Cheatsheet datagerelateerde EU-wetgeving

buro berk

Cheatsheet datagerelateerde EU-wetgeving

Steeds meer organisaties vallen onder de recente EU-wetgeving met betrekking tot “data”, denk daarbij bijvoorbeeld aan cybersecurityregels. Naast de uitbreiding van het aantal organisaties dat onder EU-wetgeving gaat vallen worden voor andere organisaties de reeds bestaande verplichtingen aangescherpt en verzwaard.

Deze cheatsheet geeft een beknopt overzicht van recente EU-regelgeving die betrekking heeft op data in de meest brede zin van het woord.

Sommige van de opgenomen regelgeving is reeds in werking getreden, terwijl andere regelgeving nog niet is vastgesteld en dus mogelijk nog aanpassingen ondergaat voordat ze definitief wordt aangenomen. Dit overzicht geeft de stand van zaken weer per 20 september 2023.

Vragen naar aanleiding van deze cheatsheet? Neem contact op met Martijn Berk op 06-29575351 of mail@martijnberk.com

Foto voorblad: atelier Marieke Schoonderbeek
Ontwerp slides: Aclara Legal Design

Data Act

Regels over de data die bedrijven en consumenten zelf genereren door het gebruik van een product of een dienst

* Van toepassing op

- Datahouders, ontwerpers en fabrikanten van (IoT) producten die gegevens genereren en/of verzamelen;
- Partijen aan wie data door gebruikers ter beschikking wordt gesteld (“data-ontvangers”);
- Aanbieders van dataverwerkingsdiensten (in de EU).

* Status en tijdlijnen

- Onderdeel Europese Data Strategie;
- Voorstel nog ter instemming aan de Raad en Europees Parlement;
- Verwacht medio 2025.

* Korte samenvatting

- Regels voor het beschikbaar stellen van data gegenereerd door apparaten (“Internet of Things”) aan gebruikers (art. 3 e.v.) of aan door de gebruiker aangewezen derden (art. 5 e.v.);
- Regels voor het verschaffen van toegang aan overheidsinstanties tot data in het bezit van de private sector in exceptionele situaties (art. 14 e.v.);
- Maatregelen om klanten makkelijk te laten migreren van de ene naar de andere aanbieder van clouddiensten (dataportabiliteit) (art. 23 e.v.);
- Een lijst met oneerlijke bedingen om contractuele onevenwichtigheden in datadelingsovereenkomsten te voorkomen (art. 13);
- Vereisten om interoperabiliteit mogelijk te maken tussen data verwerkende diensten en bevoegdheid voor de EC om normen hiervoor te stellen (art. 28 e.v.)
- Verduidelijking databankenrecht, databanken met data afkomstig uit het gebruik van producten valt niet onder bescherming Databankrichtlijn (art. 35).

* Toezichthouder & handhavingsinstrumenten

Nationale autoriteit

Bevoegdheden:

- klachtenmechanisme;
- onderzoeksrecht;
- sancties (boetes en dwangsommen;
- afdwingen toegang tot data;
- schrappen overstapkosten dataverwerkingsdiensten.

* Boetes

Hoofdregel: €20 miljoen of 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

Schendingen beschikbaarheid data aan overheidsinstanties: tot €50.000 per inbreuk en tot een totaal van €500.000 per jaar.

* Vindplaats

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

Data Governance Act (DGA)

Regels om het vertrouwen in vrijwillige gegevensuitwisseling door bedrijven en burgers te vergroten

buro berk

Van toepassing op

- Overheidsinstanties;
- Databemiddelingsdiensten.

Status en tijdlijnen

- Onderdeel Europese Data Strategie;
- Van kracht per 23 juni 2022, met een verschoningsperiode tot 24 September 2023.
- Verplichtingen voor databemiddelingsdiensten gelden vanaf 25 September 2025.

