een data bericht vereist dat in een specifieke niet-elektronische vorm wordt gepresenteerd, is aan dit vereiste voldaan als de informatie of vastlegging in elektronische vorm of het data bericht:

(a) in wezen dezelfde informatie bevat; en
(b) toegankelijk is en op te slaan zodat het gebruikt kan worden ter referentie.

Originele vorm

Artikel 12.
(1) Waar een wet informatie, vastlegging of data bericht vereist dat in een originele vorm wordt gepresenteerd, wordt aan die vereiste voldaan indien de informatie, vastlegging of data bericht wordt gepresenteerd in een elektronische vorm waarbij:

(a) er een betrouwbare zekerheid ('reliable assurance') bestaat voor het behoud van de integriteit van de informatie of vastlegging in elektronische vorm of de data bericht door de persoon die de informatie presenteert; en
(b) hetgeen dat wordt gepresenteerd aan een persoon, de informatie, vastlegging in elektronische vorm of de data bericht in elektronische vorm toegankelijk is of bewaard kan worden ter referentie.

(2) Het criterium voor beoordeling van de integriteit onder lid (1) zal zijn of de informatie of vastlegging in elektronische vorm of een data bericht compleet en onveranderd is gebleven, waarbij elke verandering is meegenomen als gevolg van de normale gang van zaken bij communicatie, opslag en weergave.

(3)Betrouwbaarheid onder lid (1) zal worden bepaald in het licht van alle omstandigheden, inclusief het doel waarvoor de informatie of vastlegging in elektronische vorm of de data bericht was gecreëerd.

Behoud van informatie, data berichten of vastleggingen in elektronische vorm

Artikel 13. Indien een wet vereist dat bepaalde informatie, vastleggingen of data berichten worden bewaard, wordt aan die vereiste voldaan indien bewaring plaatsvindt van de informatie, data berichten of vastleggingen in elektronische vorm.

Mogelijkheid om informatie, een data bericht of een vastlegging te bewaren

Artikel 14. Informatie of vastleggingen in elektronische vorm of een data bericht wordt geacht niet te kunnen worden bewaard als de persoon die voorziet in informatie, vastlegging of data bericht, voorkomt of verhindert dat kan worden geprint, geluidsopname of video opname kan worden opgenomen door de ontvanger.

Kopieën

Artikel15. Waar informatie, een vastlegging of een data bericht is voorzien in elektronische vorm, is voldaan aan het vereiste om onder elke geschreven wet voor een of meer kopieën van de informatie, vastlegging of data bericht te voorzien van een geadresseerde op het zelfde moment van het verstrekken van een enkelvoudige kopie in elektronische vorm.

Elektronisch getekende boodschap wordt geacht het originele document te zijn

Artikel 16. Een kopie van een data bericht dat een elektronische handtekening bevat, zal geldig, uitvoerbaar en effectief worden verklaard als een document, vastlegging of andere communicatie dat een niet-elektronische handtekening bevat.

Toelaatbaarheid en het gewicht van het bewijs van elektronische vastleggingen

Artikel 17. Informatie of een vastlegging in elektronische vorm of een data bericht wordt niet ontoelaatbaar geacht als bewijs:

(a) enkel op grond dat het in elektronische vorm is; of
(b) op grond dat het niet in de originele niet-elektronische vorm is, indien het de beste bewijsvorm is.

Elektronische legalisatie

Artikel 18. Waar informatie of een handtekening, document of elektronische vastlegging is vereist door een statutaire bepaling of wetgeving, of door een contract of akte te legaliseren, erkennen, verifiëren, zal aan het vereiste te zijn voldaan, in relatie tot in relatie tot een elektronische handtekening, elektronisch document of elektronische vastlegging, de elektronische handtekening van de persoon die is geautoriseerd om deze handelingen te plegen, samen met alle andere informatie dat vereist is in andere relevante wetgeving, is toegevoegd aan of logisch geassocieerd met de elektronische handtekening, elektronisch document of elektronische vastlegging die gelegaliseerd, erkend of geverifieerd dient te worden.

Hoofdstuk III
Contractvorming en in gebrekenstelling

E-commerce

Artikel 19.
(1) E-commerce dient steeds als zodanig herkenbaar te zijn.

(2) De natuurlijke persoon of de rechtspersoon namens wie e-commerce plaatsvindt, moet in dat kader duidelijk identificeerbaar zijn.

(3) Wanneer de aanbieder van e-commerce gebruik maakt van wedstrijden en spelen, moeten deze als zodanig herkenbaar zijn, terwijl de deelnemingsvoorwaarden gemakkelijk te vervullen moeten zijn en nauwkeurig en ondubbelzinnig moeten worden voorgesteld. Het is de aanbieder van e-commerce verboden daarbij gebruik te maken van een bij wettelijk voorschrift gereguleerde wedstrijd of gereguleerd spel.

Artikel 20.
Bij staatsbesluit kunnen:
a. categorieën van e-commerce activiteiten worden aangewezen die zijn verboden;
b. categorieën van personen worden aangewezen tot wie het verboden is e-commerce te richten;
c. soorten overeenkomsten worden aangewezen die:
   1°. niet via internet of niet met behulp van een of meer met name genoemde elektronische technieken mogen worden gesloten, dan wel
   2°. ook niet via internet toegankelijk moeten blijven;
d. in het kader van e-commerce activiteiten verplichte mededelingen worden voorgeschreven;
e. nadere regels worden gesteld ten aanzien van de inhoud en aard van de e-commerce activiteiten, de aard of omvang van elektronische handel en de doelgroep.

Artikel 21.
(1) Ongevraagde e-commerce activiteiten dienen steeds duidelijk en ondubbelzinnig als zodanig herkenbaar te zijn.

(2) De ontvanger van ongevraagde e-commerce activiteiten wordt bij iedere zodanige uiting een goed herkenbare en eenvoudige mogelijkheid gegeven om bezwaar te maken tegen nieuwe uitingen. Is een zodanig bezwaar eenmaal te kennen gegeven, dan is het versturen van ongevraagde e-commerce activiteiten naar deze ontvanger verboden.

Aanbieder van e-commerce

Artikel 22.
(1) De aanbieder van e-commerce is gehouden bij zijn e-commerce activiteiten ten minste de volgende gegevens volledig en duidelijk te vermelden:
   a. de naam, plaats van vestiging en het adres van de aanbieder van e-commerce;
   b. de gegevens die een snel contact en een rechtstreekse en effectieve communicatie met de aanbieder van e-commerce mogelijk maken, met inbegrip van diens elektronische postadres;

c. waar en wanneer de aanbieder van e-commerce in het handelsregister is ingeschreven, met inbegrip van het inschrijvingsnummer, dan wel waar en wanneer de aanbieder van e-commerce op andere wijze staat geregistreerd, tenzij daarvan geen sprake is;
d. de verschillende te volgen etappes om tot een overeenkomst via internet te komen;
e. een nauwkeurige en ondubbelzinnige aanduiding van het product of de dienst, de prijs, provisie of andersoortige vergoedingen en kosten;
f. de wijze van betalen en van de levering of uitvoering;
g. de van toepassing zijnde voorwaarden waaronder, voor zover van toepassing, onder meer zijn begrepen een aanduiding van de regio waarvoor het aanbod geldt, de herroepelijkheid of onherroepelijkheid van het aanbod en de duur daarvan, de leveringstijd, de eventuele bijkomende kosten, met inbegrip van transportkosten en verzekeringspremies;
h. de overige rechten en verplichtingen van partijen, met inbegrip van opzeggings- en andere beëindigingsmogelijkheden, alsmede
i. het toepasselijke recht en de wijze van geschillenbeslechting.

(2) Wanneer dit in redelijkheid nodig is voor de uitvoering en afwikkeling van een overeenkomst via internet vermeldt de aanbieder van e-commerce voorts de naam, plaats van vestiging en het adres van zijn vertegenwoordigers in het land waar de wederpartij woont of gevestigd is.

(3) De aanbieder van e-commerce die een beroep uitoefent dat in zijn land van vestiging, en in het land waarin hij regelmatig zijn diensten verleent, door of vanwege de overheid of een semi-publiekrechtelijk lichaam, met inbegrip van een orde van beroep of soortgelijke instelling, is gereglementeerd, is voorts gehouden om informatie te verstrekken bij wie en sinds wanneer hij staat ingeschreven, alsmede een correcte omschrijving van zijn beroep en van relevante van toepassing zijnde beroepsregels, met inbegrip van een bestaande klachtprocedure.

(4) Bij of krachtens staatsbesluit kunnen nadere regels worden gesteld ter zake van de verstrekken informatie en kunnen categorieën van beroepsbeoefenaren geheel of gedeeltelijk van de in lid 3 bedoelde verplichting worden ontheven.

(5) Wanneer de aanbieder van e-commerce zich bedient van aanbiedingen, waaronder onder meer kortingen, premies en geschenken worden begrepen, dan moeten deze als zodanig herkenbaar zijn, terwijl de voorwaarden om van deze aanbiedingen gebruik te maken, gemakkelijk te vervullen moeten zijn en nauwkeurig en ondubbelzinnig moeten worden voorgesteld.

Vorming en geldigheid van contracten

Artikel 23. In de context van contractvorming:

(a) een aanbieding van of de acceptatie van een aanbieding of elke andere zaak die van belang is in de uitvoering of vorming van een contract kan worden geuit door middel van informatie of vastlegging in elektronische vorm van een data bericht; en

(b) het feit dat een transactie is uitgevoerd in elektronische vorm of die informatie of een vastlegging of de onderhandeling of vorming van een contract in elektronische vorm heeft geen invloed op de juridische werking, geldigheid of bekrachtiging.

Elektronische uiting van een aanbieding en acceptatie

Artikel 24. Tenzij partijen anderszins overeenkomen, kan een aanbieding of de acceptatie van een aanbieding of elke andere zaak die van belang is om de uitvoering of vorming van een contract mogelijk te maken, uitgedrukt worden door middel van informatie, een data bericht of een vastlegging in elektronische vorm, inclusief door een activiteit in elektronische vorm zoals het aanraken of klikken van een daarvoor bestemde icoon of plaats op de computer scherm of anderszins gecommuniceerd op een elektronische wijze dat bedoeld is om een aanbieding, acceptatie of anderszins uit te drukken.

Het gebruik van elektronische agenten voor contractvorming

Artikel 25. Een contract gevormd door een interactie van een elektronische agent en een persoon of door de interactie van elektronische agenten kan geen juridische rechtsgeldigheid en uitvoerbaarheid worden ontkend enkel op grond van dat er geen persoon beoordeelt of tussenkomt bij elk van de handelingen van de individu uitgevoerd door de elektronische agent.

Fout dat ontstaat gedurende het proces met een elektronische agent

Artikel 26.
(1) Een contract afsluiten of een transactie plegen in een elektronische omgeving met de interactie van een persoon en een elektronische agent of een andere persoon is nietig verklaard waar:

(a) de eerste verwezen persoon (‘verwezen persoon’) een materiële fout maakt in de informatie of data bericht;
(b) de elektronische agent of de tweede verwezen persoon niet de gelegenheid krijgt om de fout te voorkomen of te corrigeren;
(c) bij het constateren van de fout, de eerst verwezen persoon de tweede verwezen persoon op de hoogte stelt van de fout;
(d) de tweede verwezen persoon heeft geen redelijke stappen genomen om de fout te corrigeren; en
(e) de eerste verwezen persoon heeft niet ontvangen of niet gebruik gemaakt van elke materiële voordeel of waarde van de tweede verwezen persoon.

(2) Lid (1) zal niet van toepassing zijn bij elektronische veilingen.

Toekenning of data berichten of vastleggingen

Artikel 27. Een data bericht of vastlegging in elektronische vorm wordt toegekend aan een bepaalde persoon resulterend uit een handeling van die persoon of via een agent of elektronische agent van die persoon.

Moment van verzending van de data bericht

Artikel 28. Tenzij de verzender en geadresseerde anders overeenkomen, is informatie in elektronisch vorm van een bericht verzonden:

(a) wanneer het informatiesysteem onder de beheer van de verzender verlaat; of
(b) in het geval waar de verzender en de geadresseerde op hetzelfde informatiesysteem zijn, wanneer de informatie in elektronische vorm of data bericht beschikbaar wordt gemaakt voor ontvangst en verwerkt door de geadresseerde.

Moment van ontvangst van de data bericht

Artikel 29.
(1) Tenzij de verzender en geadresseerde anders zijn overeengekomen, waarbij informatie in elektronische vorm of een data bericht ter beschikking wordt gesteld om ontvangen te worden door een geadresseerde, wordt het geacht ontvangen te zijn door de geadresseerde:

(a) wanneer het een aangewezen informatiesysteem betreedt voor gebruik door de geadresseerde voor het doel van het ontvangen van informatie in elektronische vorm of data berichten van de verzonden type; of
(b) op het moment dat de geadresseerde bewust wordt van de informatie in elektronische vorm of data bericht in de geadresseerde's informatiesysteem, indien de geadresseerde niet heeft aangewezen of geen gebruik maakt van een informatiesysteem voor het doel van het ontvangen van informatie in elektronische vorm of data berichten van het verzonden type.

(2) Lid (1) zal van toepassing zijn ondank het feit dat die de plaats waar het informatiesysteem, dat de elektronisch adres ondersteunt, is gevestigd op een andere plaats dan waar de informatie in elektronische vorm of de data bericht wordt geacht te zijn ontvangen onder artikel 26.

