De EU digitale marktregelgeving in beweging: de ambitie om te vereenvoudigen en de cyberweerbaarheid te vergroten

ISACA, Norea 22 April 2026

KPMG. Make the Difference.

Agenda

01	Ontwikkelingen
02	Kader
03	Data
04	Platforms
05	Cyber security
06	Digital Omnibus
07	Praktisch

Ontwikkelingen

01

Compliancedruk neemt verder toe

Het juridische en regelgevende (L&R) landschap is complex en voortdurend in beweging.
De druk op organisaties om te voldoen aan wet- en regelgeving neemt toe, onder meer in verband met:

- Geopolitieke instabiliteit: Amerikaanse invloed vergroot
- Cyberdreigingen (IT & OT): (bijv. Odido), maar ook statelijke actoren
- Klimaatverandering: invloed op energievoorziening
- Digitalisering: AI disruptie al goed zicht- en voelbaar
- Persoonlijke aansprakelijkheid van bestuurders (bijv. NIS2)
- Strenger toezicht op wet- en regelgeving door toezichthouders, inclusief hogere boetes
- AI-geletterdheid, nu verplicht !

De realiteit hier en nu …. en in de toekomst

De traditionele scheiding tussen bedrijfsstrategie en geopolitiek bestaat niet meer:

Vroeger

Slechts een externe risicofactor

Nu

Bepaalt geopolitiek direct:

- Waar organisaties mogen opereren;
- Welke technologieën ze mogen ontwikkelen en gebruiken; en
- Hoe ze kapitaal inzetten.

Onzekere tijden

Geopolitical climate

Geopolitical wheather

Geopolitical climate

- Verschuiving machtsbalans en systeemverschuiving van unipolariteit naar multipolariteit
- Instabiliteit in het Midden Oosten
- Oplopende spanningen tussen China en US
- Aggressief Rusland
- **Intensieve digitalisering**
- **Toenemend gebruik van economische sancties, subsidies en industrie politiek door staten**

Geopolitical wheather

- Exportverboden en –controles op specifieke technologisch hoogwaardige producten
- Nieuwe regelgeving en industriepolitiek
- Oorlog in Gaza
- Aanvallen van Houthi-rebellen rond Rode Zee
- Uitbraak van covid-pandemie
- Kwetsbaarheden van just-in-time-toeleverketens
- Energieschokken
- **cyberhacks**

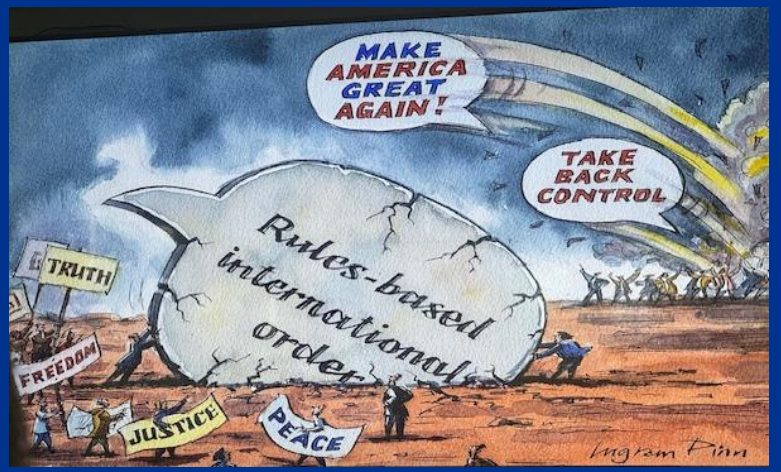
Geopolitieke risico's

Geopolitical risks

Einde van het globaliseringsdenken

De veronderstelling dat markten wereldwijd steeds meer geïntegreerd raken is ingestort. Staten zien economische middelen nu als **strategische assets**.

- Investeringsstromen
- Supply chains
- Data en technologie soevereiniteit
- Handelsbeleid
- Exportcontroles



Bron: S. Lindstrom

Supply chains en technologie als geopolitiek strijdtoneel

Supply chains worden nu beoordeeld op geopolitieke veerkracht, niet alleen kosten.

Technologie wordt beïnvloed door:

Data-lokalisatiewetten

AI-, Platform & Cyber regulering

Exportcontroles

Nationale veiligheidseisen

Fouten hierin kunnen leiden tot sancties of uitsluiting van markten.

Waarom bestaande organisatie-inrichting tekortschiet

Hoewel veel bedrijven geopolitieke risico's *monitoren*, doen ze dat via versnipperde, reactieve processen. Drie structurele fouten:

Geopolitiek wordt als plotselinge schok gezien.

Reactief

Afdelingen interpreteren signalen verschillend

Gesiloed

Focus op risicobeperking, niet op het benutten van kansen

Defensief

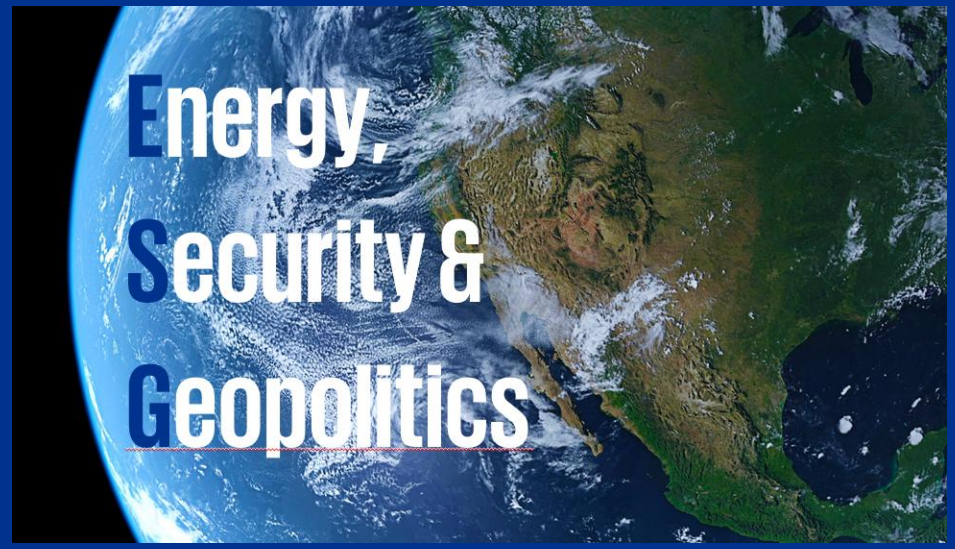
Einde van het globaliseringsdenken

Geopolitiek beïnvloedt bedrijfsvoering op fundamentele manieren:

Efficiëntiegedreven supply chains zijn strategisch kwetsbaar gebleken (bijv. Solvinity)

Productie en technologie worden steeds vaker gefriendshored of regionaal opgesplitst

R&D wordt geografisch gescheiden om aan lokale of regionale regelgeving te voldoen



Bron: S. Lindstrom

3 trends

1. Shift from working on the basis of rules (treaties) to working on the basis of power
2. Thinking in terms of security rather than economic logic (using economic means for political purposes; misusing strategic reserves, etc.)
3. Countries and companies need to work on resilience instead of just thinking about efficiency (e.g. building up stock, robust organization, backup in connection with cyber risks)

Recente ontwikkelingen

Nov 2025

Digitaal pakket Europese Commissie

Voorstel **Digitale Omnibus** over AI (COM(2025)836) en de **Digitale Omnibus** (COM(2025)837).
Doel: bestaande digitale regelgeving te vereenvoudigen en stroomlijnen, met name op het gebied van data, AI en gegevensbescherming. Dit om innovatie en concurrentiekracht te versterken zonder het beschermingsniveau voor persoonsgegevens en fundamentele rechten aan te tasten.

De Eerste Kamer benoemde voor het eerst in haar geschiedenis rapporteurs — een primeur — vanwege de omvang en complexiteit van de voorstellen en hun potentieel verstrekkende gevolgen.

Feb 2026

AI Act

Vanaf 2 februari gelden de eisen voor AI geletterdheid

Feb 2026

Rechtbank Den Haag

Rechtbank Den Haag bevriest twee overheids- ICT aanbestedingen t.w.v. EUR 3,3mrd. Grote cloud/ICT aanbieders wilden hun eigen leveringsvoorwaarden niet aanpassen. Oplossing via een tussenpersoon (distributeur) niet acceptabel.

Recente ontwikkelingen

Maa 2026

Overheidsaanbestedingen

Motie Boujdaini (D66) aangenomen door Tweede Kamer: Digitale soevereiniteit en strategisch autonomie moeten als expliciet criterium worden opgenomen in overheidsaanbestedingen.

Maa 2026

President Trump's Cyberstrategie for America

Cyberspace is Amerikaans territorium. ("*Cyberspace was born in America*." Wie draait op Amerikaanse infrastructuur, speelt op Amerikaans terrein, onder Amerikaanse regels.

Deregulering als aanval op het Europese model.
- "*We will fight the curtailment of free speech*": rechtstreekse verwijzing naar Europese regelgeving zoals de DSA (Digital Services Act) en AI Act - die de VS consequent framen als censuur en rem op innovatie.

"*We will streamline regulations globally*" en "*We will engage internationally ... to ensure norms and standards reflect our values*": de VS wil internationale regelgeving hervormen naar haar eigen standaard - wat een directe aanval is op de Europese aanpak van dataprivacy, AI-regulering, online platform en cybersecurity-normen.

AI en kritieke technologie zijn wapens, geen gedeelde goederen. De VS wil "superiority" handhaven. Buitenlandse AI die "censureert en surveilleert" moet worden tegengehouden - maar offensieve Amerikaanse AI-inzet is wél legitiem deel van de VS strategie.

Offensieve cyberoperaties zijn expliciet beleid. De VS behoudt zich het recht voor om buiten het cyber-domein te antwoorden op aanvallen. Europese systemen op Amerikaanse cloud of hardware zijn structureel blootgesteld, ook als collateral damage.

"*Move away from adversary vendors*". Het document waarschuwt voor Chinese technologie in kritieke infrastructuur. Dit document maakt ons alvast expliciet duidelijk dat Amerikaanse tech voor Europa ook als vijandig kan worden beschouwd.

