JAAROVERZICHT 2023

De meest besproken ontwikkelingen in ICT-recht

Van ChatGPT tot NIS2-richtlijn voor cybersecurity

LEGALZ
ICT-ADVOCATENKANTOOR

Inhoudsopgave

Colofon

Kantoorgebouw Minervahuis III
Rodezand 34
3011 AN Rotterdam

www.legalz.nl
contact@legalz.nl
010 2290 646

Inleiding

Aan het einde van het jaar blikken we graag met u terug op de belangrijkste ontwikkelingen in ICT-recht. Ook dit jaar was weer veelbewogen met impactvolle Europese Verordeningen en nieuwe privacy- en cyberissues door het gebruik van AI-tools als ChatGPT.

Meest opvallend dit jaar was waarschijnlijk de vrij plotse komst van de langverwachte opvolger van het Privacy Shield. Deze zomer kwam het nieuws dat er een akkoord was bereikt tussen de Verenigde Staten en Europa. Ineens was het EU-U.S. Data Privacy Framework daar. Groot nieuws! Data delen met de VS is na jaren weer eenvoudiger geworden. Natuurlijk staan we hier uitgebreid bij stil in ons jaaroverzicht.

Ook aandacht voor een nieuwkomer met enorme populariteit: ChatGPT. Een geweldige tool met ongekende mogelijkheden, maar waar ook de nodige risico's aan kleven. Zijn de AVG en ChatGPT eigenlijk wel te combineren? En hoe staat het eigenlijk met de regulering ervan? Aan beide vragen besteden we in dit overzicht aandacht.

Op het gebied van cybersecurity staan we stil bij de NIS2-richtlijn om de cyber- en informatiebeveiliging in Europa naar een hoger niveau te tillen. Let op! Deze opvolger van de NIS1-richtlijn raakt veel meer organisaties: tijdige voorbereiding is dus essentieel.

Tot slot zoomen we in op diverse nieuwe, Europese wetsvoorstellen die dit jaar zijn goedgekeurd. Denk aan de Digital Operational Resilience Act (DORA), die bedoeld is om de digitale weerbaarheid van de financiële sector te vergroten. Deze wetgeving heeft overigens ook gevolgen voor IT-dienstverleners die voor financiële entiteiten werken. Ook besteden we onder meer aandacht aan de nog in behandeling zijnde Artificial Intelligence Act en de onlangs goedgekeurde EU Data Act.

Mocht u na het lezen van dit jaaroverzicht nog vragen hebben, bel of mail ons dan. Geheel vrijblijvend, want wij helpen u graag verder. Ook in 2024.

Op een succesvol nieuw jaar!

Mr. Robert Grandia
Oprichter en eigenaar ICT-advocatenkantoor Legalz

1. Vijf jaar AVG: ChatGPT en Data Privacy Framework gamechangers

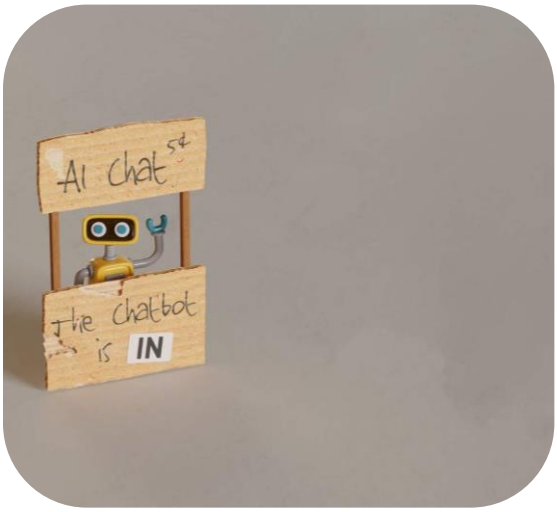
Op 25 mei 2018 werd de AVG van kracht. Het was voor de meeste organisaties een megaklus om aan alle vereisten van de AVG te voldoen en de deadline werd lang niet overal gehaald. Inmiddels zijn we 5 jaar verder, maar de privacyregels zijn misschien wel actueler dan ooit. Daarnaast verandert het speelveld continu. Dit jaar waren de privacy schijnwerpers gericht op ChatGPT en de lang verwachte opvolger van het Privacy Shield: het EU-U.S. Data Privacy Framework.