Plaats van verzending en ontvangst van de data bericht

Artikel 30. Tenzij de verzender en geadresseerde anders zijn overeengekomen, wordt een data bericht geacht te zijn verzonden van de verzenders zakelijke adres en te zijn ontvangen op de geadresseerde's zakelijke adres.

Zakelijke adres

Artikel 31.
(1) Afhankelijk van lid (2) en tenzij de verzender en geadresseerde van een data bericht anders overeenkomen, wordt het zakelijke adres van elk partij geacht te zijn:

(a) het zakelijke adres dat het dichtst gerelateerd is aan de onderliggend elektronische transactie van een partij die meer dan een zakelijke adres; of
(b) als er geen onderliggende elektronische transactie is, dan geldt de zakelijke hoofdadres van de verzender of geadresseerde van de communicatie.

(2) Een locatie is niet een zakelijke adres enkel omdat die locatie is:

(a) waar apparatuur en technologie die een informatiesysteem ondersteunen, gebruikt worden door een partij in relatie tot de vorming van een contract zijn gelegen; of
(b) waar het informatiesysteem kan worden betreden door andere partijen.

(3) Het enkele feit dat een partij gebruik maakt van een domeinnaam of een e-mail adres dat verbonden is met een specifieke land, kan niet hieruit worden verondersteld dat het zakelijk adres is gelegen in dat land.

Gebruikelijke residentie

Artikel 32. Als de verzender of geadresseerde van een data bericht geen zakelijke adres heeft, dan de gebruikelijke residentie ('habitual residence') van de verzender of geadresseerde is de relevante criteria voor de plaats van verzending en ontvangst van het data bericht.

Aansprakelijkheid van de dienstenaanbieder van e-commerce

Artikel 33.
(1) Een dienstenaanbieder van e-commerce is niet aansprakelijk voor de inhoud van e-commerce of andere informatie die door zijn tussenkomst via internet wordt verzonden of opgeslagen, op voorwaarde dat hij:

a. niet degene is van wie de informatie stamt;
b. de ontvanger van de informatie niet heeft geselecteerd;
c. de doorgegeven informatie niet heeft geselecteerd noch gewijzigd;
d. niet daadwerkelijk kennis ervan heeft dat de informatie onwettig is of onwettige activiteiten betreft, en
e. geen verbod overtreedt door zijn diensten aan te bieden.

(2) Een dienstenaanbieder van e-commerce is gehouden om informatie te verwijderen of de toegang daartoe onmogelijk te maken, zodra hem door of namens de Minister de verwijdering van de informatie is gelast of de toegang daartoe is verboden, alsmede wanneer het hem duidelijk moet zijn dat deze informatie onwettig is of onwettige activiteiten betreft.

(3) De Minister kan de in lid (2) bedoelde verwijdering slechts gelasten en de toegang slechts verbieden, wanneer de informatie onwettig is of onwettige activiteiten betreft, of in strijd is met de openbare orde en goede zeden dan wel wanneer het algemeen belang of de veiligheid van Suriname dat bepaaldelijk vordert.

Hoofdstuk IV
Elektronische handtekening

Elektronische handtekening

Artikel 34. Partijen in een elektronische transactie kunnen met elkaar overeenkomen door gebruik te maken van een bepaalde methode of vorm van een elektronische handtekening, tenzij anderszins bepaald door een wet.

Minimum standaarden voor wettelijk vereiste handtekeningen

Artikel 35.Waar een geschreven wet vereist dat de handtekening van een persoon, is aan die vereiste voldaan bij een elektronische vastlegging of data bericht door het gebruik van een elektronische handtekening die voldoet aan de minimum standaarden voor betrouwbaarheid en integriteit of conform de standaard welke de partijen overeen zijn gekomen door een contract.

Betrouwbaarheid en integriteit van elektronische handtekeningen

Artikel 36.
(1) De criteria die zal worden gebruikt om de betrouwbaarheid en integriteit van een elektronische handtekening vast te stellen, omvatten:

(a) de authenticatie technologie op een unieke wijze de gebruiker koppelt aan de handtekening;
(b) de handtekening is in staat om de gebruiker te identificeren;
(c) de handtekening is gecreëerd door gebruik te maken van een middel dat uitsluitend onder beheer staat van de gebruiker;

(d) de handtekening wordt gekoppeld aan de informatie waar het op betrekking heeft op een zodanige wijze dat elke opvolgende verandering in de informatie detecteerbaar is;
(e) zulk andere criteria zoals voorgeschreven door regelgeving.

(2) Informatie of een vastlegging in elektronische vorm of een data bericht die is getekend met een elektronische handtekening die voldoet aan de betrouwbaarheid criteria zoals gesteld in lid (1) wordt geacht to onveranderd te zijn op het moment van ondertekening.

(3) De Elektronische authenticatie producten waar verwezen wordt naar in de schema [nog te bepalen door de overheid] zijnde producten die kunnen worden gebruikt voor het valideren van een elektronische handtekening onder lid (1).

(4) De Minister mag het schema bij staatsbesluit veranderen.

Elektronische handtekening dat geassocieerd is met een geaccrediteerde elektronische authenticatie product

Artikel 37. Een elektronische handtekening die is geassocieerd met een elektronische authenticatie product uitgebracht door een Elektronische Authenticatie Dienstverlener geaccrediteerd onder hoofdstuk V (hierna verwezen naar als een "gekwalificeerde elektronische authenticatie product"), wordt geacht te zijn voldaan aan de vereisten onder artikel 36 voor betrouwbaarheid en integriteit.

Hoofdstuk V
Elektronische Authenticatie Dienstverleners

Encryptie

Artikel 38.
(1) Het gebruik van encryptietechnieken is toegestaan, op voorwaarde dat de gebruiker op wettige wijze de beschikking over deze technieken heeft verkregen en deze niet gebruikt voor onwettige activiteiten.

(2) Bij staatsbesluit kunnen nadere regels worden gesteld met betrekking tot het gebruik van encryptietechnieken, met inbegrip van regels die beogen misbruik te voorkomen.

Registratie van de Elektronische Authenticatie Dienstverlener

Artikel 39.
(1) Geen enkel persoon zal een gekwalificeerd elektronische authenticatie product uitbrengen aan de overheid tenzij geregistreerd als een geaccrediteerd Elektronische Authenticatie Dienstverlener door een aangewezen autoriteit door de Minister (hierna verwezen naar als "de aangewezen autoriteit") en heeft voorzien in de informatie voorgeschreven in deze wet.

(2) Een persoon die in strijd handelt met lid (1) begaat een overtreding.

(3) De Minister zal zoals vermeld in lid (1) voorschrijven:
(a) de bevoegdheden en functies van de aangewezen autoriteit; en
(b) elke andere zaak gerelateerd aan de aangewezen autoriteit welke de Minister nodig acht voor het doel van dit wetsartikel.

Aanvraag voor registratie

Artikel 40.
(1) Een persoon die zich wilt registreren als een geaccrediteerd Elektronische Authenticatie Dienstverlener (hierna verwezen naar als de "de inschrijver") zal zijn aanvraag doen bij de aangewezen autoriteit op de voorgeschreven manier en betaald de voorgeschreven inschrijfgeld.

(2) de aanvraag onder lid (1) zal ten minste de volgende informatie bevatten:
(a) de naam en zakelijke adres van de persoon; en
(b) bewijs van accreditatie van zijn activiteiten.

(3) Waar een inschrijver een geldige voorgaande accreditatie heeft van een andere erkende jurisdictie, zal als bewijs van accreditatie de volgende informatie nodig zijn:

(a) de naam en adres van de accreditatie autoriteit;
(b) de periode van de geldigheid van de accreditatie; en
(c) elke andere informatie vereist door vereiste regelgeving.

(4) Waar een inschrijver geen geldige voorgaande accreditatie heeft, zal hij hetzelfde aangeven aan de aangewezen autoriteit die zal vereisen dat de inschrijver onderworpen wordt aan een controle van zijn activiteiten en systemen om vast te stellen dat voldaan is aan de vereisten van artikel 41 en elke andere standaarden welke de Minister voorschrijft middels regelgeving.

(5) Waar de aangewezen autoriteit vaststelt dat de inschrijver heeft voldaan aan de vereisten van deze Wet, zal de aangewezen autoriteit een accreditatieverklaring verzenden naar de inschrijver.

(6) De Minister kan regelgeving maken waarbij de procedures voor registratie en accreditatie nader worden gespecificeerd.

Vereisten voor een Elektronische Authenticatie Dienstverlener die gekwalificeerde elektronische authenticatie producten uitbrengt

Artikel 41. Een Elektronische Authenticatie Dienstverlener die gekwalificeerde elektronisch authenticatie producten uitbrengt aan de overheid zal zijn activiteiten verrichten op een betrouwbare manier en zal:

(a) werknemers in dienst nemen die de expertise en ervaring hebben die nodig zijn voor de activiteiten, met name met betrekking tot beheer, technologie, elektronisch authenticatie en beveiligingsprocedures;

(b) bestuurlijke procedures en beheersprocedures verrichten conform de erkende standaarden;

(c) gebruikmaken van betrouwbare systemen en producten die zijn beveiligd tegen modificatie en die technische encryptiebeveiliging veilig stellen;

(d) voldoende financiële middelen hebben om activiteiten te verrichten in overeenstemming met de vereisten en elke andere voorzieningen zoals in de wet vermeld en het aansprakelijkheidsrisico draagt voor eventuele schade;

(e) veilige procedures hebben om de identiteit van de ondertekenaars te verifiëren aan wie gekwalificeerde elektronische authenticatie producten zijn uitgebracht;

(f) onderhouden van een stipt en veilig systeem voor registratie en eventueel onmiddellijke herroeping van een gekwalificeerd elektronische authenticatie product;

(g) maatregelen nemen tegen vervalsing van een gekwalificeerd elektronische authenticatie product en waar van toepassing, volledige confidentialiteit garandeert gedurende het proces van de handtekening creërende data;

(h) voldoen aan artikel 56; en

(i) voldoen aan elke andere vereisten zoals door de Minister is vastgesteld.

Toekenning van registratie

Artikel 42.
(1) Indien de aangewezen autoriteit akkoord gaat met de geldige voorgaande accreditatie van de inschrijver en voldaan is aan de vereisten van artikel 62, is de aangewezen autoriteit, die bevoegd is om de registratie toe te kennen.

(2) Indien de aangewezen autoriteit akkoord gaat met de indiening, waarbij de inschrijver geen geldige voorgaande accreditatie heeft, maar wel voldoet aan de vereisten zoals vermeld in de artikelen 34 en 35, mag de aangewezen autoriteit een bekendmaking van accreditatie naar die inschrijver versturen, en de registratie toekennen.

Erkenning of de gekwalificeerd externe Elektronische authenticatie producten

Artikel 43. De Minister mag bij staatsbesluit een gekwalificeerd elektronische authenticatie product of categorieën van gekwalificeerde elektronische authenticatieproducten, zoals uitgebracht door Elektronisch Authenticatie Dienstverleners van categorieën van Elektronische Authenticatie Dienstverleners die gevestigd zijn in een andere jurisdictie, erkennen als gekwalificeerde elektronische authenticatie producten in Suriname.

Registratie van Elektronische Authenticatie Dienstverleners

Artikel 44. De aangewezen autoriteit zal een overheidsregistratie bijhouden van geaccrediteerde Elektronische Authenticatie Dienstverleners die informatie omvat zoals vereist door de Minister.

Herziene notificatie van naleving van wetgeving

Artikel 45. Een geregistreerde Elektronische Authenticatie Dienstverlener die gekwalificeerde elektronische authenticatie producten uitbrengt zal jaarlijks de aangewezen autoriteit voorzien met een herziene notificatie van het naleven van de vereisten van artikel 41 en betaalt het voorgeschreven honorarium.

Controle door de aangewezen autoriteit

Artikel 46.
(1) De aangewezen autoriteit mag een controle verrichten om te verifiëren of de Elektronische Authenticatie Dienstverlener heeft voldaan aan de vereisten van deze wet.

(2) Bij de uitvoering van de controle, mag de aangewezen autoriteit deskundigen in dienst nemen die zij nodig acht.

Verantwoordelijkheid om mee te werken aan de controle

Artikel 47. Van een Elektronische Authenticatie Dienstverlener wordt medewerking verwacht en alle redelijk geachte assistentie bij de controle door de aangewezen autoriteit en zal de nodige informatie beschikbaar stellen aan de aangewezen autoriteit om te voldoen aan de vereisten van deze wet.

Geheimhouding

Artikel 48.
Een ieder die betrokken is bij de uitvoering van deze wet en daarbij de beschikking krijgt over gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden en voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding daarvan behoudens voor enig wettelijk voorschrift hem tot bekendmaking verplicht of uit zijn taak bij de uitvoering van deze wet de noodzaak tot bekendmaking voortvloeit.