Bron: J. Caudron

Buitenlandse wetgeving vs EU Rechtspraak

Toegang US veiligheidsdiensten tot vertrouwelijke klantgegevens

Veel Amerikaanse wetgeving

- Patriot Act
- FISA (Foreign Intelligence Surveilance Act 702)
- CLOUD Act (Clarifying Lawful Overseas Use of Data Act)

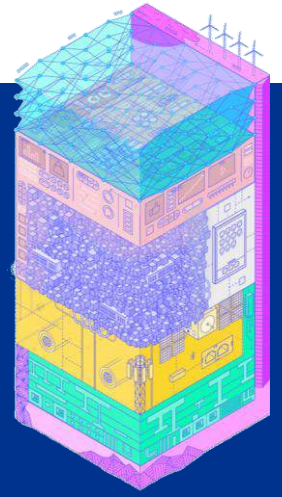
Potentiële toegang tot persoonsgegevens is beslissend geweest in EU Hof van Justitie beslissingen over mogelijkheid tot verstrekking naar derde landen (bijv. US)

• HvJ Schrems I (C-362/14 van 6 oktober 2015)
"Safe Harbour niet geldig"

• HvJ Schrems II (C-311/18 van 16 juli 2020) EU-US
"Privacy Shield niet geldig"

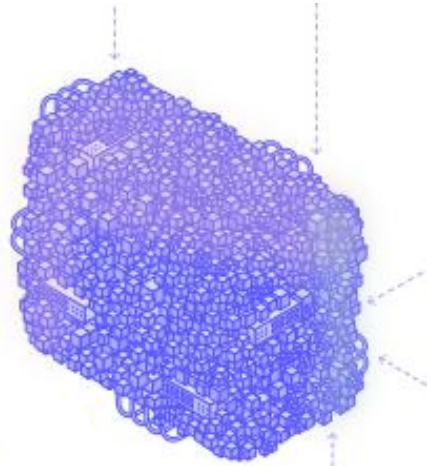
• Gerecht HvJ Latombe (T-553/23 van 3 september 2025)
"EU-US Data Privacy Framework is geldig"

Digitale soevereiniteit en data autonomie ontwikkelingen



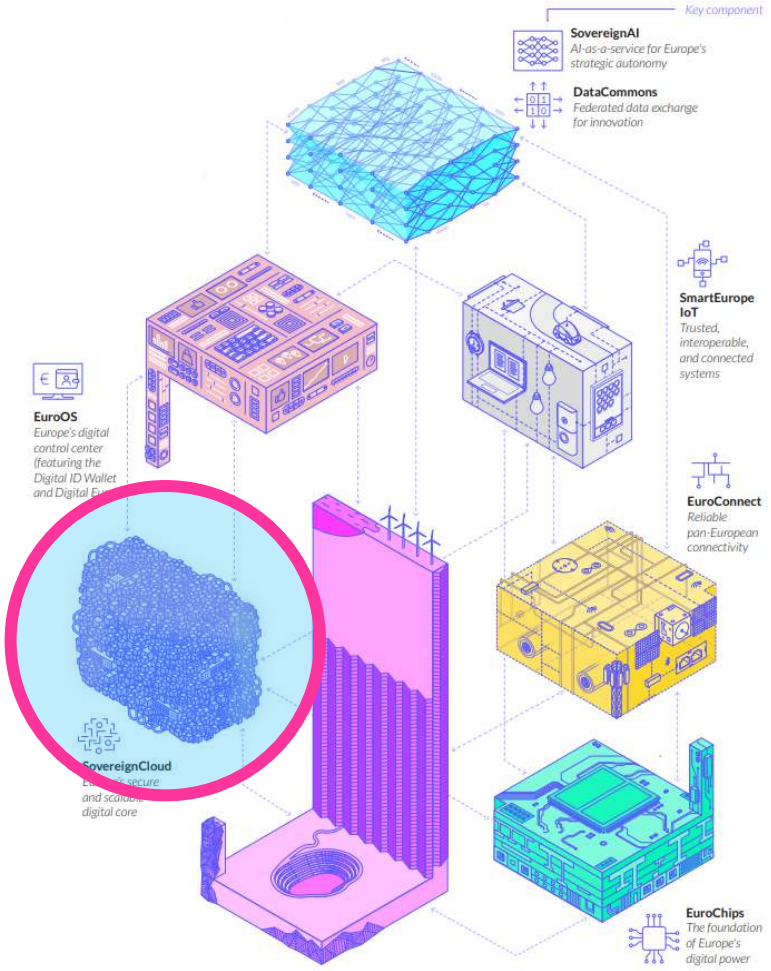
EuroStack is a European initiative and policy concept aimed at building a**sovereign, end-to-end European digital technology stack so that the EU is less dependent on non-European (especially U.S. and Chinese) technology providers**. It is not a single product or company, but a strategic vision and coordinated set of initiatives. Key goals include:

- **Digital sovereignty**: European control over critical digital infrastructure
- **Strategic autonomy**: Reducing reliance on foreign vendors for essential technologies
- **Resilience**: Protection against geopolitical risks (e.g. vendor ‘kill switches’)
- **Value-driven technology**: Ensuring alignment with EU values such as privacy, openness and sustainability



SovereignCloud
Europe’s secure and scalable digital core

Focus CloudNova case

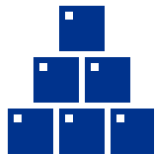


Source visuals: https://www.euro-stack.info/

Kader

02

Europese interne markt | De vier vrijheden



Vrij verkeer van goederen

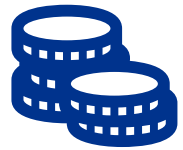
- Afschaffing van douanerechten en kwantitatieve beperkingen
- Verbod op maatregelen van gelijke werking
- Opheffing van materiële en technische belemmeringen

Vrij verkeer van personen

- EU-, EER- en Zwitserse burgers hebben het recht zich vrij te verplaatsen op het grondgebied van de Europese Unie, de Europese Economische Ruimte en Zwitserland
- Zowel voor burgers als voor werknemers

Vrij verkeer van diensten

- Vrijheid om een economische activiteit in een andere EU-lidstaat uit te oefenen
- Vrijheid om tijdelijk diensten te verrichten in andere lidstaten en tegelijkertijd in het land van oorsprong te blijven



Vrij verkeer van kapitaal

- Denk aan het openen van bankrekeningen in het buitenland, het kopen van aandelen in buitenlandse bedrijven, investeren waar het beste rendement te behalen valt en het kopen van onroerend goed in een ander land

Ontwikkeling van de Europese interne markt

1958

Common Market

Totstandkoming douane-unie, vrij verkeer van burgers en werknemers en de invoering van belasting over de toegevoegde waarde (BTW)

1987

Single European Act

Besluitvormingsmechanismen van de EER worden hervormd door invoering van stemming met gekwalificeerde meerderheid

1997

Amsterdam Treaty

Invoering van het Schengengebied waardoor grenscontroles verdwijnen en politiële en justitiële samenwerking tussen de lidstaten toeneemt

2007

INSPIRE Directive

De richtlijn verplicht overheidsinstanties in de EU tot het delen van milieugegevens in het ruimtelijke domein.

2010

Single Market I

Breed pakket aan voorstellen ter versteviging van de interne markt

2012

Single Market Act II

Vervolg op Single Market Act I, bestaande uit een reeks van 12 kernacties

2015

Digital Single Market

Initiatief ter versterking van de Europese digitale economie

2018

GDPR

Harmonisering van de privacyregelgeving van de lidstaten

Drie pilaren van Digital Single Market ('DSM')

In scope vandaag

01

Toegang

Betere toegang voor consumenten en bedrijven tot onlinegoederen en -diensten in heel Europa

- Regels voor grensoverschrijdende elektronische handel
- Betaalbare grensoverschrijdende pakketbezorging van hoge kwaliteit
- Voorkomen van ongerechtvaardigde geo-blocking
- Modern Europees kader voor auteursrechten

02

Omgeving

De juiste voorwaarden scheppen voor de bloei van digitale netwerken en diensten

- Media kader
- Geschikte telecomregels
- Regelgeving voor platforms en tussenpersonen
- Versterking van het vertrouwen in en de veiligheid van digitale diensten

03

Economie en samenleving

Het groeipotentieel van de Europese digitale economie maximaliseren

- Het bouwen van een Europese Data Economie
- Versterking van het concurrentievermogen door interoperabiliteit en normalisatie
- Een inclusieve e-samenleving

Overview of EU Legislation in the Digital Sector

Applicable law	Published in the Official Journal of the European Union
In negotiation	Proposal by the European Commission entered the legislative process.
Planed initiative	Mentioned by the European Commission as potential legislative initiative