ChatGPT: hoe zit het met de privacy?

De ontwikkeling van kunstmatige intelligentie gaat razendsnel. De enorme populariteit van ChatGPT bewijst hoe graag we er met z'n allen gebruik van maken, maar zijn we er ook klaar voor? En ook: hoe passen dit soort oplossingen binnen onze wet- en regelgeving? ChatGPT kreeg het in 2023 op het vlak van privacy in ieder geval flink te verduren. Hoe zit dat precies?

ChatGPT & privacy

De eind vorig jaar verschenen chatbot ChatGPT werd direct al razendsnel populair. ChatGPT kan door gebruik van Artificial Intelligence (AI) antwoord geven op vragen van gebruikers en ook hele teksten schrijven op commando.



De chatbot wordt gevoed en getraind met vrij beschikbare data, dat verkregen wordt op het internet. Daar zijn ook persoonsgegevens te vinden, die ChatGPT kan verzamelen en gebruiken.

Mag dat volgens de strenge privacyregels van de AVG?

ChatGPT verboden in Italië

Eind maart verscheen het bericht dat de Italiaanse privacytoezichthouder ChatGPT verbood in het land vanwege schending van de privacy. Daarbij werden 4 hoofdredenen benoemd.

1. Er is geen juridische basis (grondslag, in de AVG genoemd) voor het massaal verzamelen en opslaan van data.
2. De chatbot heeft geen mechanisme voor leeftijdscontrole van minderjarigen.
3. Mensen worden niet geïnformeerd dat hun data verzameld wordt.
4. Het is mogelijk dat de informatie die verstrekt wordt over mensen niet accuraat is.

Na een verbod van bijna een maand mocht de chatbot na diverse aanpassingen wel weer gebruikt worden in Italië. Zo is er in Italië een knop toegevoegd, waarmee gebruikers verklaren meerderjarig te zijn of toestemming hebben van hun ouders. Ook krijgt het privacybeleid meer zichtbaarheid.

Voor alle EU-burgers is er een formulier in het leven geroepen, waarmee ze bezwaar kunnen maken tegen het gebruik van hun persoonsgegeven door ChatGPT. Daarnaast is er een mogelijkheid aan het systeem toegevoegd om het bewaren van chatgesprekken uit te zetten.

ChatGPT Taskforce Europese toezichthouders
In navolging op het besluit van de Italiaanse toezichthouder, zette de Europese privacytoezichthouder European Data Protection Board (EDPB) in april een taskforce voor ChatGPT op.

Deze taskforce moet de samenwerking tussen verschillende toezichthouders bevorderen en ervoor zorgen dat de neuzen in Europa dezelfde kant op staan. Informatie over mogelijke handhavingsmaatregelen rondom ChatGPT moeten beter uitgewisseld worden.

In Europa wordt er druk gewerkt aan de Artificial Intelligence Act (zie bladzijde 17). Hierin zijn strenge regels opgenomen over de inzet van kunstmatige intelligentie.

AVG & ChatGPT: een (on)mogelijke combinatie?

De vraag is echter in hoeverre de AVG überhaupt nageleefd kan worden door AI-oplossingen als ChatGPT. Het recht om je gegevens te laten verwijderen of wijzigen is vrijwel onuitvoerbaar als de AI-dienst de data overal en nergens vandaan haalt.

Daarnaast lijkt het lastig om in alle gevallen een AVG grondslag voor verwerking (er zijn er 6: van toestemming tot algemeen belang) te vinden, waarmee ChatGPT het massaal verzamelen en opslaan van data kan rechtsvaardigen.

