Vaststelling van Geharmoniseerde Beleidsregels voor de ICT-Markt in de ACS-landen

Privacy en gegevensbescherming: Richtlijnen voor Model Beleid & Wetteksten

HIPCAR

Harmonisatie van Beleid, Wetgeving en Regelgevings procedures op het stuk van ICT in het Caribisch gebied

Europese Commissie

CARICOM

CTU

ITU

Vaststelling van Geharmoniseerde Beleidsregels voor de ICT-Markt in de ACP-landen

Privacy en gegevensbescherming:

Richtlijnen voor Model Beleid & Wetteksten

HIPCAR

Harmonisatie van Beleid, Wetgeving en Regelgevings procedures op het stuk van ICT in het Caribisch gebied

Dit document is tot stand gekomen met de financiële ondersteuning van de Europese Unie. De standpunten die hierin tot uiting worden gebracht zijn geenszins een weergave van de mening van de Europese Unie.

De gehanteerde benamingen en de presentatie van materiaal, waaronder begrepen kaarten, houden geen uiting in van enige mening van de ITU met betrekking tot de juridische status, of de afbakening van de grenzen, van enig land, territorium, stad of gebied. De vermelding van specifieke ondernemingen of van bepaalde producten betekent niet dat deze worden onderschreven of aanbevolen door de ITU boven andere van soortgelijke aard die niet worden vermeld. Dit Rapport heeft geen redactionele revisie ondergaan.

Denk aan het milieu voordat u dit rapport print.

© ITU 2011

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, op enige manier dan ook, zonder voorafgaande schriftelijke toestemming van de ITU.

Voorwoord

Informatie- en communicatietechnologie (ICT) geeft vorm aan het proces van het globalisatie. Het potentieel hiervan erkennend voor het bespoedigen van de economische integratie van de Caribische regio en daarbij haar grotere welvarendheid en sociale transformatie, heeft de CARICOM Interne Markt en Economie (CSME) een ICT-strategie ontwikkeld die gefocust is op versterkte connectiviteit en ontwikkeling.

Liberalisatie van de telecommunicatiesector is een van de sleutelelementen van deze strategie. Coördinatie binnen de gehele regio is essentieel indien beleid, wetgeving en praktijken voortvloeiend uit de liberalisatie door elk land niet dermate verschillend moeten zijn dat ze een belemmering gaan vormen voor de ontwikkeling van een regionale markt.

Het project 'Versterking van het Concurrentievermogen in het Caribisch Gebied door de Harmonisatie van Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT' (HIPCAR) was gericht op het aanpakken van deze potentiële belemmering door het samenbrengen en begeleiden van alle 15 Caribische landen in de Groep van Staten in Afrika, het Caribisch Gebied en de Stille Oceaan (ACP) terwijl zij hun geharmoniseerd Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT formuleerden en aannamen. Uitgevoerd door de Internationale Telecommunicatie-Unie (ITU), is het project ondernomen in nauwe samenwerking met de Caribische Telecommunicatie-Unie (CTU), die de voorzitter is van de HIPCAR-Stuurgroep. Een mondiaal stuurcomité bestaande uit de vertegenwoordigers van het ACP-Secretariaat en het Directoraat-generaal EuropeAid Ontwikkeling en Samenwerking (DEVCO, Europese Commissie) houdt toezicht op de totale implementatie van het project.

Het project vindt plaats in het kader van het programma ACP Informatie- en Telecommunicatietechnologie (@CP-ICT) en wordt gefinancierd uit het 9^{e} Europees Ontwikkelingsfonds (EDF), dat het voornaamste instrument is voor het verstrekken van Europese hulp voor ontwikkelingssamenwerking in de ACP-Staten, met medefinanciering van de ITU. Het @CP-ICT is gericht op het ondersteunen van de ACP-regeringen en -instituten bij het harmoniseren van hun ICT-beleid in de sector door het bieden van beleidsadvies, training en gerelateerde capaciteitsopbouw van hoge kwaliteit, met referentiepunten over de hele wereld doch van plaatselijke relevantie.

Alle projecten die meerdere belanghebbenden bij elkaar brengen worden geconfronteerd met de dubbele uitdaging van het creëren van een gevoel van gedeeld ownership en het waarborgen van optimale resultaten voor alle partijen. HIPCAR heeft bijzondere aandacht besteed aan deze kwestie vanaf het prille begin van het project in december 2008. Overeenstemming bereikt hebbend over gedeelde prioriteiten, werden werkgroepen van belanghebbenden gevormd voor het aanpakken daarvan. De specifieke noden van de regio werden vervolgens geïdentificeerd evenals potentiële succesvolle regionale praktijken, welke daarna werden getoetst aan elders gevestigde praktijken en standaarden.

Deze gedetailleerde beoordelingen, die bijzonderheden die specifiek waren voor de landen weerspiegelen, dienden als basis voor het modelbeleid en de modelwetteksten die het vooruitzicht boden van een wetgevingslandschap waarop de hele regio trots kan zijn. Het project zal zeker andere regio's tot voorbeeld strekken bij hun pogingen de katalytische kracht van ICT bruikbaar te maken voor het bespoedigen van economische integratie en sociale en economische ontwikkeling.

Ik maak gebruik van deze gelegenheid om dank uit te brengen aan de Europese Commissie en het ACP-Secretariaat voor hun financiële bijdrage. Ik breng ook dank uit aan het Secretariaat van de Caribische Gemeenschap (CARICOM) en het Secretariaat van de Caribische Telecommunicatie-Unie (CTU) voor hun bijdrage aan dit werk. Zonder de politieke wil van de zijde van de begunstigde landen zou niet veel zijn bereikt. Ik breng daarom mijn hartgrondige dank uit aan alle ACP-regeringen voor hun politieke wil welke dit project tot een groot succes heeft gemaakt.

Brahima Sanou,
BDT, Directeur

Dankwoord

Dit document vertegenwoordigt een van de resultaten van de regionale activiteiten uitgevoerd in het kader van het HIPCAR-project “Versterking van het Concurrentievermogen in het Caribisch Gebied door de Harmonisatie van Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT” officieel van start gegaan in Grenada in december 2008.

In reactie op zowel de uitdagingen als de kansen voortvloeiende uit de bijdrage van de informatie- en communicatietechnologie (ICT) aan de politieke, sociale, economische en ecologische ontwikkeling, hebben de Internationale Telecommunicatie-Unie (ITU) en de Europese Commissie (EC) hun krachten gebundeld en een overeenkomst getekend voor het geven van “Assistentie bij de vaststelling van geharmoniseerde beleidsregels voor de ICT-markt in de ACP”, als onderdeel van het Programma “ACP-Informatie- en Communicatietechnologie (@CP-ICT)” in het kader van het 9e Europees Ontwikkelingsfonds (EDF), i.e. het ITU-EC-ACP-project.

Dit wereldwijd ITU-EC-ACP-project wordt geïmplementeerd via drie aparte subprojecten die zijn afgestemd op de specifieke behoeften van elke regio: het Caribisch Gebied (HIPCAR), sub-Sahara Afrika (HIPSSA) en de Stille Zuidzee Eilandstaten (ICB4PAC).

De HIPCAR-Stuurgroep - voorgezeten door de Caribische Telecommunicatie-Unie (CTU) - zorgde voor de begeleiding en ondersteuning van een team van adviseurs, onder wie Gilberto Martíns de Almeida, Kwesie Prescod en Karen Stephen-Dalton. Het concept document werd vervolgens bestudeerd, gefinaliseerd en met een ruime consensus aangenomen door de participanten van twee consultatieworkshops voor de HIPCAR-Werkgroep Kwesties de Informatiemaatschappij rakende, gehouden te Saint Lucia van 8-12 maart 2010 en Barbados van 23-26 augustust 2010 (zie Bijlagen). De toelichting bij de modelwettekst in dit document is opgesteld door Gilberto Martíns de Almeida en behandelt onder andere de punten die tijdens de tweede workshop naar voren werden gebracht.

ITU wil een bijzonder woord van dank uitbrengen aan de delegaties van de Caribische ministeries belast met ICT en telecommunicatie die hebben deelgenomen aan de workshops, alsook aan vertegenwoordigers van ministeries van justitie en juridische zaken en andere lichamen uit de publieke sector, regelgevende lichamen, de academische wereld, het maatschappelijk middenveld, aanbieders van diensten en regionale organisaties, voor hun harde werk en toewijding bij het produceren van de inhoud van dit rapport. Door deze brede participatie van de publieke sector vertegenwoordigende verschillende sectoren heeft het project kunnen profiteren van een dwarsdoorsnede van standpunten en belangen. De bijdragen vanuit het Secretariaat van de Caribische Gemeenschap en de Caribische Telecommunicatie-Unie worden ook met dank gememoreerd.

Zonder de actieve betrokkenheid van al deze belanghebbenden, zou het niet mogelijk zijn geweest documenten zoals deze te produceren, welke niet alleen de algemene vereisten en voorwaarden van de Caribische regio weergeven maar ook de internationale beste praktijk vertegenwoordigen.

De activiteiten zijn ten uitvoer gelegd door Kerstin Ludwig, verantwoordelijk voor de coördinatie van activiteiten in het Caribisch Gebied (HIPCAR-Projectcoördinator), en Sandro Bazzanella, verantwoordelijk voor het beheer van het volledig project voor de landen in Afrika ten zuiden van de Sahara, het Caribisch Gebied en de Stille Oceaan (ITU-EC-ACP-Projectmanager), met algemene ondersteuning van Nicole Darmanie, HIPCAR-Projectassistent, en van Silvia Villar, ITU-EC-ACP-Projectassistent. Het werk is uitgevoerd onder de algemene leiding van Cosmas Zavazava, Hoofd, afdeling Projectondersteuning en Kennisbeheer (PKM). Het document is verder verbeterd aan de hand van de commentaren van de ITU Telecommunication Development Bureau’s (BDT) ICT-applicaties en Cybersecurity Divisie (CYB), evenals van Michael Tetelmann. Philip Cross van het ITU Regionaal Kantoor voor het Caribisch gebied verleende ondersteuning. De vooropmaak werd verzorgd door Pau Puig Gabarró. Het team van ITU’s Publication Composition Service (dienst samenstelling publicaties) is verantwoordelijk voor de publicatie.

Inhoudsopgave

Bladzijde

Inleiding

1.1. HIPCAR-Project – Doelstellingen en begunstigden

Het door de EU-ITU gefinancierd HIPCAR – project[1] met een looptijd van drie jaar werd door de Internationale Telecommunicatie Unie (ITU) en de Europese Unie (EU) gelanceerd in september 2008, in nauwe samenwerking met het Secretariaat van de Caribische Gemeenschap (CARICOM) en de Caribische Telecommunicatie Unie (CTU). Het maakt deel uit van een globaal ITU-EU-project voor de ACP-staten en omvat tevens de landen in Afrika ten zuiden van de Sahara en in de Stille Oceaan.

Het doel van HIPCAR is CARIFORUM[2] landen in het Caribisch gebied te assisteren bij het harmoniseren van hun beleid en procedures voor wet- en regelgeving op het vlak van informatie- en communicatietechnologie (ICT) met het oog op het scheppen van een gunstig klimaat voor ICT-ontwikkeling en connectiviteit, om zo de marktintegratie te bevorderen, de investering in verbeterde ICT-capaciteit en -diensten aan te moedigen en de bescherming van de belangen van ICT-gebruikers in de hele regio te vergroten. Het uiteindelijk doel van het project is het versterken van het concurrentievermogen en de sociaaleconomische en culturele ontwikkeling in het Caribisch gebied door middel van ICT.

Overeenkomstig artikel 67 van het Herziene Verdrag van Chaguaramas, kan HIPCAR worden beschouwd als een integrerend deel van het streven van de regio om de CARICOM Interne Markt & Economie (CSME) te ontwikkelen via de progressieve liberalisatie van zijn ICT-dienstensector. Het project biedt ook ondersteuning aan de CARICOM-Agenda voor Connectiviteit en de verplichtingen van de regio tegenover de Wereldtop over de informatiemaatschappij (WSIS), de Algemene Overeenkomst van de Wereldhandelsorganisatie inzake de Handel in Diensten (WTO-GATS) en de Millenniumdoelstellingen voor Ontwikkeling (MDG's). Het houdt tevens rechtstreeks verband met het bevorderen van het concurrentievermogen en een grotere toegang tot diensten in de context van verdragsverplichtingen zoals de Economische Partnerschapsovereenkomst van de CARIFORUM-landen met de Europese Unie (EU-EPA).

De begunstigde landen van het HIPCAR-project zijn Antigua en Barbuda, de Bahama's, Barbados, Belize, Gemenebest Dominica, de Dominicaanse Republiek, Grenada, Guyana, Haïti, Jamaica, St. Kitts en Nevis, St. Lucia, St. Vincent en de Grenadines, Suriname, en Trinidad en Tobago.

---

1 De volledige titel van het HIPCAR-project is "Versterking van het Concurrentievermogen in het Caribisch Gebied door de Harmonisatie van Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT". HIPCAR is deel van een mondiaal ITU-EC-ACP-project ondersteund en gefinancierd door de Europese Unie met EUR 8 miljoen en een aanvulling van USD 500,000 van de Internationale Telecommunicatie Unie (ITU). Het wordt uitgevoerd door de Internationale Telecommunicatie Unie (ITU) in samenwerking met de Caribische Telecommunicatie Unie (CTU) en met betrokkenheid van andere organisaties in de regio.
(zie **www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html**).

2 Het CARIFORUM is een regionale organisatie van vijftien onafhankelijke staten in het Caribisch gebied (Antigua en Barbuda, Bahama's, Barbados, Belize, Dominica, de Dominicaanse Republiek, Grenada, Guyana, Haïti, Jamaica, Saint Christopher en Nevis, Saint Lucia, Saint Vincent en de Grenadines, Suriname, en Trinidad en Tobago). Deze staten zijn alle ondertekenaars van de ACP-EU-verdragen.

1.2. Stuurcomité en Werkgroepen van het project

HIPCAR heeft een Stuurcomité voor het project ingesteld om te zorgen voor de nodige begeleiding en supervisie. Het Stuurcomité bestaat onder andere uit vertegenwoordigers van het Secretariaat van de Caribische Gemeenschap (CARICOM), de Caribische Telecommunicatie Unie (CTU), de Oost-Caribische Telecommunicatie Autoriteit (ECTEL), de Caribische Associatie van Nationale Telecommunicatie Organisaties (CANTO), de Caribische ICT-Virtuele Gemeenschap (CIVIC), en de Internationale Telecommunicatie Unie (ITU).

Om de inbreng van de belanghebbenden en de relevantie voor elk land te garanderen, werden ook HIPCAR-Werkgroepen geïnstalleerd bestaande uit leden die zijn aangewezen door de respectieve overheden van de landen – met inbegrip van specialisten van ICT-agentschappen, justitie en juridische zaken en andere publieke sector lichamen, nationale regelgevende instanties, nationale ICT-contactpersonen en personen verantwoordelijk voor het ontwikkelen van nationale wetgeving. Door deze brede participatie van de publieke sector uit verschillende sectoren heeft het project kunnen profiteren van een dwarsdoorsnede van standpunten en belangen. De Werkgroepen bestaan verder uit vertegenwoordigers van relevante regionale lichamen (CARICOM-Secretariaat, CTU, ECTEL en CANTO) en waarnemers van overige belanghebbende entiteiten in de regio (zoals het maatschappelijk middenveld, de particuliere sector, aanbieders van telecommunicatiediensten, de academische wereld, enz.).

De Werkgroepen waren verantwoordelijk voor het uitdiepen van de volgende twee werkgebieden:

1. *ICT-Beleidskader en Wetgevingskader voor Kwesties de Informatiemaatschappij rakende*, omvattende zes deelgebieden: e-commerce (transacties en bewijs), privacy & gegevensbescherming, onderscheppen van berichten, cybercriminaliteit, en toegang tot publieke informatie (vrijheid van informatie).
2. *ICT-Beleidskader en Wetgevingskader voor Telecommunicatie*, omvattende drie deelgebieden: universele toegang/diensten, interconnectie, en vergunningenbeleid.

De rapporten van de Werkgroepen gepubliceerd in deze documentenreeks zijn opgebouwd rond deze twee voornaamste werkgebieden.

1.3. Projectuitvoering en – inhoud

De aanzet tot de projectactiviteiten werd gegeven door middel van een rondetafelbespreking voor de lancering van het project gehouden in Grenada, van 15 tot 16 december 2008. Tot heden hebben alle begunstigde landen van het HIPCAR-project – uitgezonderd Haïti – samen met de als partners van het project optredende regionale organisaties, regelgevende instanties, aanbieders van telecommunicatiediensten, academische wereld en het maatschappelijk middenveld actief geparticipeerd in de HIPCAR-evenementen, met inbegrip van – naast de projectlancering in Grenada – regionale workshops in Trinidad & Tobago, St. Lucia, St. Kitts en Nevis, Suriname en Barbados.

De inhoudelijke activiteiten van het project staan onder leiding van teams van regionale en internationale deskundigen die samenwerken met de leden van de Werkgroepen die zich concentreren op de twee bovengenoemde werkgebieden.

Tijdens *Fase I* van het project – net afgerond – heeft HIPCAR:

1. een beoordeling gemaakt van de bestaande wetgeving van de begunstigde landen vergeleken met de internationale beste praktijk en in de context van harmonisatie in de gehele regio; en
2. model beleidsregels en model wetteksten opgesteld voor de bovengenoemde werkgebieden, waaruit het nationaal ICT-beleid en de nationale ICT-wetgeving/regelgeving kunnen worden ontwikkeld.

Het is de bedoeling dat deze voorstellen worden bekrachtigd of onderschreven door CARICOM/CTU en de autoriteiten van de landen in de regio als basis voor de volgende fase van het project.

Fase II van het HIPCAR-project is erop gericht begunstigde landen die daar belangstelling voor hebben assistentie te verlenen bij het omzetten van de eerder genoemde modellen in nationaal ICT-beleid en nationale ICT-wetgeving aangepast aan hun specifieke eisen, omstandigheden en prioriteiten. HIPCAR heeft fondsen gereserveerd om te kunnen inspelen op de verzoeken van de landen voor technische bijstand – met inbegrip van capaciteitsopbouw – nodig voor dit doel.

1.4. Overzicht van de zes HIPCAR-richtlijnen voor model beleid en wetteksten inzake kwesties de informatiemaatschappij rakende

Wereldwijd zijn landen, ook in het Caribisch gebied, op zoek naar manieren om wettelijke kaders te ontwikkelen voor het aanpakken van de behoeften van de informatiemaatschappij met het oog op het gebruikmaken van de groeiende aanwezigheid van het wereldwijde web als een kanaal voor de levering van diensten, ter garantie van een veilige omgeving en ter verhoging van de verwerkingskracht van informatie-systemen voor zakelijke efficiëntie en effectiviteit.

De informatiemaatschappij is gebaseerd op het uitgangspunt van toegang tot informatie en diensten en het gebruik van geautomatiseerde verwerkingssystemen ter verbetering van de levering van diensten aan markten en personen *overal in de wereld*. Voor zowel gebruikers als bedrijven biedt de informatiemaatschappij in het algemeen en de beschikbaarheid van informatie- en communicatietechnologie (ICT) unieke kansen. Terwijl de belangrijkste vereisten van de handel ongewijzigd blijven, creëert de directe overdracht van commerciële informatie mogelijkheden voor verbeterde zakelijke relaties. Dit gemak van uitwisseling van commerciële informatie brengt ook nieuwe paradigma's met zich mee: ten eerste, waar informatie wordt gebruikt om transacties met betrekking tot fysieke goederen en traditionele diensten te ondersteunen, en ten tweede, waar informatie zelf het product is dat wordt verhandeld.

De beschikbaarheid van ICT en nieuwe netwerk-gebaseerde diensten bieden een aantal voordelen voor de samenleving in het algemeen, met name voor ontwikkelingslanden. ICT-toepassingen, zoals e-overheid, e-handel, e-onderwijs, e-gezondheidszorg en e-milieu, worden gezien als faciliterend voor ontwikkeling, aangezien zij een efficiënt kanaal bieden voor de levering van een breed scala aan basisdiensten in afgelegen en landelijke gebieden. ICT-toepassingen kunnen de vervulling van de millennium ontwikkelingsdoelstellingen vergemakkelijken, armoede terugdringen en de gezondheids- en milieuomstandigheden in ontwikkelingslanden verbeteren. Onbelemmerde toegang tot informatie kan de democratie ondersteunen, als de informatiestroom buiten de controle valt van overheidsinstanties (zoals is gebeurd, bij voorbeeld in Oost-Europa). Met de juiste aanpak, context en uitvoeringsprocessen, kunnen investeringen in ICT-toepassingen en -instrumenten resulteren in productiviteit en kwaliteitsverbetering.

Echter, het transformatieproces gaat gepaard met uitdagingen aangezien het bestaande wettelijk kader niet noodzakelijk de specifieke eisen van een snel veranderende technische omgeving dekt. In gevallen waar informatie de handel in traditionele goederen en diensten ondersteunt, moet er duidelijkheid zijn in de manier waarop traditionele commerciële veronderstellingen worden toegepast, en in het geval waarin informatie het product is dat wordt verhandeld, moet de maker/ eigenaar van het product worden beschermd. In beide gevallen, moet er vastgesteld worden hoe het misdrijf aan het licht wordt gebracht, vervolgd en stopgezet in de realiteit van grensoverschrijdende transacties op basis van een immaterieel product.

De zes met elkaar verbonden model kaders

Het HIPCAR-project heeft zes (6) met elkaar verbonden model kaders ontwikkeld die een alomvattend wettelijk kader vormen voor de aanpak van de hierboven genoemde veranderende omgeving van de informatiesamenleving door het begeleiden en ondersteunen van de invoering van geharmoniseerde wetgeving in de HIPCAR begunstigde landen.

Inleiding

In de eerste plaats werd een juridisch kader ontwikkeld om het recht van gebruikers te beschermen in een veranderende omgeving en daarmee, naast andere aspecten, te zorgen voor vertrouwen van de consument en beleggers in rechtszekerheid en bescherming van privacy, en HIPCAR model wetteksten werden ontwikkeld om overwegingen aan te pakken met betrekking tot: **de toegang tot publieke informatie (Vrijheid van Informatie)** – gericht op het stimuleren van de juiste cultuur van transparantie in regelgeving in het voordeel van alle belanghebbenden; en **privacy en gegevensbescherming** – gericht op het waarborgen van de bescherming van de privacy en persoonlijke gegevens naar tevredenheid van het individu. Dit laatste kader is gericht op passende geheimhoudingspraktijken binnen zowel de publieke als private sector.

In de tweede plaats, werd een HIPCAR model wettekst ontwikkeld voor **elektronische handel (transacties)**, met inbegrip van elektronische handtekeningen voor het vergemakkelijken van de harmonisatie van de wetten met betrekking tot de standaardverwachtingen en rechtsgeldigheid van contract formuleringspraktijken. Dit kader is erop gericht om te voorzien in de gelijkwaardigheid van papieren en elektronische documenten en contracten en voor het leggen van een basis voor het aangaan van handel in cyberspace. Een wettekst over **elektronische handel (bewijs)** – de bijbehorende tekst voor het kader voor elektronische handel (transacties) werd toegevoegd ter regulering van het wettig bewijs, in zowel civiele en criminele procedures.

Om ervoor te zorgen dat ernstige schendingen van de vertrouwelijkheid, integriteit en beschikbaarheid van ICT en de gegevens kunnen worden onderzocht door de rechtshandhaver, werden model wetteksten ontwikkeld om wetgeving te harmoniseren op het gebied van het strafrecht en het strafprocesrecht. De wettekst inzake **cybercriminaliteit** definieert strafbare feiten, onderzoeksinstrumenten en de strafrechtelijke aansprakelijkheid van de belangrijkste actoren. Een wettekst over het **onderscheppen van elektronische communicatie** verschaft een passend kader dat het wederrechtelijk onderscheppen van communicatie verbiedt en heeft een minieme mogelijkheid geschapen zodat de rechtshandhaver in staat wordt gesteld om rechtmatig communicatie te onderscheppen, indien aan bepaalde duidelijk omschreven voorwaarden is voldaan.

Ontwikkelen van de model wetteksten

De model wetteksten werden ontwikkeld rekening houdend met de belangrijkste elementen van internationale trends, alsmede juridische tradities en beste praktijken uit de regio. Dit proces werd ondernomen zodat de kaders het beste beantwoorden aan de realiteit en de behoeften van de regio van HIPCAR begunstigde landen waarvoor en waarmee zij zijn ontwikkeld. Daarom was er tijdens het proces veel interactie met belanghebbenden in elk stadium van de ontwikkeling.

De eerste stap in dit complexe proces is een evaluatie van de bestaande juridische kaders binnen de regio door middel van een beoordeling van de wetgeving betreffende alle relevante gebieden. Naast uitgevaardigde wetgeving, werd in het overzicht opgenomen, indien relevant, wetsontwerpen die waren voorbereid, maar die nog niet het proces van afkondiging hadden voltooid. In een tweede stap werden de beste internationale praktijken (bijvoorbeeld van de Verenigde Naties, OESO, EU, het Gemenebest, UNCITRAL en CARICOM), alsmede geavanceerde nationale wetgeving (bijvoorbeeld uit het Verenigd Koninkrijk, Australië, Malta en Brazilië, onder andere) geïdentificeerd. Deze beste praktijken werden gebruikt als maatstaf.

Voor elk van de zes gebieden, werden complexe juridische analyses opgesteld, die de bestaande wetgeving in de regio vergeleek met deze maatstaven. Deze rechtsvergelijkende analyse leverde een momentopname van de mate van vooruitgang op belangrijke beleidsterreinen binnen de regio. Deze bevindingen waren leerzaam, en toonden aan dat er een meer geavanceerde ontwikkeling was in wetgevingskaders met betrekking tot elektronische transacties, cybercriminaliteit (of "computermisbruik") en toegang tot publieke informatie (vrijheid van informatie) dan is gebleken in de andere kaders.

Inleiding

Op basis van de resultaten van de rechtsvergelijkende analyses, hebben de regionale belanghebbenden “bouwstenen” ontwikkeld voor basisbeleid, die – zodra deze zijn goedgekeurd door de betrokken partijen – de basis bepalen voor de verdere beraadslaging over het beleid en ontwikkeling van de wettekst. Deze bouwstenen voor het beleid bevestigden een aantal gemeenschappelijke thema's en trends in de internationale precedenten, maar identificeerden ook bepaalde overwegingen die moeten worden opgenomen binnen de context van een regio die bestaat uit soevereine kleine eiland-ontwikkelingslanden. Een voorbeeld van een belangrijke overweging betreffende de situatie die de beraadslagingen beïnvloedde in deze fase en in andere fasen van het proces was de kwestie van institutionele capaciteit om adequaat beheer van deze nieuwe systemen te faciliteren.

De beleidsbouwstenen werden vervolgens gebruikt om aangepaste model wetteksten te ontwikkelen die zowel aan de internationale normen en de vraag van de HIPCAR begunstigde landen voldoen. Elke model tekst werd vervolgens opnieuw geëvalueerd door de betrokken partijen vanuit het perspectief van de levensvatbaarheid en de mogelijkheid om te worden vertaald naar de regionale context. Als zodanig, heeft de groep belanghebbenden – bestaande uit een mix van wetgevingsjuristen en beleidsdeskundigen uit de regio – teksten ontwikkeld die het beste het samenvallen van de internationale normen met lokale overwegingen weerspiegelen. Een brede betrokkenheid van vertegenwoordigers van bijna alle 15 HIPCAR begunstigde landen, regelgevers, aanbieders van telecommunicatiediensten, regionale organisaties, het maatschappelijk middenveld en de academische wereld heeft ervoor gezorgd dat de wetteksten verenigbaar zijn met de verschillende wettelijke normen in de regio. Het werd echter ook erkend dat elke begunstigde staat misschien specifieke voorkeuren heeft met betrekking tot de uitvoering van sommige bepalingen. Daarom bieden de model teksten ook een keuze in de benadering binnen de algemeenheid van een geharmoniseerd kader. Deze aanpak is gericht op het faciliteren van brede acceptatie van de documenten en het verhogen van de mogelijkheid van een tijdige uitvoering in alle begunstigde rechtsgebieden.