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance
Digital Europe Programme Regulation, (EU) 2021/694	Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EEC) 1987/372	General Data Protection Regulation (GDPR), (EU) 2016/679	Database Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/881	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)	Unfair Contract Terms Directive (UCTD), (EEC) 1993/13	Technology Transfer Block Exemption, (EC) 2014/316	Satellite and Cable I Directive, (EEC) 1993/83	Common VAT system, (EC) 2006/112, 2022/0407(CNS)
Horizon Europe Regulation, (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation, (EU) 2021/523	Radio Spectrum Decision, (EC) 2002/676	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Community Design Directive, (EC) 2002/6, 2022/0391(COD)	Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment, (EU) 2019/713	European Standardization Regulation, (EU) 2012/1025	E-commerce Directive, (EC) 2000/31	Company Law Directive, (EU) 2017/1132, 2023/0089(COD)	Information Society Directive, (EC) 2001/29	Payment Service Directive 2 (PSD2), (EU) 2015/2366, 2023/0209(COD)
Regulation on a pilot regime distributed ledger tech. market, (EU) 2022/858	Connecting Europe Facility Regulation, (EU) 2021/1153	Broadband Cost Reduction Directive, (EU) 2014/61, 2023/0046(COD)	Regulation on the free flow of non-personal data, (EU) 2018/1807	Enforcement Directive (IPR), (EC) 2004/48	NIS 2 Directive, (EU) 2022/2555	Regulation on terrorist content online, (EU) 2021/784	Radio Equipment Directive (RED), (EU) 2014/53	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU) 2019/1020	Audio-visual Media Services Directive (AVMSD), (EU) 2010/13	Digital Operational Resilience Act (DORA Regulation), (EU) 2022/2554
	Regulation on High Performance Computing Joint Undertaking, (EU) 2021/1173	Open Internet Access Regulation, (EU) 2015/2120	Open Data Directive (PSI), (EU) 2019/1024	Directive on the protection of trade secrets, (EU) 2016/943	Information Security Regulation, 2022/0084(COD)	Temporary CSAM Regulation, (EU) 2021/1232, 2022/0155(COD)	eIDAS Regulation, (EU) 2014/910, 2021/0136(COD)	Directive on Consumer Rights (CRD), (EU) 2011/83	P2B Regulation, (EU) 2019/1150	Portability Regulation, (EU) 2017/1128	Crypto-assets Regulation (MiCA), (EU) 2023/1114
	Regulation on Joint Undertakings under Horizon Europe, (EU) 2021/2085, 2022/0033(NLE)	European Electronic Communications Code Directive (EECC), (EU) 2018/1972	Data Governance Act (DGA Regulation), (EU) 2022/868	Standard essential patents, 2023/0133(COD)	Cybersecurity Regulation, 2022/0085(COD)	E-evidence Regulation, 2018/0108(COD)	Regulation for a Single Digital Gateway, (EU) 2018/1724	e-invoicing Directive, (EU) 2014/55	Vertical Block Exemption Regulation (VBER), (EU) 2022/720	Satellite and Cable II Directive, (EU) 2019/789	Digital euro, 2023/0212 (COD)
	Decision on a path to the Digital Decade, (EU) 2022/2481	Roaming Regulation, (EU) 2022/612	ePrivacy Regulation, 2017/0003(COD)	Design Directive, 2022/0392(COD)	Cyber Resilience Act, 2022/0272(COD)	Digitalization of travel documents	General Product Safety Regulation, (EU) 2023/988	Geo-Blocking Regulation, (EU) 2018/302	Digital Market Act (DMA Regulation), (EU) 2022/1925	Copyright Directive, (EU) 2019/790	Financial Data Access Regulation, 2023/0205 (COD)
	European Chips Act (Regulation), 2022/0032(COD)	Regulation on the Union Secure Connectivity Programme, (EU) 2023/588	European Data Act (Regulation), 2022/0047(COD)	Compulsory licensing of patents, 2023/0129(COD)	Cyber Solidarity Act (Regulation), 2023/0109(COD)		Machinery Regulation, (EU) 2023/1230	Digital content Directive, (EU) 2019/770	Regulation on distortive foreign subsidies, (EU) 2022/2560	European Media Freedom Act, 2022/0277(COD)	Payment Services Regulation, 2023/0210(COD)
	European critical raw materials act (Regulation), 2023/0079(COD)	.eu top-level domain Regulation, (EU) 2019/517	European Health Data Space (Regulation), 2022/0140(COD)				AI Act (Regulation), 2021/0106(COD)	Directive on certain aspects concerning contracts for the sale of goods, (EU) 2019/771	Horizontal Block Exemption Regulations (HBER), (EU) 2023/1066, (EU) 2023/1067		Revising of the late payments Directive
	Establishing the Strategic Technologies for Europe Platform (STEP), 2023/0199(COD)	New radio spectrum policy programme (RSPP 2.0)	Regulation on data collection for short-term rental, 2022/0358(COD)				Eco-design Regulation, 2022/0095(COD)	Digital Services Act (DSA Regulation), (EU) 2022/2065	Platform Work Directive, 2021/0414(COD)		
		Telecoms Act / Fair Share Initiative	Harmonization of GDPR enforcement 2023/0202(COD)				AI Liability Directive, 2022/0303(COD)	Right to repair Directive, 2023/0083(COD)	Single Market Emergency Instrument (SMEI), 2022/0278(COD)		
			Interoperable Europe Act, 2022/0379(COD)					Political Advertising Regulation, 2021/0381(COD)			
			Access to vehicle data, functions and resources					Multimodal digital mobility services (MDMS)			
			GreenData4all					Consumer protection: strengthened enforcement cooperation			
								Consumer rights: adapting ADR to digital markets			

Bron: A dataset on EU legislation for the digital world', Kai Zenner, J. Scott Marcus, Kamil Sekut and Hèctor Badenes Rodríguez published by Bruegel.

De EU Digitale wetten

UPDATED

Research&Innovatie:
3 Adopted

Industry policy:
9 Adopted
1 in negotiation
1 proposed

Connectiviteit:
8 Adopted
2 proposed

Data & Privacy:
10 Adopted
2 in negotiation
2 proposed

Intellectual eigendom:
4 Adopted
3 in negotiation

Cybersecurity:
4 Adopted
3 in negotiation

Law enforcement:
7 Adopted
2 in negotiation
1 proposed

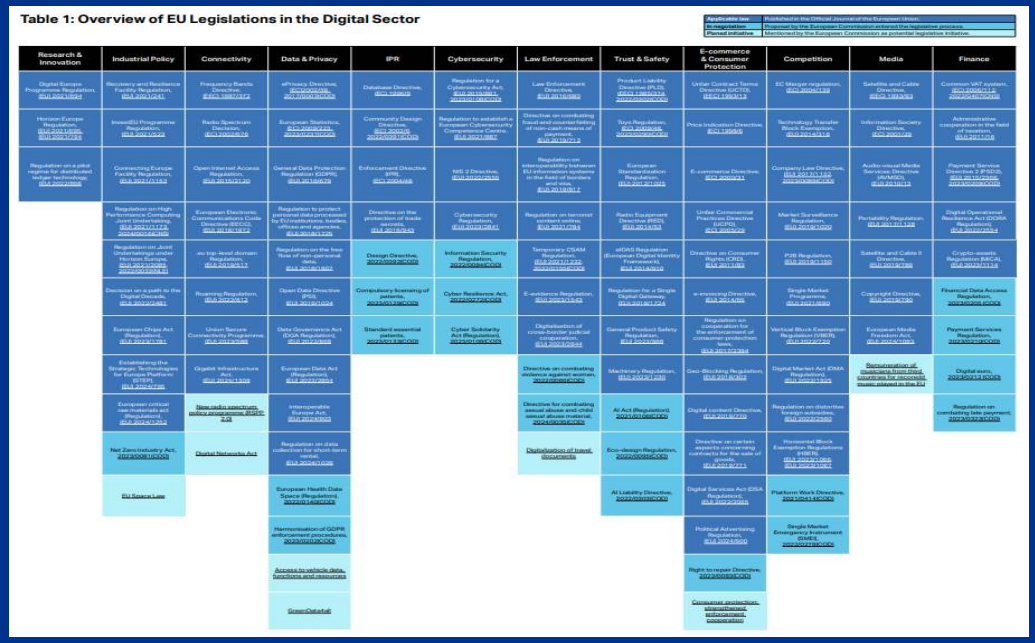
Trust&Safety:
8 Adopted
3 in negotiation

E-commerce & consumerprotection:
12 Adopted
1 in negotiation
1 proposed

Mededinging:
10 Adopted
2 proposed

Media:
7 Adopted
1 proposed

Finance:
5 Adopted
4 proposed



Februari/ Maart 2024
DSA/DMA

Augustus 2024
AI Act

Oktober 2024
NIS2

Januari 2025
DORA

September 2025
Data Governance Act

Augustus 2026
EU Digital Omnibus AI Act

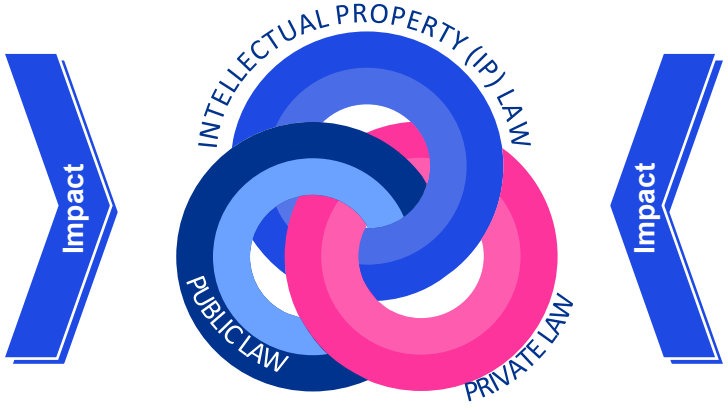
September 2026
- Cyber Resilience
- Cyberbeveiligingswet

December 2026
eIDAS

Overzicht Europese en nationale digitale wet en regelgeving. VWEU en CFREU zijn de fundamenten

Verdrag betreffende de werking van de EU (VWEU)

Bepaling van de beginselen en doelstellingen van de EU, zoals de Europese interne markt, innovatie, eerlijke concurrentie en consumentenbescherming



Handvest van de grondrechten van de EU (CFREU)

Juridisch bindend document dat de belangrijkste persoonlijke vrijheden en grondrechten voor EU-burgers bundelt

EU Digital Market Strategie						Nederlandse DDigitale Strategie	
Niet wetgevende initiatieven	Wetgevende initiatieven					Wetgevende initiatieven	
EU Data Spaces	DSA/DMA	Data Act	CSA,CRA	eiDAS	AI Act	Wdo	Woo
AVG						(U)AVG	
Bestaande wetgeving (zoals de Archiefwet)							

Data

03

Spannende ontwikkeling: de notie van "eigendom" verschuift verder door de waarde van data

Volgens John Deere zijn niet de boeren (die de tractoren hebben aangeschaft en gebruiken), maar is John Deere de eigenaar van de tractoren (ook al heeft de boer het gekocht):

*'John Deere---the world's largest agricultural machinery maker --- told the Copyright Office that farmers **don't own their tractors**. Because computer code snakes through the DNA of modern tractors, farmers receive "an implied license for the life of the vehicle to operate the vehicle."*

Bron: Wired.com April 2015 'We Can't Let John Deere Destroy the Very Idea of Ownership'

De Europese Data Strategie als startpunt

2020 | Europese Data Strategie

Strategie om van de EU een leider te maken in een datagedreven samenleving, om zo het onbenutte potentieel van data te ontsluiten.

2022 | Data Governance Act

Regels om de processen en structuren voor (vrijwillig) delen van data door bedrijven, individuen en overheden te faciliteren.

2024 | Data Act

Op 11 januari 2024 in werking getreden. Regels voor het gebruik van en de toegang tot gegevens die in alle economische sectoren van de EU zijn gegenereerd.

2024 | Interoperable Europe Act

Op 11 April 2024 in werking getreden. Versterkt grensoverschrijdende interoperabiliteit en samenwerking in de publieke sector in de hele EU.

