Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Eerste Kamer
der Staten-Generaal
Kazernestraat 52
2514 CV DEN HAAG

Directie Europese en Internationale Zaken

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Overheidsidentificatienr
00000001003214369000

T 070 379 8911 (algemeen)
F 070 378 6100 (algemeen)
www.rijksoverheid.nl/ezk

Ons kenmerk
DEIZ / 21305307

Bijlage
1

Datum 14 december 2021
Betreft Verslag formele Telecomraad 3 december 2021

Geachte Voorzitter,

Hierbij bied ik u het verslag aan van de formele Telecomraad van 3 december 2021. Tevens informeer ik u hierbij over een Nederlands non-paper met de voorlopige inzet op de *European Cyber Resilience Act*.

Stef Blok
Minister van Economische Zaken en Klimaat

Verslag formele Telecomraad 3 december

Richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIB2-richtlijn)

Algemene oriëntatie

Tijdens de Telecomraad heeft de Raad ingestemd met een algemene oriëntatie op de NIB2-richtlijn. Het voorzitterschap benadrukte het belang van het voorstel voor de versterking van de cyberbeveiliging in de EU. Het voorzitterschap benoemde nog enkele belangrijke punten die gedurende de onderhandelingen aan bod zijn gekomen en waarover een compromis is bereikt. Het voorzitterschap heeft onder meer een goede balans proberen te vinden ten aanzien van welke sectoren wel of niet onder de reikwijdte van de NIB2-richtlijn zouden vallen. Dit was volgens het voorzitterschap met name een lastige kwestie bij de toepasbaarheid van het voorstel op overheden. In de algemene oriëntatie is uiteindelijk gekozen voor een aanpak waarbij het voorstel van toepassing is op centrale overheden en lidstaten zelf een keuze kunnen maken om de toepasbaarheid uit te breiden naar decentrale overheden. Tevens heeft het voorzitterschap getracht de afstemming tussen de NIB2-richtlijn en sectorspecifieke regelgeving zoals de DORA en CER-richtlijn te faciliteren.[1] Tot slot benoemde het voorzitterschap dat de algemene oriëntatie artikelen bevat die wederzijdse bijstand met betrekking tot rechtsbevoegdheid en territorialiteit verbetert.

De Raad, waaronder Nederland, heeft unaniem de algemene oriëntatie op de NIB2-richtlijn aangenomen. Nederland heeft aangegeven dat in het licht van het zich ontwikkelende dreigingsbeeld waarbij de dreiging van cyberaanvallen toeneemt en de constatering dat de weerbaarheid tegen digitale dreigingen van netwerk- en informatiesystemen nog niet overal op orde is, een uitbreiding van de reikwijdte van de richtlijn naar extra sectoren en aanbieders via de herziening van de NIB2-richtlijn noodzakelijk is. Lidstaten brachten vooral aandachtspunten in voor de verdere onderhandelingen met het Europees Parlement. Zo heeft Nederland, net als enkele andere lidstaten, het belang benadrukt van een op risico's gebaseerde benadering van de richtlijn, zodat de inspanningen en middelen gericht worden op waar ze het meest nodig zijn voor de verbetering van cyberbeveiliging in de EU. Vrijwel alle lidstaten onderstreepten het belang van de doelstelling van NIB2-richtlijn om de weerbaarheid op het gebied van cyberbeveiliging in de EU te vergroten. Verschillende lidstaten hebben onderstreept dat de maatregelen in het voorstel proportioneel moeten blijven en de administratieve lasten beperkt. Verder wilden enkele lidstaten dat het toepassingsgebied verduidelijkt zou worden. Tevens onderstreepten een aantal lidstaten dat meer geharmoniseerde cybervoorschriften in de NIB2-richtlijn tevens de interne markt voor cyberproducten en -diensten versterkt.