Interactie en het overlappen van de model teksten

Als gevolg van de aard van de kwesties die worden overwogen, weerspiegelen alle zes kaders een aantal algemene aspecten.

In eerste instantie moet aandacht worden besteed aan de kaders die zorgen voor het gebruik van elektronische middelen in communicatie en uitvoering van handel: **Elektronische handel (transacties), elektronische handel (bewijs), cybercriminaliteit** en **onderscheppen van communicatie**. Alle vier kaders handelen over kwesties in verband met de behandeling van berichten verzonden via communicatienetwerken, de vaststelling van passende testen om de geldigheid van documenten of andere bescheiden te bepalen en de integratie van systemen gericht op de gelijke behandeling van papieren en elektronisch materiaal bij bescherming tegen onheuse behandeling, consumentenzaken en procedures voor geschillenbeslechting.

Als zodanig, zijn er verschillende gemeenschappelijke definities in deze kaders die rekening moeten houden met, waar nodig, overwegingen betreffende een uiteenlopende reikwijdte van de toepasbaarheid. Gemeenschappelijke concepten zijn onder meer: “elektronisch communicatienetwerk" – wat moet worden afgestemd op de bestaande definitie van het rechtsgebied in de heersende telecommunicatiewetten; "elektronisch document" of "elektronische bescheiden" – die een brede interpretatie moeten hebben zodat bijvoorbeeld audio- en videomateriaal daaronder vallen; en "elektronische handtekeningen", "geavanceerde elektronische handtekeningen", "certificaten", "geaccrediteerde certificaten", "certificaat dienstverleners" en "certificatie-instanties" – die allemaal te maken hebben met de toepassing van encryptietechnieken voor elektronische validatie van authenticiteit en de erkenning van de technologische en economische sector, die is opgezet rond het verlenen van dergelijke diensten.

In deze context, legt **elektronische handel (transacties),** onder andere, kernbeginselen neer van de erkenning en toekenning die nodig zijn voor de effectiviteit van de andere kaders. De nadruk ligt op het definiëren van de fundamentele beginselen die gebruikt moeten worden bij het bepalen van de gevallen van een civiele of commerciële aard. Dit kader is ook van essentieel belang bij het bepalen van een

geschikte marktstructuur en een realistische strategie voor de sector toezicht in het belang van het publiek en het vertrouwen van de consument. Beslissingen over de kwesties gerelateerd aan een dergelijk administratief systeem hebben vervolgens een invloed op hoe elektronische handtekeningen procedureel worden gebruikt ten behoeve van bewijsvoering, en hoe de verantwoordelijkheden en verplichtingen in de wet gedefinieerd op de juiste manier kunnen worden toegeschreven.

Deze veronderstelling van gelijkwaardigheid geeft de overige kaders de mogelijkheid op adequate wijze om te gaan met de vertrekpunten betreffende de passende behandeling van elektronische informatieoverdracht. Het kader voor **cybercriminaliteit**, bij voorbeeld, definieert strafbare feiten met betrekking tot de onderschepping van communicatie, verandering van communicatie- en computergerelateerde fraude. Het kader voor **elektronische handel (bewijs)** voorziet in een basis die elektronisch bewijsmateriaal introduceert als een nieuwe categorie van bewijs.

Een belangrijke rode draad die **e-transacties** en **cybercriminaliteit** aan elkaar verbindt is de vaststelling van de passende aansprakelijkheid en verantwoordelijkheid van dienstverleners van wie diensten worden gebruikt in situaties van elektronisch gepleegde misdrijven. Speciale aandacht werd besteed aan de samenhang bij het bepalen van de doelpartijen voor deze relevante delen en te zorgen voor de juiste toepassing van de verplichtingen en de handhaving daarvan.

In het geval van de kaders gericht op het verbeteren van gereglementeerd overzicht en vertrouwen van de gebruiker, behandelen de model teksten ontwikkeld door HIPCAR de twee uitersten van hetzelfde probleem: terwijl het model **toegang tot publieke informatie** de bevordering van de openbaarmaking van publieke informatie bevordert op specifieke uitzonderingen na, stimuleert het model **privacy en gegevensbescherming** de bescherming van een subset van deze informatie, die onttrokken is aan het vorige model. Belangrijk is dat beide kaders zijn gericht op het stimuleren van beter documentbeheer en archiveringspraktijken binnen de publieke sector en – in het geval van het laatstgenoemde kader – een aantal aspecten van de particuliere sector. Het is echter opmerkelijk dat – in tegenstelling tot de andere vier modelteksten – deze kaders niet uitsluitend van toepassing zijn op het elektronisch medium, noch voor het creëren van een gunstig kader waarbij overwegingen van een nieuw medium worden overgebracht naar bestaande procedures. Om te zorgen voor consistentie, zijn de kaders gericht op het reguleren van een passend beheer van informatiebronnen, in zowel elektronische en niet-elektronische vorm.

Er zijn een aantal structurele en logistieke overlappingen die bestaan tussen deze twee wettelijke kaders. Onder andere in de definitie van de belangrijkste concepten van "overheidsinstantie" (de personen op wie de kaders van toepassing zouden zijn), "informatie", "gegevens" en "document", en de relatie tussen deze. Een andere belangrijke vorm van overlapping betreft het gepaste toezicht op deze kaders. Beide kaders vereisen de instelling van toezichthoudende instanties, die voldoende onafhankelijk van invloeden van buitenaf moeten zijn om zo het publiek te verzekeren van de integriteit van hun beslissingen. Deze onafhankelijke instanties moeten ook de capaciteit hebben om boetes en/of sancties op te leggen tegen partijen die activiteiten ondernemen om de doelstellingen van een van deze kaders te frustreren.

Conclusie

De zes HIPCAR model wetteksten voorzien de begunstigde landen van het project met een uitgebreid kader om het meest relevante gebied van regelgeving aan te pakken met betrekking tot vraagstukken van de informatiemaatschappij. In de formulering werden zowel de meest actuele internationale normen, alsook de eisen van kleine eiland-ontwikkelingslanden in het algemeen en – meer specifiek – die van de begunstigde HIPCAR-landen opgenomen. De brede betrokkenheid van de belanghebbenden uit deze begunstigde landen in alle fasen van de ontwikkeling van de model wetteksten zorgt ervoor dat zij probleemloos en tijdig kunnen worden aangenomen. Hoewel de nadruk ligt op de behoeften van de landen in het Caribisch gebied, zijn de genoemde model wetteksten reeds geïdentificeerd als mogelijke richtsnoeren door bepaalde landen in andere regio's van de wereld.

Gezien de specifieke en nauw met elkaar verbonden aard van de HIPCAR model teksten, zal het voor de begunstigde projectlanden het voordeligst zijn wetgeving te ontwikkelen en introduceren op basis van deze modellen op een gecoördineerde wijze. De modellen voor de elektronische handel (transacties en bewijs) zullen het meest effectief functioneren in geval van gelijktijdige ontwikkeling en adoptie van de kaders voor cybercriminaliteit en onderscheppen van communicatie, aangezien die zo nauw verbonden en afhankelijk van elkaar zijn voor het aanpakken van de zorgpunten betreffende de ontwikkeling van een gedegen regelgeving. De kaders voor toegang tot publieke informatie en privacy en gegevensbescherming bevatten ook dergelijke synergieën in de administratieve kaders en kerncompetentie vereisten dat de gelijktijdige aanname slechts beide kaders kan versterken in de uitvoering ervan.

Op deze manier zal er een optimale mogelijkheid gecreëerd worden om de holistische kaders te benutten die zijn ingesteld in de regio.

1.5. Dit rapport

Dit rapport handelt over privacy en gegevensbescherming, een van de werkterreinen van de Werkgroep inzake ICT-Beleidskader en Wetgevingskader voor Kwesties de Informatiemaatschappij rakende. Het omvat Richtlijnen voor Model beleid en een Model Wettekst met Memorie van Toelichting die de landen in het Caribisch gebied zouden kunnen gebruiken wanneer zij hun eigen nationaal beleid en wetgeving op dit gebied ontwikkelen of bijwerken.

Voorafgaand aan het formuleren van dit document, heeft een team van deskundigen van HIPCAR – in nauwe samenwerking met de bovenstaande leden van de Werkgroep – een evaluatie voorbereid en beoordeeld van bestaande wetgeving in de vijftien begunstigde HIPCAR-landen in de regio die zich op zes gebieden heeft geconcentreerd: Elektronische Transacties, Elektronisch Bewijs bij e-commerce, Privacy en gegevensbescherming, Onderschepping van Communicatie, Cybercriminaliteit, en Toegang tot publieke informatie (Vrijheid van Informatie). Deze evaluatie hield rekening met geaccepteerde internationale en regionale beste praktijken.

Deze regionale evaluatie – apart gepubliceerd als bijbehorend document voor het huidige rapport[3] – betrof een vergelijkende analyse van de huidige wetgeving met betrekking tot Privacy en gegevensbescherming in de begunstigde HIPCAR-landen en de identificatie van eventuele lacunes met betrekking hiertoe, waardoor de basis werd gelegd voor de ontwikkeling van een raamwerk voor model beleid en wettekst hierin gepresenteerd. Doordat de nationale, regionale en internationale beste toepassing in de praktijk en standaarden worden weerspiegeld, terwijl tegelijkertijd de compatibiliteit met de juridische tradities in het Caribisch gebied zijn gegarandeerd, beantwoorden de model documenten in dit rapport aan de specifieke vereisten van de regio.

De model wettekst inzake privacy en gegevensbescherming werd in drie fasen ontwikkeld: (1) het opstellen van een evaluatierapport; (2) de ontwikkeling van richtlijnen voor model beleid; en (3) het formuleren van een model wettekst. Het beoordelingsrapport werd voorbereid in twee fasen door HIPCAR-consultants. De eerste fase werd uitgevoerd door Mw. Karen Stephen-Dalton, en de tweede fase door dhr. Kwesi Prescod. Hierna werden de concept documenten bekeken, besproken en met een brede consensus aangenomen door de HIPCAR-werkgroep inzake Kwesties de Informatiemaatschappij rakende tijdens twee consultatieworkshops gehouden te Saint Lucia van 8-12 maart 2010 en St. Kitts en Nevis van 19-22 juli 2010 (zie Bijlagen). De Memorie van Toelichting bij de model wettekst in dit document is opgesteld door dhr. Prescod waarin onder andere de zaken die naar voren zijn gebracht in de tweede workshop worden behandeld. Dit document bevat daarom gegevens en informatie zoals bekend in juli 2010.

[3] Zie HIPCAR “Privacy en gegevensbescherming: Evaluatierapport” beschikbaar op www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

Volgend op dit proces werden de documenten afgerond en verspreid onder alle belanghebbenden ter overweging van de overheden van de HIPCAR begunstigde landen.

1.6. Het belang van effectief beleid en wetgeving inzake privacy en gegevensbescherming

Privacy is geïdentificeerd als een mensenrecht, zoals neergelegd in verschillende bepalingen van de Universele Verklaring van de Mensenrechten, Internationaal Verdrag inzake Burgerrechten en Politieke Rechten, evenals het Amerikaans en Europees Mensenrechtenverdrag. Dit recht op privacy wat het privéleven van het individu beschermt tegen willekeurige, onrechtmatige of grove inmenging geeft bij uitbreiding bescherming van de persoonsgegevens van een individu, en de bescherming tegen een verzending van dergelijke informatie.

De hedendaagse discussie over privacy en gegevensbeschermingskaders zouden betekenisloos zijn zonder de alomtegenwoordigheid van informatie- en communicatietechnologie te bespreken evenals de capaciteit die deze verschaft voor de analyse, verwerking en het delen van informatie. Terwijl de bedrijven uitkijken naar het gebruik van nieuwe kanalen om hun concurrentiepositie in de lokale en mondiale markt te verbeteren, is het vertrouwen van de gebruiker dat informatie die is ingediend voor het afronden van een transactie wordt beschermd tegen gebruik door andere partijen zonder hun kennis van essentieel belang voor het adopteren en het succes van de elektronische revolutie via het Internet. Op deze manier, kunnen de implementatie van privacy en gegevensbeschermingskaders de doelstelling van wetgeving inzake elektronische handel ondersteunen door een holistisch kader aan te dragen voor het versterken van het gewenste gevoel van integriteit binnen het bredere regelgevingskader, en het vermogen daarvan om de klant te beschermen te schragen.

Privacy en gegevensbescherming wetten zijn gebaseerd op de vooronderstelling dat het individu enige mate van controle moet bezitten over hoe persoonsgegevens die over hem wordt verzameld door de overheid of bedrijven wordt gebruikt, verwerkt of openbaar gemaakt. De controle wordt voornamelijk bevestigd op het punt waar de informatie wordt verzameld, op welk moment de verzamelende partij volledig zijn intenties moet onthullen waarom de informatie wordt verzameld, en het op zich neemt zich op die wijze te beperken bij het gebruik van de persoonsgegevens nadat die verzameld is. De andere belangrijke bevordering van de controle van het individu is de verplichting van de verzamelende partij om het individu de kans te geven alle informatie te bekijken die wordt opgeslagen door de partij over het individu. Ondanks dit, zouden er uitzonderingen moeten zijn op de algemene regels die zijn geassocieerd met de beperking van het gebruik van persoonsgegevens, met de toepassing van specifieke, verschillende richtlijnen op het gebied van medische dienstverlening en nationale veiligheid waarvoor het verkrijgen van de instemming van het individu niet praktisch is.

Op die wijze, zijn beleidslijnen en wetgevingskaders die handelen over privacy and gegevensbescherming gericht op het behandelen van slechts het beheren van privé en persoonsgegevens. Op deze manier, werken dergelijke kaders samen met de regels handelend over de overheid die toegang geeft aan het publiek tot niet-gevoelige informatie die het bezit, aangezien dergelijke kaders over het algemeen niet handelen over het beheer van persoonsgegevens anders dan de algemene uitzonderingen op de bepalingen van dergelijke wetten.

Hoewel er specifieke overweging dient te worden gegeven aan de supervisie van de overheid, zouden privacy en gegevensbeschermingskaders niet beperkt moeten worden tot de publieke sector, maar alle partijen moeten omvatten die om zakelijke redenen persoonsgegevens van klanten verzamelen, opslaan en analyseren. Privacy en gegevensbeschermingswetten zijn van kritiek belang voor de betekenisvolle opzet van e-overheidssystemen die zijn gericht op het verbeteren van de efficiëntie van de levering van overheidsgoederen en -diensten, evenals het verbeteren van de economische concurrentiepositie van de commerciële sector.

Inleiding

Overheidslichamen en andere agentschappen hebben bij de levering van publieke diensten traditioneel, als onderdeel van hun mandaat, persoonsgegevens gebruikt van klanten uit het publiek. Echter, met de beweging naar meer transparantie en gelijkheid in het beheer van overheidszaken zijn er een aantal zorgpunten die betrekking hebben op hoe deze informatie gebruikt zal worden. Deze zorgpunten kunnen variëren van het beperken van de invloed van een oneerlijk vooroordeel op basis van ras, religie, etniciteit, geslacht of seksuele geaardheid bij de toewijzing van publieke middelen, goederen of diensten die niet direct verband houden met deze kenmerken, tot zorgpunten met betrekking tot de systemen die aanwezig zijn voor de bescherming van opgeslagen informatie tegen de illegale toegang door andere partijen. Op die wijze, net wanneer er een verplichting is voor het vaststellen van kaders voor het minimaliseren van de overweging van privé karakteristieken bij de evaluatie van toegang tot publieke middelen, tenzij deze kenmerken, volgens de wet, de wezenlijke discretionaire factor zijn in het evaluatieproces, moet er ook bescherming zijn tegen onbevoegde openbaarmaking of toegang tot persoonsgegevens door te verzekeren dat enkele toepasselijke minimumstandaarden van informatiebeveiliging voorhanden zijn.

Gezien vanuit het perspectief van de private sector, eisen de klanten steeds meer zekerheden dat persoonsgegevens verzameld tijdens het uitvoeren van een bepaalde zakelijke transactie niet wordt gebruikt of misbruikt door derden. Dergelijke garantie moet de verkoop of openbaarmaking van persoonsgegevens aan derden anderszins beperken zonder de kennis, en stilzwijgende toestemming van het individu.

Privacy en gegevensbeschermingswetten moeten ook de opkomende aard van elektronische handel erkennen en de de stimulans voor grensoverschrijdende informatieoverdracht. Bedrijven die informatie- en communicatietechnologie aangrijpen hebben de neiging te zoeken naar mogelijkheden voor het rationaliseren van investeringen om kosten te verminderen en efficiëntie te vergroten. In veel van deze gevallen houden dergelijke strategieën in het bijeenvoegen van informatie die is verzameld in de loop van het zakendoen naar een enkele locatie. In het geval van multinationals betekent dit meestal dat de bijeenvoeging van zakelijke informatie van de verschillende landen op een enkele locatie die zich niet bevindt binnen een van de rechtsgebieden waarin de informatie is verzameld. In dit geval, indien de regels voor de bescherming van persoonsgegevens niet zo strikt zijn als die van het land waarin de onderneming informatie verzameld, kan deze onevenwichtigheid resulteren in het compromitteren van de privacy van personen in de wezenlijke rechtsgebieden van de bedrijfsvoering. Dit is een dusdanig essentieel punt, dat de wederzijdse bescherming van persoonsgegevens een belangrijk onderdeel vormt van hedendaagse handelsovereenkomsten tussen naties, en/ of regelgevende beperkingen die zijn opgelegd aan multinationals. De implementatie van privacy en gegevensbeschermingsregels stelt landen dan in staat om nieuwe gebieden van economische inspanning te betreden, daarin te participeren en voordeel van te hebben op het gebied van internationale handel die betrekking hebben op het leveren van diensten op afstand.

Tenslotte, is er een recente discussie over de economische mogelijkheden die zijn geassocieerd met het beheer, gebruik en de analyse van informatie verzameld via internetinhoud bijeenvoegingssoftware of marketingbedrijven. Dit heeft geleid tot de bespreking van de “waardeketen persoonsgegevens”, en de erkenning van het economisch potentieel dat is geassocieerd met de verschillende actoren in deze keten. De kern van het kader voor de nieuwe informatie-economie omvat een erkenning van de rechten van het individu om macht uit te oefenen over hoe bepaalde persoonsgegevens gebruikt moet worden. Daarom, als de internet economische revolutie op drift komt, zullen de implementatie en handhaving, en dus de geloofwaardigheid van de privacy en gegevensbeschermingregels van een rechtsgebied een belangrijk concurrentievoordeel worden voor dat rechtsgebied als een investeringsspeerpunt in dit ontluikend gebied voor bedrijfsactiviteiten – welke voornamelijk het beheren van persoonsgegevens betreft.

Daarom, zal de implementatie van effectieve beleidslijnen, wetgeving en systemen voor het waarborgen van privacy en gegevensbescherming substantiële veelvormige voordelen opleveren aan een land dat bijdraagt aan de verbetering van bestuur en democratie, evenals het land voorbereidt, en de bedrijven daar gevestigd, op het aangrijpen van nieuwe mogelijkheden die zich voordoen in het informatietijdperk. De implementatie van dergelijke beleidslijnen, wetgeving en systemen moeten de administratieve kaders weerspiegelen die de potentie voor ongepaste inmenging beperken voor zowel de uitvoerende arm van de staat of commerciële ondernemingen om zo het belang te versterken van privacy en gegevensbescherming voor de regels en principes van goed bestuur.

Deel I
Richtlijnen voor model beleid
Privacy en gegevensbescherming

Hieronder volgen de richtlijnen voor model beleid die een land kan overwegen met betrekking tot privacy en gegevensbescherming.

1. CARICOM/CARIFORUM-LANDEN ZULLEN ZICH EROP RICHTEN OM DUIDELIJKE WETTELIJKE EN INSTITUTIONELE KADERS TE INTRODUCEREN OM DE BESCHERMING VAN PERSOONLIJKE EN PRIVE INFORMATIE TE GARANDEREN

- Er is een duidelijk wettelijk mandaat in de wet ter ondersteuning van het instellen van een systeem om de bescherming van persoonlijke en/of privé informatie te waarborgen.
- Het systeem van gegevensbescherming dient niet technologiespecifiek te zijn, en moet daarom gelijkaardige relevantie hebben in omgevingen die met papieren werken of ICT-technologie toepassen.
- De wet/het wettelijk mandaat moet duidelijk aangeven dat de wet de de staat verbindt.
- De wet/het wettelijk mandaat moet verzekeren dat de verplichting om privacy te beschermen toepasselijk is op zowel de publieke en private sector.
- De wet/het wettelijk mandaat identificeert duidelijk het aangewezen agentschap voor de implementatie van het privacy en gegevensbeschermingskader.
- De wet/het wettelijk mandaat voorziet duidelijk in de onafhankelijkheid van het aangewezen agentschap.
- De wet/het wettelijk mandaat voorziet er duidelijk in dat persoonsgegevens moet worden verzameld en verwerkt met de instemming van het subject van de persoonsgegevens.
- De wet/het wettelijk mandaat voorziet duidelijk in de omstandigheden waaronder persoonsgegevens kunnen worden verzameld en verwerkt zonder de instemming van of kennisgeving aan het subject van de persoonsgegevens.
- De wet/het wettelijk mandaat moet een categorie persoonsgegevens identificeren als “gevoelige informatie”, waarvoor een strikter toezicht en controle vereist is.

2. CARICOM/CARIFORUM-LANDEN ZULLEN WAARBORGEN DAT ESSENTIELE BEGINSELEN OVER GEGEVENSBESCHERMING DUIDELIJK ZIJN GEDEFINIEERD IN DE RELEVANTE WETTEN

- Essentiële beginselen over het gegevensbeschermingskader zijn duidelijk gedefinieerd in de wetten.
- Onder de essentiële beginselen over gegevensbescherming zouden dergelijke bepalingen moeten zijn die waarborgen dat op het moment van het verzamelen van de gegevens het datasubject bewust wordt gemaakt wat de doelstelling/ het gebruik van dergelijke gegevens zal zijn en duidelijk instemt met dergelijke doelstelling/ gebruik van die gegevens.
- Onder de essentiële beginselen van gegevensbescherming moeten dergelijke bepalingen aanwezig zijn die de verantwoordelijkheid bij de persoon en/ of het lichaam plaatsen die de persoonsgegevens verzamelt en/of verwerkt voor de beveiliging, nauwgezetheid en juist gebruik van die informatie.
- Onder de essentiële beginselen van gegevensbescherming moeten dergelijke bepalingen zijn die vertrouwen bij het publiek scheppen door toe te laten dat het datasubject deze kan controleren en de nauwgezetheid van de informatie kan verzekeren die wordt bijgehouden over hem door om het even welke persoon.

- Onder de essentiële beginselen van gegevensbescherming moeten dergelijke bepalingen zijn die de grensoverschrijdende overdracht van persoonsgegevens beperkt naar rechtsgebieden die niet dezelfde beschermingsmechanismen voor privacy en gegevensbescherming delen.

3. CARICOM/CARIFORUM-LANDEN ZULLEN STREVEN NAAR HET INSTELLEN VAN JUISTE BESTUURSKADERS WAARBIJ IN INSTITUTEN WORDT VOORZIEN DIE TOEPASSELIJKE BEVOEGDHEDEN HEBBEN VOOR HET VERGEMAKKELIJKEN VAN HET TOEZICHT

- De wet/het wettelijk mandaat zal duidelijk aangeven dat er bepalingen moeten zijn voor de duidelijke identificatie van de verzamelaars, gebruikers en verwerkers van persoonsgegevens dergelijke bepaling kan een kennisgeving inhouden aan of registratie bij de aangewezen persoon.
- De instantie die is aangewezen voor het waarborgen van de naleving van de wet/ het wettelijk mandaat zal een aparte rechtspersoon zijn die de bevoegdheid heeft activa te bezitten en daar afstand van te doen, het vermogen heeft contracten aan te gaan, en die onafhankelijk zal zijn bij de uitvoering van zijn taken.
- Het hoofd van de aangewezen instantie zal worden benoemd op een wijze die de onafhankelijkheid en onpartijdigheid van de functies waarborgt.
- Het hoofd van de aangewezen instantie zal dergelijke functievoorwaarden en bepalingen worden aangemeten, waaronder bepalingen betreffende verankering en voorwaarden voor herbenoeming, opgenomen in de wet/ het wettelijk mandaat die voldoende zijn om mogelijkheden tot overreding en dwang te beperken.
- Het hoofd van de aangewezen instantie zal in de wet/ het wettelijk mandaat de nodige onderzoeksbevoegdheden worden toegekend om de uitvoering van de functies van het gegevensbeschermingskader te vergemakkelijken.
- Het hoofd van de aangewezen instantie zal in de wet/ het wettelijk mandaat de bevoegdheid worden toegekend bepaalde rechten te delegeren naar erkende vertegenwoordigers om de uitvoering van zijn functie te vergemakkelijken.
- De aangewezen instantie kan controles of onderzoeken instellen naar de activiteiten van personen op wie het kader van toepassing is, zowel op eigen initiatief als in antwoord op klachten van het publiek. De kosten van dergelijke controles of onderzoeken zullen worden gedragen door de persoon bepaald in de regelgeving.
- Personen op wie de wet van toepassing is, zullen meewerken met de aangewezen instantie in de uitvoering van zijn taken, op straffe van een civiele en/of strafrechtelijke sanctie.
- De aangewezen instantie kan verzoeken doen, waaraan relevante personen moeten voldoen, voor de indiening van bepaalde documenten ter vergemakkelijking van het onderzoek. De instantie kan een bevelschrift van de rechter aanvragen om dit te bereiken, indien dat gerechtvaardigd mocht zijn.
- In de wet/het wettelijk mandaat, kan de aangewezen instantie beschermd worden tegen enige aansprakelijkheid voor handelingen die zijn uitgevoerd in goed vertrouwen bij de uitoefening van zijn taken.
- De aangewezen instantie zal jaarlijks rapporteren aan het parlement/ wetgevende raad betreffende zijn activiteiten in het voorgaande jaar.
- De wet /het wettelijk mandaat zal een tijdskader aangeven waarbinnen de aangewezen instantie in werking zal treden na de aanname van de wet.

Deel I

4. CARICOM/CARIFORUM-LANDEN ZULLEN BEPAALDE VEREISTEN EN VERPLICHTINGEN MET BETREKKING TOT DE VERGARING VAN PERSOONLIJKE GEGEVENS VASTLEGGEN

- De wet/het wettelijk mandaat zal herbevestigen dat de overheid slechts persoonsgegevens vergaart die uitdrukkelijk zijn toegestaan door een geschreven wet.
- De wet/het wettelijk mandaat zal voorzien in de uitdrukkelijke kennisgeving aan het datasubject van het doel waarvoor de persoonsgegevens worden vergaard, en dat de informatie die wordt vergaard relevant is voor dat doel.
- De wet/het wettelijk mandaat zal erin voorzien dat het datasubject uitdrukkelijk instemt met de vergaring van gegevens.
- De wet/het wettelijk mandaat zal in de vergaring voorzien van persoonsgegevens slechts van het datasubject, behoudens specifieke uitzonderingen die worden geassocieerd met nationale veiligheidsoverwegingen of management van de gezondheid.
- De wet/het wettelijk mandaat zal voorzien in uitzonderingen die duidelijk, precies en beperkt zijn zodat er voldoende beveiliging blijft van het datasubject tegen ongerechtvaardigde gegevensverzameling.
    - In aanverwante wetten of regelgeving, zullen er specifieke overwegingen worden opgenomen om te waarborgen dat er voldoende checks-and-balances zijn voor de toegang en het gebruik van persoonsgegevens met betrekking tot de uitzonderingen die zijn geïdentificeerd in de algemene privacy en gegevensbeschermingswetten.
- De wet/het wettelijk mandaat voorziet erin dat het datasubject in kennis moet worden gesteld op het moment van de gegevensverzameling, betreffende de persoon die de houder zal zijn van de gegevens, de verwachte bewaartermijn van de gegevens en de wijze waarop de gegevens zullen worden verwijderd bij het verstrijken van de bewaartermijn, behalve in omstandigheden voor de management van de gezondheid of nationale veiligheid.
- De wet/het wettelijk mandaat beperkt de verzameling van gevoelige gegevens behalve in specifieke gevallen en voor specifieke doelen. Dergelijke uitzonderingen kunnen omvatten:
    - De ontwikkeling van statistieken;
    - Management van de gezondheid
    - Vereisten van de rechtshandhaving;
    - Vereisten van de rechtsstaat;
    - Vereisten van een rechterlijke bevelschrift;
- De wet/het wettelijk mandaat schrijft civiele en strafrechtelijke sancties voor in het geval van schending van de vastgestelde bepalingen die betrekking hebben op de verzameling van persoonsgegevens. Dergelijke strafsancties kunnen worden opgelegd aan de verzamelende partij, of enige functionaris of directeur waarvan kan worden bewezen dat die opzettelijk de wet/ het wettelijk mandaat heeft geschonden.