Bevoegdheid van de aangewezen autoriteit indien niet voldaan wordt aan de vereisten

Artikel 49. Waar de aangewezen autoriteit van mening is dat een Elektronische Authenticatie Dienstverlener niet langer voldoet aan de vereisten om gekwalificeerde elektronische authenticatie producten uit te brengen, mag hij/zij:

(a) de accreditatie van de Elektronische Authenticatie Dienstverlener annuleren;

(b) verordenen dat de Elektronische Authenticatie Dienstverlener enkele of alle activiteiten stop te zetten, inclusief het stopzetten van het uitreiken van gekwalificeerde elektronische authenticatie producten;

(c) verordenen dat de Elektronische Authenticatie Dienstverlener verwijderd wordt van de registratie;

(d) elke actie neemt die redelijk wordt geacht om vast te stellen dat de Elektronische Authenticatie Dienstverlener in overeenstemming handelt met de vereisten zoals vastgelegd in artikel 41; of

(e) geeft elke andere opdracht die de aangewezen autoriteit redelijk acht in de omstandigheden inclusief, maar niet gelimiteerd tot, het schadeloosstellen van de honoraria en kosten aan gebruikers van de diensten van de Elektronische Authenticatie Dienstverlener of publieke openbaarmaking van het beëindigen van de business activiteiten.

Pseudoniemen

Artikel 50. Een Elektronische Authenticatie Dienstverlener mag, op verzoek van een bepaalde ondertekenaar, in de relevante elektronische authenticatie product een pseudoniem opnemen in plaats van de naam van ondertekenaar.

Additionele verantwoordelijkheden van een Elektronische Authenticatie Dienstverlener

Artikel 51. Een Elektronische Authenticatie Dienstverlener zal de uitvoering van een tijdige en veilige bestand verzekeren van houders van elektronische authenticatie producten en een onmiddellijke herroeping dienst aanbieden dat het mogelijk maakt om zich te verzekeren:

(a) dat een gekwalificeerd elektronische authenticatie product was ingetrokken;
(b) de geldigheidsperiode van de gekwalificeerde elektronische authenticatie product; of
(c) dat de gekwalificeerd elektronische authenticatie product geen enkele beperkingen bevat op de reikwijdte van de waarde van de elektronische transacties voor welke de handtekening kan worden gebruikt.

Onmiddellijke herroeping op verzoek

Artikel 52.
(1) Een Elektronische Authenticatie Dienstverlener zal een elektronische authenticatie product onmiddellijk intrekken op verzoek van een ondertekenaar of als anderszins is gerechtvaardigd in de gegeven omstandigheden.

(2) Een Elektronische Authenticatie Dienstverlener zal garanderen dat de datum en tijd wanneer een elektronische authenticatie product is ingetrokken exact kan worden bepaald.

Aansprakelijkheid van de Elektronische Authenticatie Dienstverlener

Artikel 53.
(1) Een Elektronische Authenticatie Dienstverlener is, tenzij hij bewijst dat hij niet nalatig heeft gehandeld, aansprakelijk voor schade die natuurlijke of rechtspersonen die in redelijkheid op een door de Elektronische Authenticatie Dienstverlener afgegeven elektronische authenticatie product vertrouwen ondervinden, in samenhang met:

a. de juistheid, op het tijdstip van afgifte, van alle gegevens in het elektronische authenticatie product en de opneming in een elektronische authenticatie product van alle voor een dergelijk elektronische authenticatie product voorgeschreven gegevens;

b. de garantie dat de in het elektronische authenticatie product geïdentificeerde ondertekenaar, op het tijdstip van afgifte van het elektronische authenticatie product, houder was van de gegevens voor het aanmaken van de handtekening, die met de in het elektronische authenticatie product gegeven of geïdentificeerde gegevens voor het verifiëren van een handtekening overeenstemmen;

c. de garantie dat de gegevens voor het aanmaken van de handtekening en die voor het verifiëren van de handtekening, ingeval zij beide door de Elektronische Authenticatie Dienstverlener worden gegenereerd, complementair kunnen worden gebruikt.

(2) Een Elektronische Authenticatie Dienstverlener is, tenzij hij bewijst dat hij niet nalatig heeft gehandeld, voorts aansprakelijk voor schade die bij natuurlijke of rechtspersonen die in redelijkheid op een door de Elektronische Authenticatie Dienstverlener afgegeven elektronische authenticatie product hebben vertrouwd, is ontstaan doordat de intrekking van het elektronische authenticatie product niet werd geregistreerd.

(3) Een Elektronische Authenticatie Dienstverlener is niet aansprakelijk voor schade die voortvloeit uit het gebruik van een elektronische authenticatie product, waarbij de door de elektronische authenticatie productdienstverlener op het elektronische authenticatie product aangegeven beperkingen, mits die voor derden kenbaar zijn, worden overschreden.

Ontheffing van aansprakelijkheid

Artikel 54.
(1) Een Elektronische Authenticatie Dienstverlener die een gekwalificeerd elektronische authenticatie product brengt kan worden vrijgesteld van aansprakelijkheid als de provider kan aantonen dat de schade of verlies niet was veroorzaakt door zijn eigen nalatigheid.

(2) De Elektronische Authenticatie Dienstverlener is ook niet aansprakelijk voor schade voor of verlies als gevolg van het gebruik van een gekwalificeerde elektronische authenticatie product in overtreding met de beperkingen van het gebruik of reikwijdte van de transactie dat duidelijk is omschreven in de gekwalificeerd elektronische authenticatie product.

(3) Dit artikel ook van toepassing op een Elektronische Authenticatie Dienstverlener die garandeert dat de elektronische authenticatie product van een andere aanbieder is gekwalificeerd.

Kosten van een controle

Artikel 55. De aangewezen autoriteit mag eisen dat een Elektronische Authenticatie Dienstverlener de kosten betaald die redelijkerwijs zijn ontstaan bij de uitvoering van de controle conform artikel 46.

Hoofdstuk VI
Intermediairs en telecommunicatie dienstverleners

Aansprakelijkheid van intermediairs en telecommunicatie dienstverleners

Artikel 56.
(1) Een intermediair of telecommunicatie dienstverlener die enkel voorziet in een transmissielijn voor data berichten, vastleggingen of informatie in elektronische vorm zal niet aansprakelijk worden gesteld voor de inhoud van de data berichten, vastleggingen of informatie in elektronische vorm als de intermediair of telecommunicatie dienstverlener geen feitelijke kennis heeft of niet bewust is van feiten die een verstandige persoon, met een mogelijke strafrechtelijke aansprakelijkheid of aansprakelijkheid voor een onrechtmatige daad met betrekking tot materiaal dat op het netwerk van een intermediair of telecommunicatie dienstverlener van wie, bij het verkrijgen van de feitelijke kennis of bewustwording van zulke feiten, de procedures volgt zoals vereist in artikel 57.

(2) Niets in dit artikel ontlast een intermediair of telecommunicatie dienstverlener van het voldoen aan elke gerechtelijk bevel, injunctie, exploot, wettelijke vereiste of contractuele verplichting in relatie tot data berichten, vastleggingen of informatie in elektronische vorm.

(3) Van een intermediair of telecommunicatie dienstverlener wordt niet verwacht dat elke data bericht dat door middel van haar systeem is verwerkt, wordt doorgelicht om te verifiëren of de verwerking, anders dan dit artikel, kan leiden tot een delict of civielrechtelijke aansprakelijkheid.

(4) Een intermediair of een telecommunicatie dienstverlener, gedurende een controle, zal niet aansprakelijk zijn voor:

(a) de schending van auteursrechten bij werkzaamheden of andere objectzaken waarop auteursrechten berust; of

(b) het ongeautoriseerd gebruik van openbare voorstellingen, waarvan de duur van auteursrechtelijke periode niet is overschreden.

Artikel 57.
(1) Als een intermediair of telecommunicatie dienstverlener feitelijke kennis heeft van informatie in een data bericht of een elektronische vastlegging dat aanleiding geeft tot een civielrechtelijke of strafrechtelijke aansprakelijkheid dan, zo snel als praktisch haalbaar na het verkrijgen van de kennis, zal de intermediair of telecommunicatie dienstverlener:

(a) de informatie verwijderen en veiligstellen van elke informatiesysteem in het beheer van de intermediair of telecommunicatie dienstverlener en stopt met het voorzien van diensten met betrekking tot die informatie of neemt elke andere actie als door de wet voorgeschreven of conform de gevestigde gedragscode; en

(a) in geval van strafrechtelijke aansprakelijkheid, wordt de verantwoordelijke weetshandhavende autoriteit op de hoogte gesteld van de relevant feiten en van de identiteit van de persoon voor wie de intermediair of telecommunicatie dienstverlener diensten levert met betrekking tot de informatie, zoals de identiteit van die persoon die bekend is bij de intermediair of telecommunicatie dienstverlener.

(2) Een intermediair of telecommunicatie dienstverlener is niet aansprakelijk, hetzij in een contract, onrechtmatige daad, onder een statuut of anderszins, naar elke persoon, inclusief elke persoon namens wie de intermediair of telecommunicatie dienstverlener diensten verleent, met betrekking tot informatie in een data bericht of een elektronische vastlegging, voor elke handeling die de intermediair of telecommunicatie dienstverlener neemt, in goed vertrouwen, bij het uitoefenen van de bevoegdheden zoals verleend in dit artikel.

(3) Elke persoon die een notificatie van onwettelijke activiteiten onderbrengt bij een intermediair of telecommunicatie dienstverlener, en op hoogte is dat het materieel feiten verkeerd weergeeft, begaat een overtreding en is aansprakelijk voor schade voor het onterecht verwijderen van de informatie in een data bericht of elektronische vastlegging onder lid (1).

Gedragcodes en dienstverleningstandaarden voor intermediairs en telecommunicatie dienstverleners

Artikel 58.
(1) De Minister mag gedragcodes en standaarden voor intermediairs en telecommunicatie dienstverleners ontwikkelen ter verduidelijking van deze wet.

(2)Waar de Minister een gedragscode of dienstverleningstandaarden heeft ontwikkeld voor intermediairs en telecommunicatie dienstverleners, zullen laatstgenoemden dienen te voldoen aan deze gedragscodes of dienstverleningsstandaarden.

(3) Naleving van de relevante gedragscodes en dienstverleningsstandaarden kunnen meegenomen worden door het gerechtshof bij het bepalen van aansprakelijkheid.

Hoofdstuk VII
Overheid en andere overheidsinstanties

Algemene volmacht ('general authorization')

Artikel 59.
(1) Een overheidslichaam dat conform de wetgeving:
- (a) de archivering van documenten accepteert of informatie in welke vorm dan ook verkrijgt;
- (b) vereist dat die documenten worden gecreëerd of bewaard;
- (c) vereist documenten, vastleggingen of informatie dat voorzien of bewaard wordt in de originele vorm; of
- (d) elke vergunning, licentie of goedkeuring uitbrengt, mag ondanks het tegendeel in betreffende wet, betreffende functie uitoefenen door elektronische wijze;

(2) Waar een overheidslichaam besluit om elke van de functies in lid (1) door elektronisch wijze te verrichten, mag de overheidslichaam specificeren:
- (a) de wijze en formaat in welke documenten, vastleggingen of informatie in elektronische vorm zal worden gearchiveerd, gecreëerd, bewaard, uitgebracht of geleverd;
- (b) de wijze en formaat in welke handtekening zal worden toegevoegd aan de documenten, vastlegging of informatie in elektronische vorm, en de identiteit of criteria die zal worden gehanteerd door de Elektronische Authenticatie Dienstverlener en gebruikt door de persoon voor het archiveren van de document;

(c) Zulke beheersingsprocessen en procedures als nodig om het volgende te garanderen integriteit, veiligheid en vertrouwelijkheid van documenten, vastlegging van informatie in elektronische vorm; of
(d) elke andere vereiste attributen voor documenten, vastlegging van informatie in elektronische vorm die gangbaar zijn en gespecificeerd voor gerelateerde papieren documenten.

(3) Indien bij een document, vastlegging of informatie in elektronische vorm onder lid (2) vereist is te ondertekenen, kan de Minister door regelgeving specificeren welke type handtekening vereist is, inclusief, waar van toepassing, het vereiste van type versleutelde elektronische handtekening die de verzender kan gebruiken.

(4) Ter voorkoming van twijfel, doordat het tegendeel blijkt uit wetgeving, maar nader gespecificeerd is volgens lid (2), is elke persoon vereist om bij wet:
(a) elke document op te slaan met of voorzien van informatie in elke vorm gerelateerd aan een overheidslichaam;
(b) creëren of bewaren van elke document voor een overheidslichaam;
(c) gebruikmaken van een voorgeschreven vorm voor een aanvraag of notificatie van of andere transactie met een overheidslichaam;
(d) voorzien van of bewaren voor een overheidslichaam van elke document, vastlegging of informatie in de originele vorm; of
(e) houden van een licentie, vergunning of andere goedkeuring van een overheidslichaam, welke vereiste is voldaan door een document, vastlegging of informatie in elektronische vorm, hetgeen is gespecificeerd door de overheidslichaam voor dat doel.

Documenten voor inspectie

Artikel 60. Waar documenten, vastleggingen of informatie zijn vereist bij wet beschikbaar moeten zijn voor inspectie, kan voldaan worden aan dit vereiste door deze documenten, vastleggingen of informatie voor inspectie ter beschikking te stellen in elektronische vorm.

Hoofdstuk VIII
Consumentenbescherming

Minimum aan informatie in e-commerce

Artikel 61.
(1) Een persoon die gebruik maakt van een elektronisch middel om goederen of diensten te verkopen aan consumenten zal voorzien in accurate, duidelijke en toegankelijke informatie over hun organisatie, voldoende om toe te staan dat:
(a) de juridische naam van de persoon, zijn geografische hoofdadres, en elektronisch contactgegevens en telefoonnummer;
(b) tijdige, eenvoudige en effectieve communicatiemogelijkheden tussen de consument en de verkoper; en
(c) hulpverlening bij het juridische proces.