Commissaris Interne Markt Breton bedankte het voorzitterschap namens de Europese Commissie (hierna: Commissie) voor al het werk en voor het bereiken van een algemene oriëntatie. Gelet op de dagelijkse cyberaanvallen is gezamenlijk handelen in EU-verband op coherente wijze de enige manier. De NIB2-richtlijn kan een stevig horizontaal kader bieden en dienen als referentie voor sectorale cyberveiligheid-regelgeving. De Commissie benadrukte het belang van een snel

[1] COM2020 (596) Verordening digitale operationele weerbaarheid (DORA) en COM2020 829 Richtlijn inzake de veerkracht van kritieke entiteiten (Critical Entities Resilience, CER).

besluitvormingsproces, ook met het oog op de triloog-onderhandelingen. De Commissie noemde drie punten uit het Commissievoorstel welke niet in het Raadscompromis zijn opgenomen, maar de Commissie zelf belangrijk acht: dat decentrale overheden binnen het toepassingsgebied van de NIB2-richtlijn vallen, dat *root servers* binnen de reikwijdte van het voorstel zouden moeten vallen en extra aandacht voor de samenhang tussen de NIB2-richlijn en de CER-richtlijn.

Artificial Intelligence Act (AI Act)
Voortgangsrapportage
Tijdens de Telecomraad heeft de Raad kennisgenomen van de voortgangsrapportage over de *AI Act*. Het voorzitterschap gaf aan dat het gelukt is om een eerste compromistekst op papier te zetten voor onder meer de artikelen gerelateerd aan het toepassingsgebied, de definities, verboden AI-systemen en de indeling van hoog-risico AI-systemen.

Enkele lidstaten namen het woord, waarin zij onder meer aangaven dat de *AI Act* moet worden benut om de AI capaciteit in de EU te vergoten. Tevens werd benadrukt dat onderzoek in AI niet moet worden belemmerd en dat het mkb moet worden beschermd. Tevens werd benadrukt dat de *AI Act* nationale autoriteiten niet moet belemmeren in de rechtshandhaving.

De Commissie complimenteerde het voorzitterschap met de geboekte voortgang en onderstreepte dat er is geluisterd naar de inbreng van lidstaten, met name voor wat betreft het domein rechtshandhaving en binnenlandse zaken. De Commissie gaf aan dat het voorstel rekening houdt met sectorspecifieke eigenschappen, maar dat het tegelijkertijd een horizontaal karakter behoudt waarbij een systemische en mensgerichte aanpak op basis van Europese normen en waarden het uitgangspunt is.

Verordening betreffende de invoering van een raamwerk voor een Europese Digitale Identiteit
Voortgangsrapportage
Tijdens de Telecomraad heeft de Raad kennisgenomen van de voortgangsrapportage over het raamwerk voor een Europese Digitale Identiteit. Het voorzitterschap gaf aan dat een eerste volledige lezing van het voorstel is afgerond. Het voorzitterschap benoemde enkele elementen waarover lidstaten in de Raadswerk van gedachten hebben gewisseld, waaronder de structuren van de *ewallet*, kosten, unieke identificatie en vertrouwensdiensten.

Een enkele lidstaat heeft geïntervenieerd. Er werd benadrukt dat *eID's* gebruikt moeten worden door de hele EU en dat gebruikers centraal moeten staan. Waar het gaat om de harmonisatie van *eID's* is cyberveiligheid een belangrijk aandachtspunt. Tevens werd onderstreept dat voldoende flexibiliteit moet worden ingebouwd en dat moet worden voortgebouwd op nationale initiatieven waar mogelijk.

De Commissie benadrukte dat grote commerciële partijen al bezig zijn met oplossingen te ontwikkelen voor digitale identiteiten zonder de nodige veiligheidsgaranties. Het voorstel voor een raamwerk voor een Europese Digitale Identiteit moet een homogene oplossing bieden dat veilig, betrouwbaar en

grensoverschrijdend is. *eID's* zijn daarom een voorwaarde voor de digitale soevereiniteit van de EU. De Commissie hoopt onder het Franse voorzitterschap flink vooruitgang te boeken, zodat gestart kan worden met het gebruik van *ewallets*.