5. CARICOM/CARIFORUM-LANDEN ZULLEN BEPAALDE VEREISTEN EN VERPLICHTINGEN MET BETREKKING TOT DE VERWERKING VAN PERSOONSGEGEVENS VASTLEGGEN

- De wet/het wettelijk mandaat beperkt de verzamelende partij tot het gebruik of de verwerking van de gegevens voor de gespecificeerde doelen waarmee was ingestemd door het datasubject op het moment van de verzameling.
- De wet/het wettelijk mandaat beperkt de bewaring van verzamelde gegevens tot een termijn die nodig is voor het gespecificeerde doel.
- De wet/het wettelijk mandaat verplicht de partij die de gegevens gebruikt ("de verwerkende partij") te waarborgen dat het nauwkeurig die gegevens vastlegt en verwerkt.
- De wet/het wettelijk mandaat verplicht de verwerkende partij de opgeslagen gegevens te beveiligen door geschikte systemen toe te passen die in voldoende veiligheid voorzien.
- De wet/het wettelijk mandaat vereist dat de verwerkende partij voor het ondernemen van specifieke soorten verwerking deze laat controleren en goedkeuren door de aangewezen instantie.
- De wet/het wettelijk mandaat voorziet erin dat het datasubject toegang heeft, op verzoek, tot de persoonsgegevens die worden bewaard over dat datasubject door de verwerkende partij.
- De wet/het wettelijk mandaat voorziet in de mogelijkheid dat het hoofd van de verwerkende partij een aanvraag voor toegang tot opgeslagen gegevens van een datasubject kan weigeren indien:
  - de vrijgave van de gegevens de anonimiteit van een andere persoon kan compromitteren;
  - het verzoek vexatoir is van aard en de activiteiten te veel zou verstoren.
- De wet/het wettelijk mandaat voorziet in een beroepsmogelijkheid betreffende de besluiten van het hoofd van de verwerkende partij bij de aangewezen instantie.
- De wet/het wettelijk mandaat verbiedt de verwerking van gevoelige persoonsgegevens, behalve in specifieke gevallen en voor specifieke doelen. Dergelijke uitzonderingen kunnen omvatten:
  - Statistieken;
  - Management van de gezondheid
  - Vereisten van de rechtshandhaving;
  - Vereisten van de rechtsstaat;
  - Vereisten van een rechterlijke bevelschrift;
- De wet/het wettelijk mandaat schrijft civiele en strafrechtelijke sancties voor in het geval van schending van de vastgestelde bepalingen die betrekking hebben op de verzameling van persoonsgegevens. Dergelijke strafsancties kunnen worden opgelegd aan de verzamelende partij, of enige functionaris of directeur waarvan kan worden bewezen dat die opzettelijk de wet/ het wettelijk mandaat heeft geschonden.

6. CARICOM/CARIFORUM-LANDEN ZULLEN BEPAALDE VEREISTEN EN VERPLICHTINGEN MET BETREKKING TOT DE OPENBAARMAKING VAN PERSOONSGEGEVENS VASTLEGGEN

- De wet/het wettelijk mandaat verplicht de partij die persoonsgegevens verzamelt, verwerkt of gebruikt deze persoonsgegevens niet openbaar te maken zonder eerst de toestemming te hebben van het datasubject.
- De wet/het wettelijk mandaat voorziet in de vrijstelling van de verplichting om toestemming te krijgen van het datasubject waar dat vereist is door een wetsregel, indien er overwegingen zijn van nationale veiligheid, rechtsbedeling en management van de gezondheid.
- De wet/het wettelijk mandaat beperkt de grensoverschrijdende overdracht van persoonsgegevens naar rechtsgebieden die geen vergelijkbaar persoons- en gegevensbeschermingswetten en systemen hebben. In dat geval, zal de wet er in voorzien dat slechts zoveel informatie wordt overgedragen die niet zal resulteren in het compromitteren van de bescherming van de gegevens van het datasubject.
- De wet/het wettelijk mandaat voorziet erin, niettegenstaande enige standaardbeperkingen, dat de overdracht van persoonsgegevens kan worden gefaciliteerd in geval van uitdrukkelijke toestemming van het datasubject om gegevens over te dragen naar dat rechtsgebied, nadat het datasubject in kennis is gesteld van de mogelijke risico's.
- De wet/het wettelijk mandaat zal voorzien in de openbaarmaking van persoonsgegevens in antwoord op een verzoek daartoe van het datasubject. In het geval dat die openbaarmaking tot gevolg kan hebben dat andere niet-openbare gegevens openbaar worden gemaakt, dan zal de wet/ het wettelijk mandaat een geschikt richtsnoer voorschrijven voor het hoofd van de verwerkende partij.
- De wet/het wettelijk mandaat schrijft civiele en strafrechtelijke sancties voor in het geval van schending van de vastgestelde bepalingen die betrekking hebben op de openbaarmaking van persoonsgegevens. Dergelijke strafsancties kunnen worden opgelegd aan de verwerkende partij, of enige functionaris of directeur waarvan kan worden bewezen dat die opzettelijk de verplichtingen opgelegd door de wet/ het wettelijk mandaat heeft geschonden.

Deel II
Model wettekst –
Privacy en gegevensbescherming

Onderstaand volgt een model wettekst die een land in overweging kan nemen bij de ontwikkeling van nationale wetgeving die betrekking heeft op privacy en gegevensbescherming. Deze model tekst is gebaseerd op de richtlijnen voor model beleid hierboven aangegeven.

Indeling van de artikelen

Deel II

Deel II

HOOFDSTUK I – INLEIDING

Citeertitel en inwerkingtreding

1. Deze wet kan aangehaald worden als de "Privacy en gegevensbeschermingswet", en wordt van kracht en treedt in werking [op xxx/ na publicatie in het Staatsblad].

Doelstelling

2. De doelstelling van deze wet is het voorzien in een juridisch kader voor het ontwikkelen van een cultuur en praktijk van bescherming van privacy door:

   a. Het definiëren van algemene beginselen aan de hand waarvan persoonsgegevens van een individu moeten worden behandeld;

   b. Het definiëren van beheersrichtlijnen (waaronder systemen en technologie) waaraan personen die persoonsgegevens beheren zich moeten houden; en

   c. Het opzetten van een administratief kader voor het waarborgen van een open toezicht, en onpartijdige geschillenbeslechting die de bescherming van persoonsgegevens door zowel de publieke als private sector zal versterken.

Definities

3. (1) In deze Wet, zullen de volgende woorden en zinsneden de betekenis hebben daaraan toegekend hieronder:

   a. "gegevens" of "informatie" betekent elk bescheiden, document, correspondentie, memorandum, boek, plan, kaart, tekening, beeld- of grafisch werk, foto, film, microfilm, geluidsopname, videoband, machineleesbare bescheiden en enig ander documentair materiaal, ongeacht de fysieke vorm of kenmerken, en elke kopie van deze zaken.

   b. "Commissaris Gegevensbescherming": de Commissaris Gegevensbescherming benoemd krachtens Hoofdstuk VII artikel 49 van deze wet.

   c. "Houder van persoonsgegevens": een persoon die (alleen of gezamenlijk of in gemeenschap met andere personen) de doelstellingen bepaalt waarvoor en de manier waarop welke persoonsgegevens dan ook zijn, of zullen worden verzameld, verwerkt of openbaar gemaakt.

   d. "datasubject": een individu dat het onderwerp is van persoonsgegevens.

   e. "Minister": de Minister die is verantwoordelijk gesteld voor [informatie/publieke administratie].

   f. "instelling voor gezondheidszorg": verwijst naar instellingen die zijn geregistreerd als faciliteiten voor het voorzien in gezondheidszorg in overeenstemming met [relevante Openbare Gezondheidszorg Wet] en omvat ziekenhuizen, hospitalen, gezondheidscentra, klinieken [en artsenpraktijken].

   g. "gezondheidswerker": een professional die is geregistreerd om medische handelingen uit te voeren in overeenstemming met [relevante Openbare Gezondheidszorg Wet].

   h. "persoonsgegevens": gegevens over een identificeerbaar individu dat is vastgelegd in welke vorm dan ook, waaronder—

      i. informatie die betrekking heeft op de nationaliteit, het adres, de

leeftijd of de burgerlijke status van het individu;

ii. informatie over de raciale of etnische afkomst van het individu;

iii. informatie over de politieke mening of overtuiging van het individu;

iv. informatie over religieuze of andere overtuigingen van een gelijksoortige aard van het individu;

v. informatie betreffende de fysieke of geestelijke gezondheid of toestand van het individu;

vi. informatie betreffende de biometrie van het individu

vii. informatie betreffende de seksuele geaardheid of het seksuele leven van het individu; of

viii. informatie betreffende het strafblad of de financiële achtergrond van het individu

ix. informatie betreffende de opleiding of de arbeidsgeschiedenis van het individu;

x. om het even welk identificerend nummer, symbool of ander kenmerk ontworpen om het individu te identificeren;

xi. de opvattingen en meningen van enig ander persoon over het individu.

i. "overheid" omvat -

i. een Parlement of een commissie van enig Parlement;

ii. het Kabinet zoals samengesteld krachtens de grondwet;

iii. een Ministerie of enig departement of divisie van een Ministerie,

iv. een lokale autoriteit;

v. een publiekrechtelijk bedrijfsorgaan of lichaam;

vi. lichaam met rechtspersoonlijkheid opgezet met een publiek doeleinde, dat in het bezit is of wordt beheerd door de staat;

vii. enig ander lichaam aangewezen door de Minister krachtens regelgeving uitgegeven onder deze wet, dat een publieke autoriteit zal zijn voor de doelstellingen van deze *Wet*.

j. "verwerken", "verwerkt": betekent in relatie tot gegevens het vergaren, opnemen of houden van de gegevens of het uitvoeren van enige activiteit of serie van activiteiten betreffende die data, waaronder –

i. organiseren, aanpassen of veranderen van de gegevens;

ii. terugvinden, raadplegen of gebruiken van de gegevens; of

iii. harmoniseren, combineren, blokkeren, wissen of vernietigen van de gegevens.

k. "relevant bestand": elke serie informatie die betrekking heeft op individuen in de mate dat, hoewel de informatie niet wordt verwerkt met gebruik van apparatuur die automatisch werkt in antwoord op instructies die met dat doel worden gegeven, de serie is gestructureerd, of met verwijzing naar individuen of met verwijzing naar criteria die betrekking hebben op individuen, op dergelijke wijze

dat specifieke informatie betreffende een bepaald individu direct toegankelijk is.

(2) In het geval een lidstaat gelooft dat het gerechtvaardigd is om een bepaalde serie gevoelige persoonsgegevens te definiëren, kan zij dit alsvolgt doen:

a. "gevoelige persoonsgegevens": gegevens over een persoon zijn/ haar—

ii. raciale of etnische afkomst;

ii. politieke overtuigingen;

iii. religieuze of andere overtuigingen van een gelijksoortige aard;

iv. fysieke of geestelijke gezondheid of toestand;

v. seksuele geaardheid of seksuele leven; of

vi. strafblad of financiële achtergrond;

Verbindt de Staat

4. Deze wet zal de Staat verbinden.

Toepasselijkheid van de wet

5. Deze wet is van toepassing op de houder van persoonsgegevens met betrekking tot alle gegevens indien-

a. de houder van persoonsgegevens is gevestigd (normaal residerend, een rechtspersoon of filiaal) in [naam van de lidstaat] en de gegevens worden verwerkt binnen de context van de bedrijfsactiviteiten van die vestiging; of

b. de houder van persoonsgegevens niet is gevestigd in [naam van de lidstaat] maar apparatuur gebruikt in [naam van lidstaat] voor het verwerken van gegevens anderszins dan met als doel de doorvoer door [naam van lidstaat].

Niet-toepasselijkheid van de wet

6. Deze wet zal niet -

a. gegevens weerhouden die beschikbaar zijn bij wet aan een partij in om het even welk proces;

b. de macht van een rechtbank of tribunaal beperken om een getuige te verplichten een verklaring af te leggen of te verplichten een document of ander bewijsstuk te overleggen; of

c. toepasselijk zijn op nota's opgesteld door of voor een individu die een rechtbank voorzit in [land] of een tribunaal indien die nota's waren opgesteld voor het persoonlijk gebruik van dat individu in verband met het proces.

Algemene privacy beginselen

7. In overeenstemming met deze wet, zijn alle personen die persoonsgegevens verwerken in hun zakenpraktijk verantwoordelijk voor het zich houden aan de volgende algemene beginselen:

a. Persoonsgegevens zullen eerlijk en rechtmatig worden verwerkt, en zullen in het bijzonder, niet worden verwerkt tenzij aan bepaalde voorwaarden wordt voldaan.

b. Persoonsgegevens zullen slechts worden vergaard voor een of meer specifieke en rechtmatige doelstellingen, en zullen niet verder worden verwerkt op een wijze die niet in overeenstemming is met die

doelstelling of doelstellingen.

c. Persoonsgegevens zullen adequaat, relevant en niet overdadig zijn in relatie tot de doelstelling of de doelstellingen waarvoor zij zijn verwerkt.

d. Persoonsgegevens zullen nauwgezet zijn, en waar nodig, bijgewerkt worden.

e. Persoonsgegevens verwerkt voor enige doelstelling of doelstellingen zullen niet langer worden bewaard dan nodig is voor die doelstelling of doelstellingen.

f. Persoonsgegevens zullen worden verwerkt in overeenstemming met de rechten van datasubjecten krachtens deze wet.

g. Toepasselijke technische en institutionele maatregelen zullen worden genomen tegen het onrechtmatig verwerken van persoonsgegevens en tegen het niet-bedoelde verlies of de vernietiging van, of schade aan, dergelijke gegevens.

h. Persoonsgegevens zullen niet worden overgedragen naar een land of territorium buiten de [*naam van het rechtsgebied*] tenzij dat land of territorium een adequaat niveau van bescherming waarborgt voor de rechten en vrijheden van datasubjecten in relatie tot het verwerken van persoonsgegevens.

HOOFDSTUK II – VERPLICHTINGEN VAN DE HOUDERS VAN PERSOONSGEGEVENS

Beperking op de verzameling en verwerking van persoonsgegevens

8. (1) Geen enkele persoon zal de verzameling en of verwerking van persoonsgegevens veroorzaken tenzij een invoerveld betreffende die persoon als de houder van persoonsgegevens is opgenomen in het register dat wordt bijgehouden door de commissaris.

(2) Persoonsgegevens mogen niet verzameld worden door of voor de houder van persoonsgegevens tenzij—

a. de verzameling van die gegevens als rechtvaardig wordt beschouwd, en noodzakelijk als onderdeel van een overeenkomst tussen de houder van persoonsgegevens en het datasubject;

b. de verzameling uitdrukkelijk is toegestaan door of krachtens enige geschreven wet.

Persoonsgegevens die rechtstreeks worden verzameld

9. (1) In het geval dat de houder van persoonsgegevens persoonlijke informatie van een individu nodig heeft, zal het zorgen dat deze persoonsgegevens rechtstreeks worden verzameld van dat individu met hun expliciete instemming.

(2) Het datasubject, behalve waar anderszins daarin wordt voorzien door een andere wet, zal recht hebben bezwaren te maken bij de houder van persoonsgegevens op basis van verplichtende rechtmatige gronden tegen de verwerking van dergelijke gegevens.

(3) Niettegenstaande lid (1) kunnen persoonsgegevens worden verzameld van een bron anders dan het individu in geval -

a. een andere verzamelmethode is toegestaan door het individu, door

de gegevenscommissaris of door enige andere geschreven wet; en

b. de informatie wordt verzameld met als doelstelling -

i. het bepalen van de geschiktheid voor een onderscheiding of prijs, waaronder een eredoctoraat, beurs, prijs of studietoelage;

ii. proces bij een rechtbank of een judicieel of quasi-judicieel tribunaal;

iii. innen van een schuld of boete of het doen van een betaling; of

iv. rechtshandhaving.

Informeren van datasubject over doel

10. Op het moment van de verzameling van de persoonsgegevens of daarvoor zal de houder van persoonsgegevens waarborgen dat het datasubject geïnformeerd wordt over -

a. het doel van het verzamelen daarvan;

b. de bedoelde ontvangers;

c. of het geven van antwoorden op vragen vrijwillig is of verplicht en de mogelijke consequentie in geval men weigert te antwoorden;

d. waar van toepassing, de wettelijke bevoegdheid deze te verzamelen; en

e. de titel, het werkadres, telefoonnummer en andere contactpersonen van een functionaris van de houder van persoonsgegevens die vragen kan beantwoorden van het datasubject over de verzameling.

Bewaring van persoonsgegevens

11. Persoonsgegevens die zijn gebruikt door de houder van persoonsgegevens voor een administratief doeleinde zullen worden bewaard door de houder van persoonsgegevens slechts voor de tijdsperiode nadat het is gebruikt zoals kan worden voorgeschreven door de regelgeving, om te waarborgen dat het datasubject een redelijke mogelijkheid heeft om toegang te krijgen tot die informatie.

Verwijdering van persoonsgegevens

12. De houder van persoonsgegevens zal alle persoonsgegevens in zijn beheer of onder zijn hoede verwijderen in overeenstemming met de regelgeving gemaakt door de Minister krachtens deze wet.

Nauwgezetheid van persoonsgegevens

13. De houder van persoonsgegevens zal zich elke mogelijke inspanning getroosten om te waarborgen dat persoonsgegevens onder zijn hoede betreffende een bepaald datasubject accuraat zijn en compleet.

Bescherming van persoonsgegevens

14. (1) De houder van persoonsgegevens zal persoonsgegevens onder zijn hoede of in zijn beheer beschermen door redelijke technische en institutionele beveiligingsmaatregelen te treffen tegen zulke risico's als ongeoorloofde toegang, verzameling, gebruik, verandering, openbaarmaking of onbedoelde verwijdering.

(2) In het geval dat enige andere persoon persoonsgegevens verwerkt namens de houder van persoonsgegevens, zal de houder van persoonsgegevens waarborgen dat die persoon:

a. de beveiligingsmaatregelen kan treffen die genomen moeten worden;

b. werkelijk de maatregelen neemt die als dusdanig zijn geïdentificeerd door de houder van de persoonsgegevens.

Deel II

Verwerking van persoonsgegevens in overeenstemming met het doel

15. (1) Persoonsgegevens in het beheer van of onder de hoede van de houder van persoonsgegevens zullen niet, zonder de instemming van het individu waarop het betrekking heeft, worden verwerkt met uitzondering van het doel waarvoor de gegevens waren verkregen of samengebracht door de houder van persoonsgegevens, of voor een gebruik dat in overeenstemming is met dat doel.

(2) Het verwerken van persoonsgegevens is in overeenstemming met het doel waarvoor het was verkregen indien het verwerken een redelijk en direct verband heeft met dat doel, en dat doel in overeenstemming is met de criteria die zijn aangegeven in lid (3).

(3) Persoonsgegevens mogen slechts verwerkt worden indien:

a. het datasubject ondubbelzinnig zijn instemming heeft gegeven; of

b. door een gezondheidswerker die de nodige taken uitvoert in een instelling voor de gezondheidszorg;

c. het openbaar is gemaakt door het datasubject;

d. voor wetenschappelijke of statistische doeleinden in overeenstemming met artikel 17;

e. in het belang van de rechtshandhaving en nationale veiligheid; of

f. het doel het bepalen van toegang tot sociale dienstverlening is.

g. verwerking nodig is voor het uitvoeren van een contract waarbij het datasubject een partij is of om stappen te nemen op verzoek van het datasubject voordat het contract wordt afgesloten; of

h. verwerking nodig is voor de naleving van een wettelijke verplichting waar de houder van persoonsgegevens aan is onderworpen; of

i. verwerking nodig is om de vitale belangen van het datasubject te beschermen; of

j. verwerking nodig is voor het uitvoeren van een activiteit die wordt uitgevoerd in het openbaar belang of bij het uitoefenen van een officiële bevoegdheid die is toegekend aan de houder van persoonsgegevens of aan een derde aan wie de gegevens zijn onthuld; of

k. verwerking nodig is voor een doel dat een legitiem belang betreft van de houder van persoonsgegevens of van dergelijke derde aan wie de persoonsgegevens zijn verstrekt, behalve indien dergelijk belang wordt te niet gedaan door het belang om het recht op privacy van het datasubject te beschermen.

(4) In het geval dat het rechtsgebied het nodig acht om “gevoelige persoonsgegevens” verder te onderscheiden, kan het de verzameling en verwerking van dergelijke informatie verder beperken, met uitzonderingen geassocieerd met (b) tot (f) hierboven.

Openbaarmaking van persoonsgege

16. Behalve zoals voorzien onder enige andere geschreven wet, kunnen persoonsgegevens in het beheer van de houder van persoonsgegevens slechts openbaar worden gemaakt -

a. voor de doeleinden waarvoor de gegevens waren verzameld door de

vens

houder van persoonsgegevens, of voor een gebruik dat in overeenstemming is met dat doel.

b. voor enig doel in overeenstemming met enige geschreven wet of enige regelgeving gemaakt krachtens dergelijke geschreven wet die dergelijke openbaarmaking toestaat;

c. met als doel het naleven van een dagvaarding of bevelschrift afgegeven of bevelschrift van een rechter, persoon of lichaam met rechtsbevoegdheid om de overlegging van gegevens af te dwingen of met als doel het naleven van de regels van het hof met betrekking tot de overlegging van gegevens;

d. door de Procureur Generaal van [naam van het rechtsgebied] voor gebruik in een juridisch proces waarbij de Staat betrokken is

e. door een onderzoekslichaam gespecificeerd in een Ministerieel besluit, op schriftelijk verzoek van het onderzoekslichaam, met als doel het onderzoeken van de naleving van enige geschreven wet of het uitvoeren van een rechtmatig onderzoek, indien het verzoek het doel specificeert en de te verstrekken informatie beschrijft;

f. door een rechtshandhavingsinstituut in [naam van het rechtsgebied] aan een ander rechtshandhavingsinstituut in [naam van het rechtsgebied] met als doel de handhaving van een geschreven wet;

g. aan een rechtshandhavingsinstituut in het buitenland krachtens een schriftelijke overeenkomst, verdrag of onder de bevoegdheid van de Regering van [naam van het rechtsgebied];

h. indien het hoofd van de houder van persoonsgegevens het ermee eens is dat er dringende omstandigheden zijn die de gezondheid of veiligheid van een persoon beïnvloeden en indien, behoudens artikel 23 onder (d), kennisgeving van de openbaarmaking wordt verzonden naar het laatst bekende adres van het datasubject,

i. opdat contact kan worden opgenomen met de familieleden of vriend van een gewonde, zieke of overleden persoon;

j. met als doel het innen van gelden die een datasubject schuldig is aan de Regering van [naam van het rechtsgebied] of aan de houder van persoonsgegevens;

k. om statistische redenen in het geval waar de openbaarmaking voldoet aan de eisen van artikel 17; of

k. om archivalische redenen in het geval waar de openbaarmaking voldoet aan de eisen van artikel 18.

Openbaarmaking voor onderzoek of statistieken

17. De houder van persoonsgegevens kan persoonsgegevens onder zijn hoede of in zijn beheer ten behoeve van onderzoek laten openbaar maken, waarbij inbegrepen statistisch onderzoek slechts indien -

a. het onderzoeksdoel niet redelijkerwijs kan worden bereikt tenzij die informatie wordt voorzien in individueel te identificeren vorm;

b. de informatie openbaar wordt gemaakt op voorwaarde dat het niet wordt gebruikt met als doel het in contact treden met een persoon om deel te nemen aan een onderzoek;

c. enig vastgelegd verband niet schadelijk is voor het datasubject en de

voordelen behaald met het verband leggen tussen de bescheiden duidelijk in het openbaar belang zijn;

d. het hoofd van de betrokken houder van persoonsgegevens voorwaarden heeft goedgekeurd in verband met het volgende:

i. veiligheid en vertrouwelijkheid;

ii. de verwijdering of vernietiging van individuele kentekens op het vroegst mogelijke tijdstip;

iii. het verbod van enig daaropvolgend gebruik of openbaarmaking van die gegevens in een individueel te herkennen vorm zonder de uitdrukkelijke toestemming van de houder van persoonsgegevens; en

e. de persoon aan wie de gegevens worden onthuld een overeenkomst heeft getekend om zich te houden aan de goedgekeurde voorwaarden, deze wet en enige beleidslijn en procedure van de houder van persoonsgegevens die betrekking hebben op de vertrouwelijkheid van persoonsgegevens.

Openbaarmaking voor archiefdoeleinden

18. De Nationale Archieven van de Regering van [naam van het rechtsgebied] of de archieven van de houder van persoonsgegevens kan persoonsgegevens openbaar maken of persoonsgegevens onder zijn hoede of in zijn beheer openbaar laten maken ten behoeve van archivalische of historische doeleinden indien -

a. de openbaarmaking geen onredelijke invasie van professionele of persoonlijke privacy zou inhouden;

b. de openbaarmaking voor historisch onderzoek en in overeenstemming is met artikel 18;

c. de informatie iemand betreft die is overleden voor [...] jaren of meer; of

d. de gegevens zich in bescheiden bevinden die reeds voor een [...] jaren of meer.

Beperking van overdracht aan derde rechtsgebieden

19. (1) Behoudens de bepalingen van het volgende, mag de overdracht van persoonsgegevens die verwerkt zullen worden naar een derde rechtsgebied slechts plaatshebben behoudens de bepalingen van deze wet en mits het derde rechtsgebied aan wie de gegevens worden overgedragen een vergelijkbaar niveau van bescherming waarborgt.

(2) De toereikendheid van het beschermingsniveau van een derde rechtsgebied kan worden beoordeeld in het kader van alle omstandigheden die een gegevensoverdracht activiteit omringen; speciale overwegingen moeten worden gegeven aan de aard van de gegevens, het doel en de duur van de voorgestelde verwerkingsactiviteit of -activiteiten, het land van oorsprong en land van uiteindelijke bestemming, de wetgeving, zowel algemeen als per sector, die van kracht is in het derde land en de professionele regels en veiligheidsmaatregelen die worden nageleefd in dat land.

(3) De Commissaris Gegevensbescherming zal bepalen of een derde land een passend beschermingsniveau waarborgt. Bij die beoordeling zal de Commissaris Gegevensbescherming aangeven:

a. de relevante overheidsinstelling die verantwoordelijk is voor

gegevensbescherming in het andere rechtsgebied;

b. zijn beoordeling van de vergelijkbare beschermingsniveaus die zijn voorzien; en

c. in geval waar bescherming wordt geacht onverenigbaar te zijn, de aspecten van de persoonsgegevens (en gevoelige persoonsgegevens) die niet voldoende beschermd zouden zijn.

