

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

Datum 30 september 2021

Betreft Geannoteerde agenda informele Telecomraad 14 oktober 2021

Ons kenmerk

DEIZ / 21240879

Bijlage(n)

1

Geachte Voorzitter,

Op 14 oktober vindt de informele Telecomraad plaats via videoconferentie. Bijgevoegd bij deze brief vindt u de geannoteerde agenda met daarin een beschrijving van de discussiepunten en de Nederlandse inzet hiervoor. Tevens informeer ik u graag over de laatste ontwikkelingen rondom de onderhandelingen ten aanzien van de *Data Governance Act* en over een Nederlands non-paper met de voorlopige inzet op de *Data Act*.

Stef Blok
Minister van Economische Zaken en Klimaat

Geannoteerde agenda informele Telecomraad 14 oktober 2021

Ons kenmerk
DEIZ / 21240879

AI-verordening (Artificial Intelligence Act)

Beleidsdebat

Het voorzitterschap heeft voor de informele Telecomraad een beleidsdebat geagendeerd over de AI-verordening. De AI-verordening is op 21 april jl. door de Europese Commissie gepubliceerd. Het voorstel heeft als doel om ervoor te zorgen dat AI-systemen die op de Europese markt worden gebracht en gebruikt veilig zijn en in overeenstemming zijn met de geldende fundamentele rechten en waarden binnen de EU. Het streven is om zo een interne markt voor veilige en betrouwbare AI-systemen te faciliteren terwijl marktfragmentatie wordt voorkomen. Ook beoogt de verordening te zorgen voor juridische zekerheid om investeringen en innovatie in AI te faciliteren. Het BNC-fiche met de kabinetsreactie op deze verordening is op 31 mei jl. met uw Kamer gedeeld¹. Het beleidsdebat zal zich richten op het juridisch raamwerk en de uitdagingen van effectieve implementatie van de AI-verordening.

Sinds de publicatie van het voorstel in april zijn de onderhandelingen in de Raad van start gegaan. De eerste reacties van lidstaten, waaronder Nederland, op de verordening zijn overwegend positief en er is steun voor de overkoepelende doelen van de verordening. Wel hebben lidstaten, net als Nederland, nog meerdere bezwaren en vragen, onder andere over de reikwijdte van hoog-risico en verboden AI-systemen, de praktische uitvoerbaarheid en haalbaarheid, en de relatie met bestaande wetgeving.

Waar het gaat om het juridisch raamwerk van de AI-verordening vindt het kabinet het wenselijk dat op EU-niveau geharmoniseerde regelgeving is voorgesteld om te borgen dat er betrouwbare AI-systemen, in overeenstemming met de geldende fundamentele rechten en waarden, de Europese interne markt op komen. Op die manier kunnen mogelijke grensoverschrijdende risico's voor veiligheid en fundamentele rechten die AI-systemen met zich mee brengen gemitigeerd worden. Door alleen betrouwbare AI-systemen toe te laten op de interne markt heeft de EU het vermogen om met de AI-verordening wereldwijd de standaard te zetten. Dit kan bijdragen aan de versterking van het concurrentievermogen van de EU.

Het is vooralsnog lastig te beoordelen wat de uitdagingen zijn van effectieve implementatie, gelet op het feit dat de verordening een brede impact heeft op aspecten zoals innovatie, het mkb, toezicht en het maatschappelijk middenveld. Wel is voor het kabinet van belang dat de regeldruk die de verordening met zich meebrengt geen belemmering vormt voor innovatie en moeten administratieve verplichtingen lastenluw zijn, vooral voor mkb-bedrijven. De voorgestelde toegang tot *regulatory sandboxes*² kan mkb-bedrijven, in combinatie met begeleiding door de toezichthouder, hierbij helpen. Verder zal het kabinet ook aandacht vragen voor het feit dat het bij de gehanteerde definities en formuleringen ontbreekt aan helderheid. Onduidelijke definities en formuleringen kunnen onzekerheid geven

¹ Kamerstuk 22112, nr. 3129

² *Regulatory sandboxes* zijn gecontroleerde omgevingen waar de ontwikkeling, het testen en het valideren van AI-systemen worden gefaciliteerd voordat deze op de markt worden gebracht of in gebruik worden genomen.