Beleidsprogramma 2030: "Weg naar een Digitaal Decennium"
Voortgangsrapportage
Tijdens de Telecomraad heeft de Raad kennisgenomen van de voortgangsrapportage over beleidsprogramma 2030: "Weg naar een Digitaal Decennium". Het voorzitterschap gaf aan dat zij een eerste volledige bespreking van het voorstel nastreven voor het einde van het jaar. De discussies in raadskader tot dusver hebben laten zien dat er consensus bestaat over de doelstelling van het beleidsprogramma, maar dat het wel noodzakelijk is om nader te spreken over de strategische routekaart en het samenwerkingsmechanisme.

De Commissie heeft erop gewezen dat haast geboden is bij het behandelen van het voorstel, omdat de EU gezamenlijk de kar moet trekken om de digitale transformatie verder te brengen. Het is de bedoeling dat iedereen hier deel van uit maakt. Om die reden is er gekozen voor een steviger instrument, zonder een te strak kader te schetsen. De Commissie benadrukte extra werklast te willen beperken door deze monitoringscyclus te laten aansluiten bij de reeds bestaande *Digital Society and Economy Index (DESI)*.

Digitale rechten en principes
Beleidsdebat
Tijdens de Telecomraad heeft een beleidsdebat plaatsgevonden over digitale rechten en principes. Met deze discussie beoogde het voorzitterschap input op te halen van lidstaten om mee te geven richting de Commissie met het oog op de inter-institutionele verklaring over digitale rechten en principes. Er stonden twee discussievragen centraal. Er is gediscussieerd over de vraag of een Europese verklaring over digitale rechten en principes de weg moet uitstippelen voor het komende decennium en de eerste stap moet vormen om een mondiale benchmark vast te stellen. Tevens werd stilgestaan bij de vraag of de Raad het eens is dat de thema's gerelateerd aan het Digitaal Kompas (zoals universele toegang tot internet, goede scholing in digitale vaardigheden en mensgerichte AI) een goede basis vormen voor een overkoepelende verklaring over digitale principes voor een digitaal decennium.

Nederland, met steun van enkele lidstaten, heeft aangegeven dat het van belang is dat een dergelijke verklaring aansluit bij bestaande EU-wetgeving en internationale (mensenrechten)verdragen. Veel lidstaten verwelkomden het initiatief voor een nieuwe verklaring over digitale rechten en principes om te zorgen dat de Europese waarden zichtbaar worden in de digitale transformatie. Daarbij benoemden veel lidstaten dat de rechten die offline gelden ook online moeten gelden. Lidstaten benoemden verschillende digitale rechten en principes ter overweging voor de inter-institutionele verklaring, waaronder het belang van universele toegang tot het internet, een groene digitale transitie, digitale inclusie, bescherming van kinderen online, digitale geletterdheid, en *ehealth* diensten. Verder werd het belang van samenwerking met verschillende organisaties benadrukt, zowel op nationaal, Europees als internationaal niveau. Het belang van

samenwerking met gelijkgezinde partners, waaronder de VS, werd ook als belangrijk aandachtspunt genoemd.

De Commissie gaf aan dat tijdens de COVID-19 pandemie de afhankelijkheid van digitale technologieën is gebleken. Daarom is de discussie over rechten en principes in het digitale domein van belang om te voorkomen dat er een digitale kloof ontstaat in de EU. In de EU moet elke burger de mogelijkheid hebben om mee te draaien in een inclusieve digitale transitie. De Commissie benadrukte dat de verklaring niet bedoeld is om bestaande rechten te wijzigen, maar bedoeld is als aanvulling hierop. Deze aanvullingen zien onder meer op toegang tot het open internet en publieke diensten, digitale kennis en competenties voor iedereen, beveiliging online (vooral voor kinderen) en controle over wat er gebeurt met persoonsgegevens online. De verklaring moet een representatie zijn van de EU waarden en normen, waarmee de EU wereldwijd als standaard kan worden gezien. De verklaring wordt gepresenteerd in het nieuwe jaar, tijdens het Franse voorzitterschap.