Niet voor niets hebben vooraanstaande experts op het gebied van IT en technologie wereldwijd opgeroepen tot een pauze in de ontwikkelingen van AI-oplossingen als ChatGPT. De techniek heeft namelijk op diverse ethische, juridische en zeker ook privacyvraagstukken nog geen goed antwoord.

Ondanks de juridische knelpunten rondom privacy, is het een mooie tool die steeds vaker door zowel bedrijven als particulieren wordt ingezet. Wij zullen de ontwikkelingen dan ook nauwlettend in de gaten houden.

Data Privacy Framework: gegevens delen met de VS eindelijk weer toegestaan

Na 2 jaar is het weer mogelijk om probleemloos en zonder extra maatregelen data te delen met partijen in de VS! In juli heeft de Europese Commissie het adequaatheidsbesluit voor veilige gegevensuitwisseling met de Verenigde Staten goedgekeurd. Het EU-U.S. Data Privacy Framework is de opvolger van het Privacy Shield. Een enorme opluchting voor velen, na 2 jaar van onzekerheid en vooral veel gedoe om AVG-proof gebruik te mogen maken van Amerikaanse software, platforms en apps.

Over het EU-U.S. Data Privacy Framework
In de zomer van 2020 werd het Privacy Shield na de rechtszaak Schrems II ongeldig verklaard. De reden?

Door middel van het Privacy Shield zou datadoorgifte niet voldoen aan de eisen die Europa stelt aan privacy en gegevensbescherming.

De afgelopen 2 jaar was het delen van gegevens met Amerikaanse partijen een regelrechte ramp. Officieel was dit enkel mogelijk met behulp van Standard Contractual Clauses (SCC) en door data met aanvullende waarborgen te verzenden, zoals encryptie zonder sleutel in Amerika.

Het EU-U.S. Data Privacy Framework (DPF) komt dan ook als een opluchting voor velen. Op basis van het nieuwe adequaatheidsbesluit kunnen persoonsgegevens veilig van de EU worden doorgegeven naar Amerikaanse bedrijven die deelnemen aan het Data Privacy Framework.

Grootste winst?

Er hoeven GEEN aanvullende waarborgen meer voor gegevensbescherming te worden getroffen. Met aangesloten organisaties binnen de VS kan dus op dezelfde wijze gecontracteerd worden als met organisaties binnen de EER.

Let op!

Amerikaanse bedrijven moeten eerst deelnemen aan het Data Privacy Framework, voordat deze op hen van toepassing is. Dit doen zij door akkoord te gaan met de naleving van een gedetailleerde reeks privacyverplichtingen. Denk hierbij bijvoorbeeld aan AVG-principes zoals doelbinding, dataminimalisatie en dataretentie, maar ook aan specifieke verplichtingen rondom databeveiliging en het delen van data met derden.

Waarom is data delen met de VS nu wel weer mogelijk?
Er waren een aantal redenen waarom het Privacy Shield in 2020 nietig werd verklaard. De belangrijkste?

1. Amerikaanse inlichtingen- en veiligheidsdiensten hebben het recht om gegevens van EU-burgers in te zien en te gebruiken. Ze hebben toegang tot alle gegevens en mogen deze naar eigen inzicht verwerken.
2. Het Amerikaanse ombudsman-mechanisme biedt onvoldoende bescherming aan EU-burgers met een klacht over de verwerking van hun persoonsgegevens in de VS.

Het EU-U.S. Data Privacy Framework introduceert nieuwe bindende waarborgen om tegemoet te komen aan alle zorgen van het Europese Hof van Justitie.

Zo wordt de toegang tot EU-gegevens door Amerikaanse inlichtingendiensten beperkt tot wat noodzakelijk en evenredig is om de Amerikaanse nationale veiligheid te beschermen.