Korte samenvatting

- Voorwaarden voor het hergebruik van overheidsgegevens die niet publiekelijk toegankelijk zijn en buiten de Open Data richtlijn vallen (art. 3 e.v.);
- Het instellen van databemiddelingsdiensten: een nieuw soort tussenpersoon die gegevensdeling tussen gegevenshouders en gegevensgebruikers faciliteert (art. 10 e.v.);
- Een regeling voor data-altruïsme zodat (persoons)gegevens voor doeleinden van algemeen belang gedeeld kunnen worden (art. 16 e.v.);
- Oprichting van een een Europees Comité voor gegevensinnovatie dat adviseert over de werking van deze verordening (art. 29 e.v.).

Toezichthouder & handhavingsinstrumenten

Nationale autoriteit

Ten aanzien van databemiddelingsdiensten:
- eisen dat de inbreuk wordt gestopt;
- sancties (dwangsommen en boetes);
- stopzetting dienstverlening databemiddelingsdienst;
- nationale regels en sancties.

Boetes

Geen

Vindplaats

https://eur-lex.europa.eu/eli/reg/2022/868/oj

Digital Services Act (DSA)

Regels voor onlinediensten met name voor het bewaken van content

buro berk

Van toepassing op

Tussenhandelsdiensten

Status en tijdlijnen

- Aanvulling op E-commerce richtlijn 2000/31/EU;
- Inwerkingtreding per 16 november 2022;
- Voor ”Very Large Online Platforms” (VLOP’s) van kracht per 25 augustus 2023;
- Voor alle andere tussenhandelsdiensten per 17 februari 2024.

Korte samenvatting

- Drie soorten tussenhandelsdiensten: (i) mere conduit (doorgifte), (ii) caching en (iii) hostingdiensten;
- Onderscheid tussen Very Large Online Platfroms (VLOP’s, Verly Large Online Search Engines (VLOSE’s) en overige onlineplatforms;
- Verschillende aansprakelijkheidsregelingen per soort tussenhandelsdienst (art. 4 t/m 6);
- Procesregels voor contentmoderatie (art. 14 e.v.);
- Transparantieregels reclame (art. 26);
- Transparantieregels geprioriteerde content (art. 27);
- Aanvullende maatregelen voor VLOP’s en VLOSE’s om systeemrisico’s te beheersen zoals het uitvoeren van een jaarlijkse risicobeoordeling, jaarlijkse audits en jaarlijkse transparantierapportages (art. 33 e.v.).

Toezichthouder & handhavingsinstrumenten

VLOP’s & VLOSE’s: Europese Commissie en nationale toezichthouders (NL: ACM)
Overige: nationale toezichthouders (NL: ACM)

Bevoegdheden: bevelen stopzetten inbreuken, opleggen geldboetes en/of dwangsommen, bevelen tot onderzoek en een actieplan, beperking diensten.

Boetes

- niet-naleving van verplichtingen: maximaal 6 % van de wereldwijde jaarlijkse omzet;
- verstrekken van informatieverplichtingen: 1 % van de wereldwijde jaarlijkse omzet;
- maximale dwangsom per dag: 5 % van de wereldwijde jaarlijkse omzet.

Vindplaats

https://eur-lex.europa.eu/eli/reg/2022/2065/oj

Digital Markets Act (DMA)

Regels voor de grootste online platforms om consumenten en tot de markt toetredende ondernemingen te beschermen

buro berk

* Van toepassing op

Kernplatformdiensten en poortwachters

* Status en tijdlijnen

- Inwerkingtreding per 1 november 2022, van toepassing sinds 2 mei 2023.
- Poortwachters op 6 september 2023 aangewezen door de EC, regels voor poortwachters gelden vanaf 6 maart 2024.