(2) Een persoon die gebruik maakt van een elektronisch middel om goederen of diensten te verkopen aan consumenten zal voorzien in accurate en toegankelijke informatie die de goederen of diensten beschrijven, voldoende om de consumenten in staat te stellen om een goed geïnformeerde beslissing te kunnen maken over de voorgestelde transactie en een adequate vastlegging van de informatie te kunnen bewaren.

(3) Een persoon die gebruik maakt van een elektronisch middel om goederen of diensten te verkopen aan consumenten zal voordat tot het finaliseren van de elektronisch contract wordt besloten op basis van een dergelijke transactie, de volgende informatie verschaffen aan de consumenten met betrekking tot de elektronische contract:

(a) de voorwaarden, condities en betalingsmethoden;
(b) de details van, en condities en beleid met betrekking tot privé gegevens, terugtrekking, beëindiging, terugbrengen, ruilen, annuleren of restituties.
(c) de leveringsafspraken of voorwaarden voor uitvoering van diensten; en
(d) een kopie van het contract voor de consument in een formaat dat kan worden bewaard.

Minimum aan informatie met betrekking tot authenticatie producten

Artikel 62. Voordat een elektronisch contract wordt overeengekomen dat een gekwalificeerd elektronische authenticatie product vereist, zal een Elektronische Authenticatie Dienstverlener het volgende op schrift informeren aan de partij, die vraagt om de elektronische authenticatie product:

(a) de voorwaarden en condities met betrekking tot het gebruik van de elektronische authenticatie product, inclusief eventuele beperkingen op de reikwijdte van de bedragen;

(b) elke vereiste met betrekking tot opslag en bescherming van de handtekeningcreërende data door de ondertekenaar;

(c) de kosten voor het verkrijgen en gebruiken van de elektronische authenticatie product en of gebruik van de andere diensten van de Elektronische Authenticatie Dienstverlener;

(d) of de Elektronische Authenticatie Dienstverlener is geaccrediteerd; en

(e) procedure voor klachtenafhandeling.

Recht op intrekking

Artikel 63. Een consument die niet is voorzien in de informatie die is vereist volgens artikelen 61 en 62 heeft het recht op intrekking van de contract binnen dertig kalenderdagen behoudens dat de consument geen enkel materieel voordeel heeft ontvangen als gevolg van de transactie.

Ongevraagde communicatie

Artikel 64.
(1) Elke persoon die ongevraagde e-commerce uitingen verzend via een elektronisch medium naar consumenten in Suriname of bewust gebruik maakt van een intermediair of een telecommunicatie dienstverlener in Suriname om te verzenden of die een zakelijke adres heeft in Suriname en ongevraagde elektronisch correspondentie verzendt naar consumenten, zal de consument met een duidelijk gespecificeerd en eenvoudig te activeren optie geven om in de toekomst geen commerciële uitingen te ontvangen.

(2) Een persoon die zich niet houdt aan lid (1) begaat een overtreding.

Bescherming vertrouwelijkheid en privacy

Artikel 65.
(1) Persoonsgegevens die door een aanbieder van e-commerce worden verkregen mogen slechts worden verwerkt voor:

a. dit is gerechtvaardigd in het kader van de normale bedrijfsvoering;
b. dit voor de betrokkene duidelijk is;
c. de gegevens ter zake dienend en niet bovenmatig zijn voor het tot stand komen van overeenkomsten via internet;
d. de gegevens juist, volledig en op rechtmatige wijze verkregen zijn, en
e. de verwerking rechtmatig plaatsvindt.

(2) Het is verboden persoonsgegevens zonder uitdrukkelijke instemming van de betrokkene aan derden te verstrekken, tenzij dat geschiedt op grond van een wettelijke verplichting.

(3) Persoonsgegevens waarvan de opslag met het oog op reeds aangegane of mogelijk nog aan te gane overeenkomsten via internet niet meer nodig is worden geanonimiseerd of vernietigd.

(4) Bij staatsbesluit kunnen nadere regels worden gesteld die de opslag, verwerking, het doorgeven, de anonimisering, de vernietiging van persoonsgegevens en de inzage door de betrokkene betreffen.

Vertrouwelijke behandeling

Artikel 66.
(1) De informatie die een aanbieder van e-commerce ontvangt en waarvan hij weet of redelijkerwijs kan weten dat deze als vertrouwelijk behandeld dient te worden, zal als zodanig worden behandeld.

(2) Voor zover nodig en mogelijk zal een aanbieder van e-commerce of dienstenaanbieder duidelijk en ondubbelzinnig kenbaar maken wanneer aan het versturen van informatie met behulp van door hem gebruikte of ter beschikking gestelde elektronische technieken bijzondere risico's voor het handhaven van de vertrouwelijkheid verbonden zijn.

(3) Bij staatsbesluit kunnen nadere regels worden gesteld met betrekking tot het waarborgen van de vertrouwelijkheid van de informatie als bedoeld in lid 1.

Hoofdstuk IX
Overtredingen en wetshandhaving

Valse of misleidende informatie

Artikel 67.
Een persoon die:

(a) informatie indient dat vereist is onder deze wet die valse of misleidende informatie bevat; of
(b) een consument of een gebruiker van een elektronische authenticatie product voorziet met valse of misleidende informatie, begaat een overtreding.

Obstructie van een controle

Artikel 68.
Een persoon die, met betrekking tot een uitgevoerde controle conform artikel 46
(a) bewust valse of misleidende verklaringen aflegt, al dan niet mondeling of in schrift naar de personen die de controle verrichten; of
(b) anderszins de personen belemmeren die de controle uitvoeren uit hoofde van hun functies en bevoegdheden, begaan een overtreding.

Doorbreking van verplichtingen van vertrouwelijkheid

Artikel 69. Een persoon die de vertrouwelijkheid (privacy) verplichtingen doorbreekt begaat volgens artikel 48 een overtreding.

Buitengerechtelijke geschillenbeslechting

Artikel 70.
(1) Bij staatsbesluit kan een college voor buitengerechtelijke beslechting van geschillen in het leven worden geroepen, onder daarin te bepalen regels, voorwaarden en procedures, met inbegrip van beslechting met behulp van daartoe geëigende elektronische technieken.

(2) Partijen kunnen zich voor de beslechting van hun geschillen onderwerpen aan het college, bedoeld in lid 1, wanneer deze geschillen betrekking hebben op e-commerce, aansprakelijkheid van de dienstenaanbieder, bescherming van de vertrouwelijkheid en privacy, alsmede certificaten en certificatiedienstverleners.

(3) Bij staatsbesluit kunnen ook andere categorieën van geschillen worden aangewezen, waarvan de beslechting aan het in lid 1 bedoelde college kunnen worden voorgelegd.

Toezicht en opsporing

Artikel 71.
(1) Met het toezicht op de naleving van het bij of krachtens deze wet bepaalde zijn belast de daartoe bij staatsbesluit aangewezen ambtenaren of personen. Een zodanige aanwijzing wordt bekendgemaakt in het blad waarin van overheidswege de officiële berichten worden geplaatst.

(2) De krachtens lid 1 aangewezen ambtenaren en personen zijn, uitsluitend voor dat voor de vervulling van hun taak redelijkerwijze noodzakelijk is, bevoegd:
a. alle inlichtingen te vragen;
b. inzage te verlangen van alle boeken, bescheiden en andere informatiedragers en daarvan afschrift te nemen of deze daartoe tijdelijk mee te nemen;
c. goederen aan opneming en onderzoek te onderwerpen, deze daartoe tijdelijk mee te nemen en daarvan monsters te nemen;
d. alle plaatsen met uitzondering van woningen zonder de uitdrukkelijke toestemming van de bewoner te betreden, eventueel vergezeld van door hen aangewezen personen;
e. woningen of tot woning bestemde gedeelten van vaartuigen zonder de uitdrukkelijke toestemming van de bewoner binnen te treden.

(3) Zo nodig, wordt de toegang tot een plaats als bedoeld in lid 2, onderdeel d, verschaft met behulp van de sterke arm.

(4) Op het binnentreden van woningen of van tot woning bestemde gedeelten van vaartuigen als bedoeld in lid 2, onderdeel e, is de vijfde afdeling van Titel IV van het Wetboek van Strafvordering van overeenkomstige toepassing, met dien verstande dat de last wordt verleend door de Procureur-generaal.

(5) Een ieder is verplicht aan de toezichthouder alle medewerking te verlenen die op grond van lid 2 wordt gevorderd.

(6) Zij die uit hoofde van ambt, beroep of wettelijk voorschrift verplicht zijn tot geheimhouding, kunnen het verlenen van medewerking weigeren, voor dit uit hun geheimhoudingsplicht voortvloeit.

Legitimatie bij taakuitoefening van de toezichthouders

Artikel 72.
(1) Bij de uitoefening van hun taak dragen de toezichthouders een door de Minister te verstrekken legitimatiebewijs bij zich.

(2) Desgevraagd tonen zij hun legitimatiebewijs aanstonds.

(3) Het legitimatiebewijs bevat een foto van de toezichthouder en vermeldt in ieder geval diens naam en hoedanigheid.

(4) Bij staatsbesluit kunnen regels worden gesteld met betrekking tot de wijze van taakuitoefening van de toezichthouders.

Opsporingsambtenaren

Artikel 73.
(1) Met de opsporing van de strafbaar gestelde feiten zijn, naast de in het Wetboek van Strafvordering bedoelde opsporingsambtenaren, belast de daartoe bij staatsbesluit aangewezen personen. Een zodanige aanwijzing wordt bekendgemaakt in het blad waarin van overheidswege de officiële berichten worden geplaatst.

(2) Bij staatsbesluit kunnen regels worden gesteld omtrent de vereisten waaraan de ingevolge lid (1) aangewezen personen dienen te voldoen.

Plichten van de leden van de raad van commissarissen en directie

Artikel 74. Elke toezichthouder en directeur van een rechtspersoon zal elke redelijke zorg nemen om te garanderen dat de organisatie voldoet aan:
(a) deze Wet en de bijbehorende regelgeving; en
(b) elke staatsbesluit dat is uitgevaardigd door de Minister of zijn afgevaardigde.

Aansprakelijkheid van de leden van de raad van commissarissen en directie

Artikel 75.
Wanneer een rechtspersoon overtredingen begaat onder deze wet, is elke toezichthouder, directeur of vertegenwoordiger van de rechtspersoon, die gericht, geautoriseerd, met instemming om deel te nemen bij uitvoering van de overtreding naar een partij, begaat een overtreding en is aansprakelijk voor bestraffing voor de overtreding.

Bestuursdwang

Artikel 76.
De Minister is bevoegd tot het doen wegnemen, ontruimen, beletten, in de vorige toestand herstellen of verrichten van hetgeen in strijd met de in deze wet en de daarop berustende bepalingen is of wordt gedaan, gehouden of nagelaten.

Artikel 77.
(1) Een beslissing tot toepassing van bestuursdwang wordt op schrift gesteld en geldt als een beschikking. De beschikking vermeldt welk voorschrift is overtreden.

(2) De bekendmaking ervan geschiedt aan de overtreder en andere belanghebbenden.

(3) In de beschikking wordt een termijn gesteld waarbinnen de overtreder en eventuele andere belanghebbenden de tenuitvoerlegging kunnen voorkomen door zelf de in de beschikking vermelde maatregelen te treffen. Geen termijn behoeft te worden gegund, indien de vereiste spoed zich daartegen verzet.

(4) Indien de situatie dermate spoedeisend is dat de Minister de beslissing tot toepassing van bestuursdwang niet tevoren op schrift kan stellen, zorgt de Minister alsnog zo spoedig mogelijk voor de opschriftstelling en de bekendmaking.

Artikel 78.
(1) De overtreder is de kosten verbonden aan de toepassing van bestuursdwang verschuldigd, tenzij de kosten redelijkerwijze niet of niet geheel te zijnen laste behoren te komen.

(2) De beschikking vermeldt dat de toepassing van bestuursdwang op kosten van de overtreder plaatsvindt.

(3) Indien echter de kosten geheel of gedeeltelijk niet ten laste van de overtreder zullen worden gebracht, wordt dat in de beschikking vermeld.

(4) Onder de kosten worden begrepen de kosten verbonden aan de voorbereiding van bestuursdwang, voor deze kosten zijn gemaakt na het tijdstip waarop de termijn bedoeld in artikel 77, lid (3) is verstreken.

(5) De kosten zijn ook verschuldigd indien de bestuursdwang door opheffing van de onrechtmatige situatie niet of niet volledig is uitgevoerd.

Artikel 79.
(1) De Minister kan van de overtreder bij dwangbevel de verschuldigde kosten, verhoogd met de op de invordering vallende kosten, invorderen.

(2) Het dwangbevel wordt op kosten van de overtreder bij deurwaardersexploot betekend en levert een executoriale titel op in de zin van het Wetboek van Burgerlijke Rechtsvordering.

(3) Gedurende zes weken na de dag van betekening staat verzet tegen het dwangbevel open door dagvaarding van de Staat.

(4) Het verzet schorst de tenuitvoerlegging. Op verzoek van de Staat kan de rechter de schorsing van de tenuitvoerlegging opheffen.

Artikel 80.
De kosten verbonden aan de toepassing van bestuursdwang zijn bevoorrecht op het goed ten aanzien waarvan zij zijn besteed.