Ook wordt een Data Protection Review Court (DPRC) geïntroduceerd voor EU-burgers, waarmee ze verhaal kunnen halen over het gebruik van hun gegevens door deze inlichtingendiensten. De DPRC zal klachten onafhankelijk onderzoeken en oplossen, onder meer door bindende corrigerende maatregelen vast te stellen.

Schrems spreekt zich uit: "grotendeels een kopie van mislukte Privacy Shield"

Max Schrems - die eerder verantwoordelijk was voor de nietigverklaring van het Privacy Shield - laat het er niet bij zitten. Hij noemt het nieuwe Data Privacy Framework grotendeels een kopie van het mislukte Privacy Shield.

Op de site van zijn organisatie NOYB valt te lezen dar er ondanks de public relations inspanningen van de Europese Commissie weinig verandert aan de Amerikaanse wetgeving of de aanpak van de EU.

Er wordt gesproken over goocheltrucs met woorden en interpretaties, maar niet van feitelijke verbeteringen. Max Schrems en zijn organisatie gaan de zaak aanvechten en verwachten dat deze begin 2024 terugkomt bij het Europese Hof van Justitie.

Wordt vervolgd dus....

2. Cybersecurity: nieuwe NIS2-richtlijn + gemeente zelf aansprakelijk voor grote hack

Cybersecurity staat volop in de belangstelling. Iedere organisatie raakt doordrongen van de noodzaak ervan. Opvallend dit jaar waren de aankondiging van de NIS2-richtlijn om de cyber- en informatiebeveiliging in Europa naar een hoger niveau te tillen en de opvallende uitspraak in de zaak over de grote ransomware aanval bij de gemeente Hof van Twente.

Let op! Nieuwe NIS2-richtlijn voor cybersecurity raakt veel meer organisaties

Er komen nieuwe regels aan op het gebied van cybersecurity. De NIS2-richtlijn is de opvolger van de NIS1-richtlijn en in het leven geroepen om de cyber- en informatiebeveiliging in Europa naar een hoger niveau te tillen. Waar de NIS1 zich vooral richtte op organisaties van kritieke aard, raakt de NIS2 veel meer organisaties en sectoren. Wat betekent dit voor u?

Van NIS1 naar NIS2

De NIS2-richtlijn (Network and Information Systems-richtlijn) is de opvolger van de NIS1-richtlijn. De NIS1 was de eerste richtlijn om de cybersecurity in de EU te verbeteren en eenheid te brengen in het Europees beleid voor netwerk- en informatiebeveiliging. De NIS1 is vooral gericht op bedrijven en instellingen van kritieke aard.

De NIS2 heeft een ruimer toepassingsgebied, waardoor er meer sectoren en entiteiten onder de richtlijn vallen. Daarnaast worden er strengere, aanvullende eisen gesteld aan cybersecurity, waaronder op het gebied van cyberrisicobeheer, controle en toezicht en bedrijfscontinuïteit.

Voor wie gaat de NIS2 gelden?

De NIS1 (ook bekend als de NIB1: netwerk- en informatiebeveiliging-richtlijn) leidde in Nederland tot de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni). Die wet is van toepassing op vitale aanbieders die zich onder meer in de energie-, de financiële en vervoerssector begeven.

Met de NIS2 wordt het aantal entiteiten en sectoren aardig uitgebreid. Overheidsdiensten, middelgrote en grote bedrijven gaan onder de richtlijn vallen, binnen de sectoren zoals opgenomen in bijlage 1 en 2 van de richtlijn.

Bijlage 1 - zeer kritieke sectoren	Bijlage 2 - andere kritieke sectoren
• energie • vervoer • bankwezen • infrastructuur financiële markt • gezondheidszorg • drinkwater • afvalwater • digitale infrastructuur • beheer van ICT (B2B) • overheid • ruimtevaart	• post- en koeriersdiensten • afvalstoffenbeheer • chemische stoffen • levensmiddelensector • vervaardiging van medische • hulpmiddelen, informatica- en elektronische producten, machines, motorvoertuigen en andere transportmiddelen • digitale aanbieders van online marktplaatsen, online zoekmachines en social media platforms • onderzoeksorganisaties

Zorgplicht en meldplicht

Op basis van de richtlijn is er de zorgplicht en de meldplicht. Vanwege de zorgplicht zal een organisatie straks passende en evenredige technische, operationele en organisatorische maatregelen moeten nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen te beheren, om incidenten te voorkomen en de gevolgen van incidenten te beperken.