2024 | Artificial Intelligence Act

Op 1 augustus 2024 in werking getreden. Introductie van procedurele en materiële eisen voor AI-systemen.

2024 | European Health Data Space

Treedt naar verwachting later dit jaar in werking. Schetst kaders voor (grensoverschrijdend) primair en secundair gebruik van data in de zorgsector.

? | ePrivacy Regulation

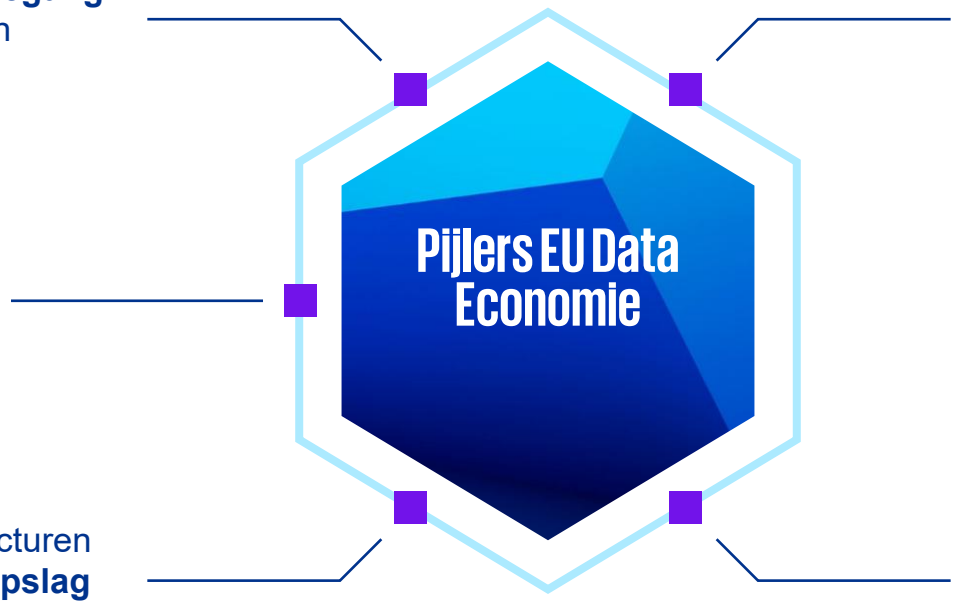
Introductie van aanvullende eisen met betrekking tot de verwerking van persoonsgegevens

Pijlers van de Europese Data Economie

Vaststelling van duidelijke en eerlijke **regels** voor de **toegang** tot en het **hergebruik** van **gegevens**

Bundeling van krachten in Europese **cloudcapaciteit**

Investering in normen, instrumenten en infrastructuren voor de **verwerking** en **opslag** van **gegevens**



Bundeling van Europese gegevens in sleutelsectoren, met gemeenschappelijke en interoperabele **dataruimten** voor de hele EU

Gebruikersrechten, instrumenten en vaardigheden geven, zodat zij de volledige **controle** over hun **gegevens** behouden

De Data Act heeft ten doel de toegang tot en het gebruik van data te vergemakkelijken

"Om tegemoet te komen aan de behoeften van de digitale economie en om belemmeringen voor een goed functionerende interne datamarkt weg te nemen, moet er een geharmoniseerd kader worden vastgesteld [...]"

Tijdige toegang tot gegevens

Ter beschikking stellen van gegevens onder eerlijke, redelijke en niet-discriminerende voorwaarden

Overheidsorganisaties hebben toegang tot gegevens indien er sprake is van een uitzonderlijke noodzaak, zoals algemene noodsituaties

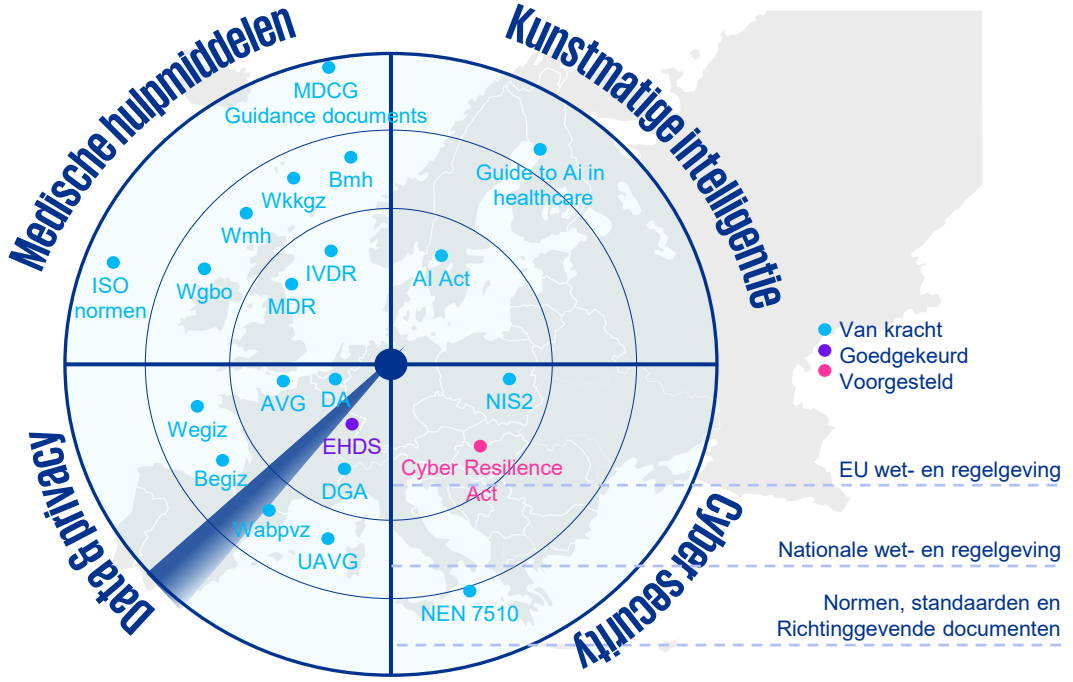
Gemakkelijk overstappen tussen dataverwerkingsdiensten en interopabiliteit verbeteren

De Data Act moet worden bezien in samenhang met andere wetgevingsinitiatieven in het kader van de Europese Datastrategie

Horizontale wetgeving
De Data Act is **horizontale wetgeving** die voorziet in basisregels voor alle sectoren.

Sectorale wetgeving
De toegang tot en het gebruik van data zijn ook op **sectoraal niveau** in verschillende mate gereguleerd. De Data Act zal bestaande wetgeving niet wijzigen, maar toekomstige wetgeving zal worden afgestemd op de horizontale beginselen van de Data Act.

Interactie tussen Data Act en (aanpalende) wetgeving
Data Act sluit aan op en hangt nauw samen met (toekomstige) Europese en nationale wet- en regelgeving zoals de Algemene Verordening Gegevensbescherming ('AVG') en sector specifieke wetgeving zoals de MDR en Wet op de geneeskundige behandelingsovereenkomst ('Wgbo')



De Data Act reguleert onder andere gegevensdeling tussen bedrijven onderling (B2B), tussen bedrijven en consumenten (B2C) en tussen bedrijven en overheden (B2G)

Verbonden producten en gerelateerde diensten

Het delen van gegevens tussen bedrijven en consumenten in het kader van IoT

B2B gegevensdeling

Het delen van gegevens tussen bedrijven

Oneerlijke contractuele bedingen

Oneerlijke bedingen met betrekking tot de toegang tot en het gebruik van gegevens

B2G gegevensdeling

Het delen van gegevens tussen bedrijven en overheden op grond van een uitzonderlijke noodzaak

Overstappen

Overstappen naar andere dataverwerkingsdiensten

Internationale overheidstoegang

Internationale overheidstoegang en overdracht van niet-persoonsgebonden gegevens

Interoperabiliteit

Essentiële eisen inzake interoperabiliteit van gegevens

Slimme contracten

Essentiele eisen met betrekking tot slimme contracten

Verbonden producten en gerelateerde diensten

De Data Act geeft een kader voor verbonden producten en gerelateerde diensten

01

"*Dergelijke gegevens zijn potentieel* ***waardevol voor de gebruiker en ondersteunen innovatie*** *en de ontwikkeling van digitale en andere diensten die het milieu, de gezondheid en de circulaire economie beschermen* […]"

02

Het doel van de Data Act is om **gebruikers van verbonden producten** (bedrijven of personen die een dergelijk product bezitten, leasen of huren) **meer controle** te geven over de gegevens die ze genereren, terwijl ze prikkels behouden voor degenen die investeren in datatechnologieën.

03

Voorbeelden van verbonden producten zijn "*voertuigen, gezondheids- en lifestyleapparatuur, schepen, vliegtuigen, huishoudelijke apparatuur en consumptiegoederen, medische en gezondheidsapparatuur of landbouw- en industriële machines*."

Wat zijn verbonden producten en gerelateerde diensten?

Verbonden product

- Een product dat gegevens over het gebruik of de omgeving ervan verkrijgt, genereert of verzamelt;
- En deze gegevens doorgeeft via een elektronische-communicatiedienst, fysieke verbinding of apparaattoegang;
- Waarvan de hoofdfunctie niet het opslaan, verwerken of doorgeven van gegevens namens anderen dan de gebruiker is.

Gerelateerde dienst

Een gerelateerde dienst is een digitale dienst, anders dan een elektronische communicatiedienst, die:

- Op het moment van aankoop, huur of lease zodanig met het product is verbonden dat het product zonder deze dienst een of meerdere functies niet kan uitvoeren; of
- Die later door de fabrikant of een derde met het product wordt verbonden om functies aan het product toe te voegen of functies van het product aan te passen of te updaten.

Voorbeeld: Verbonden producten en gerelateerde diensten binnen de zorgsector

Gezondheids- en lifestyleapps
Waaronder fitness, dieet- en algemene gezondheidsapps en lifestyletrackers.

Implanteerbare medische hulpmiddelen
Zoals pacemakers, neurostimulators,binnenoorprotheses etc.

Remote patient monitoring
Thuismonitoring of monitoring op afstand met behulp van wearables of medische hulpmiddelen zoals bloeddrukmeters.