Artikel 81.
Om aan een beslissing van bestuursdwang uitvoering te geven, komen de ambtenaren of personen die daartoe door de Minister zijn aangewezen, de bevoegdheden toe, genoemd in artikel 71 leden (2) en (3). Artikel 71 lid (4) is van toepassing.

Artikel 82.
Tot de bevoegdheid tot toepassing van bestuursdwang behoort het verzegelen van gebouwen, terreinen en hetgeen zich daarin of daarop bevindt.

Artikel 83.
(1) Tot de bevoegdheid tot toepassing van bestuursdwang behoort het meevoeren en opslaan van daarvoor vatbare zaken voor de toepassing van bestuursdwang dit vereist.

(2) Indien zaken zijn meegevoerd en opgeslagen, doet de Minister daarvan proces-verbaal opmaken, waarvan afschrift wordt verstrekt aan de rechthebbende.

(3) De Minister draagt zorg voor de bewaring van de opgeslagen zaken en geeft deze zaken terug aan de rechthebbende, zodra dat redelijkerwijze nodig is.

(4) De Minister is bevoegd de afgifte op te schorten totdat de verschuldigde kosten zijn voldaan. Indien de rechthebbende niet tevens de overtreder is, is de Minister bevoegd de afgifte op te schorten totdat de kosten van bewaring zijn voldaan.

(5) De Staat is niet aansprakelijk voor afgifte van het opgeslagene aan een onbevoegde.

Artikel 84.
(1) De Minister is bevoegd indien een opgeslagen zaak niet binnen dertien weken na de opslag kan worden teruggegeven aan de rechthebbende, deze te doen verkopen of, indien verkoop naar zijn oordeel niet mogelijk is, de zaak om niet aan een derde in eigendom over te dragen of te laten vernietigen.

(2) Gelijke bevoegdheid heeft de Minister ook binnen die termijn zodra de aan de toepassing van bestuursdwang verbonden kosten vermeerderd met de voor de verkoop, de eigendomsoverdracht om niet of de vernietiging geraamde kosten, in verhouding tot de waarde van de zaak onevenredig hoog worden.

(3) Verkoop, eigendomsoverdracht of vernietiging vindt niet plaats binnen twee weken na de verstrekking van het afschrift van het proces-verbaal betreffende het meevoeren en opslaan, tenzij het gevaarlijke stoffen of eerder aan bederf onderhevige stoffen betreft.

(4) Gedurende drie jaren na het tijdstip van verkoop heeft degene die op dat tijdstip rechthebbende was, recht op de opbrengst van het goed onder aftrek van de aan de toepassing van bestuursdwang verbonden kosten en de kosten van de verkoop. Indien de rechthebbende niet tevens de overtreder is, wordt van de opbrengst de kosten van bestuursdwang niet in mindering gebracht.

(5) De Staat is niet aansprakelijk voor afgifte van de opbrengst uit de verkoop aan een onbevoegde.

Artikel 85.
(1) De Minister kan in plaats van het uitoefenen van bestuursdwang aan de overtreder een last onder dwangsom opleggen.

(2) De Minister stelt de dwangsom vast hetzij op een bedrag ineens hetzij op een bedrag per tijdseenheid waarbinnen de last niet is uitgevoerd of op een bedrag per overtreding van de last. De Minister stelt tevens een bedrag vast waarboven geen dwangsom meer wordt verbeurd. Het vastgestelde bedrag van de dwangsom dient in redelijke verhouding te staan tot de zwaarte van het geschonden belang en de beoogde werking van de dwangsomoplegging.

(3)In de beschikking tot oplegging van een last onder dwangsom die strekt tot het ongedaan maken of het beëindigen wordt een termijn gesteld gedurende welke de overtreder de last kan uitvoeren zonder dat een dwangsom wordt verbeurd.

Artikel 86.
(1) Verbeurde dwangsommen komen toe aan de Staat. De Minister kan bij dwangbevel het verschuldigde bedrag invorderen.

(2) Artikel 77 leden (2), (3) en (4) is van toepassing.

Artikel 87.
(1) De Minister kan op verzoek van de overtreder de last opheffen, de looptijd ervan opschorten voor een bepaalde termijn of de dwangsom verminderen ingeval van blijvende of tijdelijke gehele of gedeeltelijke onmogelijkheid voor de overtreder om aan zijn verplichtingen te voldoen.

(2) De Minister kan op verzoek van de overtreder de last opheffen indien de beschikking een jaar van kracht is geweest zonder dat de dwangsom is verbeurd.

Artikel 88.
(1) De bevoegdheid tot invordering van verbeurde bedragen verjaart door verloop van een jaar na de dag waarop zij zijn verbeurd.

(2) De verjaring wordt gestuit door faillissement en ieder wettelijk beletsel voor invordering van de dwangsom.

Aanwijzingen

Artikel 89.
De Minister kan, wanneer de uitvoering van deze wet en de daarop berustende bepalingen dat vordert, aan een aanbieder van e-commerce of dienstenaanbieder een of meer aanwijzingen geven.

Strafbepalingen

Artikel 90.
(1) Overtreding van het in artikel 19 lid (3), artikel 21 lid (2), artikel 65 lid (2) of krachtens artikel 20 onderdelen een en b gestelde verbod, is, voor opzettelijk begaan, een misdrijf en wordt gestraft met, hetzij gevangenisstraf van ten hoogste twee jaren en geldboete van ten hoogste vijfhonderdduizend Surinaamse Dollar, hetzij met één van beide straffen.

(2) Overtreding van het in artikelen 19 lid (3), artikel 21 lid (2), artikel 65 lid (2) of krachtens artikel 20 onderdelen een en b gestelde verbod, is, voor niet opzettelijk begaan, een overtreding en wordt gestraft met, hetzij hechtenis van ten hoogste zes maanden en geldboete van ten hoogste

driehonderdduizend Surinaamse Dollar, hetzij met één van beide straffen.
(3) Handelen in strijd met de bij de bij of krachtens artikel 20 onderdelen c, d, en e, artikel 22 leden (1), (3) en (4), artikel 33 lid (2), artikel 65 leden (3) en (4), artikel 66 lid (3), artikel 38 lid (2), artikel 70 lid (3) of artikel 71 lid (5) gestelde voorschriften, of krachtens artikel 89 gegeven aanwijzingen, is een overtreding en wordt gestraft met hechtenis van ten hoogste zes maanden of geldboete van ten hoogste tweehonderdduizend Surinaamse Dollar.

Artikel 91.
(1) Degene die opzettelijk de bij artikel 48 opgelegde geheimhouding schendt, wordt gestraft hetzij met gevangenisstraf van ten hoogste twee jaren hetzij met een geldboete van ten hoogste vijfhonderdduizend Surinaamse Dollar, hetzij met beide straffen. Het in dit lid strafbaar gestelde feit is een misdrijf.

(2) Degene aan wiens schuld schending van de geheimhouding is te wijten, wordt gestraft met hechtenis van ten hoogste zes maanden hetzij met een geldboete van ten hoogste tweehonderdduizend Surinaamse Dollar, hetzij met beide straffen. Het in dit lid strafbaar gestelde feit is een overtreding.

(3) Geen vervolging wordt ingesteld dan op klacht van degene te wiens aanzien de geheimhouding is geschonden.

Artikel 92.
(1) Waar een rechtspersoon bepaalde artikelen in deze Wet overtreedt, kan het gerechthof, in aanvulling op elke boete een strafrechtelijke overtreding overeenkomen, waarbij de boete niet tien procent van de jaarlijkse omzet van de rechtspersoon overschrijdt.

(2) Bij het opleggen van een boete onder lid (1) zal het gerechtshof rekening houden met:
- (a) de schatting van de economische kosten van inbreuk naar de consumenten, gebruikers van de diensten of andere personen die geraakt worden door de overtreding;
- (b) de schatting van de economische voordeel van de inbreuk voor de onderneming;
- (c) de periode dat de overtreding zich heeft voorgedaan;
- (d) het aantal en Ernst van andere overtredingen, indien van toepassing, die door de organisatie is begaan;
- (e) elke andere zaak mag het Gerechtshof indien van toepassing in de omstandigheden.

Hoofdstuk X
Slotbepalingen

Artikel 93.
(1) Zij treedt in werking met ingang van […..]

(2) Zij wordt in het Staatsblad va de Republiek Suriname afgekondigd.

(3) De Minister van Arbeid, Technologische Ontwikkeling en Milieu is belast met de uitvoering van deze wet.

Gegeven te Paramaribo, de .....

WET van .....,
houdende regels inzake
Elektronische Transacties
(Elektronische Transacties Wet)

ONTWERP

MEMORIE VAN TOELICHTING

A. Algemeen

§ *1. Doel*

1. Handel, financiële dienstverlening en andere commerciële activiteiten verlopen in snel groeiend tempo via internet. Elektronische handel of *e-commerce* krijgt een steeds grotere maatschappelijke en economische betekenis.

2. Elektronische transacties (als samenvattend begrip) betreft niet alleen handel via internet, maar meer in het algemeen alle zakelijke handelingen via internet. De zakelijke handelingen kunnen overheden en bedrijven onderling (government/*business-to-business/government*), overheden/bedrijven en consumenten (government/*business-to-customer*).

3. Met e-commerce hangen bijzondere aspecten samen. Zo heeft e-commerce in de regel een grensoverschrijdend karakter en raakt derhalve meerdere jurisdicties. Er is sprake van gedematerialiseerde communicatie, kennis, diensten en informatie: deze worden niet in een tastbare vorm neergelegd. Bij digitale vastlegging is informatie niet meer gebonden aan een bepaalde fysieke drager of plaats. Digitaal vastgelegde informatie is bovendien onuitputtelijk, in die zin, dat deze oneindig kan worden gekopieerd zonder dat dit leidt tot kwaliteitsverlies of vernietiging. Voorts kan een technologische turbulentie worden vastgesteld. Nieuwe informatietechnieken en -producten volgen elkaar in hoog tempo op, of convergeren tot nieuwe media. De ontwikkeling van de techniek, het maatschappelijk gebruik daarvan en de sociale en juridische problemen die daardoor worden opgeroepen, zijn in belangrijke mate onvoorspelbaar. Er is dus sprake van vergaande veranderingen, maar die brengen nog geen radicale breuk met het verleden mee. De centrale rol van de overheid blijft voorlopig beperkt tot ordening.

4. Het overheidsbeleid is onder meer gericht op het bevorderen van de transparantie en toegang tot de markt, alsmede de betrouwbaarheid van het elektronische verkeer, en het wegnemen van belemmeringen in de bestaande juridische infrastructuur. Daarnaast wordt een brede toegankelijkheid tot de elementaire voorzieningen beoogd: voorzieningen die nodig zijn voor het maatschappelijk functioneren van burgers en bedrijven.

5. Het onderhavige ontwerp, dat is ontleend aan de Nederlands-Antilliaanse Landsverordening overeenkomsten via internet van 29 december 2000 (*Publicatieblad van de Nederlandse Antillen* 2000, no. 168), beoogt enerzijds onzekerheden weg te nemen en elektronisch verkeer te faciliteren, en anderzijds een aantal fundamentele waarden en normen in een elektronische omgeving te waarborgen. Hierbij gaat het om de vastlegging van rechten en verplichtingen, het verzekeren van rechtshandhaving en het bieden van rechtszekerheid. Uit het ontwerp volgt dat aan elektronische handtekeningen dezelfde rechtsgevolgen kunnen zijn verbonden als aan schriftelijke handtekeningen, en dat aan rechtshandelingen niet de geldigheid kan worden

ontzegd uitsluitend omdat deze via internet zijn verricht. Ook een elektronisch document kan als bewijsmiddel worden gebruikt.

Vervolgens is het document in juli 2012 verder herzien doordat de behoefte bestond om nader aansluiting te vinden in de regio. Als referentiekader zijn de Electronic Transactions Act gebruikt van Trinidad & Tobago, Jamaica, Barbados en Bahamas. Daarnaast is gebruik gemaakt van inzichten uit het onderzoeksrapport "Harmonization of ICT Policies, Legislation and Regulatory and Regulatory Procedures in the Caribbean" van International Telecommunication Union dat gefinancierd is door de European Union (2011).

Om de uitbreidingen in de wettekst te benadrukken en hiermee de aansluiting met hetgeen internationaal als best practices wordt beschouwd, heeft een naamsverandering plaatsgevonden van de concept ' Wet Overeenkomsten langs Electronische Weg' (2008) naar de 'Elektronische Transacties Wet' (2012).

§ *2. Begrenzing*

1. Het ontwerp brengt geen wijziging in de in Suriname van toepassing zijnde wet- en regelgeving, behoudens voor zover een afwijking expliciet uit het ontwerp blijkt. Uitgangspunt is geweest dat alleen die onderwerpen worden geregeld ten aanzien waarvan de behoefte tot een wettelijke regeling bestaat en waarin de bestaande wetten derhalve niet of niet adequaat voorzien. Het bestaande kader aan juridische normen uit de 'fysieke wereld' is namelijk in beginsel evenzeer van toepassing in de 'elektronische wereld'. Zo bevatten bijvoorbeeld het Burgerlijk Wetboek en het Wetboek van Koophandel grotendeels technologie-neutrale bepalingen. Dat neemt niet weg dat buiten twijfel moet worden gesteld dat overeenkomsten ook via internet tot stand kunnen komen, dat aan elektronische handtekeningen niet de rechtsgeldigheid wordt ontzegd en dat beiden, net als een elektronisch document, ook in het bewijsrecht een rol kunnen spelen, al is de waardering daarvan in ieder concreet geval aan het oordeel van de rechter overgelaten.