Diversenpunt Roamingverordening
Het voorzitterschap informeerde de Raad over de laatste stand van zaken ten aanzien van de onderhandelingen over de Roamingverordening. Gedurende het Sloveense voorzitterschap zijn in de triloog-onderhandelingen tussen de Raad en het Europees Parlement vier punten van discussie geïdentificeerd. Dit betreft het beleid inzake de fair-use-policy, de keuze tussen een gedelegeerde handeling of nieuwe wetgeving om de tarieven tussentijds te herzien, intra-EU bellen en de hoogte van de *wholesale* roaming tarieven. Het voorzitterschap zet zich in om nog voor het einde van dit jaar een akkoord te bereiken en roept de lidstaten op om het onderhandelingsmandaat te herbevestigen.

Meerdere lidstaten, waaronder Nederland, benadrukten het belang om snel een akkoord te bereiken omdat de huidige verordening op 30 juni 2022 afloopt en de voordelen van Roaming in de EU moeten worden behouden. Het huidige roam-like-at-home beleid is volgens lidstaten een concreet voorbeeld van de meerwaarde van de EU voor burgers. Daarbij werd door enkele lidstaten benadrukt dat het voor een goede werking van de interne markt belangrijk is dat de *wholesale* roaming tarieven in lijn zijn met daadwerkelijke prijzen. Een enkele lidstaat gaf aan zich zorgen te maken over de positie van het Europees Parlement om de fair-use-policy af te schaffen en een enkele lidstaat benoemde dat het van belang is dat intra-EU bellen buiten de roaming regulering moet blijven.

De Commissie heeft aangegeven de oproep van de lidstaten voor een snel akkoord te hebben gehoord en zich in te spannen om hierbij te assisteren om dit mogelijk te maken in de triloog-onderhandelingen.

Diversenpunt Data Governance Act
Het voorzitterschap informeerde de Raad over de laatste stand van zaken ten aanzien van de onderhandelingen over de Data Governance Act (DGA). Er is een akkoord bereikt over het voorstel tussen de onderhandelaars in de triloogfase.

Er is tot op het moment van schrijven van dit verslag geen akkoordtekst gedeeld met de lidstaten. Zij hebben dan ook niet geïntervenieerd. Op een later moment

zal in de Raad hun instemming met het akkoord worden gevraagd. Ook het Europees Parlement zal hier nog over stemmen.

De Commissie bedankte het voorzitterschap voor het goede werk in de onderhandelingen. De Commissie zal komend jaar met de Data Act een nieuw wetgevend voorstel over data publiceren. Deze en andere voorstellen moeten volgens de Commissie de basis zijn van een sterke Europese markt voor data, welke cruciaal is voor de Europese economie.

Diversenpunt ePrivacyverordening
Het voorzitterschap informeerde de Raad over de laatste stand van zaken ten aanzien van de onderhandelingen over de ePrivacyverordening. In de triloog-onderhandelingen met het Europees Parlement zijn de artikelen over de rechten voor eindgebruikers, over handhaving en rechtsmiddelen , en over gedelegeerde en uitvoeringshandelingen behandeld. Het is gelukt om voortgang te boeken op deze hoofdstukken over onder andere definities, het toepassingsgebied, noodcommunicatie en rechtsmiddelen.

De Commissie bedankte het voorzitterschap en benadrukte dat het van belang is om zo snel mogelijk voortgang te boeken. De huidige ePrivacy regels zijn verouderd en niet langer geschikt en toekomstbestendig. De Commissie zal de Raad en het Europees Parlement zo goed mogelijk ondersteunen om een compromis te bereiken met een hoog beschermingsniveau van de privacy van gebruikers van elektronische communicatiediensten zonder innovatie te belemmeren.