(4) Waar, ondanks niet-vergelijkbare beschermingsniveaus de Commissaris Gegevensbescherming bepaald dat een beperkte vorm van overdracht kan worden gefaciliteerd, die de inbreuk op de rechten van het datasubject zou beperken in overeenstemming met deze wet, kan de Commissaris Gegevensbescherming een dergelijke overdracht goedkeuren in geval dat:

a. het datasubject instemt met de overdracht van informatie naar het derde rechtsgebied; en

b. er een passende afscheiding of redactie van die aspecten van de informatie heeft plaatsgehad die de Commissaris Gegevensbescherming passend acht.

(5) [In het geval dat er een geschikte regeling is voor het verwerken van de gegevens of informatie in een derde rechtsgebied kan een redelijke overgangsperiode worden toegestaan door de Commissaris om de houder van persoonsgegevens toe te laten de verwerking naar een ander rechtsgebied te verplaatsen, indien nodig.]

(6) Behoudens leden (4) en (5) is de overdracht van persoonsgegevens naar een derde rechtsgebied dat geen passende bescherming waarborgt, verboden.

Gedragscode

20. De Commissaris Gegevensbescherming zal de industrie consulteren voor het bevorderen van de toepassing van de Algemene privacy beginselen door de ontwikkeling van gedragscodes door middel van -

a. het geven van aanwijzingen betreffende de ontwikkeling van gedragscodes;

b. het geven van aanwijzingen betreffende soepele oplossingsmechanismen;

c. het bevorderen van educatie betreffende Algemene privacy beginselen;

d. het werken met de overheid en de private sectorlichamen voor het bevorderen van bewustzijn over gedragscodes bij de consument; en

e. het ondernemen van enige actie die de Commissaris Gegevensbescherming passend lijkt te zijn.

Verplichte gedragscode

21. (1) Waar, naar de mening van de Commissaris Gegevensbescherming, het openbaar belang de ontwikkeling van verplichte gedragscodes rechtvaardigt die handelen over de toepassing van Algemene privacy beginselen op een bepaalde industrie, economische sector, of activiteit, kan de Commissaris Gegevensbescherming, bij bestuursmaatregel, de ontwikkeling eisen van een gedragscode en een tijdslijn stellen voor de ontwikkeling daarvan.

(2) Behoudens lid (1) in het geval dat er een passende overheidsregelgevend lichaam is van een industrie, economische sector of activiteit, kan de Commissaris Gegevensbescherming het regelgevend lichaam verzoeken toezicht te houden op de ontwikkeling van de gedragscode voor die industrie, economische sector of activiteit.

Deel II

HOOFDSTUK III – RECHTEN VAN HET DATASUBJECT

Recht op toegang tot eigen persoonsgegevens

22. (1) Elk individu dat burger of ingezetene is van [naam van rechtsgebied] heeft het recht op en zal op verzoek en na betaling van de voorgeschreven vergoeding toegang worden gegeven tot -

a. persoonsgegevens over dat individu vervat in een persoonsgegevens bestand onder de hoede van of in beheer van de houder van persoonsgegevens;

b. enige andere persoonsgegevens over dat individu onder de hoede van of in beheer van een houder van persoonsgegevens met betrekking waartoe het individu in staat is voldoende specifieke informatie te geven zodat het redelijkerwijs terug te vinden moet zijn door de houder van persoonsgegevens.

(2) Een verzoek om toegang tot persoonsgegevens zal worden gedaan door de houder van persoonsgegevens die het beheer heeft over het persoonsgegevens bestand of over de gegevens, wat het geval ook mocht zijn, in de vorm die is goedgekeurd door de Commissaris Gegevensbescherming.

Houder van persoonsgegevens kan toegang weigeren

23. (1) De houder van persoonsgegevens kan weigeren persoonsgegevens openbaar te maken aan het individu op wie de gegevens betrekking hebben in geval -

a. de onthulling een onterechte inbreuk zou maken op de persoonlijke privacy van een ander individu;

b. het gevangenisbescheiden zijn waarvan de openbaarmaking naar verwachting informatie zou kunnen onthullen die was verstrekt in vertrouwen;

c. het gegevens zijn die onderhevig zijn aan vertrouwelijkheid van communicatie of die zijn verkregen tijdens een onderzoek of een juridisch proces,

d. het gezondheids- of medische gegevens zijn waarvan het hoofd van de houder van persoonsgegevens een redelijk vermoeden heeft dat het geven van toegang tot de gegevens de gezondheid of veiligheid van enig persoon zou kunnen schaden;

e. het materiaal een beoordeling of mening omvat die slechts is samengebracht met als doel het bepalen van de geschiktheid voor tewerkstelling, het toekennen van een overheidscontract en andere voordelen waarvan de openbaarmaking de identiteit van de bron die de informatie heeft verschaft zou kunnen onthullen in omstandigheden waarvan het redelijkerwijs verwacht mocht worden dat de identiteit van de bron geheim zou worden gehouden.

(2) Het hoofd van de houder van persoonsgegevens kan verzoeken van een individu negeren om toegang tot de persoonsgegevens van dat individu indien het onredelijkerwijs de activiteiten van de houder van persoonsgegevens zou verstoren vanwege de herhalende of systematische aard van de verzoeken of waar de verzoeken pietluttig of vexatoir zijn.

Afscheiding van

24. (1) De houder van persoonsgegevens zal alles in het werk stellen om

vrijgestelde informatie

informatie die is vrijgesteld van openbaarmaking af te scheiden in overeenstemming met artikel 24 van gegevens die beschikbaar gemaakt kunnen worden aan het individu dat verzoekt toegang te krijgen tot zijn persoonsgegevens en de niet-vrijgestelde gegevens beschikbaar te stellen.

(2) Het hoofd van de houder van persoonsgegevens kan weigeren het bestaan van gegevens openbaar te maken waar de erkenning van het bestaan kritieke aspecten zou onthullen over de vrijgestelde aard van de gegevens.

Delegeren van rechten van het datasubject

25. Enig recht of enige bevoegdheid toegekend aan een individu door deze wet kan worden uitgeoefend -

a. in het geval dat het individu is overleden, door de persoonlijke vertegenwoordiger van dat individu indien het uitoefenen van het recht of de bevoegdheid verband houdt met de administratie van de nalatenschap van het individu;

b. door de advocaat van het individu krachtens een machtiging;

c. door de curator van het individu; of

d. in het geval dat het individu jonger dan achttien jaar oud is, door een persoon die rechtmatig gezagsrecht heeft over het individu.

Tijdlimiet voor het beantwoorden van een verzoek

26. (1) In het geval dat een verzoek is gedaan voor toegang tot persoonsgegevens krachtens artikel 23 zal het hoofd van de houder van persoonsgegevens binnen [...] nadat het verzoek was ontvangen -

toegang verlenen geheel of gedeeltelijk, waarbij de gegevens worden verstrekt aan het individu dat het verzoek heeft gedaan; of

weigeren toegang te verlenen geheel of gedeeltelijk, waarbij een schriftelijk antwoord wordt verstrekt aan het individu waarin wordt aangegeven

i. dat de gegevens niet bestaan; of

ii. de specifieke bepaling van de wet waarop redelijkerwijs verwacht kan worden dat de weigering is gebaseerd indien de gegevens zouden bestaan; en

iii. gegevens betreffende het recht op beroep bij de Commissaris Gegevensbescherming.

(2) In het geval dat toegang wordt verleend geheel of gedeeltelijk, zal het hoofd van de houder van persoonsgegevens waarborgen dat de informatie beschikbaar is in een bondig formaat, waarbij indien redelijk, begrijpelijk voor een individu met een zintuigelijke handicap.

Correctie van fouten in opgeslagen persoonsgegevens

27. (1) Waar een individu gelooft dat er een fout of omissie voorkomt in zijn persoonsgegevens, kan het individu het hoofd van de houder van persoonsgegevens die de gegevens onder zijn hoede heeft of in zijn beheer, verzoeken om de informatie te corrigeren.

(2) Indien de correctie niet is gemaakt in antwoord op een verzoek onder lid (1), zal het hoofd van de houder van persoonsgegevens de gegevens van een aantekening voorzien met de correctie die was verzocht maar niet is gemaakt en het individu dat het verzoek had gedaan in kennis stellen dat er geen correctie is gepleegd.

(3) Bij het corrigeren of annoteren van persoonsgegevens onder dit artikel, zal het hoofd van de houder van persoonsgegevens elke andere houder van persoonsgegevens of derde aan wie de gegevens openbaar waren gemaakt

in het jaar voorafgaand aan het moment waarop de correctie was verzocht, informeren over dergelijke correctie of aantekening.

(4) Bij de in kennis stelling onder lid (3) van een correctie of annotatie van persoonsgegevens, zal de houder van persoonsgegevens de correctie of annotatie aanbrengen op alle bescheiden van die gegevens onder zijn hoede of in zijn beheer.

HOOFDSTUK IV – SPECIFIEKE VERPLICHTINGEN VAN DE OVERHEID

Privacy effectbeoordeling

28. (1) Elk Ministerie zal een privacy effectbeoordeling voorbereiden, op de manier voorgeschreven door de Commissaris Gegevensbescherming, voor elke voorgestelde wet, systeem, project, programma of activiteit.

(2) Bij de voorbereiding van een privacy effectbeoordeling, zal elk Ministerie dergelijke privacy effectbeoordeling indienen bij de Commissaris Gegevensbescherming ter goedkeuring.

(3) In het geval dat een privacy effectbeoordeling is ingediend in overeenstemming met lid (2) zal de Commissaris Gegevensbescherming dergelijke privacy effectbeoordeling evalueren in overeenstemming met de Algemene privacy beginselen en waar nodig, aanbevelingen doen aan het Ministerie voor wijzigingen om naleving te garanderen.

(4) In het geval dat de Commissaris Gegevensbescherming een aanbeveling doet onder lid (3), zal het Ministerie de nodig wijzigingen maken aan de voorgestelde wet, systeem, project, programma of activiteit.

(5) Elk Ministerie zal alle redelijke stappen ondernemen in overeenstemming met de privacy effectbeoordeling om onnodige inbreuken op de persoonlijke privacy te voorkomen bij het ontwerpen, implementeren of handhaven van wetten, systemen, projecten, programma's of activiteiten.

Opslagsysteem voor persoonsgegevens

29. Het hoofd van een publiek lichaam die een geregistreerde houder is van persoonsgegevens zal zorgen dat wordt opgenomen in opslagsystemen voor persoonsgegevens, alle persoonsgegevens onder de hoede of in het beheer van de houder van persoonsgegevens die -

a. verwerkt zijn, verwerkt worden, of beschikbaar zijn voor gebruik voor een administratief doeleinde; of

b. zijn georganiseerd of bedoeld zijn om te worden opgevraagd door middel van de naam van een individu of een identificatienummer, symbool of ander kenmerk toegekend aan een individu.

Uitzondering voor de nationale archieven

30. Niettegenstaande artikel 31, zullen persoonsgegevens onder de hoede van of in het beheer van de archieven van de Regering van [naam van het rechtsgebied] die zijn overgedragen daaraan door een publiek lichaam vanwege historische of archiefdoeleinden niet worden opgenomen in bestanden met persoonsgegevens.

Vertegenwoordiger bescherming

31. (1) De houder van persoonsgegevens zal de Commissaris

persoonsgegevens

Gegevensbescherming in kennis stellen van de aanstelling of het ontslag van een vertegenwoordiger bescherming persoonsgegevens.

(2) De vertegenwoordiger bescherming persoonsgegevens zal de taak hebben onafhankelijk te waarborgen dat de houder van persoonsgegevens deze gegevens op een rechtmatige en correcte wijze verwerkt en in overeenstemming met goede praktijk en in het geval dat een vertegenwoordiger bescherming persoonsgegevens een onvolkomenheid identificeert, dan zal hij dit onder de aandacht brengen van de houder van persoonsgegevens.

(3) Indien de vertegenwoordiger bescherming persoonsgegevens een reden heeft te vermoeden dat de houder van persoonsgegevens de bepalingen heeft geschonden die van toepassing zijn op de verwerking van persoonsgegevens en indien de rectificatie niet zo snel als mogelijk wordt geïmplementeerd nadat dergelijke schending is bekendgemaakt, dan zal de vertegenwoordiger bescherming persoonsgegevens de Commissaris Gegevensbescherming op de hoogte stellen van deze situatie.

Goed te keuren gegevensuitwisseling

32. In het geval dat een publiek lichaam van plan is gegevens uit te wisselen met andere publieke lichamen dient dit slechts te gebeuren krachtens een overeenkomst voorgeschreven en goed te keuren door de Commissaris Gegevensbescherming.

Commissaris zal rapporteren over bestanden met persoonsgegevens

33. De Commissaris Gegevensbescherming zal periodiek, maar minimaal jaarlijks, een index publiceren van de persoonsgegevens die worden bijgehouden door de overheid, waarin een samenvatting van het volgende wordt opgenomen:

a. de opslagsystemen voor persoonsgegevens die onder de hoede zijn of in het beheer van elk publiek lichaam;

b. de overeenkomsten inzake gegevensuitwisseling aangegaan door een publiek lichaam met een ander publiek lichaam of andere persoon;

c. de gegevens matching activiteiten goedgekeurd door de Commissaris Gegevensbescherming;

d. de contactinformatie van de functionaris aan wie verzoeken betreffende persoonsgegevens opgenomen in het gegevensbestand gezonden kunnen worden;

e. een verklaring over de doelstellingen waarvoor de persoonsgegevens in het gegevensbestand zijn verkregen of samengevoegd en een verklaring over het gebruik dat in overeenstemming is met die doelstellingen waarvoor de informatie wordt gebruikt of openbaar gemaakt;

f. een verklaring over de normen en praktijken inzake het bewaren en verwijderen die van toepassing zijn op de persoonsgegevens in het gegevensbestand; en

g. privacy effectbeoordelingen voorbereid door om het even welk Ministerie.

HOOFDSTUK V – SPECIALE VRIJSTELLINGEN

Huishoudelijke doeleinden

34. Een individu is vrijgesteld van de bepalingen van Hoofdstukken 3, 4 en 5 in het geval dat de gegevens verwerkt worden door het individu slechts voor doeleinden die betrekking hebben op persoonlijke, familie of huishoudelijke

zaken van dat individu of voor recreatieve doeleinden.

Nationale veiligheid, misdaad en belasting

35. (1) De Minister kan bij besluit gepubliceerd in het gouvernementsblad de houder van persoonsgegevens vrijstellen van het naleven van een bepaling van deze wet in het belang van nationale veiligheid.

(2) De houder van persoonsgegevens die een publiek lichaam is zal worden vrijgesteld van de bepalingen van [Hoofdstukken II en III] indien het verwerken van gegevens is vereist voor -

a. het voorkomen of vaststellen van een misdrijf;

b. de aanhouding of vervolging van overtreders; of

c. de aanslag of inning van enige belasting, rechten of heffing van een gelijkaardig type.

Vrijstellingen betreffende de toepasselijkheid van regelgevende activiteiten

36. (1) Persoonsgegevens verwerkt met als doelstelling het vervullen van taken in overeenstemming met regelgevende activiteiten vereist door om het even welke geschreven wet worden vrijgesteld van Hoofdstukken II en III van deze wet, in elk geval in de mate waarin de toepassing van dergelijke bepalingen op de gegevens waarschijnlijk de juiste vervulling van die taken in gevaar kan brengen.

(2) Lid (1) is van toepassing op enige relevante taak die is bedoeld —

a. voor het beschermen van de leden van het publiek tegen—

   i. financiële verliezen als gevolg van misleiding, kwade praktijken of ander ernstig wangedrag door, of de onbekwaamheid of incompetentie van, personen betrokken in het verlenen van bank-, verzekerings-, investerings- of andere financiële diensten of in het management van lichamen met rechtspersoonlijkheid,

   ii. financiële verliezen als het gevolg van het gedrag van gerehabiliteerde en niet gerehabiliteerde gefailleerden; of

   iii. misleiding, kwade praktijken of ander ernstig wangedrag door, of de onbekwaamheid of incompetentie van, personen bevoegd enig beroep of activiteit uit te oefenen,

b. voor het beschermen van stichtingen zonder winstoogmerk tegen het wangedrag of wanbeheer (ongeacht of dat door bewindvoerders of andere personen) in hun administratie,

c. voor het beschermen van het eigendom van stichtingen zonder winstoogmerk tegen verlies of misbruik,

d. voor het herstel van het eigendom van stichtingen zonder winstoogmerk,

e. voor het veiligstellen van de gezondheid, veiligheid en het welzijn van personen aan het werk, of

f. voor het beschermen van personen anderszins dan de personen aan het werk tegen de gezondheids- of veiligheidsrisico's voortvloeiende uit of in verband met handelingen van personen aan het werk.

Vrijstellingen betreffende de toepasselijkheid op de journalistiek,

37. (1) In het geval dat persoonsgegevens in de speciale omstandigheid zijn te worden verwerkt waar –

a. het verwerken wordt gedaan met het oog op de publicatie door om het even welke persoon van enig journalistiek, letterkundig of artistiek materiaal;

b de houder van persoonsgegevens redelijkerwijs gelooft dat rekening

letteren en kunst

houdend in het bijzonder met de specifieke betekenis van het openbaar belang bij de vrijheid van meningsuiting, dat publicatie in het openbaar belang zou zijn; en

c. de houder van persoonsgegevens redelijkerwijs gelooft dat volledig rekening houdend met de omstandigheden, naleving van de relevante bepalingen van Hoofdstuk II niet verenigbaar is met de journalistieke, letterkundige of artistieke doeleinden die worden nagestreefd,

zullen die persoonsgegevens worden vrijgesteld van Hoofdstukken II en III van deze wet.

(2) Om te voorzien in lid (1) kan de Commissaris Gegevensbescherming gedragscodes vaststellen in overeenstemming met artikelen 21 en 22, die waar nodig de bepalingen van Hoofdstukken II en III zo mogen aanpassen om een passend evenwicht te bereiken van de doelstellingen van deze wet en het heersende recht op vrijheid van meningsuiting.

HOOFDSTUK VI – HERZIENING EN BEROEP

Recht van een verzoeker om in beroep te gaan tegen het besluit van de houder van persoonsgegevens

38. Een individu dat een verzoek heeft gedaan om zijn persoonsgegevens krachtens artikel 23 of die heeft verzocht om een correctie van persoonsgegevens krachtens artikel 28 kan in beroep gaan tegen elk besluit van het hoofd van de houder van persoonsgegevens bij de Commissaris Gegevensbescherming.

Tijdslimiet waarbinnen beroep moet worden aangetekend

39. Een beroep bij de Commissaris Gegevensbescherming onder artikel 39 moet worden aangetekend binnen [...] weken na de datum van de kennisgeving van het besluit waartegen beroep wordt aangetekend door het indienen van een schriftelijk beroepschrift bij de Commissaris Gegevensbescherming.

Commissaris kan een beroep afwijzen

40. De Commissaris Gegevensbescherming kan een beroep afwijzen indien in het beroepschrift geen redelijke basis wordt gelegd voor het concluderen dat de persoonsgegevens waarop het beroep betrekking heeft bestaan.

Commissaris moet houder van persoonsgegevens in kennis stellen van het beroepschrift

41. Na ontvangst van het beroepschrift zal de Commissaris Gegevensbescherming het hoofd van de betrokken houder van persoonsgegevens in kennis stellen en enige andere betrokken persoon van het beroepschrift.

De Commissaris Gegevensbescherming kan een bemiddelaar aanwijzen

42. De Commissaris Gegevensbescherming kan een bemiddelaar aanwijzen voor het onderzoeken van de omstandigheden van het aangetekende beroep en om te trachten een oplossing te vinden voor de zaak waartegen beroep is aangetekend.

Commissaris kan een onderzoek

43. (1) De Commissaris Gegevensbescherming kan een onderzoek instellen om het besluit te herzien van het hoofd van de houder van persoonsgegevens indien de Commissaris Gegevensbescherming -

instellen

a. geen bemiddelaar heeft aangewezen om een onderzoek in te stellen krachtens artikel 43; of

b. een bemiddelaar heeft aangewezen om een onderzoek in te stellen krachtens artikel 43, maar een oplossing niet is gevonden.

(2) In het geval dat de Commissaris Gegevensbescherming een onderzoek instelt onder dit artikel kan hij bij de afsluiting van dergelijk onderzoek of -

a. het besluit van het hoofd van de houder van persoonsgegevens bevestigen; of

b. het hoofd van de houder van persoonsgegevens instructies geven de persoonsgegevens vrij te geven of de verzochte correcties te maken.

Vergaderingen gehouden binnenskamers

44. Het onderzoek door de Commissaris Gegevensbescherming of een bemiddelaar en alle vergaderingen gehouden door een bemiddelaar met de partijen bij het beroep kunnen binnenskamers worden gehouden.

Vertegenwoordiging bij het onderzoek

45. Een individu die beroep aantekent tegen een weigering om toegang tot persoonsgegevens, het hoofd van de betrokken houder van persoonsgegevens en een getroffen partij mogen vertegenwoordigd zijn door een juridisch adviseur of een vertegenwoordiger.

Bewijslast ligt bij de houder van persoonsgegevens

46. In het geval dat de houder van persoonsgegevens weigert toegang te geven tot persoonsgegevens, zal de bewijslast dat de gegevens vallen binnen een van de aangegeven vrijstellingen van de wet zijn met redelijke mate van zekerheid en zal liggen bij de houder van persoonsgegevens.

Beroep bij de rechter

47. Beide partijen kunnen beroep aantekenen tegen het besluit van de Commissaris Gegevensbescherming bij de rechter in overeenstemming met artikel 80 van deze wet.

Deel II

HOOFDSTUK VII – BUREAU VAN DE COMMISSARIS GEGEVENSBESCHERMING

Instelling van het bureau van de Commissaris Gegevensbescherming

48. (1) Behoudens lid (2) zal er een Commissaris Gegevensbescherming zijn die zal worden aangesteld door het [Staatshoofd] na consultatie met de Premier en de Oppositieleider.

(2) Een persoon zal niet gekwalificeerd zijn om de functie van Commissaris te bekleden indien hij -

a. een Minister, griffier bij het parlement, of een lid is van de Nationale Assemblee; of

b. een rechter is; of

c. een overheidsfunctionaris is; of

d. lid van een lokale autoriteit is; of

e. een financieel of ander belang heeft bij een onderneming of activiteit die waarschijnlijk de uitvoering van zijn taken als een Commissaris zal beïnvloeden; of

f. een niet-gerehabiliteerde gefailleerde is; of

g. op enig moment veroordeeld is geworden voor een overtreding die te maken had met misleiding.

(3) De Commissaris Gegevensbescherming zal personeel in dienst nemen zoals nodig mocht zijn, die zullen staan onder het administratief beheer van de Commissaris Gegevensbescherming.

(4) De Commissaris Gegevensbescherming zal geen andere betaalde functie hebben ongeacht of dat voor de overheid is of anderszins en zal geen andere bezigheid ondernemen tegen een beloning.

(5) Het [Staatshoofd] zal, nadat hij de [Premier en de Oppositieleider] heeft geconsulteerd, een persoon benoemen die is gekwalificeerd om benoemd te worden als tijdelijk Commissaris indien –

h. de Commissaris Gegevensbescherming zijn ontslag indient of zijn functie anderszins vacant wordt;

i. de Commissaris Gegevensbescherming om welke reden dan ook niet in staat is zijn de taken van zijn functie uit te voeren;

j. de Commissaris Gegevensbescherming het nodig acht, op tijdelijke basis, geen van zijn functies uit te voeren in verband met zulke omstandigheden, dat indien hij een rechter bij het Hof van Justitie was, hij zich zou onthouden

en om het even welke persoon die op die wijze is benoemd, zal niet langer een tijdelijk Commissaris zijn wanneer een Commissaris wordt aangesteld om de openstaande betrekking in te vullen of, naar gelang het geval, wanneer de Commissaris Gegevensbescherming die niet in staat was de taken van zijn functie uit te voeren, die functies wederom opneemt of, in het geval van een tijdelijk doel, de tijdelijke Commissaris de functie die aan hem was toegekend heeft uitgevoerd.

(6) De benoeming van een tijdelijke Commissaris met een tijdelijk doel zoals voorzien in lid (3) onder (b) en (c) kan slechts worden uitgeoefend op laste van een verklaring getekend door de Commissaris Gegevensbescherming waarin wordt aangegeven dat naar zijn mening het nodig is voor de juiste aanpak van het werk van de Commissaris Gegevensbescherming onder deze wet, dat een tijdelijke Commissaris wordt benoemd.

Rechtspersoonlijkheid en vertegenwoordiging van de Commissaris Gegevensbescherming

49. (1) De Commissaris Gegevensbescherming zal een aparte rechtspersoon zijn en zal bevoegd zijn, behoudens de bepalingen van deze wet, om contracten aan te gaan, om het even welk eigendom aan te schaffen, bezitten en verkopen voor de doeleinden van zijn functie, om gedingen aan te spannen en voor het gerecht gedaagd te worden, en om al die zaken te doen en dergelijke transacties aan te gaan die bijkomstig of bevorderlijk zijn bij de uitoefening of uitvoering van zijn taken onder deze wet.

(2) Enig document dat een instrument lijkt te zijn, gemaakt of afgegeven door de Commissaris Gegevensbescherming en door hem getekend, zal ontvangen worden als bewijs en zal, tot het tegendeel is bewezen, worden verondersteld een instrument te zijn gemaakt of uitgegeven door de Commissaris Gegevensbescherming.

Ambtstermijn

50. (1) De Commissaris Gegevensbescherming zal zijn ambt bekleden voor een termijn van niet langer dan 5 jaren en zal in aanmerking komen voor herbenoeming wanneer zijn ambtstermijn komt te vervallen.

(2) Behoudens de bepalingen van lid (3), zal de Commissaris Gegevensbescherming zijn functie vrijgeven-

a. bij het vervallen van de termijn waarvoor hij was benoemd;

b. indien hij gediskwalificeerd wordt op grond van lid 49(2) of

c. indien hij wordt aangesteld in een andere betaalde functie of enige andere bezigheid gaat ondernemen tegen een beloning.

(3) De Commissaris Gegevensbescherming zal niet uit zijn functie worden ontheven dan door het Staatshoofd na [consultatie met de Premier en de Oppositieleider] op basis van onvermogen de taken te vervullen van zijn functie, ongeacht of dit komt door lichamelijke of geestelijke zwakte of enig ander oorzaak, of wangedrag.

Beloning van Commissaris Gegevensbescherming en personeel

51. De Commissaris Gegevensbescherming en zijn personeel zullen dergelijke beloning en toelagen voor uitgaven worden betaald, uit gelden verstrekt door het geconsolideerd fonds.

Bescherming van de Commissaris Gegevensbescherming

52. Er zal geen vervolging of ander proces voor schadevergoeding worden ingesteld tegen de Commissaris Gegevensbescherming voor een handeling uitgevoerd in goed vertrouwen tijdens de uitoefening van een taak of een bevoegdheid of discretionaire bevoegdheid onder deze wet.

Delegeren van bevoegdheden door Commissaris

53. De Commissaris Gegevensbescherming kan om het even welke onderzoeks- of handhavingsbevoegdheden die aan hem zijn toegekend ingevolge deze wet delegeren aan om het even welke bevoegde functionaris en politiefunctionaris aangewezen voor dat doeleinde door de Commissaris Gegevensbescherming.

Onafhankelijkheid van functies

54. In de uitoefening van zijn functie ingevolge deze wet zal de Commissaris Gegevensbescherming onafhankelijk handelen en zal niet onderhevig zijn aan de leiding of sturing door enige andere persoon of autoriteit.