over wanneer een AI-systeem onder de reikwijdte van het voorstel valt en wanneer een organisatie kan worden aangemerkt als een "AI provider" (de aanbieder van een AI-systeem). Meerdere lidstaten hebben aangegeven dat de huidige beschrijving van hoog risico-toepassingen nog onvoldoende duidelijk en te ruim is, wat kan leiden tot overregulering en onnodige uitvoeringslasten. Het kabinet onderschrijft dit. Het blijft daarbij ook belangrijk om een goede balans te vinden tussen de mogelijkheden voor overheden om AI-systemen te gebruiken en ontwikkelen bij de uitvoering van hun taken en het beschermen van fundamentele rechten. Diverse lidstaten hebben in dit verband de vraag gesteld of bijvoorbeeld voor de rechtshandhaving niet een afzonderlijke regeling getroffen moet worden die recht doet aan de specifieke eisen en behoeften van het rechtshandavingsdomein. De initiële inzet van het kabinet is gericht op het verduidelijken en aanscherpen van de in het voorstel gehanteerde definities, de voorziene werking van de verordening in de praktijk, en de relatie tot bestaande wetgeving. De Nederlandse inzet tijdens de informele Telecomraad zal plaatsvinden langs bovengenoemde lijnen.

Data Governance Act

Hoewel de *Data Governance Act* geen onderdeel is van de agenda van de informele Telecomraad, wordt uw Kamer hierbij geïnformeerd over de voortgang op dit dossier. Zoals aangekondigd in het verslag³ van de Telecomraad van 4 juni jl. heeft het Sloveens voorzitterschap voortvarend de onderhandelingen opgepakt. Op 1 oktober voorzien zij de agendering van de stemming over een onderhandelingsmandaat in de Raad, zodat direct daarna de trilogie kunnen aanvangen. Hoewel de compromistekst die het voorzitterschap wil agenderen op het moment van schrijven nog niet verspreid is, is Nederland op grond van de laatste ontwikkelingen in de onderhandelingen voornemens om het mandaat te steunen. Naar verwachting zal er namelijk op alle Nederlandse aandachtspunten, zoals geïdentificeerd in het BNC-fiche, een verbetering zijn gerealiseerd ten opzichte van het oorspronkelijke Commissievoorstel. Dat betreft onder meer een verduidelijking ten aanzien van de reikwijdte van datatussenpersoondiensten, de invoering van een gedragscode voor organisaties die een data-altruïsmelabel willen voeren en een notificatieplicht bij ongeoorloofd gebruik van niet-persoonlijke data. In het verslag van de informele Telecomraad zal uw Kamer geïnformeerd worden over de uitkomst van de stemming over het onderhandelingsmandaat.

Data Act

De Europese Commissie zal naar verwachting in het vierde kwartaal van dit jaar een voorstel voor een *Data Act* presenteren. In mei jl. heeft de Commissie een *Inception Impact Assessment*⁴ gepresenteerd waarin het de doelen en beleidsopties voor de *Data Act* schetst. De Commissie beoogt een eerlijkere data-economie te creëren door toegang tot en het gebruik van data te verbeteren. In reactie op de consultatie van de Commissie heeft het kabinet een non-paper opgesteld om bij te dragen aan de discussie in Europa over de *Data Act*. U vindt het non-paper bijgevoegd bij deze geannoteerde agenda dat onder andere is

³ Kamerstuk21501, nr. 869

⁴ [Data Act & amended rules on the legal protection of databases \(europa.eu\)](https://european-council.europa.eu/media/en/press-communications/asset-116221.pdf)

gebaseerd op de Nederlandse visie op datadeling tussen bedrijven⁵ uit 2019, de inzichten uit de Verkenning van verplichtingen inzake datadeling in de technologiesector die 18 maart jl. naar uw Kamer is gezonden⁶ en op de eerder geformuleerde inzet van Nederland bij de evaluatie van de Algemene Verordening Gegevensbescherming omtrent het vergroten van de mogelijkheden voor gegevensoverdraagbaarheid⁷. Het kabinet ziet de *Data Act* als een kans om de grip op gegevens voor personen en bedrijven te versterken en om concurrentie en innovatie verder te stimuleren. Daarnaast is het ook belangrijk dat er aandacht is voor de ontwikkeling van de benodigde standaarden om datadeling mogelijk te maken en voor het belang van privacy, veiligheid en gegevensbescherming bij de ontwikkeling daarvan. Het non-paper roept de Commissie verder op om door middel van de *Data Act* bij te dragen aan de overdraagbaarheid van persoonsgegevens⁸.