* Korte samenvatting

- Verplichtingen voor poortwachters, zo mogen zij geen persoonsgegevens afkomstig van andere diensten combineren, hun eigen diensten of producten gunstiger rangschikken. Daarnaast moeten zij derden in staat stellen te interageren met de eigen diensten en ondernemingen die reclame maken op het platform in staat stellen om de resultaten te verifiëren;
- Een onderneming wordt aangewezen als poortwachter indien die (i) een aanzienlijke impact heeft op de interne markt; (ii) een kernplatformdienst aanbiedt die voor zakelijke gebruikers een belangrijke toegangspoort tot eindgebruikers vormt, en (iii) met betrekking tot haar activiteiten een stevig verankerde en duurzame positie inneemt of naar verwachting in de nabije toekomst een dergelijke positie zal innemen (art 3 lid 1).

* Toezichthouder & handhavingsinstrumenten

De Europese Commissie is de enige handhaver.

Nationale bevoegde autoriteiten hebben een onderzoeksrecht

Handhavingsinstrumenten EC: verzoeken om inlichtingen, horen en verklaringen afnemen, inspecties verrichten, voorlopige maatregelen nemen, boete en/of dwangsom opleggen

* Boetes

Niet naleving door EC opgelegde maatregelen: dwangsom van maximaal 5% van de gemiddelde dagelijkse wereldwijde omzet per dag

Indien de EC vaststelt dat de poortwachter niet aan zijn verplichtingen voldoet: maximaal 10% van de jaarlijkse wereldwijde omzet, 20% indien de verplichting ook het voorgaande jaar is geschonden.

* Vindplaats

https://eur-lex.europa.eu/eli/reg/2022/1925/oj

Data spaces

Het stimuleren van de beschikbaarheid, het gebruik en de uitwisseling van data

* Van toepassing op

* Status en tijdlijnen

- Voorstel van Europees Parlement en de Raad voor een European Health Data Space (EHDS) gepubliceerd op 3 mei 2022;
- De EHDS bouwt voort op de Data Governance Act, Data Act, de NIS2-richtlijn,de Cyber Resilience Act en de AI Act (en sectorspecifieke wetgeving).

* Korte samenvatting

- Het begrip *data space* (of dataruimte) is afkomstig uit de Europese datastrategie (pijler D);
- Er worden negen gemeenschappelijke data space in strategische sectoren en gebieden van algemeen belang ontwikkeld: Gezondheid, Mobiliteit, Industrie, Financiële diensten, Energie, Landbouw, Green Deal, Overheid en Vaardigheden;
- Binnen een data space moet het voor iedereen mogelijk zijn om data te delen, uit te wisselen en te gebruiken;
- Een dataruimte is opgebouwd uit: (i) technische infrastructuur die voor iedereen toegankelijk is en veilige uitwisseling en gebruik mogelijk maakt, (ii) gereedschappen voor gebruik en delen, (iii) generieke data governance afspraken en standaarden en (iv) heldere gebruikscondities;
- Ook wordt gesproken over een ”persoonlijke data space”;
- Verdere verduidelijking volgt in de verschillende voorstellen voor de strategische sectoren.

* Toezichthouder & handhavingsinstrumenten

EHDS: (nationale) instanties voor toegang tot gezondheidsgegevens

Handhavingsinstrumenten (EHDS):
- Opvragen van informatie;
- Intrekken gegevensvergunning;
- Boetes

* Boetes

Nog niet uitgewerkt.

* Vindplaats

Europese datastrategie:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066

Europese ruimte voor gezondheidsgegevens:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:197:FIN

Digital Single Market Auteursrechtrichtlijn (DSM-auteursrechtrichtlijn)

Modernisering auteursrecht rekening houdend met technologische ontwikkelingen en nieuwe distributiekanalen

buro berk

* Van toepassing op

Aanbieders van online diensten voor het delen van content.

* Status en tijdlijnen

Van kracht per juni 2019. Geïmplementeerd door de Implementatiewet richtlijn auteursrecht in de digitale eengemaakte markt per 7 juni 2021.