Diversenpunt uitkomsten D9+ ministeriële bijeenkomst
Luxemburg informeerde de Raad over de uitkomsten van de discussie van de afgelopen D9+ bijeenkomst die het land heeft georganiseerd over de groene en digitale transities. De D9+ lidstaten, waaronder Nederland, hebben naar aanleiding van de discussie een gemeenschappelijke verklaring uitgebracht. Het doel van de verklaring is om de discussie over de kansen van digitalisering en de uitdagingen voor de ICT sector inzake verduurzaming prominent op de Europese agenda te krijgen. In de verklaring worden in dit kader zeven aandachtspunten belicht, over (i) de noodzaak van het versterken van de interne markt voor duurzame groei (ii) het belang van het ontwikkelen van duurzame digitale infrastructuur met hoge capaciteit, (iii) de circulaire economie versterken via digitalisering, (iv) het belang van private en publieke investeringen, (v) het aantrekken en behouden van talent, (vi) het ontwikkelen van sectorale data ruimtes en (vii) samenwerking tussen landen op concrete casussen.

De Commissie bedankte Luxemburg voor het agenderen en het onder de aandacht brengen van dit belangrijke thema. De Commissie steunt de conclusies. De EU heeft als ambitie om als eerste continent klimaatneutraal te zijn. Digitale technologieën bieden veel kansen om circulariteit te bevorderen en om energie efficiëntie te verhogen. Daarom wil de Commissie digitale oplossingen inzetten om de doelstellingen van de Green Deal te bereiken.

Diversenpunt non-paper EU digitale prioriteiten in het kader van de International Telecommunications Union verkiezingen
Litouwen informeerde de Raad over het gezamenlijk non-paper over een gecoördineerde aanpak van de EU en de lidstaten richting de verkiezingen van de managementposities van de *International Telecommunication Union* (ITU). Volgend jaar tussen 26 september en 14 oktober wordt in Boekarest de gevolmachtigde conferentie gehouden waar verschillende besturende functionarissen en experts binnen de ITU instellingen worden gekozen. De lidstaten en de Commissie hebben aangehoord.

Diversenpunt presentatie inkomende Frans voorzitterschap
De Franse delegatie heeft de Raad geïnformeerd over de belangrijkste prioriteiten voor de Telecomraad tijdens hun voorzitterschap. Het inkomende voorzitterschap heeft aangegeven op zoek te gaan naar een balans tussen innovatie en regelgeving. Wereldwijd is de digitale transitie gaande en op lange termijn moet de EU relevant en concurrerend te blijven ten opzichte van andere delen van de wereld, onder meer door meer startups en scaleups in de EU. Met betrekking tot nieuwe digitale regelgeving moet daarom het innovatieve vermogen van de EU in ogenschouw worden gehouden. Een raamwerk voor een Europese Digitale Identiteit is een prioriteit om economische activiteit in de EU te stimuleren en tegelijkertijd controle te behouden op de digitale identiteit van EU burgers. Daarnaast wil het Franse voorzitterschap zich inzetten voor de onderhandelingen met het Europees Parlement over de DSA, DMA en de NIB2-richtlijn en in de Raad de onderhandelingen starten over de Data Act en de onderhandelingen over de AI Act verder brengen.

Frankrijk heeft op 7-8 februari 2022 een ministeriële bijeenkomst over digitale soevereiniteit gepland, op 8-9 maart 2022 een informele Telecomraad en op 3 juni 2022 een formele Telecomraad. De agenda's voor deze bijeenkomsten zijn nog onbekend. U zult via de geannoteerde agenda over de Nederlandse inzet tijdens de Raden worden geïnformeerd.