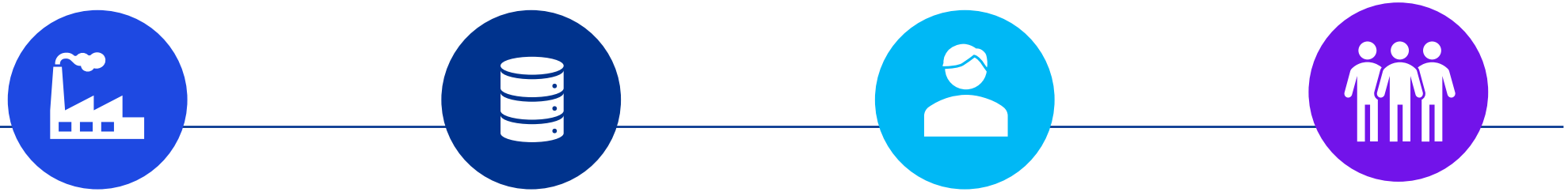
Medische hulpmiddelen voor diagnostische doeleinden
Waaronder MRI-scanners, röntgenapparaten etc.

Slimme sensoren
Slimme pleisters en sensoren voor valdetectie, dwaaldetectie, vitale functie monitoring, geluidsdetectie, persoonsalarmering etc.

In-vitro diagnostische medische hulpmiddelen
Apparatuur, toestellen en systemen voor in-vitro-onderzoek van menselijk lichaamsmateriaal.

Op wie is de Data Act van toepassing?

Verbonden producten dienen zodanig te zijn ontworpen en vervaardigd en gerelateerde diensten dienen zodanig te zijn ontworpen en verleend dat gegevens **standaard, gemakkelijk, veilig, kosteloos en in een allesomvattend, gestructureerd, algemeen en machineleesbaar formaat, rechtstreeks toegankelijk zijn** voor de gebruiker.



Verkoper, verhuurder, leasegever of leverancier

De **verkoper, verhuurder of leasegever** van een verbonden product en de **leverancier** van een gerelateerde dienst hebben een informatieplicht.

Bijvoorbeeld: **fabrikanten, distributeurs en importeurs van medische hulpmiddelen, ICT-leveranciers**

Gegevenshouder

De **gegevenshouder** is verplicht de gebruiker rechtstreeks toegang te geven tot gegevens van het verbonden product of gerelateerde dienst.

Bijvoorbeeld: **fabrikanten van medische hulpmiddelen, ICT-leveranciers, zorgaanbieders**

.

Gebruiker

De **gebruiker** heeft het recht om gegevens te delen met derden. De **gebruiker** mag de gegevens niet gebruiken om een concurrerend verbonden product of gerelateerde dienst te ontwikkelen.

Bijvoorbeeld: **patiënten en consumenten, zorgaanbieders en individuele zorgprofessionals**

Derde

De **derde** mag de gegevens alleen gebruiken voor de doeleinden die met de gebruiker zijn overeengekomen.

Bijvoorbeeld: **zorgaanbieders en individuele zorgprofessionals**

De Data Act hangt nauw samen met de AVG, AI Act en de MDR

Data Act	AVG	AI Act	MDR
Verkoper, verhuurder, leasegever van verbonden producten	Verwerkingsverantwoordelijke	Aanbieder	Fabrikant
Leverancier van gerelateerde diensten	Verwerker	Gebruikersverantwoordelijke	Distributeur
Gegevenshouder	Betrokkene	Distributeur	Importeur
Gebruiker		Importeur	Gemachtigde
Derde		Gemachtigde	

Let op:

- Gebruiker ≠ betrokkene in de zin van de AVG
- Gegevenshouders ≠ verwerker in de zin van de AVG. Enkel verwerkingsverantwoordelijken.
- Verkoper, verhuurder of leasegever kan tevens de fabrikant zijn
- De gegevenshouder kan de fabrikant van het verbonden product zijn, maar ook een andere partij

Verplichtingen voor verkopers, verhuurders, leasegevers en leveranciers

Verkopers, verhuurders, leasegevers en leveranciers hebben op grond van de Data Act onder andere de volgende verplichtingen:

1. Verbonden producten dienen zodanig te zijn ontworpen en vervaardigd, en gerelateerde diensten dienen zodanig te zijn **ontworpen** en verleend, dat de (product)gegevens onder andere gemakkelijk, **veilig, kosteloos, in een algemeen gebruikt en machineleesbaar formaat, rechtstreeks toegankelijk** zijn voor de gebruiker.
2. Verkopers, verhuurders of leasegevers van een verbonden product en de leveranciers van een gerelateerde diensten hebben een **informatieplicht**.

Verplichtingen en rechten van gegevenshouders

Gegevenshouders hebben op grond van de Data Act onder andere de volgende rechten en verplichtingen:

1. Gegevenshouders **verstrekken** op verzoek gebruikers of derde(n) eenvoudig beschikbare gegevens (inclusief metagegevens). Indien technisch mogelijk, gebeurt deze terbeschikkingstelling **continu** en in **realtime**.
2. Gegevenshouders mogen het gebruikers of derde(n) **niet onnodig moeilijk maken** om rechten uit te oefenen.
3. De gegevenshouder neemt voorafgaand aan de bekendmaking van bedrijfsgeheimen alle noodzakelijke maatregelen om de **vertrouwelijkheid te waarborgen**. De gegevenshouder mag het delen van bedrijfsgeheimen tegenhouden of opschorten wanneer de gebruiker zich niet aan deze maatregelen houdt.
4. Indien de gebruiker niet het datasubject is, verstrekt de gegevenshouder alleen persoonsgegevens wanneer er een **geldige rechtsgrond** is.
5. Gegevenshouders mogen geen **niet-persoonsgebonden gegevens beschikbaar stellen aan derden** voor andere doeleinden dan de uitvoering van de overeenkomst met de gebruiker.

Verplichtingen en rechten van gebruikers en derden

Gebruikers en derden hebben op grond van de Data Act onder andere de volgende rechten en verplichtingen:

1. Gebruikers en derden kunnen gegevenshouders **verzoeken eenvoudig beschikbare gegevens (inclusief metagegevens)** ter beschikking te stellen.
2. Gebruikers en derden mogen niet de gegevens gebruiken om een product te ontwikkelen dat **concurreert** met het verbonden product.
3. Gebruikers en derden dienen de gegevens te gebruiken op een wijze die **niet negatieve gevolgen** hebben voor gegevenshouders.
4. Gebruikers en derden mogen **geen dwangmiddelen gebruiken of misbruik maken** van leemten in de technische infrastructuur van gegevenshouders
5. Gebruikers en derden nemen maatregelen om **bedrijfsgeheimen te beschermen**.

Wat als partijen het onderling niet met elkaar eens zijn?

Indien partijen het onderling niet met elkaar eens zijn kunnen de volgende routes worden bewandeld:

Rechterlijke instantie

Een klacht indienen bij de bevoegde autoriteit

Voorleggen aan een geschillenbeslechtingsorgaan

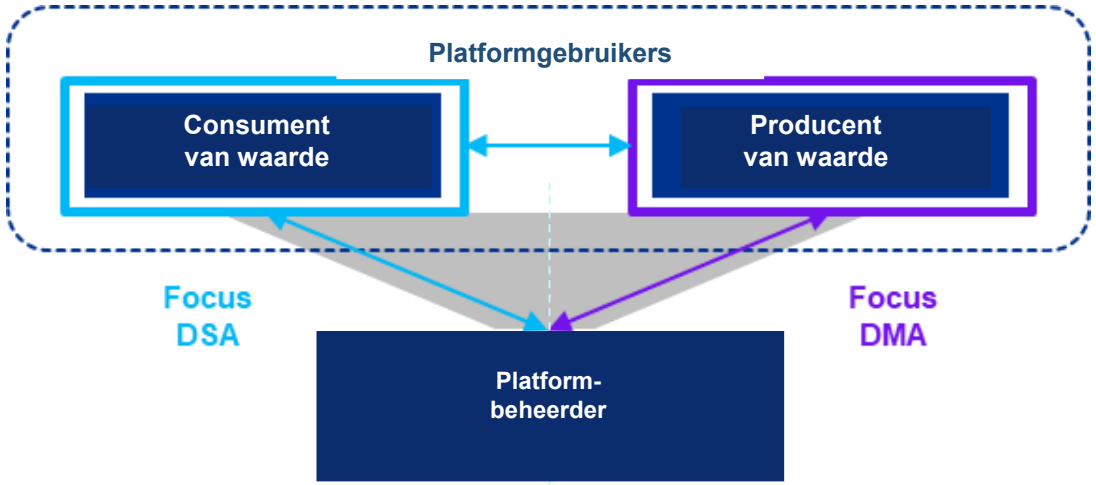
Belangrijke aandachtspunten

- De Data Act doet geen afbreuk aan de rechten van datasubjecten op grond van de AVG.
- De verplichtingen ten aanzien van verbonden producten en gerelateerde diensten zijn niet van toepassing op micro- en kleine ondernemingen.
- Contractuele bepalingen die de gebruiker benadelen zijn niet bindend voor de gebruiker.

Platforms

04

Digital Services Act (DSA) en Digital Markets Act (DMA)



De Digital Services Act (DSA)

richt zich voornamelijk op de bescherming van de belangen van consumenten en waardecreërende partijen op online intermediairs en platforms. Creëert ook een krachtig transparantiekader en een duidelijk verantwoordingskader voor online platforms.

De Digital Markets Act (DMA)

stelt een reeks nauw gedefinieerde objectieve criteria vast om een groot online platform te kwalificeren als een zogenoemde “gatekeeper”. De DMA bevat regels die gatekeeper-onlineplatforms reguleren en is vooral gericht op het beschermen van de belangen van waardecreërende producenten op het platform.

> *Europese Commissie: De auditverplichting geeft tanden aan de Digital Services Act-verordening en zal naar verwachting door andere toezichthouders wereldwijd worden overgenomen*

As of 2025, 23 Very Large Online Platforms and 2 Search Engines have a yearly external audit obligation under the DSA

The DSA applies to all providers of intermediary services offering their services to users established or located in the EU. A specific group of those, i.e., Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) that individually reach 45+ million active monthly users in the EU, have a yearly external audit obligation to undergo an assessment for compliance with the DSA.