De technische en organisatorische maatregelen zijn - in tegenstelling tot in de AVG - in deze richtlijn gedetailleerder omschreven. Hierdoor is duidelijker wat er van organisaties verwacht wordt. Zo wordt het verplicht om te kunnen monitoren wat er gebeurt op het netwerk.

Voor de volgende partijen zal de Europese Commissie uiterlijk op 17 oktober 2024 bovendien met specifieke uitvoeringshandelingen komen:

- DNS-dienstverleners;
- registers voor topleveldomeinnamen; en
- aanbieders van:
    - cloud computingdiensten
    - datacentra
    - netwerken voor de levering van inhoud
    - beheerde diensten
    - beheerde beveiligingsdiensten
    - online marktplaatsen, online zoekmachines en platforms voor sociale netwerkdiensten
    - vertrouwensdiensten

De meldplicht houdt in dat organisaties melding moeten maken bij de bevoegde autoriteit als ze getroffen zijn door een incident dat aanzienlijke gevolgen heeft voor de verlening van hun diensten. Binnen 24 uur moeten zij een waarschuwing indienen en vervolgens binnen 72 uur een incidentmelding.

Boetes
De richtlijn verplicht effectieve handhaving en vermeldt dat er waar nodig doeltreffende, evenredige en afschrikwekkende sancties worden opgelegd bij overtreding. Er kunnen boetes worden opgelegd die kunnen oplopen tot:

- voor essentiële entiteiten: 10 miljoen of 2% van de wereldwijde jaaromzet.
- voor belangrijke entiteiten: 7 miljoen of 1,4% van de wereldwijde jaaromzet.

Op dit moment is het zo dat de betreffende bevoegde autoriteit en toezichthoudende dienst afhangt van de sector waarin u actief bent.

Uitwerking in Nederland
Organisaties in tal van sectoren zullen maatregelen moeten treffen om de cybersecurity naar een hoger niveau te tillen. De details zullen uiteindelijk blijken uit de resulterende wetgeving, net zoals de Wbni het resultaat is van de implementatie van de NIS1-richtlijn.

De NIS2-richtlijn moet uiterlijk 17 oktober 2024 worden omgezet in nationale wetgeving. De richtlijn laat ruimte voor nationale invulling, dus we gaan zien wat er in Nederland tot stand komt.

Rechter oordeelt: niet IT-leverancier, maar gemeente aansprakelijk voor grote hack

In 2022 was het volop in het nieuws: de gemeente Hof van Twente eiste €4,2 miljoen van haar IT-leverancier voor geleden schade na een grootschalige hack. De rechter stuurde aan op een schikking, maar dat mislukte. In mei van dit jaar kwam er dan eindelijk de uitspraak in deze zaak. Wat blijkt? De IT-beheerder gaat vrijuit en bij de gemeente is er nog meer misgegaan dan we al dachten....

Hoe een ramsomware aanval tot een eis van 4,2 miljoen euro leidde
In 2020 wordt de gemeente Hof van Twente getroffen door een ransomware aanval. De gemeente weigert het losgeld te betalen, waarna data op back-ups en virtuele servers vernietigd wordt door de hackers. Geschatte schade is €4,2 miljoen en die wil de gemeente verhalen op haar IT-leverancier.

Op welke grond?

Volgens de gemeente is er sprake van een toerekenbare tekortkoming in de nakoming van de overeenkomst, schending van de zorgplicht dan wel een onrechtmatige daad.