§ *3. Opzet*

1. Gelet op de snelheid waarmee technische ontwikkelingen plaatsvinden en de onzekerheid in welke richting e-commerce zich kan en zal ontwikkelen, is gekozen voor een zo flexibel mogelijke opzet van de wet. Enerzijds komt dat tot uitdrukking in het gebruik van algemeen geformuleerde begrippen en bepalingen, en anderzijds in de mogelijkheden om bij staatsbesluit nadere regels omtrent één of meerdere onderwerpen te kunnen stellen. Aldus kan eenvoudig op veranderingen, vernieuwingen en knelpunten worden ingespeeld.

2. In De ontwerpwet komen eerst de algemene bepalingen (hoofdstuk I)aan de orde, waarna de vereisten voor juridische erkenning van elektronische transacties worden belicht in hoofdstuk II. Daarna worden de voorwaarden voor e-commerce activiteiten beschreven in hoofdstuk III omtrent Contractvorming en in gebrekenstelling. Hoofdstuk IV en V gaan over elektronische handtekening en de Elektronische Authenticatie Dienstverleners die de authenticiteit van de gebruikers van elektronische transacties borgen. Hoofdstuk VI en VII gaan verder kort in over de rol van intermediairs, telecommunicatie dienstverleners en de overheid. Vervolgens wordt in hoofdstuk VIII ingegaan op de consumentenbescherming. In hoofdstuk IX wordt ingegaan op o.a. toezicht en opsporing, overtredingen en wetshandhaving, waarna afgerond wordt met de slotbepalingen.

4. Toepassingsbereik

1. De ontwerpwet is van toepassing op e-commerce activiteiten. Voor de toepasselijkheid is het aanbieden van commerciële communicatie daarbij een belangrijk criterium. De nationaliteit of woon- of vestigingsplaats van de aanbieder van commerciële communicatie is daarbij op zich niet relevant. Van belang is of de Surinaamse rechtssfeer wordt geraakt. In de toelichting op het begrip commerciële communicatie wordt hierop nader ingegaan.

2. Al staat dat daar niet met zoveel woorden in, de ontwerpwet beoogt buiten twijfel te stellen dat overeenkomsten via internet tot stand kunnen komen. In verbintenisrechtelijke zin kan commerciële communicatie een concreet 'aanbod' inhouden, bijvoorbeeld bepaalde producten voor een bepaalde prijs.

3. Voor het tot stand komen van een overeenkomst via internet is vereist dat de aanbieder van commerciële communicatie de instemming van de wederpartij met het aanbod ontvangt. Dit uitgangspunt is logisch en is gebaseerd op het gemene recht: wanneer een brief houdende een aanvaarding naar een verkeerd postbusnummer wordt gestuurd en de aanbieder niet bereikt, komt immers ook geen overeenkomst tot stand. Dit uitgangspunt geldt derhalve onverkort voor het tot stand komen van overeenkomsten via internet. Elders ziet men ingewikkelde regelingen (bijvoorbeeld in de Europese Unie), waar als constitutief vereiste geldt dat de aanbieder deze instemming op zijn beurt weer aan de wederpartij moet bevestigen en zelfs dat de wederpartij de ontvangst daarvan weer moet bevestigen.

4. Een via internet gedaan aanbod kan door de wederpartij echter ook schriftelijk worden aanvaard. Er is desondanks sprake van een overeenkomst die via internet tot stand is gekomen en die derhalve valt binnen het bereik van de wet, omdat daarvoor alleen is vereist dat het aanbod via internet wordt gedaan. Verwezen wordt ook naar het begrip commerciële communicatie.

5. Daartegenover wordt opgemerkt dat indien het aanbod niet maar de aanvaarding wel via internet plaatsvindt, er dan geen sprake is van een overeenkomst via internet.

6. Wordt het aanbod gedeeltelijk via internet gedaan en gedeeltelijk op andere wijze (bijvoorbeeld per brief) dan valt de overeenkomst wel onder de werking van de wet.

7. Aanbod en aanvaarding worden overigens door het gemene verbintenissenrecht geregeld. Eén van de hoofdregels is dat een door een aanbieder gedaan aanbod onherroepelijk en niet regionaal of in de tijd begrensd is, tenzij dit bij het aanbod uitdrukkelijk en ondubbelzinnig anders is vermeld. In de regel zal bovendien een aanbod niet worden aangemerkt als een uitnodiging tot het doen van een aanbod, tenzij dit uitdrukkelijk en ondubbelzinnig is vermeld.

8. Soms kunnen geen overeenkomsten via internet tot stand komen: bijvoorbeeld wanneer het gaat om rechtshandelingen die slechts door tussenkomst van een notaris tot stand kunnen komen, of wanneer het gaat om rechtshandelingen waarvoor wettelijke vormvoorschriften bestaan, behoudens voor zover elektronische wegen worden gebruikt waarmee aan de betreffende vormvoorschriften wordt voldaan. Wanneer bijvoorbeeld de schriftelijke vorm is voorgeschreven, voldoet ook een faxbericht daaraan. Bij vormvoorschriften moet een onderscheid worden gemaakt tussen (dwingende) bewijsvoorschriften enerzijds en constitutieve vereisten anderzijds.

§ *5. Handhaving*

1. Handhaving van rechtsnormen en -waarden bij grensoverschrijdende activiteiten is bijzonder lastig. Een deel van de bepalingen in de ontwerpwet heeft betrekking op de relatie tussen een aanbieder van commerciële communicatie en zijn wederpartij. Het al dan niet afdwingen van de op die relatie van toepassing zijnde wettelijke normen ligt in handen van de betrokken partijen. De relatie tussen een aanbieder van commerciële communicatie en een dienstenaanbieder (service provider) is eveneens contractueel van karakter wanneer het om een rechtstreekse relatie gaat. Ook in dat geval is het aan partijen om de naleving al dan niet af te dwingen.

2. Bij artikel 65, eerste lid, waar het gaat om het vertrouwelijk behandelen van informatie met een zodanig karakter, is het evenzeer aan partijen om op grond van een contractuele relatie of uit hoofde van een onrechtmatige daad, tegen een inbreuk te ageren. Dat neemt niet weg dat een op artikel 65, derde lid, gebaseerd staatsbesluit strafrechtelijk te sanctioneren verboden kan bevatten.

3. Daarnaast zijn er bepalingen die zien op de aansprakelijkheid jegens de aanbieder van commerciële communicatie, de wederpartij en (andere) derden: zo is de dienstenaanbieder (service provider) niet aansprakelijk wanneer hij slechts 'doorgeefluik' van informatie is (artikel 33). Deze bepalingen beperken dus de mogelijkheden om de service provider in rechte aan te spreken, doorgaans op grond van het leerstuk onrechtmatige daad.

4. Ten slotte zijn er bepalingen op de naleving waarvan de overheid ziet, hetzij in de vorm van het geven van een aanwijzing hetzij langs strafrechtelijke weg. De strafrechtelijke bepalingen zijn doorgaans te herkennen aan het woord 'verboden'. Strafbepalingen inzake computercriminaliteit zullen in het Wetboek van Strafrecht worden opgenomen.

B. Hoofdstuksgewijze toelichting

Hst. I Algemene bepalingen

In hoofdstuk 1 worden in de artikelen 1 t/m 7 (pagina's 1 t/m 5) het volgende beschreven:

- Begripsbepalingen;
- Bindende werking;
- Geen verplichting om een document of informatie in elektronische vorm te accepteren of te verzenden;
- Ontoepasselijkheid van de Wet;
- Vrijwillig gebruik van elektronische transacties.

Naast de begripsbepalingen worden in dit hoofdstuk de reikwijdte en de toepasselijkheid van de Wet nader belicht.

Hst. II Vereisten voor juridische erkenning

In artikelen 8 t/m 18 (pagina's 5 t/m 7) wordt ingegaan op het volgende:

- Juridische erkenning van elektronische transacties;
- Op schrift;
- Bepaling omtrent informatie;
- Specifieke niet-elektronische vorm;
- Originele vorm;
- Behoud van informatie, data berichten of vastleggingen in elektronische vorm;
- Mogelijkheid om informatie, een data bericht of een vastlegging te bewaren;
- Kopieën;
- Elektronisch getekende boodschap wordt geacht het originele document te zijn;
- Toelaatbaarheid en het gewicht van het bewijs van elektronische vastleggingen;
- Electronische legalisatie.

Dit hoofdstuk beschrijft de voorwaarden waarbij data berichten en documenten in elektronische vorm geaccepteerd kunnen worden door overheidsinstellingen, verzenders en ontvangers van documenten in elektronische vorm.

Hst. III Contractvorming en in gebrekenstelling

In de artikelen 19 t/m 33 (pagina's 8 t/m 12) wordt ingegaan op de volgende onderwerpen:

- Commerciële communicatie (e-commerce);
- Aanbieder van commerciële communicatie (e-commerce);
- Vorming en geldigheid van contracten;
- Elektronische uiting van een aanbieding en acceptatie;
- Het gebruik van elektronische agenten voor contractvorming;
- Fout dat ontstaat gedurende het proces met een elektronische agent;
- Toekenning of data berichten of vastleggingen;
- Moment van verzenden van de data bericht;
- Moment van ontvangst van de data bericht;
- Plaats van verzending en ontvangst van de data bericht;

- Zakelijke adres;
- Gebruikelijke residentie;
- Aansprakelijkheid van de dienstenaanbieder van e-commerce.

Onder meer komen de activiteiten van e-commerce aan de orde alsook de voorwaarden en condities waaronder de activiteiten dienen plaats te vinden. De reikwijdte van de aansprakelijkheid van de dienstenaanbieder van e-commerce wordt behandeld in artikel 33.

Met betrekking tot artikel 33 omtrent aansprakelijkheid van de dienstenaanbieder geldt het volgende. Een dienstenaanbieder (service provider) is niet aansprakelijk wanneer hij slechts 'doorgeefluik' van informatie is. Wel is hij blijkens het tweede lid gehouden informatie te verwijderen of de toegang daartoe onmogelijk te maken wanneer dat door of namens de Minister wordt gelast, alsmede wanneer het hem duidelijk moet zijn dat de informatie onwettig is of onwettige activiteiten betreft. Wat dit laatste betreft rust op de dienstenaanbieder geen eigen of actieve onderzoeksplicht. Onwettig is bijvoorbeeld een auteursrechtinbreuk of een webpage die oproept tot rassendiscriminatie.

In het tweede lid wordt de Minister de mogelijkheid gegeven om de verwijdering van informatie te gelasten en/of de toegang daartoe te verbieden onder de in het derde lid genoemde beperkingen. Dit instrument is uitdrukkelijk niet als politiek instrument bedoeld, maar beoogt evident kwalijke praktijken tegen te gaan. Dat betekent dat een tot oordelen geroepen rechter niet kan volstaan met een marginale toetsing, maar de recht-en doelmatigheid ten volle moet toetsen. Het instrument mag bijvoorbeeld niet worden gebruikt voor het weren van politiek onwelgevallige informatie of erotisch getinte informatie. Aan laatstgenoemde uitingen kunnen uiteraard zekere beperkingen worden verbonden die zoveel mogelijk moeten waarborgen dat deze informatie niet ongevraagd wordt toegezonden, of die de toegankelijkheid voor bijvoorbeeld minderjarigen beperken.

De dienstenaanbieder die zelf weet krijgt van onwettige informatie of activiteiten is gehouden de informatie te verwijderen of ontoegankelijk te maken (lid 2). Voor de dienstenaanbieder zal het niet altijd eenvoudig zijn vast te stellen of van onwettige activiteiten of informatie sprake is. Bij twijfel moet hij de strijdende partijen naar de rechter verwijzen. Hij kan natuurlijk ook de Minister vragen of er grond voor een aanwijzing bestaat.

De mogelijkheid van ontoegankelijk maken zal als eerste stap voor hem in de regel de meest veilige zijn, omdat aan het op eigen initiatief overgaan tot verwijdering grotere risico's kleven. Vanwege zijn contractuele verplichtingen zal de dienstenaanbieder er in de regel bovendien verstandig aan doen om de houder van de website van zijn voornemen in kennis te stellen. Vanzelfsprekend doet de dienstenaanbieder er verstandig aan de mogelijkheid van eigenmachtig afsluiten of ontoegankelijk maken van de webpage in zijn algemene voorwaarden adequaat te regelen. In het algemeen bestaat voor de dienstenaanbieder niet de verplichting om de naam en adresgegevens van de betreffende site houder bekend te maken, hetgeen immers een schending van de privacy zou kunnen betekenen. Bij twijfel kan hij het op een kort geding laten aankomen: wordt hij veroordeeld deze gegevens te verstrekken, dan doet hij zulks op grond van een rechterlijk bevel, zodat hem geen schending van de privacy kan worden verweten.

Hst. IV Elektronische handtekening

Hoofdstuk IV omvat de artikelen 34 t/m 37 (pagina's 12 t/m 13), die de volgende onderwerpen behandelen:

- Elektronische handtekening;
- Minimum standaarden voor wettelijk vereiste handtekeningen;
- Betrouwbaarheid en integriteit van elektronische handtekeningen;
- Elektronische handtekening dat geassocieerd is met een geaccrediteerde elektronische authenticatie product.