Taken van de Commissaris Gegevensbescherming

55. De Commissaris Gegevensbescherming zal-

a. naleving waarborgen van deze wet en regelgeving;

b. een register van houders van persoonsgegevens instellen en onderhouden;

c. controle uitoefenen op alle gegevensverwerkingsactiviteiten en zowel uit eigen beweging als op verzoek van een datasubject, nagaan of de verwerking van gegevens wordt uitgevoerd in overeenstemming met de bepalingen van deze wet of regelgeving;

d. de houder van persoonsgegevens aanwijzingen geven voor het nemen van dergelijke maatregelen als nodig mocht blijken voor het waarborgen dat het verwerken van gegevens in overeenstemming gebeurt met deze wet of regelgeving; en

e. meldingen en beweringen van datasubjecten of verenigingen die datasubjecten vertegenwoordigen onderzoeken betreffende overtredingen van deze wet of regelgeving en corrigerende maatregelen nemen die de Commissaris Gegevensbescherming nodig mocht achten of zoals voorgeschreven mocht zijn ingevolge deze wet, en de datasubjecten of verenigingen informeren over de uitkomst;

f. dergelijke aanwijzingen of publieke verklaringen uitgeven als nodig mocht zijn door de Commissaris Gegevensbescherming voor de doeleinden van deze wet;

g. dergelijke maatregelen nemen die nodig mochten zijn om de bepalingen van deze wet onder de aandacht te brengen van het algemeen publiek;

h. door onderwijs en publiciteit begrip en aanvaarding bevorderen voor de beginselen van gegevensbescherming en de doelstellingen van die beginselen;

i. de Regering adviseren betreffende alle wettelijke maatregelen die zijn vereist om te worden genomen inzake privacy en gegevensbescherming;

j. of uit eigen beweging of op verzoek, rapporteren aan de Minister indien de noodzaak daartoe zich voordoet met betrekking tot enige zaak die de privacy van een datasubject raakt, waaronder alle aanbevelingen inzake de noodzaak voor of wenselijkheid om wettelijke, administratieve of andere acties te ondernemen voor het verlenen van bescherming, of een betere bescherming, van de privacy van het datasubject;

k. samenwerken met toezichthoudende autoriteiten van andere landen voor zover als nodig voor de uitoefening van zijn taken, in het bijzonder het uitwisselen van alle bruikbare informatie, in overeenstemming met enig verdrag waarbij [naam van de lidstaat] partij is of enige andere internationale verplichting van [naam van lidstaat] ;

l. in het algemeen toezicht houden op de naleving door overheids- en niet-overheidslichamen van de bepalingen van deze wet;

m. voorbereiden en uitgeven of goedkeuren, in consultatie met de belanghebbenden in de industrie, van passende gedragscodes of richtlijnen voor de begeleiding van zakenlieden en instellingen die met persoonsgegevens werken;

n. het ondernemen van onderzoek in en het toezicht houden op ontwikkelingen in de gegevensverwerking en informatietechnologie om te waarborgen dat alle negatieve effecten van dergelijke ontwikkelingen op de privacy van datasubjecten worden geminimaliseerd, en de resultaten van dergelijk onderzoek en monitoring omvatten, indien aanwezig, in het jaarverslag vereist ingevolge artikel 72.

o. het geven van advies, wel of niet op verzoek, aan een Minister of een overheidslichaam inzake elke kwestie die relevant is voor de werking van deze wet en aan de Minister rapporteren wanneer de noodzaak voor de wenselijkheid voor het aanvaarden van enig internationaal instrument door [naam van de lidstaat] inzake de privacy van datasubjecten opkomt;

p. alles te doen wat bijkomstig of bevorderlijk is voor de uitvoering van enige van de voorgaande taken; en

q. dergelijke andere taken uitoefenen en uitvoeren die worden toegekend of opgelegd aan de Commissaris Gegevensbescherming door of ingevolge deze wet, of enige andere wet.

Vertrouwelijkheid en eed

56. (1) De Commissaris Gegevensbescherming en elke bevoegde functionaris zullen de eed afleggen neergelegd in de bijlage bij het Staatshoofd.

(2) Een persoon die Commissaris Gegevensbescherming, een functionaris in dienst van de Commissaris Gegevensbescherming of een vertegenwoordiger van de Commissaris Gegevensbescherming is of is geweest zal van om het even welke gegevens verkregen als gevolg van het uitoefenen van een bevoegdheid of in het uitoefenen van een taak ingevolge deze wet geen gebruik maken of openbaar maken, zowel direct als indirect, behalve –

a. in overeenstemming met deze wet of enige andere wet; of

b. zoals toegestaan volgens een besluit van de rechter

(3) Een persoon die, zonder wettelijk excuus, in strijd handelt met lid (2) begaat een overtreding en is strafbaar bij veroordeling tot een boete van niet meer dan [...] dollars of inhechtenisneming voor een termijn van niet meer dan [...] maanden of tot beide.

Bevoegdheden van Commissaris

57. De Commissaris Gegevensbescherming zal de bevoegdheid hebben, met als doeleinde het uitoefenen van zijn taken om al dergelijke handelingen uit te voeren die hem vereist, voordelig of passend lijken voor of in verband met het uitvoeren van deze taken.

Bevoegdheid van de Commissaris om gegevens te verkrijgen

58. (1) De Commissaris Gegevensbescherming kan, door middel van een schriftelijke kennisgeving betekend aan enige persoon, verzoeken dat die persoon hem schriftelijk op een tijdstip door hem aangegeven-

a. toegang tot persoonsgegevens verstrekt;

b. informatie over en documentatie betreffende het verwerken van persoonsgegevens;

c. informatie inzake de veiligheid van het verwerken van persoonsgegevens ; en

d. enige andere informatie inzake kwesties aangegeven in de kennisgeving die nodig zijn of nuttig voor de uitvoering door de Commissaris Gegevensbescherming van zijn taken en de uitoefening van zijn bevoegdheden en taken ingevolge deze wet.

(2) In het geval dat de informatie opgevraagd door de Commissaris Gegevensbescherming is opgeslagen in een computer, op een schijf, cassette of microfilm of enig ander medium, of bewaard door middel van enig mechanisch of elektronisch apparaat of systeem, dan kan de persoon genoemd in de kennisgeving de gegevens overleggen of daartoe toegang verschaffen op een wijze zodat het meegenomen kan worden, verstaanbaar is en waarin het kan worden opgevraagd.

(3) Een van kracht zijnde wet in [naam van de lidstaat] of een wetsregel die de openbaarmaking van gegevens verbiedt of beperkt zal niet uitsluiten dat een persoon enige gegevens verstrekt aan de Commissaris Gegevensbescherming die nodig is of nuttig voor de uitoefening door de Commissaris Gegevensbescherming van zijn functie.

(4) Lid (3) zal niet van toepassing zijn op gegevens die volgens de Minister verantwoordelijk voor nationale veiligheid worden gehouden, of op enig moment werden gehouden, met als doeleinde het garanderen van de veiligheid van [naam van de lidstaat] of gegevens die zijn vrijgesteld van openbaarmaking tijdens een proces in enige rechtbank.

Inhoud van kennisgeving

59. In de kennisgeving aangegeven in artikel 58 zal worden opgenomen-

a. dat de persoon aan wie de kennisgeving is geadresseerd het recht heeft beroep aan te tekenen binnen dertig dagen ingevolge artikel [81] tegen de vereiste aangegeven in de kennisgeving; en

b. de termijn voor naleving van de vereiste aangegeven in de kennisgeving, welke termijn niet zal vervallen voor het eind van de periode van dertig dagen aangegeven in lid (a).

Verzuim of weigering een kennisgeving na te leven

60. (1) Een persoon zal niet, zonder redelijk excuus, verzuimen of weigeren een vereiste aangegeven in een kennisgeving na te leven.

(2) Een persoon zal niet, bij de kennelijke naleving van een kennisgeving gegevens verstrekken aan de Commissaris Gegevensbescherming waarvan de persoon weet dat die in aanzienlijke mate onjuist of misleidend zijn.

(3) Een persoon die in strijd handelt met leden (1) of (2) begaat een overtreding en is strafbaar [bij standrechtelijke veroordeling] tot een boete van niet meer dan [...] dollars of inhechtenisneming voor een termijn van niet meer dan [...] maanden of tot beide.

(4) Het is een verdediging voor een persoon die wordt aangeklaagd voor een overtreding onder leden (1) of (2) om te bewijzen dat hij de nodige zorgvuldigheid heeft betracht om de kennisgeving na te leven.

Onvoldoende gegevens ingevolge de kennisgeving

61. Indien de Commissaris Gegevensbescherming, ingevolge een verzoek onder artikel 58(1), onvoldoende gegevens kan verkrijgen om te kunnen concluderen dat de verwerking van persoonsgegevens rechtmatig is, dan kan de Commissaris Gegevensbescherming de houder van persoonsgegevens verbieden persoonsgegevens te verwerken op enige andere wijze dan door de opslag van persoonsgegevens.

Klachten aan de Commissaris en onderzoeksbevoegdheden

62. (1) De Commissaris Gegevensbescherming kan, naar aanleiding van een klacht door een datasubject of op het initiatief van de Commissaris Gegevensbescherming, onderzoeken of laten onderzoeken, of bepalingen van deze wet of regelgeving zijn, worden of mogelijkerwijs kunnen worden geschonden door een houder van persoonsgegevens in relatie tot een datasubject.

(2) Waar een klacht is neergelegd bij de Commissaris Gegevensbescherming ingevolge lid (1), zal de Commissaris Gegevensbescherming -

a. de klacht onderzoeken of doen onderzoeken door een bevoegde functionaris, tenzij de Commissaris Gegevensbescherming van mening is dat het pietluttig of vexatoir is.

b. zo gauw als redelijkerwijs mogelijk, het betrokken datasubject schriftelijk in kennis stellen van zijn besluit met betrekking tot de klacht en dat het datasubject, indien die zich benadeeld voelt door het besluit van de Commissaris Gegevensbescherming, in beroep kan gaan tegen het besluit bij de rechter ingevolge artikel [81].

(3) Niets in deze wet sluit uit dat de Commissaris Gegevensbescherming klachten ontvangt en onderzoekt die zijn ingediend door een persoon die schriftelijk gemachtigd is door het betrokken datasubject, om te handelen namens het datasubject, en een verwijzing naar een datasubject in enig ander artikel van deze wet omvat een verwijzing naar de gemachtigde.

Vorm van de klacht

63. (1) Een klacht krachtens deze wet zal worden schriftelijk worden ingediend bij de Commissaris Gegevensbescherming tenzij de Commissaris Gegevensbescherming anderszins besluit.

(2) De Commissaris Gegevensbescherming zal dergelijke redelijke bijstand verlenen als naar omstandigheden nodig om om het even welk persoon die een klacht wil neerleggen in staat te stellen een klacht in te dienen bij de Commissaris Gegevensbescherming, om die klacht schriftelijk te doen.

Inhoud van kennisgeving

64. Voordat een onderzoek wordt ingesteld naar een klacht ingevolge deze wet, zal de Commissaris Gegevensbescherming, in geval van een overheidslichaam, de Directeur in kennis stellen en in elk ander geval, de algemeen directeur, van de intentie een onderzoek in te stellen en zal in de kennisgeving de inhoudelijke klacht opnemen.

Bevoegdheid tot betreding en huiszoeking

65. (1) Behoudens lid (2) kan een bevoegde functionaris die is vergezeld van een politiefunctionaris op ieder tijdstip panden en erven betreden voor het doorzoeken, inspecteren, onderzoeken, bedienen en testen van enige apparatuur die daar wordt aangetroffen die wordt gebruikt of zal worden gebruikt voor het verwerken van persoonsgegevens en voor het inspecteren en inbeslagnemen van documenten, apparatuur of ander materiaal daar aangetroffen.

(2) Een bevoegde functionaris zal geen panden en erven betreden voor het doorzoeken en in beslag nemen tenzij hij vergezeld is van een politiefunctionaris en aan de eigenaar of bewoner van de panden en erven een bevelschrift toont uitgevaardigd door een [rechter of relevante autoriteit (afhankelijk van het rechtsgebied)].

Zaken vrijgesteld van inspectie en inbeslagname

66. (1) De bevoegdheid voor inspectie en inbeslagname toegekend door een bevelschrift is niet uitoefenbaar inzake persoonsgegevens die ingevolge Hoofdstuk V zijn vrijgesteld van enige van de bepalingen van deze wet.

(2) De bevoegdheid voor inspectie en inbeslagname toegekend door een bevelschrift is niet uitoefenbaar inzake –

a. elke communicatie tussen een professionele juridisch adviseur en zijn cliënt in verband met het verstrekken van juridisch advies aan de cliënt inzake zijn verplichtingen, aansprakelijkheid of rechten ingevolge deze wet; of

b. elke communicatie tussen een professionele juridisch adviseur en zijn cliënt, of tussen een adviseur of zijn cliënt en een andere persoon, gedaan in verband met of in overweging van een proces krachtens of voortspruitend uit deze wet.

Bevoegdheid van de Commissaris om handhavingsbevel uit te geven

67. In het geval dat de Commissaris Gegevensbescherming van mening is dat de houder van persoonsgegevens in strijd heeft gehandeld of in strijd handelt met een bepaling van deze wet, kan de Commissaris Gegevensbescherming, behoudens artikel 69, een handhavingsbevel laten betekenen aan de houder van persoonsgegevens, waarin wordt geëist dat de houder van persoonsgegevens dergelijke stappen onderneemt als aangegeven in het handhavingsbevel binnen de termijn die is aangegeven om de betrokken bepaling na te leven.

Handhavingsbevel

68. (1) Een handhavingsbevel zal schriftelijk zijn en zal-

a. de bepalingen aangeven van deze wet waarmee volgens de Commissaris Gegevensbescherming de houder van persoonsgegevens in strijd heeft gehandeld of in strijd handelt en de redenen voor de Commissaris Gegevensbescherming om tot die conclusie te zijn gekomen; en

b. de handeling aangeven die de Commissaris Gegevensbescherming verwacht dat de houder van persoonsgegevens zal nemen;

c. behoudens lid (2) de houder van persoonsgegevens informeren over zijn recht beroep aan te tekenen ingevolge artikel [81] en de termijn waarbinnen dit beroep moet worden aangetekend.

(2) Een handhavingsbevel kan, behoudens de algemeenheid van lid (1), eisen van de houder van persoonsgegevens-

a. de betrokken gegevens te corrigeren of verwijderen; of

b. een verklaring toe te voegen aan de persoonsgegevens die betrekking heeft op de zaken die zijn aangekaart door hen zoals goedgekeurd door de Commissaris Gegevensbescherming; en met betrekking tot de persoonsgegevens die onnauwkeurig zijn of niet bijgewerkt.

(3) De termijn voor naleving van de vereiste aangegeven in het handhavingsbevel, welke termijn niet zal vervallen voor het eind van de periode waarin beroep kan worden aangetekend zoals aangegeven in artikel [81]

(4) Bij naleving van een vereiste door de houder van persoonsgegevens onder lid (2), zal de houder van persoonsgegevens, zo snel als mogelijk en in elk geval niet meer dan dertig dagen na dergelijke naleving -

a. het betrokken datasubject; en

b. enige persoon, in het geval dat de Commissaris Gegevensbescherming dat redelijkerwijs doenbaar vindt, aan wie de gegevens openbaar waren gemaakt direct voorafgaand aan dergelijke naleving, van de betrokken rectificatie, verwijdering of verklaring, indien dergelijke naleving de betrokken gegevens aanzienlijk wijzigt, in kennis stellen.

(5) De Commissaris Gegevensbescherming kan een handhavingsbevel intrekken en, indien hij dat doet, zal hij de persoon aan wie het bevel was betekend bijgevolg schriftelijk in kennis stellen.

Verzuim om een handhavingsbevel van een overtreding na te leven

69. (1) Een persoon zal niet, zonder redelijk excuus, verzuimen of weigeren een vereiste aangegeven in een handhavingsbevel na te leven.

(2) Een persoon die in strijd handelt met lid (1) begaat een overtreding en is strafbaar [bij standrechtelijke veroordeling] tot een boete van niet meer dan [...] dollars of inhechtenisneming voor een termijn van niet meer dan [...] maanden of tot beide.

Onderzoek binnenskamers

70. (1) Ieder onderzoek van een klacht ingevolge deze wet zal binnenskamers worden gehouden.

(2) In de loop van een onderzoek naar een klacht ingevolge deze wet bij de Commissaris Gegevensbescherming, zal de persoon die de klacht heeft neergelegd, hoofd van de houder van persoonsgegevens of andere relevante partij in de gelegenheid worden gesteld verklaringen af te leggen bij de Commissaris Gegevensbescherming, maar niemand zal het recht hebben op grond van een gerechtigde eis aanwezig te zijn, toegang te hebben tot, of commentaar te geven op, verklaringen die gedaan zijn bij de Commissaris Gegevensbescherming door enige andere persoon.

Verwijzing naar commissaris van politie

71. Bij afronding van een onderzoek ingevolge deze wet, kan de Commissaris Gegevensbescherming, in het geval dat het onderzoek aantoont dat een overtreding kan zijn begaan ingevolge deze wet of regelgeving de zaak verwijzen naar een Commissaris van politie voor de nodige afdoening.

Jaarverslag

72. Van de Commissaris Gegevensbescherming wordt vereist dat hij een jaarverslag presenteert van de activiteiten van zijn bureau aan het Parlement binnen [...] maanden na het eind van ieder boekjaar.

HOOFDSTUK VIII – OVERTREDING EN HANDHAVING

Persoon handelend als houder van persoonsgegevens zonder registratie

73. (1) Een persoon die persoonsgegevens verzamelt, verwerkt of openbaar maakt zonder zich eerst te hebben geregistreerd bij de Commissaris Gegevensbescherming, of buiten een goedgekeurde overeenkomst namens een geregistreerde houder van persoonsgegevens, begaat een overtreding onder deze wet en is strafbaar bij standrechtelijke veroordeling tot een boete van niet meer dan [...] en inhechtenisneming voor een termijn van [...].

(2) In het geval dat het rechtsgebied het nodig acht om “gevoelige persoonsgegevens” verder te onderscheiden, kan het meer strafmaatregelen opnemen dan die hierboven onder (1) zijn opgenomen voor de onrechtmatige verzameling, verwerking of openbaarmaking van dergelijke gegevens.

Schending van de beperking van overdracht aan derde rechtsgebieden

74. (1) Een persoon die is geregistreerd als houder van persoonsgegevens ingevolge deze wet die verzuimt enige bepaling van artikel 19 na te leven begaat een overtreding onder deze wet en is strafbaar bij—

a. standrechtelijke veroordeling tot een boete van niet meer dan [...] of inhechtenisneming voor een termijn van [...]; en

b. veroordeling na dagvaarding tot een boete van niet meer dan [...] of inhechtenisneming voor een termijn van [...].

Belemmering van een bevoegde functionaris

75. (1) Een persoon zal in relatie tot de uitoefening van de bevoegdheden toegekend door artikelen [66] en [67] niet-

a. een bevoegde functionaris belemmeren of hinderen in de uitoefening van een van bij zijn functie behorende bevoegdheden;

b. verzuimen bijstand te verlenen of informatie te verstrekken verzocht door de bevoegde functionaris;

c. weigeren een bevoegde functionaris toe te laten een pand of erven te betreden in de uitoefening van een van de bij zijn functie behorende bevoegdheden;

d. een bevoegde functionaris om het even welke gegevens verstrekken die onjuist of misleidend zijn in aanzienlijke mate.

(2) Een persoon die in strijd handelt met lid (1) begaat een overtreding en is strafbaar bij standrechtelijke veroordeling tot een boete van niet meer dan [...] dollars, inhechtenisneming voor een termijn van niet meer dan [...] maanden of tot beide.

Onjuiste verklaringen door aanvragers

76. (1) Een persoon die een verzoek doet om toegang te krijgen tot of een correctie van persoonsgegevens onder valse voorwendselen begaat een overtreding onder deze wet en is strafbaar bij standrechtelijke veroordeling tot een boete van niet meer dan [...] en inhechtenisneming voor een termijn van [...];

(2) Een persoon die opzettelijk een valse verklaring aflegt ter misleiding of die poogt de Commissaris Gegevensbescherming te misleiden in de uitvoering van zijn functie ingevolge deze wet begaat een overtreding onder deze wet en is strafbaar bij standrechtelijke veroordeling tot een boete van niet meer dan [...] en inhechtenisneming voor een termijn van [...];

Schending van geheimhouding

77. Een persoon die de geheimhoudingsplichten neergelegd in artikel [57] schendt, begaat een overtreding onder deze wet en is strafbaar bij standrechtelijke veroordeling tot een boete van niet meer dan [...] en inhechtenisneming voor een termijn van [...];

HOOFDSTUK IX -OVERIGE

Bescherming van informant

78. Een werkgever ongeacht of die een publieke autoriteit is of niet, zal een werknemer niet ontslaan, schorsen, degraderen, straffen, intimideren of op andere wijze benadelen of die werknemer een voordeel ontzeggen, omdat—

a. de werknemer in goed vertrouwen heeft gehandeld en op basis van redelijk vertrouwen—

i. de Commissaris Gegevensbescherming in kennis heeft gesteld dat de werkgever of enige andere persoon deze wet heeft overtreden of zal overtreden;

ii. iets heeft gedaan of de intentie heeft kenbaar gemaakt iets te zullen doen dat nodig is voor het voorkomen dat een andere persoon deze wet overtreedt; of

iii. iets heeft geweigerd of de intentie heeft kenbaar gemaakt te weigeren iets te doen dat in strijd is met deze wet; of

b. de werkgever gelooft dat de werknemer iets zal doen dat is beschreven in lid (a).

Vergoeding 79. (1) De Minister kan, volgend op een consultatie met de aangewezen autoriteit, bij regelgeving -

a. een vergoeding vaststellen die door de houder van persoonsgegevens of een categorie van houders van persoonsgegevens wordt geheven voor het doen van een verzoek door een datasubject voor hun persoonsgegevens.

b. de manier voorschrijven waarop een vergoeding betaalbaar ingevolge deze wet moet worden berekend en het maximumbedrag dat niet mag worden overschreden.

Regelgeving 80. (1) De Minister kan, in overleg met de Commissaris Gegevensbescherming, regelgeving neerleggen om uitvoering te geven aan de doeleinden van deze wet en voor het voorschrijven van alles wat vereist of geautoriseerd is door deze wet.

(2) Niettegenstaande de algemeenheid van lid (1), kan regelgeving neergelegd ingevolge dit artikel voorschrijven -

a. voorgeschreven vergoedingen te betalen door de houder van persoonsgegevens;

b. procedurele richtlijnen voorzien voor het aantekenen van beroep tegen het besluit van de houder van persoonsgegevens;

c. voorschrijven alles wat nodig is om voorgeschreven te worden ingevolge deze wet; en

d. het uitvoering geven aan de bepalingen van deze wet.

(3) Regelgeving neergelegd onder dit artikel zal onderhevig zijn aan de goedkeuring van het Parlement.

Rol van de rechtbank 81. (1) Behoudens lid (2), wordt een beroep aangetekend bij de rechtbank tegen –

a. een vereiste aangegeven in een handhavingsbevel of een kennisgeving;

b. een besluit van de Commissaris Gegevensbescherming in verband met een klacht; of

c. elk besluit van de Commissaris Gegevensbescherming met betrekking tot de uitoefening van zijn taken en bevoegdheden ingevolge deze wet.

(2) Een beroep wordt aangetekend binnen [...] dagen na betekening aan de betrokken persoon van de relevante kennisgeving, of, naargelang het geval, de ontvangst door dergelijke persoon van de kennisgeving van de relevante weigering of het besluit.

(3) De rechtbank zal jurisdictie hebben zaken te horen en beslissen op aanvraag van de Commissaris Gegevensbescherming die een schending van de bepalingen van deze wet betreffen en rechterlijke bevelen in verband daarmee uit te vaardigen.

Deel III:
Memorie van toelichting bij de model wettekst – Privacy en gegevensbescherming

INLEIDING

1. Deze model wettekst privacy en gegevensbescherming informatie is voorbereid als deel van een serie van model wetteksten voor het mogelijk maken van de "informatiemaatschappij" onder een regionaal project dat de CARICOM-landen en de Dominicaanse Republiek behelst.
2. De informatiemaatschappij is gebaseerd op de vooronderstelling van het gebruik van geautomatiseerde verwerkingssystemen om de levering van diensten aan markten en personen waar ook ter wereld te verbeteren. In dit nieuwe paradigma, als de verwerkingskracht in overweging wordt genomen van informatiesystemen, is de kans om informatie te misbruiken die is verzameld over een persoon in de loop van een transactie exponentieel toegenomen. Het bevorderen van het gebruik van deze systemen door het algemeen publiek vereist het instellen van systemen die vertrouwen wekken bij de gebruiker en helpen dat de informatie die is verzameld niet zal worden gebruikt op een ongewettigde wijze zonder strafsanctie.
3. Het privacy en gegevensbeschermingskader is een sleutelelement van dat grotere systeem van vertrouwen scheppen.
4. De HIPCAR model wettekst inzake privacy en gegevensbescherming is gebaseerd op de beleidsbouwstenen die werden ontwikkeld in een eerdere fase van het HIPCAR Project.4. Deze bouwstenen evalueerden de internationale beste toepassing in de praktijk voor de doelstellingen, de belangrijkste gemeenschappelijke instrumenten en precedenten, en identificeerden de belangrijkste beleidsposities en -systemen die opgenomen dienden te worden in wettelijke kaders in de gehele regio5. De model wettekst is een poging de beleidsrichtlijnen in een wettelijk instrument te gieten dat poogt de concurrerende impulsen van de duidelijkheid van de bedoeling, structuur en functie in evenwicht te brengen met de nodige behoefte aan abstractie voor het vergemakkelijken van de vlotte aanpassing, waar nodig, aan het wetgevingskader van elk begunstigd HIPCAR-land.
5. Deze model wettekst privacy en gegevensbescherming omvat negen hoofdstukken en eenentachtig artikelen.
   - **Hoofdstuk een** behandelt de inleidende overwegingen, zoals de citeertitel en de interpretatie van bepaalde termen in de modeltekst en behandelt overwegingen aangaande de reikwijdte van de toepassing van de modeltekst, en definieert tevens de algemene privacy beginselen die vervat zijn in de modeltekst.

---

4 Red.: De volledige naam van het HIPCAR-project is "*Versterking van het Concurrentievermogen in het Caribisch Gebied door de Harmonisatie van Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT*". Het project met een looptijd van drie jaar werd gelanceerd in september 2008 in het kader van overkoepelend project voor de ACP-landen en wordt gefinancierd door de Europese Unie (EU) en de Internationale Telecommunicatie Unie (ITU). Het project wordt geïmplementeerd door de Internationale Telecommunicatie Unie (ITU) in samenwerking met de Caribische Gemeenschap (CARICOM) en de Caribische Telecommunicatie Unie (CTU).

5 Red.: Zie ook Hoofdstuk 1.5 van dit document waarin de methodologie wordt uitgelegd. De leden van de HIPCAR Werkgroepen bestaan uit vertegenwoordigers van Ministeries en regelgevende lichamen aangewezen door hun nationale overheden, relevante regionale lichamen en waarnemers – zoals aanbieders en andere geïnteresseerde belanghebbenden. De opdracht voor de werkgroepen zijn beschikbaar op www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/docs/ToR%20HIPCAR%20WGs.pdf.