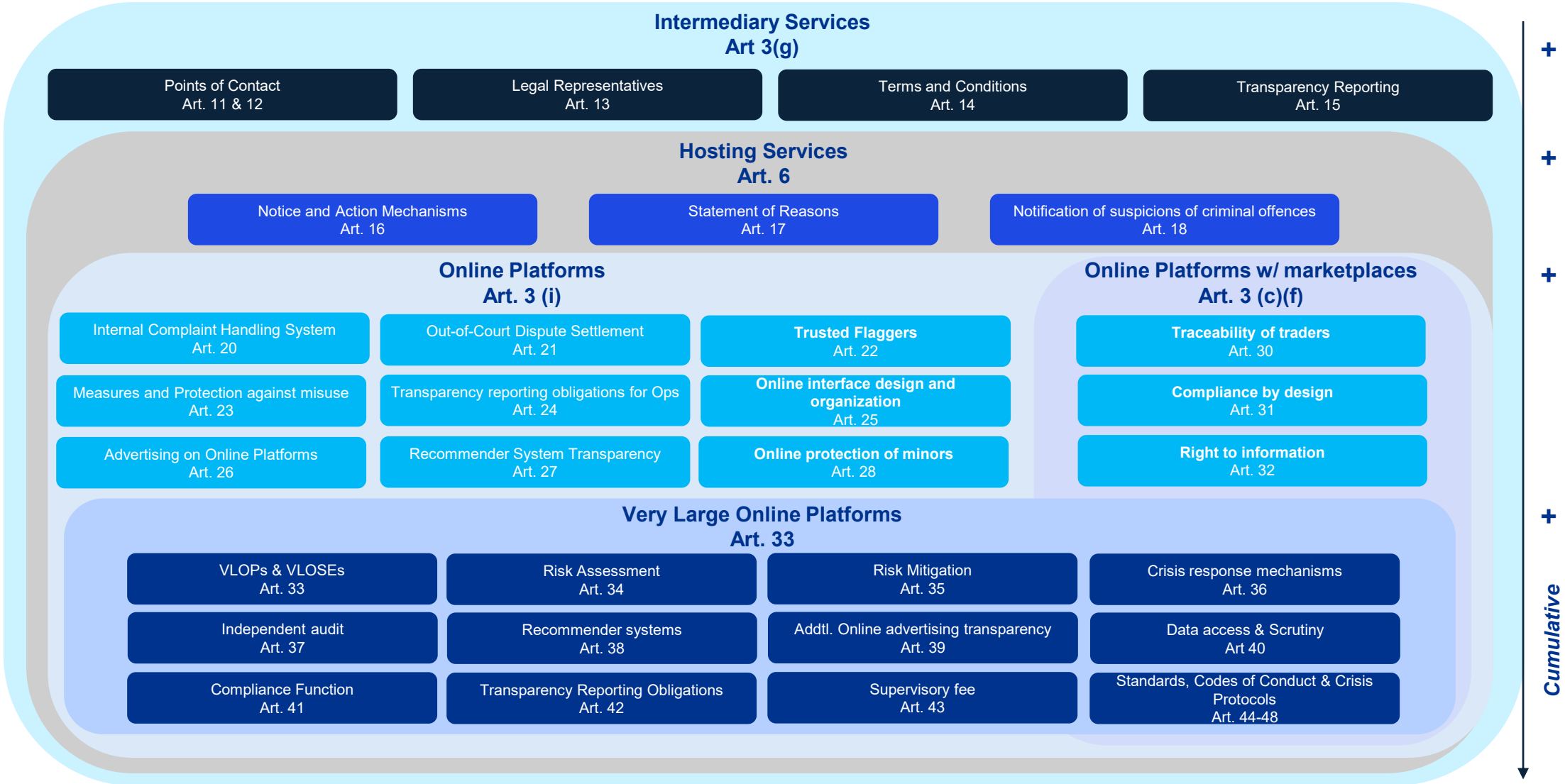
- In 2023, 17 online platforms qualified as VLOPs, and 2 search engines qualified as VLOSEs and had an audit obligation over audit year 2023/2024.
- In 2024, 6 additional VLOPs were designated as such under the DSA and have an audit obligation over audit year 2024/2025.

Designated as VLOP in 2024 (First DSA audit report in 2025)

★ Temu (designated as of 31 May 2024) and XNXX.com (designated as of 10 July 2024) did not publish a DSA audit report as of December 2025 and were therefore not included in this publication.

★ TikTok is a social media platform as well as a marketplace platform.

Online marktplaatsen moeten aan tenminste 19 artikelen voldoen



DSA audit opinions improved modestly in 2025 with fewer negative findings, but overall conclusions remain constrained by EC investigations and inconsistent testing

Key Insights

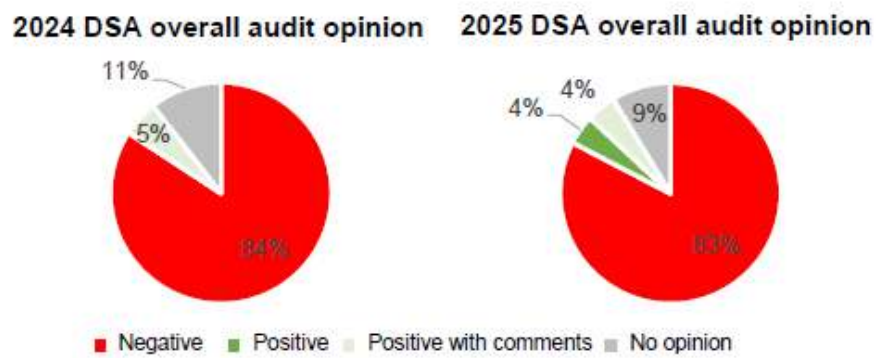
Overall trend compared to audit report year 2024:

- **In the audit report year 2024, all audit reports contained remarks:** remarks ranged from 'positive-with-comments' to 'negative' opinions or disclaimers.
- **Overall, the opinions in the audit report year 2025 were slightly more optimistic:** 1 VLOP (Stripchat) received a fully 'positive' opinion, 1 VLOP (Snapchat) received a 'positive-with-comments' opinion, and 19 VLOPs received 'negative' opinions. For Facebook and Instagram, no overall opinion was issued due to the significant number of ongoing European Commission (EC) investigations.
- **Decrease in 'negative' opinions on obligation level:** Compared to the audit report year 2024, the audit report year 2025 shows an increase of 'positive' opinions (7% increase), a slight reduction of 'positive-with-comments' opinions (2% decrease) while 'negative' opinions are almost halved (from 11% to 6%).
- **Overview of audit opinions:** Unlike audit report year 2024, in audit report year 2025, most auditors included an overall table by obligation in the audit report.

Key insights:

- We observed that X (formerly Twitter) received only 'positive' or 'positive-with-comments' opinions at the obligation level. Nevertheless, an overall 'negative' opinion was issued because of the volume of ongoing EC investigations. In contrast, for Facebook and Instagram, the same factor led auditors to refrain from issuing an overall opinion.
- For three VLOPs, the overall audit opinion was not explicitly stated in the report but inferred from obligation-level opinions (Snapchat: 'positive with comments'; Stripchat: 'positive'; Pornhub: 'negative')
- Testing approach: The disclosure of the applied testing methodology was inconsistent across the reports. While some reports included a table detailing the methodology, others did not consistently specify the testing approach for each obligation. Across most online platforms, the testing approach varied by obligation and ranged from control-based to substantive or mixed methods. Two platforms that stood out:
  - Booking.com: Primarily substantive testing was applied.
  - Zalando: Although controls were frequently implemented, they were never deemed sufficient to support an audit opinion. Consequently, either a substantive or mixed testing approach was applied.

Key Graph



Note: For 4 VLOPs, audit report year 2025 was the first year under an obligation to perform an external audit.

In 2025 verschoof Wikipedia naar het hoogste aandeel negatieve auditopinies, terwijl Stripchat en Snapchat geen negatieve opinies hadden