De relatie tussen de elektronische handtekening en de geaccrediteerde elektronische authenticatie product wordt nader benadrukt, waarbij in artikel 36 de vereisten voor betrouwbaarheid en integriteit van de elektronische handtekeningen nadere worden belicht.

Een bericht kan in een elektronische omgeving makkelijker worden gemanipuleerd dan in een 'papieren' omgeving, omdat in een elektronische omgeving de gegevens en de drager van de gegevens niet onlosmakelijk met elkaar zijn verbonden. In de elektronische omgeving is het des te belangrijker de identiteit van de afzender en de juistheid van het bericht te kunnen vaststellen. Daartoe kunnen organisatorische, technische en juridische beveiligingsmethoden worden toegepast.

Bij elektronische handtekening gaat het om een via internet verstuurde identificatie van de afzender: de ontvanger kan verifiëren dat de informatie van de verzender afkomstig is en dat de inhoud tijdens de verzending niet is veranderd. Deze identificatie vindt (thans) plaats met behulp van zogeheten Elektronische Authenticatie Dienstverleners: op betrouwbaarheid getoetste derden.

Een schriftelijke handtekening heeft verschillende functies: identificatie (uniek aan één persoon gebonden), authenticiteit van de handtekening (de onmogelijkheid om de eigen handtekening te kunnen ontkennen), wilsuiting van de betrokkene, autorisatie van een rechtshandeling, toerekening van een verklaring aan de betrokkene, kennisneming van de inhoud van een document (aangenomen mag worden dat de ondertekenaar de inhoud kent als hij het heeft ondertekend), integriteit en compleetheid van een document (door ondertekening wordt enige garantie gegeven dat er geen gegevens zijn toegevoegd of verwijderd; vergelijk het paraferen), authenticatie van het geschrift (met het zetten van een handtekening benadrukt de ondertekenaar de echtheid van het geschrift), vaststellen origineel (ter onderscheiding van een kopie) en een waarschuwingsfunctie (degene die zijn handtekening plaatst, weet dat hij zich bindt). Een elektronische handtekening kan niet al deze functies op dezelfde wijze vervullen: daarvoor zijn aanvullende hulpmiddelen en procedures nodig.

Strikt genomen is een digitale handtekening een species van de elektronische handtekening. Tot de elektronische handtekeningen behoren in de praktijk immers ook gescande handtekeningen en biometrische identificatiemethoden zoals gescande oogirissen en vingerafdrukken. Deze gescande 'handtekeningen' kunnen zelf ook weer via internet worden verstuurd. In de wet is van een ruim begrip elektronische handtekening uitgegaan.

Het verschil tussen een schriftelijke en een elektronische handtekening zal zich met name bij de ontkenning daarvan doen gevoelen. Een schriftelijke handtekening is een weergave van het handschrift van de ondertekenaar en een eigen persoonlijke creatieve uiting van de betreffende persoon. Bij de ontkenning van een schriftelijke handtekening zal de betrokkene doorgaans stellen dat het niet om zijn handtekening gaat. Bij een elektronische handtekening zal deze ontkenning veelal niet plaatsvinden, maar zal de betrokkene stellen dat deze handtekening niet door of in zijn opdracht is gebruikt maar door een onbevoegde. De bepaling van de authenticiteit van een handtekening in een digitale omgeving dient dus te worden opgesplitst in enerzijds de vaststelling van de echtheid en anderzijds de vaststelling of de handtekening door of namens de betrokkene is gebruikt. Wie dient te bewijzen dat een elektronische handtekening onbevoegd is gezet? In de regel zal dat de betrokkene zijn, omdat hem de (technische) mogelijkheden ter beschikking staan om misbruik te voorkomen en dus te waarborgen dat de wederpartij te goeder trouw erop mag afgaan dat de handtekening door een bevoegde persoon is gebruikt. De elektronische handtekening moet dan wel zodanig persoonsgebonden zijn dat deze niet ook door de ontvanger van het bericht zelf kan worden gebruikt.

De elektronische handtekening en het gebruik van encryptietechnieken ('public key' in dit geval) zijn met elkaar verbonden. Er wordt gebruik gemaakt van zogeheten 'trusted third parties' (TTP), waartoe ook de Surinaamse notarissen naar verwachting zullen gaan behoren, en van digitale elektronische authenticatie producten. Deze elektronische authenticatie producten kunnen onder andere voor identificatie worden gebruikt: ze koppelen de identiteit van de gebruiker aan een publieke encryptiesleutel. Deze elektronische authenticatie producten lijken enigszins op 'access cards' zoals bedrijven en overheden die soms gebruiken en waarmee toegang tot bepaalde afdelingen of ruimtes kan worden verkregen. Het is minder juist ze als een 'digitaal paspoort' of 'digitaal rijbewijs' te beschouwen.

Digitale of elektronische handtekeningen vloeien voort uit 'public key' cryptografie. Daarbij wordt gebruik gemaakt van sleutelparen. De *publieke* sleutel wordt aan andere gebruikers beschikbaar gemaakt in een publiek domein (bijvoorbeeld internet). De *private* sleutel blijft in het bezit van de gebruiker. Deze twee sleutels vormen het publiek/privaat sleutelpaar. De publieke sleutel kan gebruikt worden om berichten te vercijferen die vervolgens alleen met de private sleutel kunnen worden ontcijferd. De private sleutel kan worden gebruikt om berichten te vercijferen die vervolgens alleen met de publieke sleutel kunnen worden ontcijferd.

Bij elektronische handtekeningen wordt met een zogeheten hashfunctie gewerkt. Technisch gesproken is de definitie van een hashfunctie: een transformatieproces waarbij een input *m* van variabele lengte wordt omgezet in een waarde van vaste lengte, de hashwaarde *h*. De hashfunctie is een methode om een document van willekeurige lengte op een kortere manier weer te geven. Deze kortere weergave heeft altijd dezelfde lengte, ongeacht de grootte van het originele document. Hashfuncties hebben twee unieke eigenschappen waardoor ze geschikt zijn voor het gebruik van cryptografie. Ten eerste is een hashwaarde een numerieke weergave van een document. Ten tweede is het proces 'eenrichtingsverkeer'. Deze eigenschappen hebben tot gevolg dat er geen informatie uit de hashwaarde is af te leiden met betrekking tot de inhoud van het originele document, en dat het niet mogelijk is het originele document vanuit de hashwaarde te herleiden.

Het gebruik van een hashwaarde in cryptografie stelt de verzender van een bericht in staat om eerst de hashwaarde van het bericht te berekenen en deze vervolgens samen met het bericht aan de ontvanger te versturen. Wanneer de ontvanger het bericht ontvangt, kan deze met dezelfde hash algoritme opnieuw de hashwaarde van het document berekenen en deze waarde vergelijken met de meegezonden hashwaarde. Indien de twee waarden identiek zijn, kan de ontvanger er zeker van zijn dat het ontvangen document gelijk is aan het verzonden document.

Er kan niet alleen op de hashwaarde worden vertrouwd om de inhoud van een bericht te garanderen. Als een 'elektronische afluisteraar' het document en de hashwaarde zou onderscheppen, kan het document veranderd, opnieuw gehashed en doorgezonden worden. De ontvanger zal dan niet weten dat de inhoud

van het bericht is gewijzigd. Het gehele pakket (document en hashwaarde) zou met behulp van public key cryptografie kunnen worden versleuteld, waardoor de identiteit van de afzender wordt gegarandeerd, maar dat kost onacceptabel veel tijd.

De elektronische handtekening is een zeker zo veilige methode voor het garanderen van de inhoud en identiteit. Een elektronische handtekening is de hashwaarde van het originele document, dat is vercijferd met de private sleutel van de afzender. Door de elektronische handtekening aan het originele document toe te voegen, kan de ontvanger verifiëren dat het document van de verzender afkomstig is en dat de inhoud tijdens de verzending niet is veranderd.

Een hoge mate van betrouwbaarheid van de elektronische handtekening betekent overigens niet 100% betrouwbaarheid, maar dat geldt evenzeer in een 'papieren' omgeving. De mate waarin betrouwbaarheid nodig is zal in de praktijk afhankelijk zijn van de aard en/of omvang van de transactie. Naarmate de transacties gevoeliger zijn zullen de betrokken partijen meer aan allerlei soorten bescherming moeten doen, bijvoorbeeld electronic monitoring (het volgen van processen en handelingen), time stamping (zekerheid over het tijdstip waarop informatie is verwerkt), firewall (toegangsbeveiliging), EDP-audit (Electronic Data Processing), cryptografie, certificatie, call back-procedure (de verzendende computer maakt contact met de ontvangende computer, identificeert zich en verbreekt de verbinding, waarna de ontvangende computer terugbelt), enzovoort (P. Kolkman en R. van Kralingen, *Verschuivend vertrouwen. Methoden voor het waarborgen van betrouwbaarheid in het elektronische rechtsverkeer*, IteR reeks, nr. 12, 1998, blz. 205-289).

De onderhavige ontwerpwet beoogt duidelijkheid te verschaffen door aan elektronische handtekeningen niet de rechtskracht te ontzeggen en door het gebruik daarvan te vergemakkelijken. Deze erkenning strekt zich ook uit tot bepaalde elektronische authenticatie producten en Elektronische Authenticatie Dienstverleners. Het is nog niet duidelijk hoe de elektronische handtekening zich zal ontwikkelen. Evenmin staat de noodzaak vast om gebruikers te verplichten in relatie tot bijvoorbeeld consumenten van een Elektronische Authenticatie Dienstverlener gebruik te maken. De wettelijke regeling is daarom globaal van opzet.

In het eerste lid van artikel 34 wordt de term 'rechtskracht' van een elektronische handtekening gebruikt. Daarmee wordt tot uitdrukking gebracht dat aan een elektronische handtekening rechtens dezelfde gevolgen verbonden kunnen zijn als aan een schriftelijke handtekening.

In Suriname bestaat een open systeem van bewijsmiddelen, zodat een elektronische handtekening reeds nu als bewijsmiddel in een procedure kan worden gebruikt. Mogelijke misverstanden hierover zijn met de wet uit de wereld geholpen. Het wordt in dit stadium niet nodig geacht de vrije waardering van het bewijs door de rechter te sturen of te beperken. Van geval tot geval zal de betrokken rechter de concrete feiten en omstandigheden in zijn onderzoek en oordeel moeten betrekken, en nagaan op wie de bewijslast en het bewijsrisico van de echtheid van een elektronische handtekening rusten (vgl. HR 19 november 1993, NJ 1994, 622 inzake COVA). Bij belangrijke transacties doen partijen er verstandig aan een overeenkomst via internet bij een onafhankelijke derde (Trusted Third Party) in bewaring te geven, bij wie ingeval een geschil rijst een (gewaarmerkt) elektronisch afschrift kan worden verkregen.

Evenals bij iedere andere vorm van identificatie is een (digitaal) elektronische authenticatie product zo betrouwbaar als de autoriteit en procedures die daar achter staan. Een rijbewijs heeft daardoor een ander karakter dan een bibliotheekpas. Met een rijbewijs garandeert de overheid als betrouwbare 'derde partij' dat die informatie juist en waar is. Bij 'digitale' elektronische authenticatie producten verzorgen Elektronische Authenticatie Dienstverleners deze verificatie. Iedere natuurlijke persoon of rechtspersoon kan Elektronische Authenticatie Dienstverlener worden wanneer deze wil instaan voor de identiteit van degenen aan wie hij een digitaal elektronische authenticatie product uitgeeft: een bedrijf voor zijn werknemers, de universiteit voor zijn studenten, enz. Om wildgroei te voorkomen zijn in de wet een aantal waarborgen opgenomen. Zo zal een (digitaal) elektronische authenticatie product voor

bewijsdoeleinden kunnen worden erkend wanneer de Elektronische Authenticatie Dienstverlener die het heeft afgegeven aan bepaalde -bij staatsbesluit te stellen-voorschriften voldoet dan wel een zodanige Elektronische Authenticatie Dienstverlener zich borg stelt voor een door een ander afgegeven elektronische authenticatie product.

Hst. V Elektronische Authenticatie Dienstverleners

In hoofdstuk V worden in de artikelen 38 t/m 55 (pagina's 13 t/m 18) de volgende onderwerpen behandeld:

- Encryptie;
- Registratie van de Elektronische Authenticatie Dienstverlener;
- Aanvraag voor registratie;
- Vereisten voor een Elektronische Authenticatie Dienstverlener die gekwalificeerde elektronische authenticatie producten uitbrengt;
- Toekenning van registratie;
- Erkenning of de gekwalificeerd externe Elektronische authenticatie producten;
- Registratie van Elektronische Authenticatie Dienstverleners;
- Herziene notificatie van naleving van wetgeving;
- Controle door de aangewezen autoriteit;
- Verantwoordelijkheid om mee te werken aan de controle;
- Geheimhouding;
- Bevoegdheid van de aangewezen autoriteit indien niet voldaan wordt aan de vereisten;
- Pseudoniemen;
- Additionele verantwoordelijkheden van een Elektronische Authenticatie Dienstverlener;
- Onmiddellijke herroeping op verzoek;
- Aansprakelijkheid van de Elektronische Authenticatie Dienstverlener;
- Ontheffing van aansprakelijkheid;
- Kosten van een controle.