- **Hoofdstuk twee** behandelt de instelling van een algemene verplichting van de overheid en private lichamen die kunnen worden beschouwd als de houders van persoonsgegevens om bepaalde verantwoordelijkheden op zich te nemen met betrekking tot het beheer van persoonsgegevens in hun beheer.
- **Hoofdstuk drie** behandelt het algemene recht van individuen of datasubjecten toegang te hebben en om zich te verzekeren van de juistheid van hun persoonsgegevens in het bezit van overheids- en private lichamen en creëert het mechanisme en de procedures voor het vergemakkelijken van het verlenen van dergelijke toegang.
- **Hoofdstuk vier** identificeert specifieke verplichtingen van de overheid onder de modeltekst. Dergelijke verplichtingen hebben te doen met bepaalde operationele omstandigheden van publieke lichamen.
- **Hoofdstuk vijf** handelt over de speciale voorwaarden waarbij de verplichtingen van de houder van persoonsgegevens om eerst instemming te krijgen van het datasubject voor openbaarmaking niet vereist zijn.
- **Hoofdstuk zes** handelt over procedures die een datasubject kan gebruiken om een besluit van een houder van persoonsgegevens te herzien om geen toegang te verlenen, en waar nodig, beroep aan te tekenen tegen het besluit van een onafhankelijk toezichthoudend lichaam.
- **Hoofdstuk zeven** voorziet in een algemeen kader en bevoegdheden van het lichaam dat is aangewezen bij het toezichthoudend lichaam voor het toezicht houden op de implementatie van privacy en gegevensbescherming en voorziet in een forum om beroep aan te tekenen in overeenstemming met de bepalingen van hoofdstuk zes.
- **Hoofdstuk acht** geeft de specifieke overtredingen op de bepalingen van de modeltekst aan en de strafsancties geassocieerd met dergelijke overtredingen.
- **Hoofdstuk negen** voorziet in verschillende overwegingen, waaronder het verduidelijken van de rol van de rechtbank, het opzetten van een aanpak van co-regulering bij de implementatie van het toezichthoudend kader en stelt de bevoegdheden vast om regelgeving te creëren in overeenstemming met de modeltekst.

OVERZICHT VAN DE ARTIKELEN

HOOFDSTUK I – INLEIDENDE ARTIKELEN

6. **Hoofdstuk 1 van de model wettekst (wet)** omvat zeven artikelen. De eerste artikelen zijn de inleidende bepalingen, waaronder de citeertitel en de inwerkingtreding van de wet[6]. evenals de algemene doelstelling van de wet, zodat een verklarende context wordt gegeven voor de artikelen die daarna worden gepresenteerd.

Artikel 3: Interpretaties en definities

7. Artikel 3 voorziet in de interpretatie van specifieke termen in de wet.[7]. Van belang zijn de interpretaties van termen zoals die hieronder.

[6] Red.: De auteur van de memorie van toelichting gebruikt voornamelijk de term “wet” wanneer hij verwijst naar de model wettekst (wet) inzake privacy en gegevensbescherming.

[7] Beleidsbouwsteen 1.1 “Er is een duidelijk wettelijk mandaat in de wet ter ondersteuning van het instellen van een systeem om de bescherming van persoonlijke en/of privé informatie te waarborgen.”

8. "gegevens" en "informatie" (termen die gelijkgesteld zijn) benadrukken een brede interpretatie van toepasselijke vormen, formaten en technologieën (elektronisch of anderszins) waarin de gegevens kunnen worden gepresenteerd of opgeslagen. Dit is noodzakelijk omdat ondanks de heersende opvattingen geassocieerd met de alomtegenwoordigheid van informatie en communicatietechnologie (ICT), het voorziet in de toepasselijkheid van de wet en de intentie daarvan in omgevingen waarin geen ICT-systemen worden gebruikt.[8].

9. "houder van persoonsgegevens," waarvan de definitie bedoeld is om een brede perceptie te hebben van de term "personen", waaronder partijen zowel in de publieke en private sectoren. Het is opmerkelijk dat de definitie niet suggereert dat alle publieke of private sector agentschappen houders zijn van persoonsgegevens, waarmee de toepassing van de wet beperkt wordt tot degenen die een rechtmatige noodzaak hebben om met persoonsgegevens om te gaan in de loop van hun inhoudelijke zaken.9

10. Ondanks dat de beleidsbouwstenen en een internationaal precedent de vereiste suggereert van een onderscheid tussen "persoonsgegevens" en "gevoelige persoonsgegevens" werd geconstateerd dat de relevante bepalingen voornamelijk gelijk waren betreffende de behandeling van deze twee. Op die wijze, voorziet de model wettekst erin dat de definitie van de tweede is opgenomen in de eerste. Gevoelige persoonsgegevens werden voornamelijk opgenomen in gegevensbeschermingskaders als een extra middel om kwesties van seksuele, raciale of andere soorten van onwelvoeglijke discriminatie aan te pakken. Dit wordt in het algemeen bereikt door het verder beperken van de toepasselijke verwerking van dergelijke kenmerken (geslacht, seksuele geaardheid, politieke overtuiging, etniciteit of ras) buiten de algemene beperking die anderszins wordt voorzien in het wetgevingskader, evenals het voorzien in strengere strafbepalingen voor inbreuken geassocieerd met deze deelverzameling van de informatie in vergelijking met wat toepasselijk is op "niet-gevoelige" informatie. Ondanks dit, bestaat er een algemene consensus dat gegevensbescherming niet de beste plaats is voor een dergelijke bepaling. Echter, er worden leidraden gegeven door de gehele wettekst heen op welke gebieden er een verder onderscheid gemaakt moet worden indien het rechtsgebied besluit een onderscheid te maken tussen persoonsgegevens en gevoelige persoonsgegevens.10

11. "gezondheidswerker" en "instelling in de gezondheidszorg" zijn termen die een juiste definitie behoeven aangezien deze een terugkerende basis vormen voor de niet-toepasselijkheid van de wet waar het betrekking had op de instemming van het datasubject voor het verzamelen, verwerken en openbaar maken van persoonsgegevens. Deze vrijstelling, net als die betrekking heeft op rechtshandhaving, is gebaseerd op het waarborgen dat het gegevensbeschermingskader de natuurlijke werking van dergelijke diensten niet verhindert. Over het algemeen, bij de voorziening van gezondheidszorg, door de specialistische aard van het beroep, kan het onredelijk zijn te verwachten dat de behandelend arts in staat zal zijn alle partijen te identificeren met wie de medische informatie wordt gedeeld in de bepaling van een diagnose, of in een kritiekere situatie, in een noodgeval waarbij het datasubject is uitgeschakeld. Daarom, dient er een algemene vrijstelling te zijn voor personen die werken in dit specifieke milieu van het gegevensbeschermingskader, aangezien deze sector specifiek zou moeten worden behandeld in wetgeving die direct daarop is toegespitst. Het is opmerkelijk dat bepaalde administratieve functies niet direct gerelateerd aan het verstrekken van gezondheidszorg zouden moeten vallen onder deze vrijstellingsrubriek.

---

8 Beleidsbouwsteen 1.2 "Het systeem van gegevensbescherming dient niet technologiespecifiek te zijn, en moet daarom gelijkaardige relevantie hebben in omgevingen die met papieren werken of ICT-technologie toepassen".

9 Beleidsbouwsteen 1.4 "De wet/het wettelijk mandaat moet verzekeren dat de verplichting om privacy te beschermen toepasselijk is op zowel de publieke en private sector."

10 Beleidsbouwsteen 1.9 "De wet/het wettelijk mandaat moet een categorie persoonsgegevens identificeren als "gevoelige informatie", waarvoor strikter toezicht en controle vereist is."

Artikel 4: Verbindt de Staat

12. Artikel 4 stelt vast dat de wet de Staat verbindt. Deze bepaling is noodzakelijk aangezien de interpretatiewetten van de lidstaten uitdrukkelijk aangeven de welbekende regel die geldt naar aanleiding van de uitspraak in de zaak van ***Attorney General v. Hancock [1940] 1 KB 427*** dat een wet de staat niet verbindt of het recht van de staat beïnvloedt tenzij het nadrukkelijk is neergelegd in de wet.[11]

Artikel 5: De toepasselijke jurisdictiebevoegdheid van de wet

13. De multinationale aard erkennende van bepaalde bedrijfstakken, evenals de gemondialiseerde handelsomgeving vergemakkelijkt door het gebruik van ICT, tracht artikel 5 duidelijkheid te verschaffen over de limieten van de jurisdictiebevoegdheid van de wet, met betrekking tot houders van persoonsgegevens die gevestigd kunnen zijn in een bepaald rechtsgebied (waar de toepasselijkheid zeker is) en de houders van persoonsgegevens die niet gevestigd of residerend zijn in het rechtsgebied maar hulpmiddelen gebruiken die zich daarin bevinden. Dit artikel is bijzonder belangrijk in de context van de bepalingen van artikel 22.

Artikel 6: Beperking van de toepasselijkheid van de wet

14. Artikel 6 beperkt verder de toepasselijkheid van de wet met betrekking tot het beperken van de gegevens die beschikbaar zijn volgens de wet aan tribunalen en rechtbanken.

Artikel 7: Overzicht van de privacy beginselen

15. Dit hoofdstuk geeft in artikel 7 de privacy beginselen aan die de wet tracht te verankeren in de uitvoering van publieke en private sector ondernemingen.[12]. Deze beginselen, gebaseerd op het precedent gelegd door de OESO en de EU omvatten:

Beginsel van aansprakelijkheid

Een houder van persoonsgegevens zou aansprakelijk moeten zijn voor het naleven van de maatregelen die uitvoering geven aan de beginselen die hierboven zijn vastgelegd.

Beginsel van beperking van de verzameling

Er moeten beperkingen gelden op het verzamelen van persoonsgegevens en al dergelijke gegevens moeten op rechtmatige en eerlijke wijze vergaard worden en, waar van toepassing, met medeweten of instemming van het datasubject.[13.]

Beginsel van de kwaliteit van de gegevens

Persoonsgegevens dienen relevant te zijn voor de doeleinden waarvoor zij worden gebruikt, en in de mate waarin zij nodig zijn voor die doeleinden, en zouden nauwkeurig, compleet en bijgewerkt moeten zijn.

Beginsel van specificatie van het doel

De doeleinden waarvoor de persoonsgegevens worden verzameld zouden niet later moeten gespecificeerd worden dan op het moment van de gegevensverzameling en het daaropvolgend gebruik dient beperkt te zijn tot de invulling van die doeleinden of dergelijke andere die niet onverenigbaar zijn met die doeleinden en zoals die zijn aangegeven bij elk geval van wijziging van het doeleinde.[14.]

---

11 Beleidsbouwsteen 1.3 “De wet/het wettelijk mandaat moet duidelijk aangeven dat de wet de de staat verbindt”

12 Beleidsbouwsteen 2.1 “Essentiële beginselen over het gegevensbeschermingskader zijn duidelijk gedefinieerd in de [wet]”

13 Beleidsbouwsteen 1.7 “De wet/het wettelijk mandaat voorziet er duidelijk in dat persoonsgegevens moet worden verzameld en verwerkt met de instemming van het onderwerp van de persoonsgegevens.”

14 Beleidsbouwsteen 2.2 “Onder de essentiële beginselen over gegevensbescherming zouden dergelijke bepalingen moeten zijn die waarborgen dat op het moment van het verzamelen van de gegevens het datasubject bewust wordt gemaakt wat de doelstelling/ het gebruik van dergelijke data zal zijn en duidelijk instemt met dergelijke doelstelling/ gebruik van die gegevens.”

Beginsel van beperking van gebruik

Persoonsgegevens mogen nooit openbaar gemaakt worden, beschikbaar gesteld of anderszins gebruikt voor andere doeleinden dan aangegeven zijn in overeenstemming met het principe van specificatie van het doel, tenzij:

(a) met de instemming van het datasubject; of

(b) ingevolge een bevoegdheid bij wet.

Beginsel van waarborgen van beveiliging

Persoonsgegevens dienen beschermd te worden door middel van redelijke veiligheidswaarborgen tegen dergelijke risico's zoals het verlies of onrechtmatige toegang, vernietiging, gebruik, wijziging of openbaarmaking van gegevens.

Beginsel van openheid

Er dient een algemeen beleid te zijn van openheid over de ontwikkelingen, praktijken en beleidslijnen met betrekking tot persoonsgegevens. Middelen voor het vaststellen van het bestaan en de aard van persoonsgegevens, en het belangrijkste doeleinde voor het gebruik daarvan, evenals de identiteit en de gebruikelijke verblijfplaats van de houder van persoonsgegevens dient zondermeer beschikbaar te zijn.

Beginsel van individuele deelname

Een individu moet het recht hebben:

(a) van een houder van persoonsgegevens te verkrijgen, of anderszins, een bevestiging of de houder van persoonsgegevens wel of geen gegevens heeft die betrekking op hem hebben;

(b) aan hem gecommuniceerd te hebben binnen een redelijke termijn, gegevens die betrekking op hem hebben;

- tegen een vergoeding, indien van toepassing, die niet excessief is;
- op een redelijke wijze; en
- in een vorm die direct leesbaar is voor hem;

(c) redenen te worden gegeven indien een verzoek gedaan onder leden (a) en (b) wordt geweigerd, en om zich te kunnen verzetten tegen dergelijke weigering; en

(d) de gegevens die op hem betrekking hebben aan te vechten, en indien dat terecht is de gegevens te laten verwijderen, corrigeren, aanvullen of aanpassen.15.

HOOFDSTUK II – ALGEMENE VERPLICHTINGEN VAN HOUDERS VAN PERSOONSGEGEVENS

16. **Hoofdstuk 2 van de modelwet** beschrijft regels waaraan alle houders van persoonsgegevens zich moeten houden bij het implementeren van de beginselen van privacy uiteengezet in hoofdstuk 1.

[15] Beleidsbouwsteen 2.3 “Onder de essentiële beginselen van gegevensbescherming moeten dergelijke bepalingen aanwezig zijn die de verantwoordelijkheid bij de persoon en/ of het lichaam plaatsen die de persoonsgegevens verzamelt en/of verwerkt voor de beveiliging, nauwgezetheid en juist gebruik van die informatie.”

Artikel 8: Registratie van houders van persoonsgegevens.

17. Artikel 8 voorziet in de registratie van houders van persoonsgegevens en in het bijhouden van een register door de Commissaris Gegevensbescherming. Een andere mogelijkheid, waar de voorkeur voor een minder belemmerend kennisgevingsproces zou zijn, kan dit hier worden gefaciliteerd[16]. In beide gevallen, zou dit in overeenstemming zijn met de **OESO beginselen inzake aansprakelijkheid en openheid** die vereisen dat er een algemeen beleid van openheid dient te zijn betreffende de ontwikkelingen, praktijken en beleidslijnen met betrekking tot persoonsgegevens en hulpmiddelen betreffende het vaststellen van het bestaan en de aard van persoonsgegevens, en de belangrijkste doeleinden voor het gebruik daarvan, evenals de identiteit en de gebruikelijke verblijfplaats van de houder van persoonsgegevens zouden zondermeer beschikbaar moeten zijn. Op gelijke wijze, waarborgt lid (8) onder 2 naleving van **het OESO beginsel inzake de beperking op verzameling** dat er beperkingen moeten gelden op het verzamelen van persoonsgegevens en al dergelijke gegevens moeten op rechtmatige en eerlijke wijze vergaard worden en, waar van toepassing, met medeweten of instemming van het datasubject.[17,18] Het is nodig te herhalen dat het individu het doel van de verzameling, het gebruik, openbaarmaking moet kennen, en moet weten dat hij of zij toestemming daarvoor kan geven of onthouden. Uitdrukkelijke toestemming (verbaal of schriftelijk gecommuniceerd) zou in het algemeen vereist zijn, maar instemming kan stilzwijgend zijn in een beperkt aantal gevallen. Toestemming moet ook vrijwillig zijn, moet betrekking hebben op de betreffende gegevens, en mag niet worden verkregen middels misleiding of dwang. Toestemming kan ook worden teruggenomen of beperkt worden door het individu dat toestemming geeft, in ieder geval waar de toestemming (stilzwijgend of uitdrukkelijk) is vereist.

Artikel 9: Beperking van te verzamelen persoonsgegevens

18. Deze laatste verplichtingen geassocieerd met dit beginsel zijn opgenomen door middel van artikel 9 in samenhang met de bepaling dat, waar mogelijk, de gegevens altijd direct van het datasubject verkregen dienen te worden. Ingevolge dit artikel, dienen houders van persoonsgegevens te waarborgen dat zij het doel waarvoor de persoonsgegevens worden verzameld kunnen verwoorden en de namen van de persoon die de beoogde ontvanger is van de persoonsgegevens. Ondanks deze algemene rechten, artikel 9 onder (2) legt specifieke omstandigheden neer waaronder het niet praktisch is voor het agentschap dat persoonsgegevens verzamelt om dit rechtstreeks te doen van het datasubject.[19]

Artikel 10: Verzameldoel van gegevens dient te worden gespecificeerd

19. Artikel 10 legt een kader neer om overeenstemming te waarborgen met het OESO Beginsel van specificatie van het doel, waarbij het doel waarvoor de persoonsgegevens worden verzameld niet later dient te worden gespecificeerd dan op het moment van gegevensverzameling. Alszodanig, kan het datasubject bepalen of hij of zij toestemt met de verzameling van die gegevens zoals nodig om dit doel te bereiken. Verder, wordt de houder van persoonsgegevens daarom verplicht de persoonsgegevens te vernietigen wanneer die niet langer nodig zijn. Om dit

16 Beleidsbouwsteen 3.1 “De wet/het wettelijk mandaat zal duidelijk aangeven dat er bepalingen moeten zijn voor de duidelijke identificatie van de verzamelaars, gebruikers en verwerkers van persoonsgegevens dergelijke bepaling kan een kennisgeving inhouden aan of registratie bij de aangewezen persoon.”

17 Beleidsbouwsteen 4.1 “De wet/het wettelijk mandaat zal herbevestigen dat de overheid slechts persoonsgegevens vergaren die uitdrukkelijk zijn toegestaan door een geschreven wet”

18 Beleidsbouwsteen 4.3 “De wet/het wettelijk mandaat zal erin voorzien dat het datasubject uitdrukkelijk instemt met de vergaring van gegevens.”

19 Beleidsbouwsteen 1.8 “De wet/het wettelijk mandaat voorziet duidelijk in de omstandigheden waaronder persoonsgegevens kan worden verzameld en verwerkt zonder de instemming van of kennisgeving aan het onderwerp van de persoonsgegevens.”

te bereiken, moeten de houders van persoonsgegevens geschikte bestandsbeheerspraktijken toepassen, waaronder methoden voor het veilig opslaan en verwijderen.

Artikel 11: Beperking op de bewaring van persoonsgegevens

20. Artikel 11 legt daarom beperkingen neer op de bewaring van dergelijke gegevens slechts voor zo lang als nodig is voor het vervullen van het doel waarvoor die waren verzameld, en andere verplichtingen (onder artikel 13 van deze wet en andere) waarbij het datasubject het recht van toegang tot gegevens heeft.

Artikel 12: Passende verwijdering van persoonsgegevens

21. Ingevolge deze definitie van overwegingen voor bewaring, voorziet artikel 12 op gelijkaardige wijze in de definitie van passende verwijdering van gegevens in overeenstemming met de beste praktijken van bestandsbeheer. Voor het voorzien in passende consultatie (en flexibiliteit) voor de juiste termijn die kan worden toegepast in samenhang met een bredere groep belanghebbenden (waaronder, in het geval van publieke bescheiden, de nationale archieven van een rechtsgebied), wordt de uiteindelijke bepaling van deze laatste termijn uitgesteld zodat het regelgeving van de hoofdwet ondersteunt.

Artikel 13: Nauwgezetheid van persoonsgegevens

22. Artikel 13 van de modelwet zorgt voor overeenstemming met het ***OECD Data Quality Principle*** (OESO beginsel van kwaliteit van gegevens). Dit artikel, in samenhang met artikel 28 van Hoofdstuk 3, voorziet in een kader waarmee de houders van persoonsgegevens verantwoordelijk worden gesteld voor de juistheid van de gegevens bewaard of die zijn bedoeld om voor verwerking te worden gebruikt.

Artikel 14: Bescherming van persoonsgegevens

23. Artikel 14 van de modelwet zorgt voor overeenstemming met het OECD Security Safeguards Principle (OESO beginsel van waarborgen van beveiliging) dat zorg draagt dat persoonsgegevens met behulp van redelijke veiligheidsmaatregelen beschermd worden tegen risico's als:

    a) verlies of

    b) niet-geautoriseerde toegang,
        i. vernietiging,
        ii. gebruik,
        iii. wijziging, of
        iv. openbaarmaking

    van gegevens. De veiligheidsmaatregelen moeten passen bij de mate van gevoeligheid van de persoonsgegevens. Op zich tracht deze bepaling niet een bepaalde wijze van beveiliging van informatie op te leggen aan de houder van persoonsgegevens. Voldoende toezicht op het volgen van richtlijnen, codes, en in het geval van publieke lichamen, goedgekeurde risicoanalyses, zullen de aangewezen instantie de benodigde flexibiliteit geven.

Artikel 15: Beperking van het gebruik van persoonsgegevens

24. Artikel 15 zorgt voor naleving van het **OECD Use Limitation Principle** (OESO beginsel van beperking van gebruik) dat zegt dat persoonsgegevens nooit gebruikt mogen worden voor andere doeleinden dan aangegeven zijn in overeenstemming met het **Purpose Specification Principle** (beginsel van specificatie van het doel) dat hierboven besproken is, aangezien in het algemeen toestemming vereist is voor elk verzamelen, gebruik en elke openbaarmaking van

persoonsgegevens[20]. Opgemerkt wordt dat, alhoewel het ontwerp voorziet in een houder van persoonsgegevens die ná verzameling toestemming verkrijgt van het datasubject, deze gedragslijn ontmoedigd moet worden. Houders van persoonsgegevens moeten datasubjecten controle en informatie geven over hun persoonsgegevens zonder de rechtmatige en passende uitwisseling van informatie die nodig is voor elektronische handel en de ondersteuning daarvan, te belemmeren. Ondanks dit algemene principe zijn er gevallen dat de verzamelde informatie voor andere doeleinden verwerkt moet worden of wegens het algemeen belang aan andere gespecificeerde partijen verstrekt moet worden. Om te waarborgen dat de bepaling niet in ernstige mate ondermijnd wordt, moeten bij wet uitzonderingen bepaald worden. Situaties waarin het verwerken van persoonsgegevens aangemerkt moet worden als een uitzondering op het algemene principe van **Beperking van gebruik** worden beschreven in Hoofdstuk V.

25. Opgemerkt wordt dat in subsectie (4) regels gegevens worden voor het vaststellen van een andere behandeling van “gevoelige persoonsgegevens” ter onderscheid van “persoonsgegevens”. Voorbeelden voor de implementatie hiervan kunnen ontleend worden aan de EU-rechtsgebieden, waar het houders van persoonsgegevens expliciet verboden is om gevoelige persoonsgegevens te verwerken op gegeven uitzonderingen na[21], terwijl persoonsgegevens verwerkt kunnen worden zolang die verwerking in overeenstemming is met het doel waarvoor ze oorspronkelijk zijn verzameld, in overeenstemming met de bepalingen onder 15. Daarom is het redelijk te zeggen dat, in overeenstemming met het Collection Limitation Principle (principe van beperkte verzameling), gevoelige persoonsgegevens niet verzameld moeten worden, behalve in de vastgestelde uitzonderingsgevallen. Belangrijke uitzonderingen op deze beperking van (verzamelen en) verwerking, die verder gaan dan die van toepassing zijn op persoonsgegevens, zijn o.a.:

    a) gebruik door een gezondheidswerker in de specifieke omstandigheid van het uitvoeren van medische en met de gezondheid samenhangende handelingen in een instelling voor gezondheidszorg;

    b) gebruik door wetshandhavers en beveiligingspersoneel op het specifieke terrein van preventie, verijdeling of opsporing van misdaden of andere zaken van nationale veiligheid.

    c) gebruik om te bepalen of iemand in aanmerking komt voor een bepaalde sociale voorziening, waarvoor die informatie noodzakelijk is.

26. De artikelen 16, 17 en 18 beschrijven wanneer persoonsgegevens openbaar gemaakt kunnen worden zonder voorafgaande toestemming van het datasubject. Onder deze gevallen vallen de onderstaande.

[20] Beleidsbouwsteen 5.1 “De wet/het wettelijk mandaat beperkt de verzamelende partij tot het gebruik of de verwerking van de informatie voor het gespecificeerde doel waarmee ingestemd is door het datasubject dat aangegeven is en waarvoor toestemming is gegeven door het datasubject op het moment van verzameling”

[21] Beleidsbouwsteen 5.9 “De wet/het wettelijk mandaat verbiedt de verwerking van gevoelige persoonsgegevens, behalve in specifieke gevallen en voor specifieke doelen...”

Artikel 16: Openbaarmaking van persoonsgegevens in overeenstemming met het verzameldoel

27. Artikel 16 voorziet in de openbaarmaking van persoonsgegevens voor doeleinden die in overeenstemming zijn met het doel en de verwerking waarvoor het datasubject bij de inzameling toestemming heeft gegeven, tenzij de gegevens verzameld zijn ingevolge een geschreven wet, bij wetshandhavingsacties, wettelijke procedures of ten behoeve van de volksgezondheid[22].

Artikel 17: Openbaarmaking van persoonsgegevens voor onderzoek en statistieken

28. Artikel 17 voorziet in de openbaarmaking van persoonsgegevens voor het uitvoeren van onderzoek en statistische analyse, wanneer de houder van persoonsgegevens ervan verzekerd is dat de beveiligingseisen gehandhaafd blijven en dat de ontvangende partij de intentie heeft om zich aan de wettelijke bepalingen te houden.

Artikel 18: Openbaarmaking van persoonsgegevens voor archivering

29. Artikel 18 voorziet in de openbaarmaking van persoonsgegevens voor archivering, wanneer de gegevens aan specifieke criteria voldoen, of wanneer het datasubject een bepaalde periode overleden is. Dit artikel laat in essentie persoonsgegevens van een overledene die van nationaal of anderszins van cultureel belang is, die aan een Archief en dergelijke instellingen zijn overgedragen, buiten de reikwijdte van de verplichtingen van de modelwet vallen. Zonder een dergelijk artikel zou de wet het opereren van instellingen zoals het Nationaal Archief, die een aanzienlijke rol spelen bij het behoud van nationale cultuur en geschiedenis, verhinderen.

Artikel 19: Beperking van overdragen van persoonsgegevens tussen rechtsgebieden

30. Artikel 19 van dit hoofdstuk beperkt houders van persoonsgegevens met name met betrekking tot de opslag van persoonsgegevens binnen het rechtsgebied waar de wet van toepassing is of in een rechtsgebied met gelijksoortige privacybeschermingswetten. Indien de laatste situatie van toepassing is, moet de houder van persoonsgegevens eerst toestemming verkrijgen van:

    a) De Commissaris Gegevensbescherming; en

    b) het datasubject

    om de overdracht tot stand te brengen. De houder van persoonsgegevens moet het/de betrokken individu/individuen aangeven wie de privacybeschermingswetten in het andere rechtsgebied uitvoert.23. Een overgangsbepaling is opgenomen in lid (5) ter erkenning van het bestaan van enkele transregionale bedrijven die hun ondernemingen georganiseerd hebben rond gegevenshubs binnen de regio, en tevens erkennend dat het niet redelijk is te verwachten dat implementatie van een bepaling als artikel 19 gelijktijdig in de hele regio zal plaatsvinden. Op deze manier kan de Commissaris Gegevensbescherming een redelijke termijn vaststellen om de gegevenshubs te verplaatsen naar op behoorlijke wijze beschermde rechtsgebieden, voordat sancties worden opgelegd.

---

22 Beleidsbouwsteen 6.2 “De wet/het wettelijk mandaat voorziet in de vrijstelling van de verplichting om toestemming te verkrijgen van het datasubject waar dat vereist is door een wettelijke regeling, indien het gaat om belangen van nationale veiligheid, rechtsbedeling en gezondheidsmanagement.”