* Korte samenvatting

- Kopiëren van werken om tekst- en datamining mogelijk te maken voor wetenschappelijk onderzoek is toegestaan mits men reeds rechtmatige toegang heeft tot deze werken en de rechthebbenden hun rechten niet hebben voorbehouden (art. 3 e.v.);
- Online diensten die toegang geven tot grote hoeveelheden door gebruikers geüpload auteursrechtelijk beschermd materiaal hebben een licentie nodig van de rechthebbenden. Bij gebreke aan een licentie moet moeten de auteursrechtelijke werken verwijderd worden (“*Notice and Take Down and Stay Down*”) hetgeen met een automatisch filter gedaan kan worden (art. 17).

* Toezichthouder & handhavingsinstrumenten

Niet van toepassing

* Boetes

Niet van toepassing

* Vindplaats

https://eur-lex.europa.eu/eli/dir/2019/790/oj

Artificial Intelligence Act (AI-Act)

Regels om de ontwikkeling en het in de handel brengen van betrouwbare AI-systemen te waarborgen

buro berk

* Van toepassing op

- Aanbieders van AI-systemen;
- Gebruikers van AI-systemen.

* Status en tijdlijnen

- Voorstel is aangenomen (met aanpassingen) door het Europees Parlement, onderhandelingen in de Raad zijn gestart;
- Invoeringsdatum van 1 januari 2024 wordt genoemd, daarna waarschijnlijk na 2 jaar van kracht.

* Korte samenvatting

Vier risiconiveaus, ieder met eigen regels:

- Onaanvaardbaar risico: volledig verboden. Dit zijn bijvoorbeeld manipulatieve systemen die gedrag verstoren, sociale puntensystemen van overheden of grootschalige inzet van biometrische systemen (art. 5);
- Hoog risico: strenge eisen, zoals: het verplicht uitvoeren van een risico-assessement, een risicomanagementsysteem, logging van alle gebruik, menselijk toezicht tijdens gebruikt. Bijvoorbeeld AI-systemen die gebruikt worden bij recruitment, toegang tot essentiële particuliere diensten (bijv. toetsen kredietwaardigheid) en bij rechtshandhaving (art. 6 e.v.);
- Laag risico: systemen moeten voldoen aan transparantieverplichtingen, bijvoorbeeld bij gebruik van een chatbot informeren dat niet met een mens gecommuniceerd wordt (art. 52). Daarnaast worden vrijwillige gedragscodes worden gefaciliteerd (art. 69).

* Toezichthouder & handhavingsinstrumenten

Nationale autoriteiten.
Europees Comite voor AI (nog op te richten)

Handhavingsinstrumenten:
- ontvangen meldingen incidenten systemen met hoog risico;
- toegang tot data en broncode;
- verbod of beperking in gebruik;
- sancties (geldboetes)

* Boetes

Niet naleving verboden praktijken of eisen databeheer systemen hoog risico: maximaal €30.000.000 of tot 6% van de jaarlijkse wereldwijde omzet.

Non-conformiteit andere verplichtingen: maximaal €20.000.000 of tot 4% van de jaarlijkse wereldwijde omzet.

* Vindplaats

Voorstel:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

Aanpassingen Europees Parlement:
https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

Richtlijn AI-aansprakelijkheid

Regels voor niet-contractuele civielrechtelijke aansprakelijkheid in relatie tot AI-systemen

buro berk

Van toepassing op

Aanbieders en gebruikers van AI-systemen (zoals gedefinieerd in de AI-verordening)

Status en tijdlijnen

Lopend

Korte samenvatting

- Bouwt voor op de AI-verordening en bevat regels voor buitencontractuele schadevorderingen gebaseerd op onrechtmatige daad;
- Bewijsvermoeden van causaal verband tussen AI en schade, bijvoorbeeld indien aangetoond wordt dat een zorgvuldigheidsplicht is geschonden en redelijkerwijs kan worden aangenomen dat daardoor de werking van het AI-systeem is beïnvloed en het AI-systeem de schade heeft veroorzaakt (art. 4);
- Eenvoudiger toegang tot bewijsmateriaal voor de benadeelde (art. 3).