Uit onafhankelijk onderzoek blijkt namelijk dat hackers al een jaar voor de geslaagde hack tienduizenden inlogpogingen per dag deden op de servers van de gemeente. Ook werd er een maand ervoor malware geplaatst. Het IT-bedrijf greep volgens de gemeente niet in en stelde de gemeente ook niet op de hoogte.

De IT-leverancier ziet dat heel anders. De gemeente wijzigde namelijk zelf het wachtwoord van de servers naar het eenvoudig te raden 'Welkom2020'. Daarnaast wijzigde de systeembeheerder van de gemeente zonder overleg een regel in de firewall. Hierdoor kwam de poort naar buiten wagenwijd open te staan en kon iedereen via internet verbinding zoeken met de FTP-server van de gemeente.

Mislukte schikking leidt tot nieuwe zitting met saillante details
Na de eerste zitting eind vorig jaar stuurde de rechter beide partijen naar de onderhandelingstafel om te schikken. De rechter zette namelijk vraagtekens bij het wachtwoordbeleid van de gemeente en vroeg de partijen om er samen uit te komen. Er wordt geen schikking bereikt, waarop er een nieuwe zitting plaatsvindt.

Tijdens deze zitting zijn nog meer details naar buiten gekomen over de omstandigheden rondom de ransomware aanval. Aangezien de gemeente haar IT-leverancier beticht van schending van de zorgplicht, is er nader gekeken naar de overeenkomst, offertes en communicatie tussen beide partijen.

Security monitoring viel buiten de scope
De gemeente verwijt de IT-beheerder geen melding te hebben gemaakt van de vele inlogpogingen en geen actie te hebben ondernomen na het plaatsen van malware in de periode voorafgaand aan de hack. Uit de aanbestedingsstukken blijkt echter dat de IT-beheerder niet verantwoordelijk kan worden gesteld voor security monitoring, oftewel het monitoren op beveiligingsincidenten. Contractueel is het IT-bedrijf alleen verantwoordelijk voor het goed functioneren van de servers, de opslag en de netwerkvoorzieningen.

Van de IT-beheerder mocht dus niet worden verlangd dat deze specifiek op veiligheidsrisico's zou monitoren, zoals bijvoorbeeld door het instellen van een 'alarm' bij een bepaald aantal ongeautoriseerde inlogpogingen. Alleen als deze ongeautoriseerde inlogpogingen van invloed waren op de beschikbaarheid, capaciteit of performance mocht actie worden verwacht. De gemeente heeft niet bewezen dat deze inlogpogingen de beschikbaarheid, capaciteit of performance daadwerkelijk hebben beïnvloed.

Offertes anti-virus software en back-up hardening afgewezen
In de periode voorafgaand aan de hack heeft de IT-leverancier een voorstel gedaan tot vervanging van de anti-virus software, met name ter bescherming tegen gijzelsoftware. Deze offerte is afgewezen.

Daarnaast heeft de IT-beheerder in het voorjaar van 2020 nog een offerte uitgebracht, waarin wordt voorgesteld om de back-upserver en NAS te isoleren en de back-upserver buiten de Active Directory te plaatsen.

Daarbij wordt als reden opgegeven: “het ontvreemden van domein beheeraccount gegevens is één van de meest voorkomende “hack” methodes en stelt de hacker in staat de back-up server met daaraan gekoppelde opslag apparaten te benaderen en daarna te gijzelen.” Tot slot biedt de IT-beheerder ook nog de mogelijkheid tot offsite-backup. Het voorstel tot back-up hardening wordt afgewezen door de gemeente.

Overigens komt in de zaak ook naar voren dat niet alleen de IT-leverancier, maar ook de accountant van de gemeente vóór de cyberaanval diverse keren heeft gewaarschuwd voor de risico’s op het gebied van informatiebeveiliging en cyberaanvallen.