23 Beleidsbouwsteen 6.3 “De wet/het wettelijk mandaat beperkt de grensoverschrijdende overdracht van persoonsgegevens naar rechtsgebieden die geen vergelijkbare privacy en gegevensbeschermingswetten en -systemen hebben. In een dergelijk geval, voorziet de wet erin dat slechts zoveel informatie wordt overgedragen dat dit niet zal resulteren in het compromitteren van de bescherming van de gegevens van het datasubject”
Beleidsbouwsteen 6.4 “De wet/het wettelijk mandaat voorziet erin dat, , nadat het datasubject in kennis is gesteld van de mogelijke risico's en ongeacht restricties op het format, overdracht van persoonsgegevens plaats kan hebben met de uitdrukkelijke toestemming van het datasubject om de gegevens naar dat rechtsgebied over te dragen.

31. De artikelen 20 en 21 van dit hoofdstuk voorzien erin dat de Commissaris Gegevensbescherming gebruik maakt van een gezamenlijke aanpak voor de regelgeving waar dit geschikt geacht wordt, om een goede balans te kunnen vinden tussen de uit haar functie voortvloeiende noodzaak tot regelgeving en het minimaliseren van de gevolgen en kosten voor de industrie.

Artikel 20: Vaststellen van de Gedragscodes

32. Artikel 20 voorziet in de ontwikkeling van sectorspecifieke gedragscodes. Deze gedragscodes, ongeacht of ze vrijwillig of verplicht zijn, worden geacht de sleutel te zijn om de private sector te stimuleren zich aan de algemene beginselen van privacy te houden die beschreven zijn in hoofdstuk 1. Bovendien voorziet lid (2) erin dat de Commissaris Gegevensbescherming de sector of de regelgevende lichamen voor de industrie, indien deze zijn ingesteld, kan verzoeken om de ontwikkeling van deze gedragscodes ter hand te nemen.

Artikel 21: Verplichte gedragscodes

33. Dit hoofdstuk voorziet erin dat de minister, wanneer gedragscodes als verplicht gezien worden, deze gedragscodes als regelgeving kan invoeren, onder voorbehoud van goedkeuring door het parlement.

HOOFDSTUK III – RECHTEN VAN HET DATASUBJECT

34. **Hoofdstuk 3 van de modelwet** behandelt de rechten van het datasubject met betrekking tot de toegang tot persoonsgegevens die bij een houder van persoonsgegevens berusten. Het **OECD Individual Participation Principle** (OESO beginsel van individuele participatie) geeft een persoon het recht om van een houder van persoonsgegevens bevestiging te krijgen of de houder van persoonsgegevens gegevens onder zich heeft die op hem betrekking hebben; toegang tot die gegevens en de mogelijkheid om de gegevens die op hem betrekking hebben aan te vechten, en indien dat terecht is deze te laten verwijderen, corrigeren, aanvullen of aanpassen.

Artikel 22: Recht op toegang tot eigen persoonsgegevens

35. Wetgeving en jurisprudentie geven een persoon volledig toegang tot zijn eigen persoonsgegevens met erg weinig beperkingen daarop, en het is correct dat privacywetgeving dit recht in stand houdt, waarin de bepalingen van artikel 22 in zijn algemeenheid voorzien.[24]. Er zijn echter specifieke details die nadere overweging vragen. Het recht van toegang tot persoonsgegevens is niet absoluut, aangezien er een beperkt aantal uitzonderingen op dit recht kunnen zijn.

Artikel 23: De houder van persoonsgegevens kan toegang weigeren

36. Artikel 23 voorziet in een raamwerk waarbinnnen de houder van persoonsgegevens een persoon is die een aanvraag doet toegang kan weigeren, maar stelt zeker dat indien op deze wijze de toegang is geweigerd tot een deel van of een geheel document, de rechtvaardiging van de weigering bij de houder van persoonsgegevens ligt. Deze uitzonderingen houden bijvoorbeeld gevallen in waar een verzoek om toegang geweigerd wordt om de persoon zelf of een andere

[24] Beleidsbouwsteen 6.5 " De wet/het wettelijk mandaat zal voorzien in de openbaarmaking van persoonsgegevens in antwoord op een verzoek daartoe van het datasubject. In het geval dat die openbaarmaking kan leiden tot openbaarmaking van andere niet-openbare gegevens, dan zal de wet/ het wettelijk mandaat een geschikt richtsnoer voorschrijven aan het hoofd van de verwerkende partij.

persoon te beschermen[25], of anderszins, ten gevolge van vaste overwegingen van gegevensbescherming, zoals indien de gegevens vallen binnen een wettelijk privilege (bv. advocaat-cliënt privilege), of indien gegevens verzameld zijn als onderdeel van een politieonderzoek of hoofdzakelijk voor gebruik in een juridische procedure.

37. Daarnaast is er ook een redelijke verwachting dat, alhoewel de grote meerderheid van personen hun gegevens op een verantwoorde manier zal opvragen, bij tijd en wijle er personen zullen zijn die hun gegevens zonder andere reden opvragen dan het belemmeren van de werkzaamheden van de houder van persoonsgegevens. Een datasubject kan bijvoorbeeld wekelijkse verzoeken doen om informatie, zelfs indien die informatie al verstrekt is en zich geen veranderingen hebben voorgedaan. In deze gevallen kan het dienstig zijn om de houder van persoonsgegevens toe te staan het verzoek te weigeren. Zoals het meestal gebruikelijk is bij het weigeren van een recht, ligt de last van rechtvaardiging van de weigering bij de houder van persoonsgegevens. Artikel 23 lid 2 voorziet in deze mogelijkheid en geeft de houder van persoonsgegevens de basis voor een dergelijke weigering.

Artikel 24: Afscheiding van vrijgestelde informatie

38. Artikel 24 geeft de houder van persoonsgegevens een richtsnoer voor het nemen van de juiste stappen indien het antwoord op een verzoek om toegang kan resulteren in het openbaar maken van de persoonsgegevens van iemand anders. Voorgesteld wordt dat, waar mogelijk, de gegevens die zulke ongewenste geassocieerde openbaarmaking zouden veroorzaken, geredigeerd worden voordat de gevraagde gegevens worden vrijgegeven.

39. Lid 2 verheldert dat de verplichting van de houder van persoonsgegevens om persoonsgegevens van anderen te beschermen zich er zelfs toe uitstrekt dat de erkenning dat bepaalde informatie bestaat, wordt beperkt.

Artikel 25: Datasubject mag rechten delegeren aan een derde

40. Artikel 25 voorziet erin dat specifieke rechten van een datasubject aan een ander persoon gedelegeerd kunnen worden. Het belangrijkste recht dat in de context van deze wet gedelegeerd kan worden is het recht van toestemming voor het verzamelen, verwerken of openbaar maken van persoonsgegevens. Dit artikel voorziet erin dat toestemming gegeven mag worden door de persoon zelf of door zijn vervangende besluitnemer. In situaties waar van een vervangende besluitnemer gevraagd wordt om te handelen voor iemand anders, bijvoorbeeld wanneer het datasubject minderjarig is of indien wegens gezondheidsomstandigheden het datasubject niet in staat is om toe te stemmen (b.v. indien de persoon zich buiten de staat bevindt) of indien de persoon is overleden, voorziet de wetgeving in een hiërarchie van personen, in overeenstemming met wetgeving met betrekking tot ouderlijke verantwoordelijkheid, wie gevraagd zal worden om beslissingen omtrent gegevens te nemen ten behoeve van de persoon.

Artikel 26: Tijdslimiet voor beantwoorden van verzoeken

41. Artikel 26 stelt een ruim prestatiedoel vast waaraan houders van persoonsgegevens moeten voldoen ten aanzien van het beantwoorden van verzoeken van datasubjecten. Zo'n prestatiebenchmark zal houders van persoonsgegevens onder andere aansporen om een procedure vast te stellen en voorhanden te hebben om de ontvangst en de beantwoording van dergelijke verzoeken te managen. Zo een procedure kan het vaststellen van standaardprocedures voor datasubjecten inhouden, die zij moeten volgen bij het aanvragen van een kopie van hun persoonlijke gegevens. Hieronder kunnen vallen een formulier, een tijdspanne waarin de gegevens geleverd zullen worden en een bijdrage (indien van toepassing).

[25] Beleidsbouwsteen 6.5 “sic.”

Artikel 27: Correctie van fouten in opgeslagen persoonsgegevens

42. Volgens het OESO-beginsel is een ander recht dat onder privacywetgeving toekomt aan datasubjecten het recht om te verzoeken om een correctie van gegevens. Dit wordt geregeld in artikel 27. Dit kan het geval zijn wanneer een datasubject een feitelijke fout (b.v. een verkeerde geboortedatum) wil laten corrigeren. Hoewel in zulke gevallen professioneel of andere institutionele standaards niet altijd zullen toestaan dat een bescheiden veranderd wordt, geeft het raamwerk de houder van persoonsgegevens de mogelijkheid een aantekening te maken in de bescheiden zeggend dat de persoonsgegevens geverifieerd zijn en de juiste gegevens aan te geven. De houder van persoonsgegevens kan op de bescheiden ook een verklaring plaatsen waarin wordt aangegeven waarmee de persoon het oneens is.

HOOFDSTUK IV – SPECIALE OPERATIONELE VERPLICHTINGEN VAN DE OVERHEID

43. **Hoofdstuk 4 van de modelwet** beschrijft speciale regels waaraan de hoofden binnen publieke lichamen zich moeten houden bij het implementeren van de beginselen van privacy uiteengezet in hoofdstuk 1, in samenhang met de algemene richtlijnen beschreven in hoofdstuk 2. Deze speciale verplichtingen zijn erop gericht om te waarborgen dat in de wet toepasselijke controlesystemen worden opgenomen om het monitoren van de implementatie van de beginselen van privacy mogelijk te maken.

Artikel 28: Privacy effectbeoordeling

44. Belangrijke voorbeelden van zulke systemen zijn onder andere, in artikel 28 van dit hoofdstuk, de verplichting van publieke lichamen om beoordelingen te maken van de gevolgen voor de privacy van bestaande of voorgenomen gegevensverwerking in overeenstemming met de richtlijnen van de Commissaris Gegevensbescherming. Deze beoordelingen kunnen de basis vormen van een gezamenlijke aanpak van de regelgeving door de overheid en de Commissaris Gegevensbescherming die leidt tot een *ex ante* benadering van toestemming voor verwerkingsfuncties. Hoewel dit kan leiden tot enige administratieve vertraging bij het opzetten van een nieuw verwerkingssysteem, zal het een algemeen voordeel zijn voor de flexibiliteit en het reactievermogen van de overheid vergeleken met een *ex post*, of een *ad hoc* benadering van toestemming voor verwerkingsfuncties.

Artikel 29: Opslagsysteem voor persoonsgegevens

45. Artikel 29 voorziet in een functionele eis aan publieke lichamen die, wederom, opgezet is om de Commissaris Gegevensbescherming te ondersteunen bij het zorgen voor naleving van de verplichtingen uit de wet. Het wettelijk vereiste om specifieke informatieopslagsystemen op te zetten waarin alle persoonsgegevens die onder het beheer van de overheid vallen hoofdzakelijk worden opgeslagen en gemanaged, faciliteert de effectiviteit van andere dergelijke mechanismen die eventueel geïmplementeerd worden. Ondanks deze algemene eis moet onderkend worden dat de nationale archieven persoonsgegevens mogen beheren die van archivalische aard zijn.

Artikel 30: Nationaal Archief Uitgezonderd van artikel 29

46. Artikel 30 voorziet in de specifieke uitzondering van de werking van artikel 29 voor het nationaal archief, aangezien deze gegevens, geautoriseerd voor openbaar gebruik via het nationaal archief, in het algemeen niet onder de dekkingssfeer vallen die voorzien is bij het opzetten van informatieopslagsystemen voor persoonsgegevens.

Artikel 31: Aanstellen van vertegenwoordigers binnen de houder van persoonsgegevens

47. In overeenstemming met de algemene benadering van het instellen van speciale functionele eisen voor publieke lichamen om het toezicht op privacybescherming te effectueren, voorziet artikel 31 erin dat de overheid binnen haar organisaties vertegenwoordigers aanstelt om de interne evaluatie van systemen en functioneren in overeenstemming met de gegevensbeschermingswet mogelijk te maken. Zo kan verwacht worden dat operationele voordelen toenemen doordat publieke lichamen proactief hun systemen en procedures zullen structureren om naleving van de privacybeginselen en de privacybeschermingsbepalingen in de wet te waarborgen, alsook door betere communicatiekanalen met het kantoor van de Commissaris Gegevensbescherming. Hoewel deze bepaling juist is voor de werkzaamheden van een openbare instelling, kan zo'n bepaling minder van toepassing zijn voor sommige particuliere bedrijven, vandaar dat deze bepaling ingevoerd wordt als een speciale verplichting voor de publieke sector.

Artikel 32: Voorafgaande toestemming nodig voor overeenkomsten betreffende informatieuitwisseling

48. Artikel 32 maakt daarna het uitwisselen van gegevens mogelijk tussen ministeries in overeenstemming met de richtlijnen die zijn vastgesteld door, en/of waarvoor goedkeuring is verkregen van, de Commissaris Gegevensbescherming. Deze zijn bepalend voor de implementatie van e-dienstverlening door de overheid.

Artikel 33: Commisssaris Gegevensbescherming publiceert een verslag over gegevensopslagsystemen

49. Artikel 33 verplicht de Commissaris om verslagen te publiceren over de status van de verschillende mechanismen en instrumenten vallend onder dit hoofdstuk, die ingesteld zijn om toezicht te houden op het beheer van persoonsgegevens die door publieke lichamen verkregen zijn. Dit zal de tijdige verspreiding aan het publiek mogelijk maken van informatie die een gegeven overheidsinstelling onder zich heeft waardoor individuen dankzij de zichtbaarheid de bepalingen van hoofdstuk 3 kunnen gebruiken om hun recht op toegang tot informatie over hun, uit te oefenen.

HOOFDSTUK V – SPECIALE VRIJSTELLINGEN

50. **Hoofdstuk 5 van de modelwet** voorziet in algemene bepalingen die de Minister in staat stellen om per ministeriële beschikking wijzigingen aan te brengen in de toepasselijkheid van de bepalingen van hoofdstuk 2 op bepaalde groepen houders van persoonsgegevens wegens specifieke doelen en onder specifieke omstandigheden. Deze clausules zijn in belangrijke mate gevormd naar de in Groot-Brittanië en op Malta van toepassing zijnde bepalingen die gebaseerd zijn op de betreffende richtlijnen van de Europese Commissie.

Artikel 34: Persoonlijk gebruik of voor familie

51. Artikel 34 maakt duidelijk dat een individu persoonsgegevens mag gebruiken voor persoonlijke of familiezaken.

Artikel 35: Nationale veiligheid, misdaadbestrijding of belastingheffing

52. Artikel 35 voorziet in specifieke uitzonderingen op de hoofdstukken 2, 3 en 4 van de wet, in overeenstemming met internationale beste praktijk. De uitzonderingen zijn duidelijk omschreven met voorbeelden met betrekking tot het verwerken van persoonsgegevens en het vrije verkeer van zulke gegevens wanneer deze beperking noodzakelijk is om de volgende gebieden veilig te stellen:

    (a) nationale veiligheid, defensie; of openbare veiligheid;

    (b) het voorkomen, onderzoeken, opsporen en vervolgen van misdrijven of van schendingen van de ethiek bij gereguleerde beroepen;

    (c) een belangrijk economisch of financieel belang van een rechtsgebied, met inbegrip van monetaire en budgettaire zaken en belastingen.

Artikel 36: Vrijstelling voor regulerende activiteiten

53. Artikel 36 voorziet in vrijstellingen in de toezichthoudende, inspecterende of regulerende functie in verband met, zelfs incidenteel, de uitoefening van het officieel gezag, de bescherming van het datasubject of de rechten en vrijheden van anderen.

Artikel 37: Uitzondering in verband met journalistiek en de kunsten.

54. Artikel 37 voorziet in vrijstelling van de toepasselijkheid wat betreft inspanningen in verband met de bestaande vrijheden van meningsuiting, daaronder begrepen het maken van journalistieke, literaire en kunstwerken. Deze clausule is gebaseerd op gelijksoortige clausules opgenomen in gegevensbeschermingleidraden in Europa. Adequate bescherming tegen smaad is in het algemeen al van toepassing en biedt enige bescherming aan het datasubject zonder onnodige beperking van activiteiten. Verder geeft dit artikel de Commissaris de mogelijkheid om sectorale gedragscodes in het leven te roepen die de juiste balans mogelijk kunnen maken tussen de doelen van de wet en het overheersende recht van vrijheid van meningsuiting.

HOOFDSTUK VI – HERZIENING EN BEROEP VAN BESLISSINGEN VAN HOUDERS VAN PERSOONSGEGEVENS BETREFFENDE TOEGANG

55. **Hoofdstuk 6 van de modelwet** voorziet erin dat een datasubject bij de Commissaris Gegevensbescherming in beroep kan gaan en/of herziening kan vragen van een besluit van een houder van persoonsgegevens[26]. Dit artikel is cruciaal aangezien het een individu de mogelijkheid geeft om eerlijke behandeling van een houder van persoonsgegevens af te dwingen door beroep in te stellen bij een onafhankelijke autoriteit.

Artikel 38: Recht van een datasubject om in beroep te gaan tegen een beslissing

56. Artikel 38 voorziet in het algemene recht van beroep voor een persoon die ontevreden is over de uitkomst van een verzoek gedaan ingevolge artikel 23 (recht van toegang tot de eigen persoonsgegevens) en artikel 28 (recht om verbetering van de eigen persoonsgegevens te vragen). Dit artikel voorziet in een beroep tegen het betreffende besluit bij de Commissaris Gegevensbescherming, die de bevoegdheid heeft om het geschil te beslechten.

[26] Beleidsbouwsteen 5.8 “De wet/het wettelijk mandaat voorziet in een beroepsmogelijkheid betreffende de besluiten van het hoofd van de verwerkende partij bij de aangewezen instantie”

Artikel 39: De tijd waarbinnen het datasubject een beroep kan instellen

57. De artikelen 39 tot en met 41 voorzien in de algemene procedure waarmee een beroep door de Commissaris Gegevensbescherming aanvaard moet worden. Artikel 39 beschrijft de maximale periode vanaf het moment van de betreffende beslissing waarbinnen het beroep moet worden ingesteld, om een snelle start van de procedure te waarborgen.

Artikel 40: De Commissaris Gegevensbescherming mag het beroep afwijzen

58. Artikel 40 geeft de Commissaris Gegevensbescherming de mogelijkheid om een beroep te verwerpen vóór het in kennisstellen van het hoofd van de houder van persoonsgegevens indien, naar zijn mening, de basis voor het beroep onvoldoende is.

Artikel 41: De Commissaris Gegevensbescherming informeert de houder van persoonsgegevens

59. In overeenstemming met de standaardprocedure verplicht artikel 41 de Commissaris Gegevensbescherming om het hoofd van de houder van persoonsgegevens in kennis te stellen van een ingesteld beroep met betrekking tot een beslissing van de houder van persoonsgegevens.

60. De artikelen 42 tot en met 46 voorzien in het algemene mechanisme waardoor de Commissaris Gegevensbescherming alternatieve geschillenbeslechtingstechnieken kan gebruiken bij het behandelen van het beroep.

Artikel 42: De Commissaris benoemt een mediator of treedt op als arbiter

61. Onder artikel 42 mag de Commissaris een mediator benoemen om geschillen te beslechten met als uiterste de Commissaris zelf in de functie van arbiter.

Artikel 43: De Commissaris stelt een onderzoek in

62. Artikel 43 voorziet er met name in dat de Commissaris Gegevensverwerking een onderzoek instelt in antwoord op een beroep, waarbij het besluit dat valt naar aanleiding van dat onderzoek bindend is voor de partijen.

63. De artikelen 44 tot en met 46 voorzien in de procedurele en operationele voorwaarden waaronder een onderzoek uitgevoerd zal worden.

Artikel 44: De Commissaris kan onderzoeken binnenskamers uitvoeren

64. Artikel 44 voorziet erin dat de Commissaris Gegevensbescherming wegens discretie dergelijke onderzoeken achter gesloten deuren kan uitvoeren.

Artikel 45: Vertegenwoordiging van partijen bij een onderzoek

65. Artikel 45 voorziet erin dat elke partij bij het onderzoek vertegenwoordigd is door een advocaat of een andere vertegenwoordiger.

Artikel 46: Bewijslast bij een onderzoek

66. Artikel 46 beschrijft de juridische principes waaronder het onderzoek gevoerd wordt, waarbij de bewijslast wordt gelegd bij de partij die geacht wordt de beschikking te hebben over de meeste hulpmiddelen, de houder van persoonsgegevens.

Artikel 47: Toegang tot de rechter om in beroep te gaan tegen de uitkomst van een onderzoek

67. Artikel 47 voorziet erin dat de rechter een beroepsinstantie is voor elke beslissing die tijdens het onderzoek is genomen.

HOOFDSTUK VII – INSTELLING, TAKEN EN BEVOEGDHEDEN VAN HET TOEZICHTHOUDENDE LICHAAM, DE COMMISSARIS GEGEVENSBESCHERMING

68. **Hoofdstuk 7 van de modelwet** stelt het bureau van de Commissaris Gegevensbescherming in. Dit is een kritiek onderdeel van een effectief privacy wetgevingskader. De vereiste voor onafhankelijk toezicht is essentieel om op de naleving toe te zien door de houders van persoonsgegevens, zowel in de publieke als private sector. Het moet worden opgemerkt dat hoewel dit hoofdstuk is opgesteld alsof het hoofd van dit lichaam een individu was (dus de "Commissaris Gegevensbescherming", het even valide zou zijn als dit lichaam wordt bestuurd door een groep van personen (dus een "Commissie Gegevensbescherming", "College Gegevensbescherming" of iets dergelijks). De rechtsgebieden behouden de uiteindelijke beslissing over de vorm van bestuur dat wordt verkozen voor dit toezichthoudend lichaam. Wat belangrijk is, is dat het lichaam onafhankelijk is, van de politieke uitvoerende mach en dat er voldoende autonomie is van bepaalde private sector belangen die zouden vallen onder de rubriek van deze wet door de aard van de activiteiten die zij ondernemen.

Artikel 48: Instelling van het bureau van de Commissaris Gegevensbescherming

69. Gezien de reikwijdte van deze functie, om te waarborgen dat toezicht op privacy vrij blijft van de indruk van een vooringenomenheid naar enige groep van houders van persoonsgegevens, voorziet artikel 48 in de benoeming en het ontslag van een onafhankelijke Commissaris Gegevensbescherming op dezelfde wijze als en met gelijksoortige benoemingscriteria als een lid van een Parlementaire Commissie of de Ombudsman[27], waar de Commissaris slechts ontslagen kan worden met geldige reden.

70. In het geval dat een Commissaris Gegevensbescherming niet aanwezig is, voorziet het artikel tevens in de tijdelijke benoeming van een Commissaris totdat een nieuwe ambtsdrager is geïdentificeerd..

71. Als alternatief, kan de wetgeving een bepaling omvatten voor de benoeming van een Assistent Commissaris Gegevensbescherming, die zal handelen namens de Commissaris indien dat nodig mocht blijken. Verder, zal het artikel waarborgen dat de Commissaris geen andere inkomen heeft of andere uitdrukkelijke verplichting of band die de indruk van vooringenomenheid zou kunnen veroorzaken.[28]. Dit aspect van de bepaling kan worden gewijzigd in overeenstemming met het bestuursmodel dat wordt voorgesteld en de logistieke overwegingen in ieder rechtsgebied. Het wordt voornamelijk voorgesteld in deze model tekst aangezien de traditioneel regelgevende functie van de uitvoerende macht naar de markt toe, in dit geval, ook moet worden toegepast op de publieke sector. Echter, als een groep van houders van persoonsgegevens publieke en quasi-publieke sector ondernemingen kunnen zijn waarover de

[27] Beleidsbouwsteen 3.3 "Het hoofd van de aangewezen instantie zal worden benoemd op een wijze die de onafhankelijkheid en onpartijdigheid van de functies waarborgt.

[28] Beleidsbouwsteen 3.4 "Het hoofd van de aangewezen instantie zal dergelijke functievoorwaarden en bepalingen worden aangemeten, waaronder bepalingen betreffende verankering en voorwaarden voor herbenoeming, opgenomen in de wet/ het wettelijk mandaat die voldoende zijn om mogelijkheden tot overreding en dwang te beperken."

politieke uitvoerende macht enige administratief toezicht houdt, dan voorziet het algemeen bestuurskader in:

a) In het rapporteren aan de relevante Minister over de status van bescherming van privacy door de private sector;

b) In het rapporteren aan het Parlement over de status van bescherming van privacy door de overheid.

72. Dit artikel voorziet ook in, onder lid (3), het huren van personeel door de Commissaris Gegevensbescherming in uitvoering van de taken van het ambt. Tenslotte, definieert dit artikel een tijdslimiet waarbinnen de Commissaris Gegevensbescherming dient te zijn ingesteld na de afkondiging van de wet.[29]

Artikel 49: Afzonderlijke rechtspersoonlijkheid van de Commissaris Gegevensbescherming

73. In ieder geval, voorziet artikel 49 erin dat de Commissaris een aparte rechtspersoon zal zijn, zodat de Commissaris bevoegd zal zijn om contracten aan te gaan, om het even welk eigendom aan te schaffen, bezitten en verkopen voor de doeleinden van zijn functie, om gedingen aan te spannen en voor het gerecht gedaagd te worden, en om al die zaken te doen en dergelijke transacties aan te gaan die bijkomstig of bevorderlijk zijn bij de uitoefening of uitvoering van zijn taken onder deze wet.[30].

Artikel 50: Bepaling van de ambtstermijn van de ambtsdrager

74. Verder, zal als mechanisme ter behoud van de integriteit van de functie en om te voorzien in integriteit en eerlijkheid, artikel 50 een maximum ambtstermijn voorzien voor de Commissaris. Deze termijn is langer dan de verkiezingscyclus, rekening houdend met de beste praktijk.[31].

Artikel 51: Beloning van Commissaris Gegevensbescherming en personeel

75. Teneinde de onafhankelijkheid en de onpartijdigheid van de Commissaris te waarborgen voorziet artikel 51 er verder in dat de beloning van de Commissaris en zijn personeel op onafhankelijke wijze bepaald zal worden zodat de functionaris niet de schijn zal hebben dat hij aan enig bestuur gebonden is. De hier gebruikte formulering is gekozen om te zorgen voor de benodigde flexibiliteit voor rechtsgebieden om te bepalen wat het juiste mechanisme is waarmee deze onafhankelijkheid bereikt kan worden. Sommige rechtsgebieden zullen bijvoorbeeld de salarissen van dergelijke onafhankelijke instituties vast laten stellen door een onafhankelijke commissie, anderen door middel van regelgeving. De voorgestelde clausule wil niet een van de mechanismen als de juiste voorschrijven, maar wil alleen benadrukken dat nadat deze is vastgesteld de fiscale besteding op transparante wijze beschreven moet worden in de jaarlijkse begrotingscyclus van de regering onder een aparte uitgavencategorie.

Artikel 52: Bescherming van de Commissaris Gegevensbescherming

76. Verder voorziet artikel 52 erin, teneinde de onafhankelijkheid en de onpartijdigheid van de Commissaris te waarborgen, dat de Commissaris Gegevensbescherming wordt gevrijwaard van aansprakelijkheid met betrekking tot een handeling die te goeder trouw is uitgevoerd of

[29] Beleidsbouwsteen 3.12 “De wet /het wettelijk mandaat zal een tijdskader aangeven waarbinnen de aangewezen instantie in werking zal treden na de aanname van de wet.”

[30] Beleidsbouwsteen 3.2 “De instantie die is aangewezen voor het waarborgen van de naleving van de wet/ het wettelijk mandaat zal een aparte rechtspersoon zijn die de bevoegdheid heeft activa te bezitten en daar afstand van te doen, het vermogen heeft contracten aan te gaan, en die onafhankelijk zal zijn bij de uitvoering van zijn taken.