Data economie
Lunch debat
Tijdens de Telecomraad heeft een informeel lunchdebat plaatsgevonden over de data economie. Er is van gedachten gewisseld over de *Data Act*, het voorstel dat in het eerste kwartaal van 2022 wordt verwacht. Specifiek is gediscussieerd over de vraag op welke manier EU regelgeving de positie van consumenten en bedrijven kan versterken met betrekking tot de data die ze genereren. Tevens is gesproken over de wijze waarom de EU moet omgaan met *vendor lock-in* praktijken door *cloud- en edge* dienstverleners, zodat afnemers gemakkelijker tussen dienstaanbieders kunnen wisselen en kunnen profiteren van een eerlijke en concurrerende markt voor dataverwerking.[2]

Nederland heeft tijdens de lunch het non-paper over de *Data Act* onder de aandacht gebracht, waarover uw Kamer via de geannoteerde agenda van de informele Telecomraad van 14 oktober jl. is geïnformeerd.[3] Nederland heeft

[2] Vendor lock-in maakt een klant afhankelijk van een leverancier voor producten en diensten, omdat hij niet in staat is om van leverancier te veranderen zonder substantiële omschakelingskosten of ongemak.
[3] Kamerstuk II 21501, nr. 33-875

aangegeven positief te zijn over de komst van de *Data Act* omdat het kabinet hecht aan het in EU-verband creëren van een open data-economie waarin burgers en bedrijven grip houden op hun gegevens. Wettelijke kaders op dit gebied kunnen ten goede komen aan burgers en bedrijven en kunnen gelden als mondiale standaarden. Lidstaten benadrukten dat de EU met de *Data Act* de standaard kan zetten wereldwijd en waren positief over het voorstel om *vendor lock-in* te voorkomen.

European Cyber Resilience Act

Tenslotte informeer ik uw Kamer over een Nederlands non-paper met de voorlopige inzet op de *European Cyber Resilience Act*. Dit onderwerp stond overigens niet op de agenda van de Telecomraad. In de 2021 State of The Union kondigde Ursula von der Leyen de komst van een Cyber Resilience Act aan. De Europese Commissie zal naar verwachting in het derde kwartaal van 2022 een voorstel voor deze Cyber Resilience Act presenteren. De Cyber Resilience Act lijkt invulling te zijn van de horizontale regulering voor de cybersecurity van ICT-producten en -diensten waarvoor de Commissie eerder een studie heeft uitgezet. De Europese Commissie heeft in eerdere gesprekken aangegeven benieuwd te zijn naar ideeën en inzichten van Nederland omtrent de Cyber Resilience Act. Bijgaand non-paper is opgesteld om de eerste inzichten te kunnen delen en als voeding voor de dialoog met de Europese Commissie, andere lidstaten en stakeholders in het veld.

Het kabinet ziet de Cyber Resilience Act als een kans om aanvullende wettelijke cybersecurity eisen te stellen en om concurrentie en innovatie verder te stimuleren. Momenteel dragen de gebruikers van de digitale producten, processen en diensten (bedrijven en consumenten) de meeste verantwoordelijkheid voor de cybersecurity. Marktprikkels ontbreken voor de fabrikanten en aanbieders van ICT-producten, -diensten en -processen en er bestaan nog weinig verplichte wettelijke kaders. Daarom verwelkomt Nederland de komende Cyber Resilience Act als een belangrijke bouwsteen naast bestaande of toekomstige (sectorale) wet- en regelgeving zoals Radio Equipment Directive, General Product Safety Regulation, Machinery Directive, Cyber Security Act, Network and Information Systems Directive 2 en sectorale wetgeving zoals automotive.

Non-paper on the principles of a Cyber Resilience Act

Introduction

In her State of the Union speech of 2021, Commission President Ursula von der Leyen announced the need for a European Cyber Resilience Act to set common standards to improve the cybersecurity for products in the European internal market: *"If everything is connected, everything can be hacked. Given that resources are scarce, we have to bundle our forces. And we should not just be satisfied to address the cyber threat, we should also strive to become a leader in cybersecurity. This is why we need a European Cyber Defence Policy, including legislation setting common standards under a new European Cyber Resilience Act."*

The Netherlands couldn't agree more. It is of the utmost importance that the digital products, processes and services which we use in our economy and society can be trusted to be digitally secure. Currently, users of the digital products, processes and services bear most of the responsibility for securing their digital activities. Market incentives are lacking for the manufacturers and providers of ICT products, processes and services. To be most effective, we need a European and holistic approach, with a mix of policy tools across various areas of European legislation.