Toezichthouder & handhavingsinstrumenten

Niet van toepassing

Boetes

Niet van toepassing

Vindplaats

https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A52022PC0496

Herziening richtlijn productaansprakelijkheid

Aanpassing regels productaansprakelijkheid zodat AI-componenten van software en producten onder de richtlijn productaansprakelijkheid vallen

Van toepassing op

Producent, importeur, distributeur, fulfilmentdienstverlener, verlener van een bijbehorende dienst.

Status en tijdlijnen

Lopend

Korte samenvatting

- Aanpassing van de richtlijn productaansprakelijkheid die een risicoaansprakelijkheid introduceerde;
- Brengt AI-componenten van software en producten onder de werking van de productaansprakelijkheid te brengen;
- Indien benadeelde voldoende feiten en bewijsmateriaal heeft overlegd om zijn vordering aannemelijk te maken moet verweerder het bewijsmateriaal openbaar maken (art. 8). Bij gebreke daarvan wordt vermoed het product gebrekkig te zijn (art. 9);
- Gratis software en open source software is uitgezonderd (overweging 13).

Toezichthouder & handhavingsinstrumenten

Niet van toepassing

Boetes

Niet van toepassing

Vindplaats

https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52022PC0495

Terrorist Content Online Regulation

Regels om de verspreiding van terroristische content tegen te gaan

Van toepassing op

Hostingdiensten

Status en tijdlijnen

Van kracht

Korte samenvatting

- Bevoegde autoriteiten kunnen een verwijderingsbevel uitvaardigen (art. 3);
- Aanbieders moeten de betreffende content binnen één uur verwijderen of blokkeren (art. 3 lid 3);
- Indien bij de betreffende aanbieder nog niet eerder een verwijderingsbevel is uitgevaardigd verstrekt de autoriteit 12 uur vooraf informatie over de procedures en termijnen (art. 3 lid 2).

Toezichthouder & handhavingsinstrumenten

Nationale autoriteiten (NL: Autoriteit Online Terroristisch en Kinderpornografisch Materiaal (ATKM) (in oprichting))

Instrumenten:
- last onder dwangsom;
- bestuurlijke boetes.

Boetes

- Overschrijding termijn verwijderingsbevel: €4500 (tweede categorie art. 23 Sr);
- Overtreding van verschillende andere verplichtingen: €90.000 (vijfde categorie art. 23 Sr);
- Systematisch of aanhoudend overtreden termijn verwijderingsbevel: €900.000 (zesde categorie art. 23 Sr) of 4% van de mondiale jaarlijkse omzet.

Vindplaats

Verordening:
https://eur-lex.europa.eu/eli/reg/2021/784/oj

Uitvoeringswet (NL):
https://wetten.overheid.nl/BWBR0048064/2023-09-01

Open Data Richtlijn

Regels om reeds beschikbare overheidsinformatie breder beschikbaar te maken voor hergebruik

Van toepassing op

Overheden

Korte samenvatting

- Informatie die de overheid zelf gebruikt voor zijn eigen taken, ook gratis, makkelijk en vrij te gebruiken moet zijn door andere personen of bedrijven (art. 1 lid 1);
- Geldt enkel voor informatie die al openbaar is en dus niet geheim of indien er IE-rechten van derden op de informatie rust (art. 1 lid 2);
- Geen regels welke gegevens openbaar moeten zijn.

Toezichthouder & handhavingsinstrumenten

Niet van toepassing

Boetes

Niet van toepassing

Status en tijdlijnen

- Onderdeel Europese Data Strategie;
- Van kracht;
- Om te zetten in Wet implementatie Open Data Richtlijn (Wiodr) (nog niet in werking);
- EC is een inbreukprocedure gestart wegens te late omzetting.