Kerninzichten

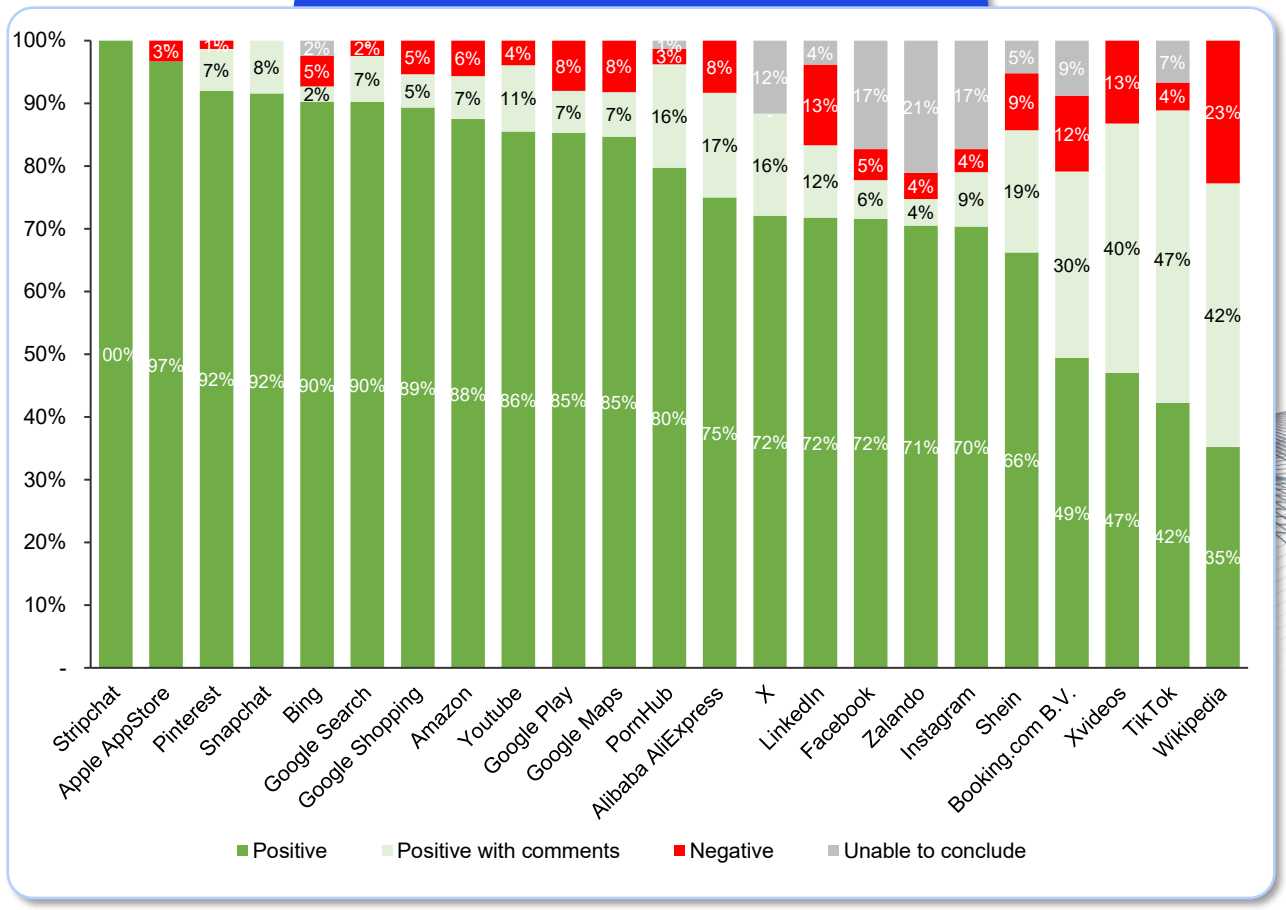
Kerninzichten

- **Verschuiving in het totaal aan 'negative'-opinies**: in het auditrapportjaar 2024 was Wikipedia de enige VLOP zonder 'negative'-opinies. In auditrapportjaar 2025 heeft het het hoogste percentage 'negative' auditopinies, wat een significante verandering markeert.
- **VLOPs zonder totaal 'negative'-opinie:** Stripchat en Snapchat vallen op als de enige VLOPs zonder 'negative'-opinies.
- **Totaal 'Geen conclusie mogelijk'-opinies:** Zalando, Facebook en Instagram hebben het hoogste percentage 'Geen conclusie mogelijk'-opinies.
  - Voor Facebook en Instagram komt dit voornamelijk door lopende onderzoeken van de Europese Commissie.
  - Voor Zalando gaven auditors aan dat er onvoldoende bewijs was om een opinie te vormen.

Aanvullende details

- **Opniecategorieën:** Het overzicht toont percentages van opinies die zijn geclassificeerd als:
  - 'Positief', 'Positief met opmerkingen', 'Negatief' en 'Geen conclusie mogelijk' (door onderzoeken of onvoldoende bewijs).
  - Voor Stripchat en Wikipedia werden opinies in eerste instantie op artikelniveau gegeven en voor deze analyse op dezelfde manier toegepast op elke onderliggende verplichting.
  - Sommige auditors gebruikten aanvullende subcategorieën (bijv. 'Positive with comments but remediated during audit period'), maar voor deze deep dive zijn alle opinies gegroepeerd in de drie hoofdcategorieën.

Kernfiguur



Cyber security

05

Ontwikkeling van de EU Cybersecurity Strategy

2016

NIS 1

Beveiligingsverplichtingen voor aanbieders van essentiële diensten, waaronder aanbieders in de financiële sector.

2019

Cybersecurity Act

EU-brede regels voor cyberbeveiligings certificering. Meer bevoegdheden en middelen voor ENISA.

2020

EU Cybersecurity Strategie

De Europese Commissie presenteerde eind 2020 een nieuwe EU-cyberbeveiligingsstrategie. Het doel is essentiële diensten beter te beschermen.

2022

NIS2

Breidt verplichtingen uit om de cyberbeveiligingscapaciteit te vergroten.

2025

FS: DORA

Operationele weerbaarheid voor financiële instellingen en ICT-derdepartijdienstverleners

Hoe verhouden Cybersecurity en Data&Privacy wet en regelgeving zich tot elkaar?

Cybersecurity

Regulation

DORA
Operational resilience within the financial sector.

Cyber Resilience Act
Cybersecurity requirements for products with digital elements

Cybersecurity Act
Mandating ENISA and further allocation of resources and powers.

Cyber Solidarity Act
Establish European cybersecurity shield

Directive

NIS2
Network and information security requirements

Further policies and initiatives

Cyber Diplomacy Toolbox
Harmonization and unified approach to cyber policy issues

European Cyber Defense Policy
Strengthen collaboration military/civilian cyber communities

European cyber strategy

- **Protecting Europe from cyber attacks**
- **Integrated approach with all stakeholders**
- **Creation of European cyber security center**
- **Stimulation of research and development**
- **International cooperation and common standards and guidelines**
- **Integration of cybersecurity into all aspects of business**
- **Enforcement of regulatory frameworks and laws.**

Data & Privacy

Regulation

GDPR
Rules for processing personal data

Data Act
Measures for a fair and innovative data economy

Digital Services Act
Legal framework on e-commerce to be updated

Directive

ePrivacy Regulation
Protection of personal data in electronic communications

Digital Markets Act
Regulation of online platforms

Data Governance
Facilitate data sharing across sectors

Further policies and initiatives

Data Spaces
Initiative to facilitate data exchange within EU

- The EU data strategy seeks a unified market for data, where data is shared openly and securely.

Other

AI Act
Rules regarding products with AI

EU Strategic Compass

CER Directive
Strengthening the resilience of critical infrastructure.

European Chips Act
Improve competitiveness and resilience with regard to chips.

Digital Omnibus

06

EU Digital Omnibus

- Digitale wetgevingskader van de EU vereenvoudigen en te moderniseren en administratieve lasten te verminderen (met name MKB).

Doel

- Kostenbesparing
- Minder administratieve lasten (reductie 25%, en SME 35%)
- Stimuleren van innovatie

Beoogde impact

- Het voorstel wijzigt en harmoniseert bestaande regelgeving, waaronder de AVG, Data Act, AI Act, ePrivacy Directive, NIS2.
- Consolidatie van regels
- Terugtrekken van verouderde wetgeving
- Single entry point voor het rapporteren van incidenten

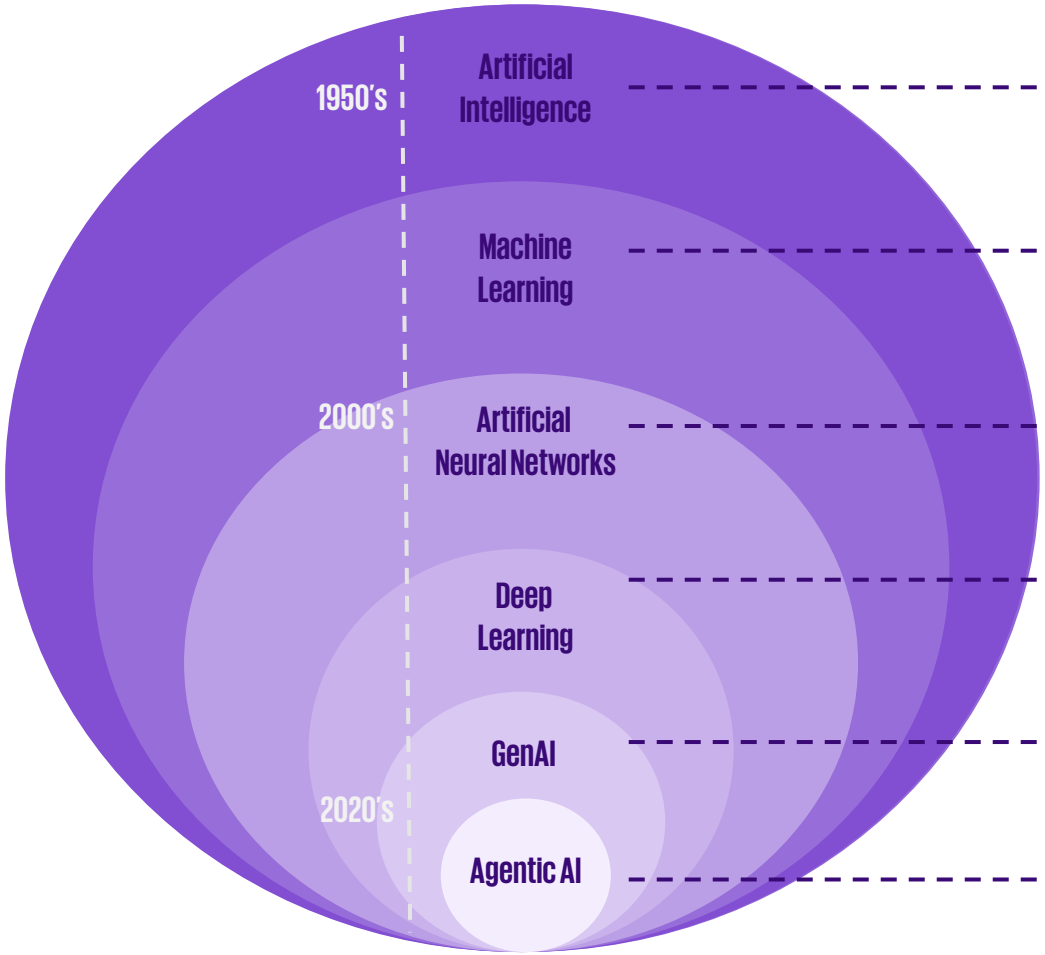
Belangrijkste wijzigingen

Belangrijkste wijzigingen (1/2)

Geraakte wetgeving	Key topics	Tijdslijnen
Data Act	Consolideert regels voor gegevensdeling; integreert ingetrokken wetten; voegt nieuwe hoofdstukken toe.	• **Direct** na inwerkingtreding
AVG	Voegt nieuwe artikelen 88a & 88b toe (cookies & toestemmingssignalen) aan de AVG, verduidelijkt definities, AI & onderzoek regels, meldingen van datalekken, DPIA-harmonisatie.	• **6M** voor cookie-regels • **24M** voor machine-leesbare signalen • **48M** voor browserverplichtingen
ePrivacy Directive	Verplaatst cookieregels naar de AVG; vereenvoudigt toestemming (naar systeem).	• **6M** na inwerkingtreding
NIS2	Eén enkel meldpunt voor incidentrapportage	• **18–24M** voor activatie
DORA	Stemmen incidentrapportage af met één enkel meldpunt.	• **18–24M** na inwerkingtreding
eIDAS	Voegt één enkel meldpunt toe voor rapportage.	• **18–24M** na inwerkingtreding

It is all about ..... AI

Maar hebben we het over hetzelfde?