Therefore, the Netherlands welcomes the upcoming Cyber Resilience Act as a key horizontal layer to regulate the cybersecurity of the products, processes and services that we use. It provides the opportunity to take additional measures to ensure that digital products, processes and services can be trusted on all relevant aspects of cybersecurity (confidentiality, integrity and availability), including specifying the necessary conditions for the placement on the market[1], alongside existing or upcoming legislation such as Radio Equipment Directive (RED), General Product Safety Regulation, Machinery Directive, Cyber Security Act (CSA), and Network and Information Systems Directive 2 (NIS2D) and sectoral legislation like automotive.

By means of this non-paper, the Netherlands intends to contribute to a broad policy discussion on cybersecurity in general and the Cyber Resilience Act in particular, outlining the necessary steps to ensure a safe and secure European Digital Single Market. Moreover, there is true potential for the EU to play a leading role globally, by setting common standards through European legislation, including through the Cyber Resilience Act.

Main goals of the Cyber Resilience Act

The Netherlands believes the Cyber Resilience Act should:

1. Be an essential building block in a European and holistic approach to the cybersecurity of digital products and services in which a mandatory horizontal approach is complementary to sectoral regulation in specialized domains.
2. Propose security requirements for digital products and services, which should
    - cover all forms of digital products, services and processes;
        - irrespective if they are offered for consumer or business/industrial purposes;
        - irrespective if they are linked to a tangible product.
    - cover the entire lifecycle of digital products and services;
    - target the manufacturers and providers of ICT products, processes and services.

1. The CRA is an essential building block in a European and holistic approach, with mandatory horizontal requirements, complementary to sectoral regulation in specialized domains

Our societies are highly digitized and connected. Mainstreaming cybersecurity across the board in the EU is crucial. We need a comprehensive holistic that addresses all levels within all policy domains. It is therefore essential to take adequate legislative measures at the EU level to create a safe

[1] PCouncil conclusions of the Telecom Council of December 2020 on cybersecurity of connects products.

European Digital Single Market so we can all trust future digital developments and reap the societal and economic benefits they bring.

With the work already done by establishing the voluntary Cyber Security Act and the mandatory Radio Equipment Directive, new cybersecurity requirements have been set with regard to ICT products, processes and services. Other relevant legislation includes the revision of the Directive on Security of Network and Information Systems, the General Safety Regulation to implement UN measures with regards to automotive security, as well as the Machinery Directive and General Product Safety Directive.

The Netherlands welcomes these steps to strengthen the cybersecurity of the EU. However, an important piece of the puzzle for a holistic and comprehensive approach to cybersecurity is still missing with regard to the cybersecurity of digital products, processes and services since many initiatives take a sectoral approach or do not cover the entire digital domain.[2] The Cyber Resilience Act can fill these gaps and complement existing EU cybersecurity efforts. The Cyber Resilience Act should be an essential building block in a European and holistic approach to the cybersecurity of digital products and services in which a mandatory horizontal approach is complementary to sectoral regulation in specialized domains.

Example of the need for a mandatory horizontal approach:

While the RED delegated act is key to set mandatory security requirements in the short term for wirelessly connect devices (including many IoT devices), it only addresses wireless products when they enter the market and cannot encompass the broader scope of ICT products, processes and services. Also, at the time the RED was not created with cybersecurity in mind. The CSA on the other hand offers the benefits of a broader scope for ICT products, processes and services, but is a voluntary system. From this perspective, horizontal legislation can contribute to a desired horizontal and mandatory level of security and ensure consistency and legal certainty for both manufacturers and consumers (citizens and businesses).