Vindplaats

Richtlijn:
https://eur-lex.europa.eu/eli/dir/2019/1024/oj

Implementatie wet:
https://zoek.officielebekendmakingen.nl/dossier/kst-36382-2.html

Network and Information Systems directive (NIS2-richtlijn)

Versterken van cyberbeveiliging in sectoren met een sterke afhankelijkheid van IT met een focus op kritische infrastructuur

* Van toepassing op

Organisaties die genoemd zijn in Bijlage I & II. Bijvoorbeeld in categorie 1: energie; vervoer; bankwezen; infrastructuur voor de financiële markt; gezondheidszorg; drinkwater; afvalwater; digitale infrastructuur; beheer van ICT-diensten; overheid;. In categorie 2: post- en koeriersdiensten; afvalstoffenbeheer; chemische stoffen; levensmiddelen; digitale aanbieders; onderzoek.

* Status en tijdlijnen

- Van kracht
- Uiterlijk 17 oktober 2024 omgezet in nationale wetgeving (NL: aanpassing van de Wet beveiliging en netwerk- en informatiesystemen (Wbni)

* Korte samenvatting

- Aanpassing van de bestaande NIS-richtlijn, voornamelijk een uitbreiding van de organisaties die onder de richtlijn vallen;
- Organisaties waarop de richtlijn van toepassing is zijn “*belangrijke entiteiten*”. Organisaties uit categorie 1 met minimaal 250 werknemers en/of een jaaromzet van €250 miljoen zijn “*essentiële entiteiten*” met een strenger toezicht en handhaving (art. 3);
- Belangrijke en essentiële entiteiten nemen passende en evenredige technische, operationele en organisatorische maatregelen voor de beveiliging van de netwerk- en informatiesystemen (art. 21);
- Het bestuur heeft een cruciale en actieve rol bij het goedkeuren en toezicht. Persoonlijke aansprakelijkheid voor het bestuur van essentiële bij schending van hun verplichting (art. 20);
- Rapportageverplichting bij een significant incident binnen 72 uur (art. 23).

* Toezichthouder & handhavingsinstrumenten

Nationale toezichthouder

Handhavingsinstrumenten: inspecties, waarschuwingen, bindende aanwijzingen, gelasten tot openbaarmaking inbreuken op de richtlijn, administratieve boetes.

Bijkomend voor essentiële entiteiten: (tijdelijke) opschorting vergunning, leidinggevende personen verbieden leidinggevende functies uit te oefenen.

* Boetes

Bij inbreuk op maatregelen beheer cyberbeveiligingsrisicos of rapportageverplichtingen:

- essentiële entiteiten: maximumbedrag van ten minste €10.000.000 of ten minste 2 % van de totale wereldwijde jaaromzet;
- belangrijke entiteiten: maximumbedrag van ten minste €7.000.000 of ten minste 1,4 % van de totale wereldwijde jaaromzet.

* Vindplaats

https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Cyber Resilience Act (CRA)

Regels voor fabrikanten met betrekking tot de cyberveiligheid van producten met digitale elementen

buro berk

Van toepassing op

Fabrikanten, vertegenwoordigers, importeur en distributeurs van producten met digitale elementen.

Status en tijdlijnen

- Voorstel van de Europese Commissie in september 2022 gepubliceerd;
- Onderhandelingen met Europees Parlement lopen.

Korte samenvatting

De CRA bevat:

- regels voor het in de handel brengen van producten met digitale elementen om de cyberbeveiliging van dergelijke producten te waarborgen;
- essentiële eisen voor het ontwerp, de ontwikkeling en de productie van producten met digitale elementen, en verplichtingen voor marktdeelnemers met betrekking tot deze producten, op het gebied van cyberbeveiliging;
- essentiële eisen voor de procedures inzake de respons op kwetsbaarheden waaronder een meldingsplicht voor digitale kwetsbaarheden en incidenten;
- verplichting voor fabrikanten om producten met digitale elementen gedurende de gehele levenscyclus te voorzien van gratis veiligheidsupdates;
- niet-commerciële open source software valt niet onder deze richtlijn.

Toezichthouder & handhavingsinstrumenten

- Nationale conformiteitsbeoordelingsinstanties (art. 25 e.v.);
- Nationale markttoezichtautoriteiten (art. 41 e.v.).