Artificial Intelligence (AI)
The science and engineering of making machines that are able to perform human-like tasks

Machine-Learning (ML)
Training of computer agents to learn and improve in perception, knowledge, reasoning and actions

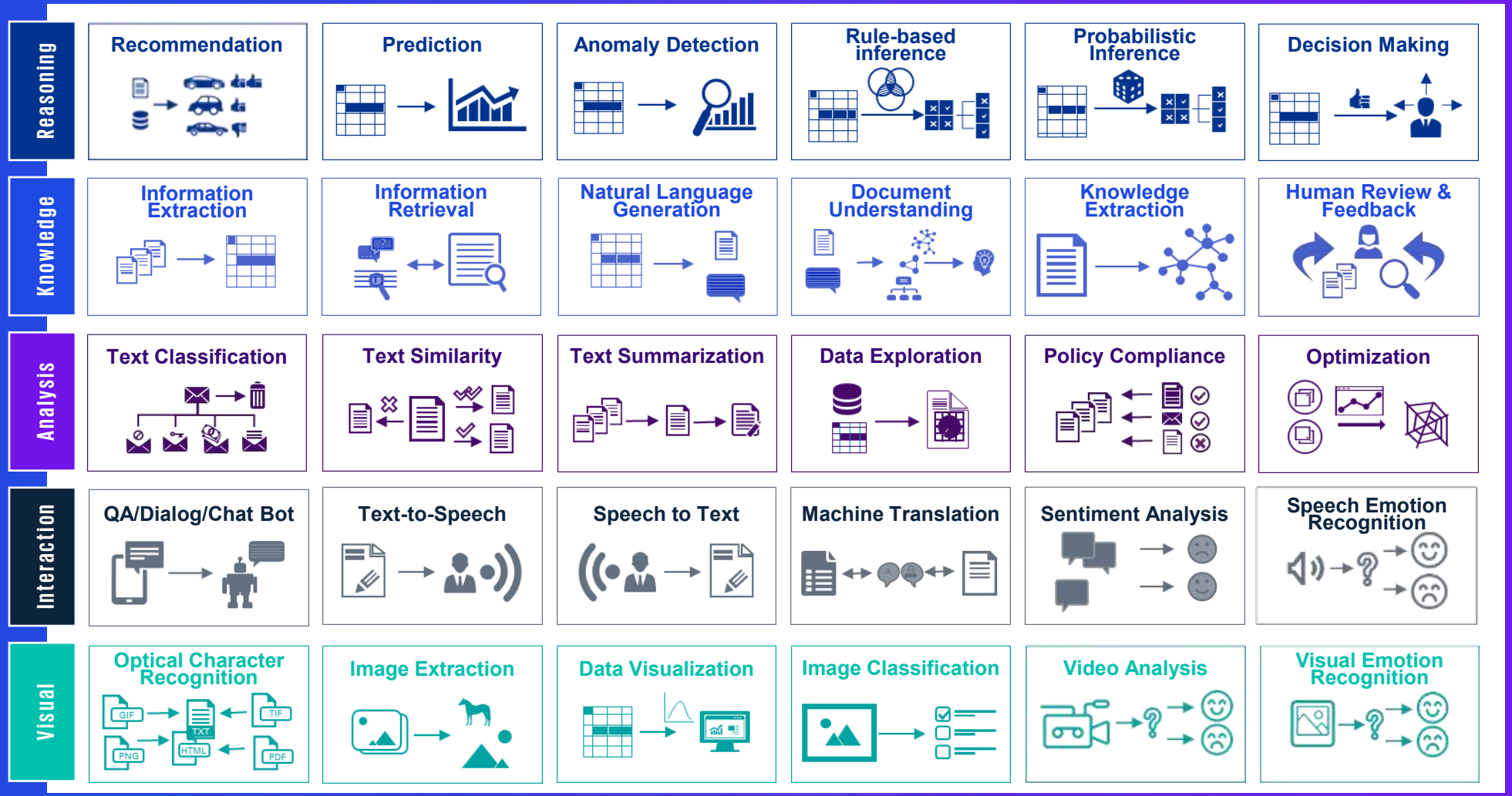
Artificial Neural Networks (ANN)
Human brain-inspired machine-learning models

Deep learning (DL)
Large multi-layer artificial neural networks able to extract complex patterns from large datasets

Generative AI (GenAI)
Large deep-learning models that generate text, images, and other contents based on the data they were trained on

Agentic AI (AAI)
AI systems that autonomously plan, decide, and act to achieve goals with minimal human input

AI kan diverse acties en handelingen verrichten



55

Belangrijkste wijzigingen (2/2)

Geraakte wetgeving	Key topics	Tijdslijnen
AI Act	• Uitgestelde deadlines voor hoog risico AI • Verruiming van de uitzondering voor verwerking van gevoelige persoonsgegevens om bias op te sporen en te corrigeren. Drempel verlaagt van strikt noodzakelijk naar noodzakelijk. Nieuw art 4a AI Act. • Overgangsperiode voor generatieve AI Aanbieders van generatieve AI die systemen vóór 2026 op de markt hebben gebracht krijgen extra de tijd om aan transparantieverplichtingen te voldoen zoals markeren via watermerken of meta data • Vereenvoudiging kwaliteitsmanagement systeem • Schrapping van registratieverplichting voor Bijlage III, niet hoog risico systemen	• 12 december 2027 (Bijlage III) (was augustus 2026); en voor ingebedde systemen 12 augustus 2028 (was 2027); ook als de standaarden nog niet gereed zijn • Februari 2027 (was augustus 2026)

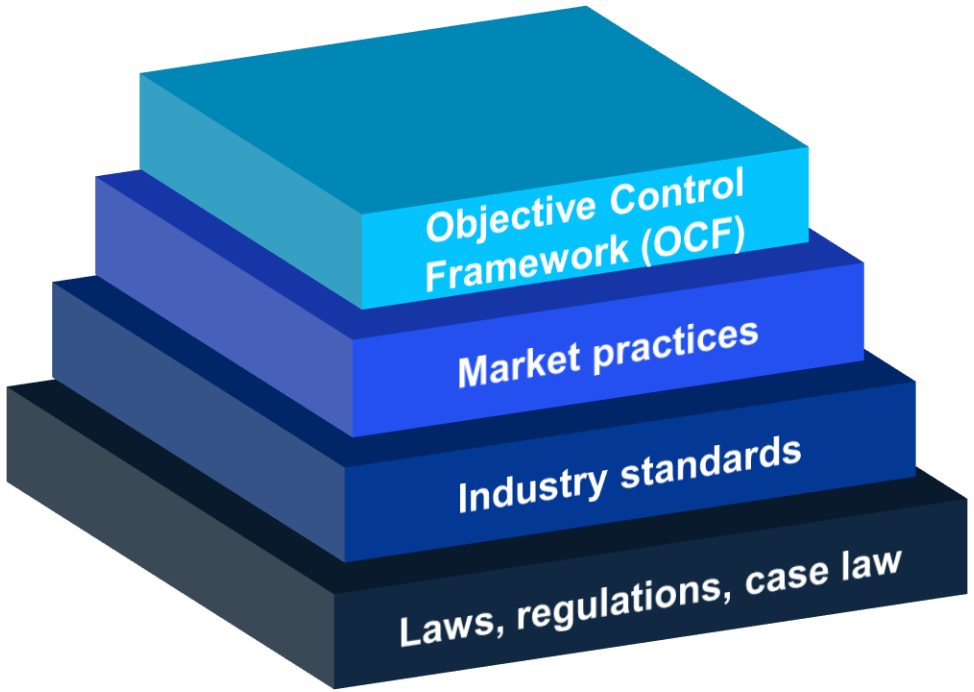
Praktisch

07

The Objective Cloud Compliance and Control Framework (OCF) – Cloud example

Objective Cloud Compliance and Control Control Framework (OCF) - set up

The OCF serves as the objectively grounded base with realistic demands and obligations. In total KPMG identified xxx requirements and controls (to be verified, validated and agreed by […]. By following and applying the OCF requirements and controls, the Contracting Authority can arrive at a process and content that is **sustainably** on par with applicable laws&regulations, current industry standards and market practices.



The **OCF** allows identification of the obligations and controls with regard to IaaS and PaaS services on the areas: process, technology and people. Such on **addressee level** (Contracting Authority or Supplier), and practical concrete, workable, enforceable (qualitively and quantitively) demands/obligations/arrangements via **MoSCoW** Indicators.

Market practices and capabilities guide what are the common industry accepted capabilities e.g. Eurostack and others

Industry standards form the second layer of the OCF. Industry standards set requirements for solutions to which cloud users and vendors should adhere. The following industry standards have been taken into account to derive the controls for the OCF:

- DICTU Toetsingsinstrument Soevereiniteit Clouddiensten
- EC Cloud Sovereignty Framework
- BIO
- NLF

Laws, regulations and case law[(a)] are the foundation of the OCF and guide for the fundamental controls and requirements that the government ánd the cloud supplier should adhere to. The following legislation and governmental documentation have been taken into account:

- GDPR
- Data Act
- AI Act
- Nis2
- Compatibiliteitswet 2012
- Aanbestedingswet
- And others according to TechRegRadar

Note: (a) For the determination of the L&R universe we use our TechRegradar

Objectively grounded realistic demands and obligations. OCF

Short description of the domain

Law&regulation, Standard or market practice

Unique number

Who is the addressee of the control?

Contracting Authority, CloudSupplier or both

Describes impact

Describes differences in impact service model *SaaS, IaaS, PaaS*

Domain	Control/requirement ID	Topic	Detailed requirement or control and source	Addressee	MoSCoW	Relative impact	Impact on SaaS/IaaS/PaaS

Describes where the control is rooted in: Laws and regulations, industry standards or market practices.

Topic of control

Legal relations, Availability, Integrity, Confidentiality, Interoperability, Legal enforcement, Persons & Governance, Public procurement, Miscellaneous

Detailed requirement/ control, includes source of control

Describes if a control or requirement is a (*M)ust Have, (S)hould Have or (C)ould Have, (W)ouldNotHave (MoSCoW)*

OCF demo

Thank you

Peter Kits
Partner
Cyber, Tech Law & Privacy
+31613001055
kits.peter@kpmg.nl

KPMG op Social media

KPMG app