⁵ Kamerstuk 26643, nr. 594

⁶ Kamerstuk 32637, nr. 449

⁷ [Kamerbrief over aanpassingen UAVG en evaluatie AVG | Kamerstuk | Rijksoverheid.nl](#) p. 18; dit standpunt vloeit voort uit de eerdere [Kamerbrief over bescherming van de horizontale privacy | Kamerstuk | Rijksoverheid.nl](#) p. 8

⁸ De minister voor Rechtsbescherming heeft tijdens het commissiedebat bescherming persoonsgegevens van 20 mei 2021 aan het lid Koekkoek (VOLT) toegezegd het belang van gegevensoverdraagbaarheid mee te nemen in de inzet van het kabinet ten aanzien van de Digital Services Act. De Data Act biedt mogelijkheid horizontaal – en dus niet slechts ten aanzien van de onder de Digital Services Act vallende diensten – tot een verbeterde effectivering van het recht op gegevensoverdraagbaarheid uit artikel 20 AVG te komen.

Introduction

Data has become increasingly important to our economy and society. It creates enormous added value by, among others, contributing to research and innovation, increasing efficiency of many societal processes and enhancing the competitiveness of industries. The full potential of the data economy is not even reached yet, as there is still a huge amount of untapped industrial data in the European economy. Moreover, data can be re-used endlessly and is non-rival. However, to utilise data to its full potential, all individuals and organisations participating in the data economy should be able to benefit from the use of data and trust that their rights and interests are protected. Therefore further measures should not only stimulate data sharing, but also address and mitigate risks concerning the privacy of European citizens and the protection of their personal data. Due to existing deficiencies in the market, such as a lack of interoperability, individuals and organisations are often hesitant or unable to share their data. This limits the potential of data to drive innovation and address societal issues and leads to competition problems such as lock-in or excessive bundling of services. Several European initiatives¹ already aim to contribute to trusted data sharing and a well-functioning data economy within the broader fabric of society. These steps are welcomed by the Netherlands, as they follow the main points of its view on a responsible data-economy as stated in the Dutch vision on data sharing between businesses, published in February 2019². A recent study commissioned by the Dutch Ministry of Economic Affairs and Climate Policy³ and a study by the Netherlands Bureau for Economic Policy Analysis (CPB)⁴ emphasize the need for governments to take additional measures.

The Netherlands is committed to preserving an open economy, cooperation with international partners, creating the right frameworks and setting global standards. The Netherlands welcomes the upcoming Data Act. It provides the opportunity to take additional measures to ensure that data is available to private and public stakeholders, such as businesses and knowledge institutions, to address societal and economic challenges and drive innovation whilst respecting the rights and interests of all parties involved. The European Commission (EC) has presented a first outline of the upcoming Data Act in the IIA⁵ and in the public consultation. By means of this non-paper, the Netherlands intends to contribute to a broad policy discussion on the Data Act by outlining the necessary steps to ensure a fair, well-functioning and competitive European data economy.

Main goals of the Data Act

The Netherlands believes the Data Act should:

1. Strengthen the rights of individuals and organisations participating in data sharing arrangements so that they can exercise more control over their provided and observed data. Specifically, the Data Act should:
 - Ensure individuals can better exercise their right to data portability (Article 20 GDPR) to stimulate unbundling of services and allow individuals to easily switch between services.
 - Ensure fairness in data access and use in data sharing between organisations to provide better safeguards for SMEs participating in the data economy.
 - Ensure service portability in data-driven markets where vendor lock-in limits competitiveness.
2. Further contribute to a framework for development and implementation of the standards necessary to increase interoperability. Increased interoperability is necessary for the further development of the data economy and to achieve the policy goals of the Data Act, especially the measures that aim to strengthen data and service portability.
3. Ensure that the use of privately-held data by the public sector to serve the public interest is organised in line with the rights, obligations and interests of all parties involved. The Data Act can contribute to fair and reliable Business-to-Government (B2G) data sharing when there is a legitimate public interest, for example to provide official statistics, while protecting individual data protection rights, privacy and intellectual property rights.