Boetes

Bij niet-naleving van de essentiële cyberbeveiligingsvereisten, de verplichtingen voor fabrikanten en de rapportageverplichtingen voor fabrikanten: tot €15.000.000 of tot 2,5 % van de totale wereldwijde jaarlijkse omzet;
Bij niet-naleving van andere verplichtingen: tot €10.000.000 of tot 2 % van de totale wereldwijde jaarlijkse omzet;

Vindplaats

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454

Digital Operational Resilience Act (DORA)

Regels om de digitale weerbaarheid van financiële organisaties te vergroten

Van toepassing op

Financiële instellingen zoals kredietinstellingen, betalingsinstellingen, beleggingsondernemingen, verzekeringsondernemingen en de aanbieders van IT-diensten aan deze financiële instellingen (Critical Third Party Providers (CTPP's).

Status en tijdlijnen

- In werking, vanaf 17 januari 2025 voldoen aan de eisen;
- Advies van EBA/EIOPA/ESMA voor criteria voor vaststellen CTPP's beschikbaar;
- Gedetailleerde uitwerking in Regulatory Technical Standards (RTS) beschikbaar op 30 september 2023;
- Implementing Technical Standards (ITS) beschikbaar per 17 januari 2024 en 17 juli 2024.

Korte samenvatting

- Eisen aan de beveiliging van netwerk- en informatiesystemen van financiële ondernemingen. Bestaat uit vijf pijlers: (i) ICT-Rrisicobeheer, (ii) ICT-gerelateerde diensten, (iii) testen van digitale operationele veerkracht, (iv) beheer van ICT-risico's van derden en (v) informatieuitwisseling cyberdreigingsinformatie;
- Eindverantwoordelijkheid voor het risicobeheer ligt bij het leidinggevend orgaan, leden daarvan zijn ook verplicht hun kennis daaromtrent up-to-date te houden;
- Maatregelen moeten worden geïmplementeerd met inachtneming van het proportionaliteitsbeginsel (art. 4) waarbij de omvang, aard schaal en complexiteit van de diensten, activiteiten en werkzaamheden, alsmede het algehele risicoprofiel, in aanmerking moeten worden genomen.

Toezichthouder & handhavingsinstrumenten

- Lead overseer voor CTPPs (art. 31 e.v.);
- Nationale autoriteiten (art. 46 e.v.), de vergunningverlenende toezichthouder gaat ook het toezicht op DORA uitvoeren.

Bij CTPPs: dwangsom, informatieverzoek, algemene onderzoeken, inspecties, openbaarmaking verzuim in geval van niet-naleving,

Bij financiële instellingen: vordering toegang tot gegevens, uitvoeren inspecties ter plaatse, eisen corrigerende maatregelen, gelasten tijdelijk of definitief staken van inbreukmakende activiteit (measure of last resort), publicatie administratieve strafmaatregelen, dwangsommen aan derde aanbieder van IT diensten, strafrechtelijke maatregelen

Boetes

Dwangsom CTPPs: 1 % van de wereldwijde gemiddelde dagomzet van de cruciale derde aanbieder van ICT-diensten in het voorafgaande boekjaar.

Vindplaats

https://eur-lex.europa.eu/eli/reg/2022/2554/oj

Extra procedurele regels naleving AVG

Aanpassing van procedurele regels die van toepassing zijn op de nationale toezichthouders zodat samenwerking tussen lidstaten kan verbeteren

Van toepassing op

Nationale gegevensautoriteiten (NL: Autoriteit Persoonsgegevens)

Korte samenvatting

- Regels om de consistentie in de interpretatie en beoordeling van geschillen inzake persoonsgegevens te verbeteren;
- Met name gericht op: klachtenrecht van betrokkenen, procedurele regels van onderzochte partijen, grensoverschrijdende samenwerking tussen de nationale autoriteiten

Toezichthouder & handhavingsinstrumenten

Ongewijzigd

Boetes

Ongewijzigd

Status en tijdlijnen

Voorstel

Vindplaats

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0348