[31] Beleidsbouwsteen 3.4 “sic.”

nagelaten in de uitoefening of vermeende uitoefening van zijn of haar taken. Deze vrijwaring hoort zich niet uit te strekken tot gevallen van persoonlijk letsel. Bovendien wordt er in het wetgevingskader een bepaling opgenomen om de Commissaris Gegevensbescherming schadeloos te stellen voor kosten van verdediging.[32].

Artikel 53: Delegatie van bevoegdheden van de Commissaris Gegevenbescherming

77. Om praktische operationele en organisatorische redenen geeft artikel 53 de Commissaris Gegevensbescherming de bevoegdheid om om het even welke onderzoeks- of handhavingsbevoegdheid die aan hem of haar is toegekend ingevolge deze wet te delegeren aan elke bevoegde functionaris die voor dat doel is aangewezen door de Commissaris.[33].

Artikel 54: Onafhankelijkheid van de Commissaris Gegevensbescherming

78. Artikel 54 benadrukt dat van de Commissaris vereist wordt dat hij/zij onafhankelijk handelt bij de uitoefening van zijn of haar taken voortvloeiend uit de wet en niet onderhevig is aan de aanwijzingen of controle van enige andere persoon of autoriteit.[34].

Artikel 55: Taken van de Commissaris Gegevensbescherming

79. Zoals beschreven in artikel 55 zijn de voornaamste taken van het toezichthoudend orgaan, een administratief kantoor onder leiding van zijn hoofd, de Commissaris Gegevensbescherming, om de naleving van de privacy wetgeving te waarborgen door -

- toezicht te houden op de wijze waarop de wetgeving wordt toegepast en evaluaties uit te voeren;
- onderzoeken te starten naar de naleving van de privacybescherming;
- oplossen van en bemiddelen bij klachten over privacyschending;
- te zorgen voor evaluatie- en overzichtsassesments van de invloed op de privacy;
- onderzoek te laten uitvoeren naar privacywetgeving;
- het ontwikkelen van publiekseducatieprogramma's;
- stimuleren van het toepassen van de best practice met betrekking tot privacy; en
- houders van persoonsgegevens te voorzien van advies en commentaar.

32 Beleidsbouwsteen 3.10 “In de wet/het wettelijk mandaat, kan de aangewezen instantie beschermd worden tegen aansprakelijkheid voor enige handeling die te goeder trouw is uitgevoerd bij de uitoefening van zijn taken.”

33 Beleidsbouwsteen 3.6 “Het hoofd van de aangewezen instantie zal in de wet/ het wettelijk mandaat de bevoegdheid worden toegekend bepaalde bevoegdheden te delegeren aan erkende vertegenwoordigers om de uitvoering van zijn taken te vergemakkelijken.

34 Beleidsbouwsteen 1.6 “De wet/het wettelijk mandaat voorziet duidelijk in de onafhankelijkheid van de aangewezen instantie.”

Artikel 56: Vertrouwenseed

80. Artikel 56 verlangt van personen die uit hoofde van het uitvoeren van taken voortvloeiend uit deze wet toegang hebben tot informatie die beschouwd kan worden als privé of persoonlijk, dat zij een eed afleggen waarbij zij verklaren geen gegevens bekend te maken die verkregen zijn door het uitoefenen van een bevoegdheid of uit hoofde van het uitvoeren van een verplichting uit hoofde van deze wet tenzij in overeenstemming met deze specifieke bepalingen van de privacybeschermingswet, enige andere regelgeving of volgens rechterlijke uitspraak.

Artikel 57: Algemene bevoegdheden van de Commissaris Gegevensbescherming

81. Artikel 57 beschouwt de Commissaris als een entiteit vergelijkbaar met een ordenend lichaam wat betreft het vervullen van zijn of haar taken, met inbegrip van de noodzakelijke bevoegdheden om alle handelingen uit te voeren die volgens hem of haar vereist, voordelig of passend lijken voor of in verband met de uitoefening van deze taken, waaronder de bevoegdheid om de bedrijfsvoering van een houder van persoonsgegevens te onderzoeken[35], op eigen initiatief of in antwoord op een klacht, om informatie te verkrijgen over documentatie, verwerking en beveiliging van gegevens, en, onder andere, te verzoeken dat een persoon hem of haar binnen de gestelde tijd schriftelijk toegang verschaft tot persoonsgegevens, of andere gespecificeerde informatie die betrekking heeft op de informatiemanagement werkwijzen van de beheerder[36].
82. Artikel 58 tot en met 61 stellen een procedure vast volgens welke de Commissaris Gegevensbescherming in het kader van een onderzoek informatie mag opvragen, het Verzoek om informatie, en bekrachtigen de verplichting door het niet voldoen aan of niet beantwoorden van een verzoek tot informatie van de Commissaris, te bestempelen als een overtreding[37].

Artikel 58: De bevoegdheid van de Commissaris Gegevensbescherming om informatie te verkrijgen van de houder van persoonsgegevens

83. Artikel 58 introduceert de procedure van voorafgaande ondervraging of gegevensverzameling – het Verzoek om informatie. Het artikel beschrijft ook wanneer het Verzoek om informatie gebruikt behoord te worden, en in welke vorm zo een verzoek gericht kan worden aan de betreffende partij. In overeenstemming met de algemene overwegingen ten aanzien van het gebruik van technische hulpmiddelen om tijdige verzending te vergemakkelijken, geeft lid 2 overwegingen voor de wijze waarop de gevraagde informatie ingediend kan worden.
84. Leden (3) en (4) herhalen uitzonderingsgevallen die eerder in de modeltekst aan de orde zijn gekomen. Deze zijn toegevoegd om twijfels over de behandeling van zulke gevallen weg te nemen.

35 Beleidsbouwsteen 3.5 “Het hoofd van de aangewezen instantie zal in de wet/ het wettelijk mandaat de nodige onderzoeksbevoegdheden worden toegekend om de uitvoering van de functies van het gegevensbeschermingskader te vergemakkelijken

36 Beleidsbouwsteen 3.7 “De aangewezen instantie kan, zowel op eigen initiatief als in antwoord op klachten van het publiek, controles of onderzoeken instellen naar personen op wie het kader van toepassing is. In de regelgeving zal bepaald worden wie de kosten van dergelijke onderzoeken zal dragen.”

37 Beleidsbouwsteen 3.8 “Personen op wie de wet van toepassing is, zullen meewerken met de aangewezen instantie in de uitvoering van haar taken, op straffe van een civiele en/of strafrechtelijke sanctie.”

Artikel 59: Inhoud en vorm van de kennisgeving

85. Artikel 59 beschrijft de noodzakelijke bestanddelen van de kennisgeving dat in essentie de aangesproken partij op de hoogte stelt van haar recht om een procedure te starten om zichzelf te beschermen in overeenstemming met het raamwerk van de modeltekst.

Artikel 60: Vaststellen van de overtreding van het niet voldoen aan een kennisgeving

86. Artikel 60 beschrijft dat het niet beantwoorden van een kennisgeving geacht wordt een materiële schending van de wet te zijn en dat de schuldige partij gestraft en beboet kan worden volgens de bepalingen van de Wet. Verder wordt in lid (3) het geldige afweermiddel tegen een dergelijke overtreding beschreven.

Artikel 61: Middelen die de Commissaris Gegevensbescherming ter beschikking heeft bij gebrekkige beantwoording van een kennisgeving

87. Artikel 61 behandelt hoe de Commissaris Gegevensbescherming moet handelen in het geval dat geoordeeld wordt dat een reactie op een kennisgeving onvoldoende is, waaronder het geven van de opdracht tot het afbreken van de handelingen betreffende het verzamelen, verwerken of openbaar maken van persoonsgegevens.

88. De artikelen 62 tot en met 66 stellen de toepasselijke procedure vast waarmee de Commissaris Gegevensbescherming een controle of een onderzoek kan laten uitvoeren, waaronder de ontvangst van een klacht van een persoon, de daaropvolgende kennisgeving aan de houder van persoonsgegevens over het komende onderzoek, en de bepaling over de bevoegheden van binnenkomst, doorzoeking en inbeslagname (onder voorwaarde van een uitgevaardigd huiszoekingsbevel en onder begeleiding van de politie).[38]

Artikel 62: Het antwoord van de Commissaris op de ontvangst van een klacht

89. Artikel 62 gaat over de verplichting van de Commissaris Gegevensbescherming om op een bepaalde manier te reageren op de ontvangst van een klacht. Deze verplichte handelingen omvatten het uitvoeren van een onderzoek en binnen een redelijke termijn de klager op de hoogte stellen van de uitkomst daarvan. Lid (3) bekrachtigt eerdere bepalingen over vertegenwoordigers die handelen ten behoeve van een persoon die deze procedure gestart is.

Artikel 63: Vorm en inhoud van een klacht

90. Artikel 63 beschrijft de algemene vorm waaraan een klacht moet voldoen nadat deze is ingediend door een klager, en verplicht de Commissaris om daarbij assistentie te verlenen die redelijkerwijs nodig is om te waarborgen dat de klacht de juiste vorm heeft. De Commissaris Gegevensbescherming mag geen assistentie verlenen betreffende de inhoud van de klacht.

Artikel 64: Start van een onderzoek door Commissaris Gegevensbescherming naar aanleiding van een klacht

91. Artikel 64 legt het proces neer dat de Commissaris Gegevensbescherming dient te volgen om de houder van persoonsgegevens onderworpen aan een klacht te betrekken. Het voorgestelde mechanisme – de onderzoekskennisgeving – moet worden betekend aan het hoofd van de houder van persoonsgegevens voorafgaand aan het begin van het onderzoek.

[38] Beleidsbouwsteen 3.9 “De aangewezen instantie kan verzoeken doen, waaraan personen moeten voldoen, om bepaalde documenten in te dienen ter vergemakkelijking van het onderzoek. De instantie kan de rechter om een bevelschrift vragen indien dit \[vereist] is”

Artikel 65: Algemene bevoegdheid om huiszoekingen te ondernemen en om inbeslagnames te doen in de loop van een onderzoek

92. Artikel 65 geeft de Commissaris Gegevensbescherming een algemene bevoegdheid om panden en erven van een houder van persoonsgegevens te betreden, een huiszoeking te doen, en indien nodig, relevante documenten in beslag te nemen in de loop van het onderzoek. Lid (2) van dit artikel beperkt de toepassing van deze algemene bevoegdheid op dergelijke wijze dat een huiszoekingsbevel eerst verkregen dient te worden, en dat de functionarissen van de Commissaris Gegevensbescherming vergezeld dienen te zijn van een politiefunctionaris.

Artikel 66: Vrijstellingen van inbeslagname

93. Artikel 66 versterkt dat eerdere bepalingen van bepaalde documenten zijn vrijgesteld van verwerking onder deze wet van gelijke toepassing zijn in het geval van een huiszoeking.

94. Zodra het onderzoek is afgerond, kan het geval zich voordoen dat de Commissaris Gegevensbescherming van mening is dat de houder van persoonsgegevens niet werkt in overeenstemming met de privacy beschermingsverplichtingen. In dat geval, leggen artikelen 67 tot 69 het mechanisme en de procedure neer waardoor de Commissaris Gegevensbescherming richtlijnen kan verstrekken aan houders van persoonsgegevens die verondersteld worden hun activiteiten uit te voeren op een wijze die niet overeenstemt met de wet.

Artikel 67: Handhavingsbevel

95. Artikel 67 stelt de Commissaris Gegevensbescherming in staat het voorgestelde mechanisme uit te geven – en geeft de juiste toepassing daarvan aan en, om twijfel te voorkomen, beperkt tevens het doel daarvan, de houder van persoonsgegevens.

Artikel 68: Vorm en inhoud van een handhavingsbevel

96. Artikel 68 geeft de specifieke vorm aan van het handhavingsbevel en past in dit mechanisme de nodige verbindende bevoegdheden toe om de houders van persoonsgegevens die in overtreding zijn te laten handelen om de vastgestelde inbreuk te rectificeren. Dit artikel voorziet ook in het mechanisme, en de vorm van dat mechanisme, waarmee de houder van persoonsgegevens dient te antwoorden op het handhavingsbevel, en omvat de maximum tijdslimiet waarin een dergelijk antwoord wordt verwacht. Op deze manier, zijn de houders van persoonsgegevens hierbij verplicht in te gaan op de instructies van het handhavingsbevel of die na te leven.

Artikel 69: Vaststellen van de overtreding van het niet voldoen aan een handhavingsbevel

97. Artikel 69 geeft aan dat een verzuim om een handhavingsbevel af te handelen zoals aangegeven in artikel 68 wordt beschouwd als een werkelijke overtreding van de wet die de houder van persoonsgegevens blootstelt aan strafrechtelijke sancties.[39]

Artikel 70: Voorwaarden voor het onderzoek

98. Artikel 70 stelt verder de logistieke voorwaarden vast waarbinnen het onderzoek moet worden gedaan. Lid (1) stelt verplicht dat alle onderzoeken moeten worden gevoerd met een eis van geheimhouding.

[39] Beleidsbouwsteen 3.8 “sic.”

99. Lid (2) voorziet erin dat de partijen daarbij ieder verklaringen kunnen afleggen aan de Commissaris Gegevensbescherming in de loop van het onderzoek. Echter, er wordt opgemerkt dat in dit stadium van het onderzoek de bepaling stelt dat de aanwezigheid van de ene of de andere partij tijdens het afleggen van de verklaring wordt uitgesloten.

Artikel 71: Verwijzing van zaken naar de commissaris van politie

100. Artikel 71 voorziet in de correcte handelingen van de Commissaris Gegevensbescherming bij de verwijzing van de bescheiden naar de juiste persoon indien er een schending wordt verondersteld te hebben plaatsgevonden.

Artikel 72: Jaarlijks rapporteren van de Commissaris Gegevensbescherming aan de wetgevende macht

101. Artikel 72 verplicht de Commissaris Gegevensbescherming om over zijn activiteiten te rapporteren in het Parlement, overeenkomstig de Parlementaire beste praktijk.[40]

HOOFDSTUK VIII – HET VASTSTELLEN VAN OVERTREDINGEN EN STRAFSANCTIES VOOR HET SCHENDEN VAN DE BEPALINGEN

102. **Hoofdstuk 8 van de modelwet** legt de strafrechtelijke overtredingen neer die zijn geassocieerd met de schending van bepaalde bepalingen van de wet.

Artikel 73: Overtreding voor het verzamelen van persoonsgegevens zonder passende kennisgeving aan het subject

103. Artikel 73 beschouwt de schending van artikel 8 als een overtreding. In het geval dat rechtsgebieden besluiten een onderscheid te maken tussen gevoelige en niet-gevoelige persoonsgegevens, bestaat er een optie om te voorzien in verschillende strafsancties die worden geassocieerd met deze overtreding waar de schending wordt verondersteld te zijn gebeurd respectievelijk met persoonsgegevens en gevoelige persoonsgegevens. In het geval dat een dergelijke aanpak wordt gevolgd, wordt geadviseerd dat de strafsanctie voor de schending van de laatste soort gegevens zwaarder zal zijn.

104. Hoewel de verplichtingen opgenomen in bepalingen 8 tot en met 15 en 20 allen essentieel zijn voor de effectieve implementatie van gegevensbescherming, kunnen schendingen hiervan adequate rechtsmiddelen zijn zonder de oplegging van strafrechtelijke sancties. Echter, er wordt gesuggereerd dat als gevolg van de implicaties van internationale handelsovereenkomsten, schendingen van artikel 19 strenger dienen te worden aangepakt dan anderen.

Artikel 74: Overtreding om extra-judicieel persoonsgegevens over te dragen tussen rechtsgebieden zonder de passende toestemming

105. Op gelijke wijze, definieert artikel 74 een schending van die specifieke bepaling 19 als een strafrechtelijke overtreding, en voorziet in de definitie van een standaard strafsanctie geassocieerd met een dergelijke overtreding.[41].

[40] Beleidsbouwsteen 3.11 “De aangewezen instantie zal jaarlijks rapporteren aan het parlement/ wetgevende raad betreffende zijn activiteiten in het voorgaande jaar.”

Artikel 75: Overtreding om een vertegenwoordiger van de Commissaris Gegevensbescherming te belemmeren

106. Artikel 75 handelt over de directe en indirecte belemmering van de bevoegde vertegenwoordigers van de Commissaris Gegevensbescherming in de uitoefening van hun taken tijdens een onderzoek en geeft de standaard strafsanctie geassocieerd met deze overtreding.

Artikel 76: Overtreding om valse verklaringen af te leggen aan de Commissaris Gegevensbescherming of zijn vertegenwoordigers.

107. Artikel 76 handelt over de personen die verondersteld worden de rechten te hebben misbruikt die Hoofdstuk 3 van de wet toekent. De overtredingen die worden begaan en de strafsancties uiteengezet dienen om personen te weerhouden deze bepalingen die een bevoegdheid verlenen vexatoir te misbruiken wat anders de operationele levensvatbaarheid van de houder van persoonsgegevens, het bureau van de Commissaris Gegevensbescherming, of beide zou ondermijnen.

Artikel 77: Overtreding de vertrouwenseed te schenden

108. Artikel 77 handelt over personen die de vertrouwenseed schenden die zij hebben afgelegd bij het opnemen van hun functie binnen het bureau van de Commissaris Gegevensbescherming. Dit is erop gericht om dit soort gevallen te beperken en om te waarborgen dat er een publiek vertrouwen is in het bureau.

109. Schendingen van de bepalingen van de wet die niet expliciet zijn aangegeven in dit Hoofdstuk van andere geldende artikelen kunnen worden behandeld in de rechtbank onder het burgerlijk recht.

HOOFDSTUK IX – ALGEMENE BEPALINGEN VOOR HET FACILITEREN VAN DE IMPLEMENTATIE VAN HET KADER

110. **Hoofdstuk 9 van de modelwet** voorziet in verschillende overwegingen die voordelig kunnen zijn voor de tenuitvoerlegging van de belangrijkste aspecten van de wet die zijn neergelegd in de voorgaande artikelen.

Artikel 78: Bescherming van informant

111. Artikel 78 voorziet in bescherming van personen die terwijl zij in dienst zijn van een houder van persoonsgegevens kennis nemen van handelingen door die partij die tegenstrijdig zijn met de doelstellingen van deze wet of de bepalingen daarin, opzettelijk de relevante autoriteit op de

---

[41] Beleidsbouwsteen 5.10 [6.6] “De wet/het wettelijk mandaat schrijft civiele en strafrechtelijke strafsancties voor in het geval van schending van de vastgestelde bepalingen die betrekking hebben op de openbaarmaking van persoonsgegevens. Dergelijke strafsancties kunnen worden opgelegd aan de verwerkende partij, of enige functionaris of directeur waarvan kan worden bewezen dat die de wet/ het wettelijk mandaat heeft geschonden.

hoogte stel van dergelijke actie. De bepaling inzake de "bescherming van de informant" is erop gericht om werknemers gerust te stellen dat zij kunnen handelen in het publiek belang door elke vergeldingsactie door het hoofd van de houder van persoonsgegevens te beperken Het effect van deze bepaling inzake informanten is om de wegen via waar gegevens over ambtsmisdrijven in privacybescherming worden gerapporteerd aan de autoriteiten voor een spoedige rectificatie en/ of handhaving te vergroten.

Artikel 79: Vergoeding te vragen voor de dienstverlening van de Commissaris Gegevensbescherming

112. Artikel 79 voorziet erin dat de Minister, die handelt op advies van de Commissaris Gegevensbescherming, een tarievenlijst neerlegt voor de dienstverlening verstrekt door dat Bureau. Dit is om te faciliteren dat sommige van de kosten geassocieerd met het draaien van he Bureau kunnen worden terugverdiend.

Artikel 80: Minister zal nodige regelgeving neerleggen

113. Artikel 80 voorziet in een algemene bepaling die de relevante Minister in staat regelgeving neer te leggen die nodig is om werking te geven aan of uit te weiden over bepaalde bepalingen in de wet.

Artikel 81: Rol van de rechtbank

114. Artikel 81 verduidelijkt de rol van de rechtbank als de laatste beroepsinstantie waar om het even welke partij die niet tevreden is met de uitkomst van een geschillenbeslechtingsprocedure door de Commissaris Gegevensbescherming terecht kan. Dit artikel versterkt ook de bevoegdheid van de rechter om civiele strafsancties op te leggen voor inbreuken op de wet die niet als overtreding worden beschouwd in Hoofdstuk 8 van de wet.[42, 43, 44]

[42] Beleidsbouwsteen 4.8 "sic."
[43] Beleidsbouwsteen 5.10 "sic."
[44] Beleidsbouwsteen 6.6 "sic."

BIJLAGEN

Bijlage 1

Deelnemers in de Eerste Consultatieve Workshop voor de Werkgroep van het HIPCAR project, van de Werkgroep inzake ICT Wetgevingskader voor Kwesties de Informatiemaatschappij rakende Gros Islet, Saint Lucia, 8-12 Maart 2010

Officieel Benoemde Deelnemers en Waarnemers

Land	Organisatie	Familienaam	Voornaam
Antigua and Barbuda	Ministry of Information, Broadcasting, Telecommunications, Science & Technology	SAMUEL	Clement
Bahamas	Utilities Regulation & Competition Authority	DORSETT	Donavon
Barbados	Ministry of Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Ministry of Trade, Industry and Commerce	COPPIN	Chesterfield
Barbados	Cable & Wireless (Barbados) Ltd.	MEDFORD	Glenda E.
Barbados	Ministry of Trade, Industry and Commerce	NICHOLLS	Anthony
Belize	Public Utilities Commission	SMITH	Kingsley
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Grenada	National Telecommunications Regulatory Commission	ROBERTS	Vincent
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Guyana	Office of the Prime Minister	RAMOTAR	Alexei
Guyana	National Frequency Management Unit	SINGH	Valmikki
Jamaica	University of the West Indies	DUNN	Hopeton S.
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts and Nevis	Ministry of Information and Technology	BOWRIN	Pierre G.
Saint Kitts and Nevis	Ministry of the Attorney General, Justice and Legal Affairs	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FELICIEN	Barrymore
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FLOOD	Michael R.
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	JEAN	Allison A.
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	ALEXANDER	K. Andre
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel

Bijlage 1

Land	Organisatie	Familienaam	Voornaam
Suriname	Telecommunicatie Autoriteit Suriname/Telecommunication Authority Suriname	LETER	Meredith
Suriname	Ministry of Justice and Police, Department of Legislation	SITALDIN	Randhir
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PHILIP	Corinne
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon

Regional/Deelnemers vanuit Regionale en/of Internationale Organisaties

Organisatie	Familienaam	Voornaam
Caribbean Community Secretariat (CARICOM)	JOSEPH	Simone
Caribbean ICT Virtual Community (CIVIC)	GEORGE	Gerry
Caribbean ICT Virtual Community (CIVIC)	WILLIAMS	Deirdre
Caribbean Telecommunications Union (CTU)	WILSON	Selby
Delegation of the European Commission to Barbados and the Eastern Caribbean (EC)	HJALMEFJORD	Bo
Eastern Caribbean Telecommunications Authority (ECTEL)	CHARLES	Embert
Eastern Caribbean Telecommunications Authority (ECTEL)	GILCHRIST	John
Eastern Caribbean Telecommunications Authority (ECTEL)	HECTOR	Cheryl
International Telecommunication Union (ITU)	CROSS	Philip
International Telecommunication Union (ITU)	LUDWIG	Kerstin
Office of Trade Negotiations (formerly CRNM) Caribbean Community Secretariat (CARICOM)	BROWNE	Derek E.
Organization of Eastern Caribbean States Secretariat (OECS)	FRANCIS	Karlene

Experts voor het HIPCAR Project

Familienaam	Voornaam
MARTÍNS DE ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[45]	J Paul
PRESCOD	Kwesi

[45] Workshop voorziter

Bijlage 2

Deelnemers in de Tweede Consultatieve Workshop (fase B) voor de Werkgroep van het HIPCAR project, van de Werkgroep inzake ICT Wetgevingskader voor Kwesties de Informatiemaatschappij rakende Frigate Bay, Saint Kitts and Nevis, 19 – 22 Juli 2010

Officieel Benoemde Deelnemers en Waarnemers

Land	Organisatie	Familienaam	Voornaam
Antigua and Barbuda	Ministry of Information, Broadcasting, Telecommunications, Science & Technology	SAMUEL	Clement
Bahamas	Utilities Regulation and Competition Authority	DORSETT	Donavon
Barbados	Ministry of Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Office of Trade Negotiations	BROWNE	Derek
Barbados	Ministry of Trade, Industry and Commerce	NICHOLLS	Anthony
Belize	Ministry of Finance	LONGSWORTH	Michelle
Belize	Public Utilities Commission	PEYREFITTE	Michael
Dominica	Ministry of Information, Telecommunications and Constituency Empowerment	CADETTE	Sylvester
Dominica	Ministry of Legal Affairs	RICHARDS-XAVIER	Pearl
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Grenada	National Telecommunications Regulatory Commission	ROBERTS	Vincent
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Guyana	Office of the President	RAMOTAR	Alexei
Guyana	National Frequency Management Unit	SINGH	Valmikki
Jamaica	Office of the Prime Minister	MURRAY	Wahkeen
Jamaica	Attorney General's Chambers	SOLTAU-ROBINSON	Stacey-Ann
Jamaica	Digicel Group	GORTON	Andrew
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts and Nevis	Ministry of National Security	ARCHIBALD	Keisha
Saint Kitts and Nevis	Department of Technology	BOWRIN	Pierre
Saint Kitts and Nevis	ICT4EDC Project	BROWNE	Nima
Saint Kitts and Nevis	Government of St. Kitts and Nevis	CHIVERTON	Eurta
Saint Kitts and Nevis	Department of Technology	HERBERT	Christopher
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	LAZAAR	Lloyd
Saint Kitts and Nevis	Ministry of Finance, Financial Intelligence Unit	MASON	Tracey
Saint Kitts and Nevis	Ministry of Sustainable Development	MUSSENDEN	Amicia

Bijlage 2

Land	Organisatie	Familienaam	Voornaam
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	PHILLIP	Glen
Saint Kitts and Nevis	Attorney General's Chambers	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Ministry of Finance, Financial Intelligence Unit	SOMERSALL-BERRY	Jacqueline
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Ministry of Communication, Works, Transport and Public Utilities	DANIEL	Ivor
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FELICIEN	Barrymore
Saint Lucia	Cable & Wireless (St. Lucia) Ltd.	LEEVY	Tara
Saint Lucia	The Attorney General's Chambers	VIDAL-JULES	Gillian
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	ALEXANDER	K. Andre
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel
Suriname	Telecommunicatiebedrijf Suriname (TELESUR)	JEFFREY	Joan
Suriname	Telecommunicatie Autoriteit Suriname	LETER	Meredith
Suriname	Ministry of Justice and Police	SITLADIN	Vyaiendra
Suriname	Ministry of Transport, Communication and Tourism	SMITH	Lygia
Trinidad and Tobago	Office of the Prime Minister, Information Division	MAHARAJ	Rishi
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PHILIP	Corinne
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon

Regional/Deelnemers vanuit Regionale en/of Internationale Organisaties

Organisatie	Familienaam	Voornaam
Caribbean Community Secretariat (CARICOM)	JOSEPH	Simone
Caribbean ICT Virtual Community (CIVIC)	HOPE	Hallam
Caribbean ICT Virtual Community (CIVIC)	ONU	Telojo
Eastern Caribbean Telecommunications Authority (ECTEL)	WRIGHT	Ro Ann
International Telecommunication Union (ITU)	CROSS	Philip
International Telecommunication Union (ITU)	LUDWIG	Kerstin
Organization of Eastern Caribbean States Secretariat (OECS)	FRANCIS	Karlene

Bijlage 2

Experts voor het HIPCAR Project

Familienaam	Voornaam
GERCKE	Marco
MORGAN[46]	J Paul
PRESCOD	Kwesi

[46] Workshop voorziter.

International Telecommunication Union
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Geneva, 2013