¹ a.o. the General Data Protection Regulation (GDPR); European Data Strategy; the proposed Data Governance Act; European Alliance for Industrial Data, Edge and Cloud; European Health Data Space and European Open Science Cloud via Horizon Europe

² <https://www.government.nl/documents/reports/2019/02/01/dutch-vision-on-data-sharing-between-businesses>

³ <https://www.government.nl/documents/reports/2020/11/30/exploring-data-sharing-obligations-in-the-technology-sector>

⁴ <https://www.cpb.nl/sites/default/files/omnidownload/CPB-Background-Documents-Policy-Options-Data-Economy-Literature-Review.pdf>

⁵ https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en

1. Strengthening the rights of individuals and organisations

Increased data usage and data sharing can have societal and economic benefits. These benefits should be fairly distributed amongst the participants in the data economy. Currently, a relatively small number of companies collect and process personal and non-personal data to create value. This data is often provided by, or observed from, individuals or organisations through all kinds of data sharing agreements and provisions. Individuals and organisations, especially SMEs, that provide data often have insufficient insight in and control over the terms of arrangements and thus the creation, collection, use or sharing of data that relates to them. With the increase in data being collected, created and used by among others Internet-of-Things(IoT)-devices this leads to several issues. This lack of insight and control *i)* hinders individuals and organisations in protecting their own rights or interests, *ii)* leads to data too often being used and shared in ways which are not necessarily in line with their interests *and iii)* limits individuals and organisations in using their provided and observed data to create value. This in turn leads to vendor lock-in and excessive bundling of data-driven products and services, which hamper competition and limit innovation. Therefore, the Netherlands is of the opinion that the rights of individuals and organisations should be strengthened to increase the control they have over their provided and observed data.

a. Individuals

The rights of data subjects towards their personal data are mainly laid down in the GDPR. The GDPR provides individuals, among others, with the right to erasure, right to restrict processing and the right to data portability.⁶ These rights aim to provide individuals control over the use of their personal data, but in practice that goal is not always achieved to the fullest of its potential. The Netherlands agrees with EC's notion in the IIA that a lack of interoperability formats limits the ability for individuals to port their data and thereby control the use of their data⁷. For some products and services that derive value from personal data, data subjects require real-time portability or portability according to certain technical specifications in order to port their data and switch or combine services in a way that is valuable to the individual. The current right to data portability does not stipulate technical specifications and the existing market lacks the coordination and incentives to develop these interoperability formats by itself, leading to vendor lock-in and excessive bundling of services.

The Netherlands believes that the EC should stipulate interoperability requirements to help individuals take advantage of the portability right for products and services which derive value from processing personal data and where issues with lock-in and bundling of services occur or can occur, such as IoT-devices. An important consideration in formulating these measures should be the allocation of the costs involved with these measures, especially the costs to SMEs.

b. Organisations

While individuals' rights over their personal data are already laid down in horizontal legislation, the legal protection of 'non-personal' data is currently very fragmented and often indirect. For example, some data is protected by intellectual property rights or as trade secret. But even then the protection is often indirect. In the IP Action Plan⁸ the EC states that a robust framework is needed to ensure organisations can generate, view, share and use data and therefore wants to stimulate access to and the exchange of data by clarifying a number of provisions of the Trade Secrets Directive and revision of the Databases Directive. The Netherlands welcomes the clarifications regarding the Trade Secrets Directive. However, concerning the Database Directive, it is very important that the right balance is struck between the interests served by the protection of databases on the one hand and the use of databases on the other.

Due to the fragmented protection of non-personal data, the access and usage rights when organisations co-generate data are often laid down in private contracts. Due to the lack of insight and control by organisations which provide data this can lead to an asymmetrical distribution of access and usage rights. Freedom of contract for organisations is an important principle, but fair data access and use rights for organisations, especially SMEs and start-ups, are essential to develop new products and services, foster innovation in general, ensure organisations can protect their own rights and interests and ensure a fair distribution of the value created with data. It is important that the Data Act ensures clear and fair data access and usage rights in data sharing arrangements where data is cogenerated which is valuable to multiple parties. Specific data types or different sectors will require different measures. While transparency obligations and fairness tests can be useful, the Netherlands believes the Data Act should contain codified access and use rights or horizontal modalities. The aim should be to set a broad standard for fairness of

⁶ Articles 15 – 18 GDPR

⁷ [Data Act & amended rules on the legal protection of databases \(europa.eu\)](#)

⁸ Making the most of the EU's innovative potential An intellectual property action plan to support the EU's recovery and resilience, COM/2020/760 final

use so that organisations can benefit from the value their provided, observed and (co-)generated data provides and the rights and interests of all parties are protected. Sectoral initiatives could then build upon this and develop specific tools, standards or agreements per sector or domain. This process could take inspiration from the FAIR-principles, which as common principles form the basis for specific standards and tools in the broader research and health sectors.