Encryptie
Denkbaar is dat bij staatsbesluit het verplichte gebruik van encryptietechnieken in bepaalde gevallen wordt voorgeschreven, bijvoorbeeld ter zake van persoonsgebonden gegevens (creditcard gegevens). In het algemeen schept encryptie de mogelijkheid om belangrijke of gevoelige informatie tijdens het transport over publieke netwerken, zoals internet, te beschermen. Misbruik daarvan moet zoveel mogelijk worden bestreden. Bij staatsbesluit kunnen daartoe wenselijk geachte regels worden gegeven.

Elektronische Authenticatie Dienstverleners
Elektronische Authenticatie Dienstverleners worden geacht zich eerst te registreren bij een aangewezen autoriteit die een register bijhoudt, voordat encryptietechnieken mogen worden aangeboden in Suriname in de vorm van gekwalificeerde elektronische authenticatie producten. De aangewezen autoriteit is bevoegd om controlewerkzaamheden te verrichten om de naleving van de Wet te toetsen.

In de artikelen 53 en 54 worden de aansprakelijkheid van de Elektronische Authenticatie Dienstverlener nader behandeld. Gelet op de rol van Elektronische Authenticatie Dienstverleners en (digitale) elektronische authenticatie producten, is het noodzakelijk de aansprakelijkheid van Elektronische Authenticatie Dienstverleners wettelijk te regelen. Een wettelijke regeling is nodig omdat niet alleen de relatie tussen de Elektronische Authenticatie Dienstverlener en diens opdrachtgever aan de orde is, maar ook belangen van derden (waaronder consumenten) in het spel zijn. Juist deze derden zullen op het opgewekte vertrouwen afgaan en aan hen moet een meer toegesneden instrument dan het reguliere leerstuk van de onrechtmatige daad ter beschikking staan. Met dit artikel staat vast dat het belang van deze derden een rechtens te beschermen belang is en dat zij niet afzonderlijk behoeven aan te tonen dat

aan het relativiteitsvereiste is voldaan.

Op de Elektronische Authenticatie Dienstverlener rust de bewijslast: hij moet aantonen niet nalatig te zijn geweest. Op dit punt voldoet de derde derhalve aan zijn stelplicht wanneer hij deze nalatigheid stelt dan wel wanneer deze uit zijn stellingen voortvloeit.

De Elektronische Authenticatie Dienstverlener is niet aansprakelijk voor in het digitale elektronische authenticatie product opgenomen beperkingen die voor derden kenbaar zijn (lid 3). Een beperking kan bijvoorbeeld ook gelegen zijn in het maximum bedrag dat met de overeenkomst waarvoor het elektronische authenticatie product wordt gebruikt gemoeid mag zijn.

Geheimhouding
Het is passend dat evenzeer tot geheimhouding zijn gehouden al diegenen die bij de uitvoering van deze wet zijn betrokken en de beschikking krijgen over vertrouwelijke gegevens, maar niet reeds uit andere hoofde tot een dergelijke geheimhouding zijn verplicht. Artikel 33 strekt ertoe dit in het ontwerp vast te leggen.

Hst. VI Intermediairs en telecommunicatie dienstverleners

In de artikelen 56 t/m 58 (pagina's 19 t/m 20) worden de aansprakelijkheid van intermediairs en telecommunicatie dienstverleners behandeld als ook de gedragcodes en dienstverleningstandaarden voor intermediairs en telecommunicatie dienstverleners.

Hst. VII Overheid en andere overheidsinstanties

In hoofdstuk VII wordt ingegaan op de regelgeving omtrent de algemene volmacht ('general authorization') van overheidslichamen en de te overleggen documenten voor inspectie, die ook in elektronische vorm mogen worden aangeboden (artikelen 59 t/m 60).

Hst. VIII Consumentenbescherming

In hoofdstuk VIII Consumentenbescherming worden de volgende onderwerpen behandeld (artikelen 61 t/m 66 op pagina's 21 t/m 23):

- Minimum aan informatie in e-commerce;
- Minimum aan informatie met betrekking tot authenticatie producten;
- Recht op intrekking;
- Ongevraagde communicatie;
- Bescherming vertrouwelijkheid en privacy;
- Vertrouwelijke behandeling.

Hierbij is met name de bescherming van de vertrouwelijkheid en privacy van de consumenten van belang, waarbij minimale vereisten worden gesteld aan de minimum aan informatie in e-commerce en authenticatie producten. Consumenten worden daarnaast beschermd doordat er een recht op intrekking van de elektronische transactie bestaat indien niet voldaan is aan de eerder genoemde minimumvereisten aan informatie. Daarnaast dient er een optie te bestaan waarbij consumenten zich op eenvoudig kunnen ontzien van ongevraagde commerciële uitingen in de toekomst.

Hst. IX Overtredingen en wetshandhaving

Het hoofdstuk over overtredingen en wetshandhaving beslaat de artikelen 67 t/m 92 (pagina's 23 t/m 29):

- Valse of misleidende informatie;
- Obstructie van een controle;
- Doorbreking van verplichtingen van vertrouwelijkheid;
- Buitengerechtelijke geschillenbeslechting;
- Toezicht en opsporing;
- Legitimatie bij taakuitoefening van de toezichthouders;
- Opsporingsambtenaren;
- Plichten van de leden van de raad van commissarissen en directie;
- Aansprakelijkheid van de leden van de raad van commissarissen en directie;
- Bestuursdwang;
- Aanwijzingen;
- Strafbepalingen.

Hierbij wordt overzichtelijke weergegeven wat onder overtredingen wordt verstaan in het kader van elektronische transacties. Hierbij wordt de rol en werkwijze van de toezichthouders en opsporingsambtenaren nader beschreven. De plichten en aansprakelijkheid van de leden van de raad van commissarissen en directie worden nader toegelicht, waarna de bepalingen volgen omtrent bestuursdwang.

Buitengerechtelijke geschillenbeslechting
Er bestaat behoefte aan efficiënte, snelle en relatief goedkope geschillenbeslechting, bij voorkeur buiten de burgerlijke rechter om. Deze buitengerechtelijke geschillenbeslechting moet voldoen aan de beginselen van onafhankelijkheid, transparantie, hoor en wederhoor, doeltreffendheid van de procedure, wettigheid van de beslissing, vrijheid van de partijen en de mogelijkheid tot vertegenwoordiging en (zonodig onder bepaalde voorwaarden) van hoger beroep. Het kan gaan om arbitrage of bindend advies: het eerste is een vorm van rechtspraak, het tweede leidt tot een uitspraak die tussen partijen de kracht van een overeenkomst heeft, waarvan de nakoming zonodig via de burgerlijke rechter (al dan niet in kort geding) moet worden afgedwongen. Nadat is onderzocht of en op welke wijze deze vorm van geschillenbeslechting in het leven moet worden geroepen, kan dat relatief eenvoudig door middel van een staatsbesluit, houdende algemene maatregelen (lid 1). Er zou ook een eventueel reeds bestaand orgaan voor buitengerechtelijke geschillenbeslechting kunnen worden aangewezen.

Partijen kunnen zich voor de beslechting van hun geschillen onderwerpen aan het college als in het eerste lid bedoeld, wanneer deze geschillen betrekking hebben op commerciële communicatie, overeenkomsten langs elektronische weg (met inbegrip van de precontractuele fase, de uitvoering van de transactie en leerstukken als dwang, dwaling, bedrog en misbruik van omstandigheden), aansprakelijkheid van de dienstenverlener, bescherming van de vertrouwelijkheid en privacy, alsmede certificaten en (aansprakelijkheid van) certificatiedienstverleners (lid 2). Partijen kunnen vooraf, al dan niet in toepasselijke algemene voorwaarden, maar ook nadat een geschil is gerezen, overeenkomen de weg van buitengerechtelijke geschillenbeslechting te bewandelen. Het is dus aan partijen of zij van deze mogelijkheid gebruik willen maken.

Het college zal, evenals een burgerlijke rechter, het op het geschil van toepassing zijnde recht moeten vaststellen. De in dit artikel bedoelde mogelijkheden van buitengerechtelijke geschillenbeslechting laten de bevoegdheid van de burgerlijke rechter om in kort geding desgevraagd voorlopige voorzieningen te treffen onverlet.

Bij staatsbesluit kunnen andere categorieën van geschillen worden aangewezen waarvan de beslechting buitengerechtelijk zou kunnen plaatsvinden (lid 3). Het kan allerhande met e-commerce samenhangende onderwerpen betreffen: geschillen over het ter beschikking gestelde netwerk, geschillen met access providers, geschillen op het terrein van intellectuele eigendomsrechten (voor zover die er niet reeds nu onder vallen), enzovoort.

Toezicht en opsporing
Artikel 71: Deze bepalingen hebben betrekking op het toezicht op de naleving van het bepaalde bij of krachtens deze wet. Hoewel ter zake van grote delen van het internet sprake is van zelfregulering is het gewenst daarnaast ten behoeve van het algemeen belang te beschikken over adequaat toezicht op de naleving van de onderhavige wetgeving. In artikel 71, eerste lid, wordt bepaald dat de zorg voor een adequate handhaving van het bepaalde bij of krachtens de onderhavige wet, behoort tot de taak van bij staatsbesluit aangewezen ambtenaren en personen. Voor alle duidelijkheid zij opgemerkt dat het hier steeds gaat om bestuurlijk toezicht op de naleving van het bij of krachtens deze wet bepaalde. De strafrechtelijke handhaving wordt uitgevoerd door opsporingsambtenaren die bij staatsbesluit, krachtens het Wetboek van Strafvordering worden benoemd. De aan opsporingsambtenaren toegekende bevoegdheden die verder gaan dan die van de toezichthouders, zijn ook opgenomen in voornoemd wetboek. Artikelen 71, tweede en derde lid, regelt de bevoegdheden van de toezichthouders.

Artikel 73: Gelet op het specialistische karakter van de onderwerpelijke materie is het gewenst dat naast de reguliere politie ook opsporingstaken kunnen worden uitgevoerd door speciaal daarvoor opgeleide personen die daartoe als bijzondere opsporingsambtenaar kunnen worden aangewezen. Artikel 73 strekt ertoe zulks mogelijk te maken.

Bestuursdwang (artikelen 76 tot en met 89)
Deze artikelen bevatten bestuurlijke sanctiemiddelen die kunnen worden toegepast bij het handelen in strijd met het bij of krachtens deze wet bepaalde. De onderhavige ontwerp-wet kent de volgende bestuurlijke sanctiemiddelen:

- Bestuursdwang - De Minister kan vorderen dat de overtreder van een bij of krachtens de onderhavige wet gesteld verbod een bepaalde activiteit terugdraait of alsnog verricht. Het nadeel van dit middel is echter in de praktijk dat de kosten vaak niet zijn te verhalen op de overtreder omdat deze daartoe financieel niet in staat is. De Minister ziet zich dan gesteld voor gemaakte kosten die ten laste van de overheidsfinanciën blijven. Dat maakt de animo om dit middel toe te passen er niet groter op.

- Dwangsom - Aantrekkelijker dan het tegenhouden of stopzetten van een activiteit of de toepassing van bestuursdwang is het middel van de bestuurlijke dwangsom. De Minister kan de overtreder van het bij of krachtens de onderhavige wet bepaalde een dwangsom opleggen voor elke dag dat de overtreding voortduurt. De dwangsom wordt per tijdseenheid of per overtreding vastgesteld. Het bestuursorgaan bepaalt de hoogte van de dwangsom. Dit bedrag dient in redelijke overeenstemming te zijn met de ernst van de overtreding. Als er een wanverhouding bestaat tussen de hoogte van de dwangsom en de ernst van de overtreding zal uiteindelijk de rechter moeten bepalen wat redelijk is. Verbeurde dwangsommen komen toe aan de Staat. De dwangsom kan bij dwangbevel worden ingevorderd; de daaraan verbonden kosten komen uiteraard voor rekening van de overtreder.

Er zij op gewezen dat het in artikel 26 om een bestuurlijke en niet om een strafrechtelijke dwangsom gaat. Het gaat hier om een eigen sanctiebevoegdheid van het overheidsbestuur die voortvloeit uit zijn bestuurlijke verantwoordelijkheid. Een dergelijke sanctie dient een ander doel dan een strafrechtelijke sanctie. De bedoeling van een bestuurlijke sanctie is dat een einde wordt gemaakt aan een situatie die de wetgever uit een oogpunt van het beschermde belang in de desbetreffende wettelijke regeling onaanvaardbaar acht.

Artikel 89 Aanwijzingen
De Minister kan aan een aanbieder van commerciële communicatie of dienstenaanbieder een of meer aanwijzingen geven, wanneer dat voor een richtige uitvoering van de wet nodig mocht blijken. In dit laatste ligt een beperking opgesloten. De beginselen van behoorlijk bestuur brengen in de regel mee dat de belanghebbende vooraf van het voornemen op de hoogte wordt gesteld en de gelegenheid krijgt zijn bezwaren naar voren te brengen. Het gaat om een volle toetsing, derhalve zowel om de doel- als de rechtmatigheid.

Strafbepalingen (artikelen 90 en 91)
In deze artikelen is de strafrechtelijke sanctionering van een aantal bepalingen in de ontwerpwet opgenomen. Expliciet is aangegeven wanneer sprake is van een misdrijf en wanneer van een overtreding. Zulks heeft, zoals uit de afzonderlijke bepalingen blijkt, gevolgen voor de maximum strafmaat.

Hst. X Slotbepalingen

In de slotbepalingen staan de datum van inwerkingtreding van de Wet benoemd, de verantwoordelijke Ministerie en de ondertekening door de President van de Republiek van Suriname

Paramaribo, de .....