The Netherlands envisions the Cyber Resilience Act to serve as a horizontal regulation containing harmonised cybersecurity requirements for manufacturers and suppliers of ICT products, processes and services. A lex specialis provision can ensure the necessary interplay with sectoral legislation in specialized domains. As such, the Cyber Resilience Act has the potential to have a comparable function as the General Product Safety Directive in the New Legislative Framework. In order to avoid overlap and unnecessary administrative burden for market players as well as regulatory authorities, careful consideration should be given to existing legislation and proposed and ongoing legislative initiatives. Targeted (sectoral) regulation should principally be the starting point in terms of public policy based on specific sectoral needs. As mentioned above, there are currently already EU initiatives underway to implement or review such targeted legislation. At the same time, sectoral legislation cannot encompass societal need to set cybersecurity requirements for the entire ICT industry. The CRA offers the opportunity to make explicit what gaps are already being addressed and for which reasons, and to determine how a horizontal approach in the form of a Cyber Resilience Act would add to existing or upcoming legislation.

2. The CRA should propose cybersecurity requirements for all forms of digital products, processes and services, covering the entire lifecycle and targeting the manufacturers and providers of ICT products, processes and services

The focus of the Cyber Resilience Act should be on setting mandatory requirements for manufacturers and providers of ICT products, processes and services. As such, horizontal regulation can contribute to a state-of-the-art cybersecurity framework and ensure consistency and legal certainty for both manufacturers and customers.

The Netherlands would like to underline that the Cyber Resilience Act should:

- cover not only digital products, but also digital processes and services. In the current state of technological and market dynamics, digital products, processes and services are interlinked and almost inseparable. In the future, this will likely continue.

[2] Draft text revised GPSD (europa.eu)

- cover all forms of ICT products, processes and services, irrespective whether they are offered for consumer or business/industrial purposes. In this way, the Cyber Resilience Act can effectively complement sectoral regulation.
- cover ICT products, processes and services, irrespective whether or not they are linked to a physical product. In this way, software products, processes and services are included and horizontal cybersecurity requirements will apply. This is necessary, as society is increasingly dependent on a wide range of software products, processes and services.
- cover the entire lifecycle, i.e. from the design phase, before a product comes on the market, while it is used during its expected (economic) life span, up to and including its decommission and disposal. In this context, the end-of-life gap is a specific policy challenge, when end-users continue to use digital products, services and processes while supply-side actors cease to provide, cybersecurity by design and cybersecurity updates, making products less secure.
- apply to manufacturers and suppliers of ICT products, processes and services. This is a necessary addition to other legislative initiatives. For instance, the NIS2D targets the cybersecurity business continuity of essential services. However, the cybersecurity of the ICT products, services and processes that their ICT suppliers provide are often not (or indirectly) regulated. This is a gap, as the operator and the integrity of the products and services the entity delivers to its end-customers are also dependent on (the quality of the products and services of) the ICT suppliers. Furthermore, companies (big and small) and consumers are all dependent on the cybersecurity that ICT manufacturers and suppliers provide in their products, services and processes. There is therefore a societal need to set cybersecurity requirements for the ICT industry through legislation. The Cyber Resilience Act can realize a duty of care for the cybersecurity of ICT products, processes and services. Certification schemes under the Cyber Security Act could then be used as a mandatory harmonized standard for the specification of the duty of care based on the latest state of technology.

To conclude

The Cyber Resilience Act should be an essential building block in a European and holistic approach to the cybersecurity of digital products and services in which a mandatory horizontal approach is complementary to sectoral regulation in specialized domains. Specifically, the Cyber Resilience Act should function as a horizontal regulation containing a lex specialis application with regard to sectoral and harmonised rules.

The focus of the Cyber Resilience Act should be on setting cybersecurity requirements that cover all forms of both digital products and services, irrespective if they are offered for consumer or business/industrial purposes and irrespective if they are linked to a physical product. It should cover the entire lifecycle of digital products, processes and services and target the manufacturers and providers of ICT products, processes and services through a duty of care based on the latest state of technology.