For certain products and services which derive value from processing data, among which cloud computing services, organisations suffer similar problems of vendor lock-in and bundling of services as individuals. For these products and services organisations, and especially SMEs, could benefit from a right to data and application portability. The Netherlands therefore supports the Commission in researching the possibilities for data portability, interoperability and application portability to establish a more competitive market for cloud computing services. Such measures are a necessary addition to the initiatives that are focusing on strengthening European cloud supply and establishing federated cloud services, like GAIA-X and the possible IPCEI Cloudinfrastructure and Services. Furthermore, several organisations have experienced similar lock-in problems in the business software market as in the market for cloud computing services⁹. We therefore urge the Commission to also research possible measures to strengthen the ability of organisations to switch between business software providers in this market as well.

2. Interoperability and standardization

Every data sharing arrangement requires a certain level of interoperability. Nonetheless, there are few common principles or generally accepted standards that effectively facilitate data sharing on a large scale, whether within an industry or between industries. Standardization and interoperability are necessary to realize the opportunities for data sharing to stimulate innovation and increase competitiveness in data-driven markets. However, developing and implementing the necessary standards for data sharing and interoperability is a complex and lengthy process which requires high levels of cooperation and coordination. The market by itself lacks the necessary coordination and incentives to achieve a meaningful level of interoperability on a broad scale, in a timely manner and in line with European legislation and values. This is further complicated by the fact that data markets are highly diverse and there are different needs and requirements per sector.

Improved interoperability is also crucial to realize the opportunities the Data Act presents. To ensure that measures to increase fairness in access and usage rights and to improve portability are effective in practice interoperability within sectors and across sectors needs to be increased. A well-functioning eco-system of sectoral and cross-sectoral initiatives is needed to develop the necessary standards to support the legislation and to adapt to future innovations. Prioritisation and coordination at European level are vital to stimulate the market and existing ecosystems to develop these standards. We therefore urge the Commission to ensure the standards necessary to support the Data Act are developed timely, using the existing European Standardisation System. Harmonised standards can provide a means to comply with European regulation where applicable. The EC should determine; based on the policy goals of the Data Act, taking into account existing initiatives and with input from stakeholders; for which sectors, services and products increased interoperability should be prioritized. Within the existing system the necessary standards can then be developed through an open process with a broad group of stakeholders, including SMEs. Data protection safeguards should be put first in development to mitigate potential risks to intellectual property and risks concerning the privacy of European citizens and the protection of their personal data. Broad implementation of the standards should be ensured by linking standards and technical specifications to portability, usage and access rights where applicable. If successful this process can further contribute to establishing an ecosystem for the prioritization, development and implementation of standards for data sharing.

3. The use of privately held data by the public sector

The Netherlands acknowledges that business-to-government (B2G) data sharing currently lacks (common) structures and dedicated functions. This can limit the benefits of data for the common good as the use of certain privately-held data can be necessary to serve the public interest. Fair and sustainable access to such privately-held data by the public sector could lead to better and more innovative delivery of public services and better policy making. The production and dissemination of reliable independent official statistics is an important example of a data-driven public service which plays a fundamental role in today's society. Sustainable access to privately held data sources is crucial for the production of better quality and timely independent official statistics by national statistics institutes in a more efficient and less costly manner. Furthermore, the recent pandemic is one of many examples which showed the value of fast and

⁹ <https://fd.nl/ondernemen/1319877/the-stranglehold-of-the-software-giants-m3f1caMuF2wb>

accurate information for policymaking. Fast occasional B2G data sharing could contribute to better-informed decision-making in such unpredictable emergencies.

Although B2G data sharing can be useful for dedicated purposes, it is essential that any such measures to promote it are carefully constructed and take into account the rights, obligations and interests of all parties involved, including individual data protection rights, the right to privacy and business secrets. Moreover, the purpose and public interest should be clearly defined and proportionality and accountability should be ensured in order to prevent misuse. With regard to the lawfulness of foreseen data sharing arrangements, it is important to emphasize that more and more datasets may be classified as personal data in the sense of the GDPR because anonymizing data is becoming, increasingly difficult. Sharing personal data with the government on a structural basis requires a specified legal basis and has to adhere to all requirements set in data protection legislation.¹⁰ Any substantive data sharing rules that aim to serve as a legal basis for processing¹¹ have to be well specified and adhere to all relevant legal requirements. Bases for data processing that are worded in a wide and general manner would not be in line with our European system of fundamental rights.

¹⁰ the GDPR, E-privacy regulation, the EUGDPR, the Law Enforcement Directive, the Charter of Fundamental Rights of the EU and the European Convention on Human Rights.

¹¹ E.g. article 6 GDPR