Uitspraak rechter: IT-leverancier heeft de zorgplicht niet geschonden
De rechter maakt tijdens de uitspraak de optelsom als volgt:

- de gemeente is zelf verantwoordelijk voor het wachtwoordbeleid;
- de gemeente heeft zelf de firewall aangepast en zo de poort naar buiten opengezet;
- de IT-leverancier was niet verantwoordelijk voor security monitoring;
- de IT-leverancier heeft voorgesteld de beveiliging en back-up te verbeteren en hier heeft de gemeente niets mee gedaan.

Aangaande het laatste punt meldt de rechter zelfs: “in zoverre heeft de gemeente de invulling van de zorgplicht door de IT-beheerder in feite verhinderd.”

De vorderingen van de gemeente worden door de rechtbank afgewezen en de gemeente wordt veroordeeld om de proceskosten te betalen.

3. Nieuwe Europese wetgeving: van DORA tot European Accessiblity Act

In 2023 stonden we uitgebreid stil bij nieuwe Europese verordeningen en richtlijnen. Sommige ervan zijn inmiddels aangenomen en over andere wordt nog onderhandeld in Europa. In dit jaaroverzicht bespreken we er 5 in het kort: de Digital Operational Resilience Act (DORA), de Artificial Intelligence Act, de EU Data Act, de richtlijn DAC7 en de European Accessibility Act.

Digital Operational Resilience Act (DORA)

Financiële instellingen zijn enorm afhankelijk van hun IT-systemen. Ernstige storingen in netwerk- en informatiesystemen - bijvoorbeeld door een cyberaanval - kunnen grote economische gevolgen hebben. Om deze risico's het hoofd te bieden heeft Europa de Digital Operational Resilience Act (DORA) aangenomen. Deze wetgeving vergroot de digitale weerbaarheid van de financiële sector. Financiële entiteiten hebben tot januari 2025 om de wet te implementeren, maar ook hun IT-dienstverleners moeten zich goed voorbereiden op DORA want bepaalde regels gelden ook voor hen.

Wat is DORA?

De wet digitale operationele veerkracht moet ervoor zorgen dat de financiële sector in Europa bij ernstige operationele verstoringen veerkrachtig blijft functioneren. Koste wat kost moet voorkomen worden dat het betalingsverkeer stil komt te liggen door cyberaanvallen of andere IT-incidenten.

Met DORA introduceert Europa één standaard op het gebied van ICT-weerbaarheid en risicomanagement in de Europese financiële sector. Deze wetgeving stelt uniforme eisen aan de beveiliging van netwerk- en informatiesystemen van bedrijven en organisaties die actief zijn in de financiële sector.

Let op!

De regels gelden ook voor cruciale derde partijen die hen ICT-gerelateerde diensten verlenen, zoals cloudplatforms, managed services en data-analyse.

Voor wie geldt DORA?
De DORA moet deelnemers aan het financiële systeem de nodige garanties geven om cyberaanvallen en andere risico's te beperken. Het gaat hierbij onder meer om banken, verzekeraars, handelsplatformen, beleggingsinstellingen en aanbieders van crypto-activadiensten. Daarnaast geldt de DORA voor ICT-leveranciers van financiële bedrijven en voor (ICT-)bedrijven die zelf financiële diensten leveren.

De DORA houdt overigens rekening met de grootte, het risicoprofiel en het systeembelang van betrokken organisaties. Het proportionaliteitsbeginsel wordt hierbij toegepast, waardoor niet alle financiële entiteiten aan dezelfde strenge eisen hoeven te voldoen.

Welke regels stelt de DORA aan de IT van financiële entiteiten?
De DORA eist van financiële instellingen en hun ICT-leveranciers dat zij bestand zijn tegen allerlei soorten ICT-verstoringen en -dreigingen. De wetgeving is opgesplitst in diverse onderdelen, namelijk:

- ICT-risicobeheer
- ICT-gerelateerde incidentrapportages
- Digitale operationele veerkrachttesten
- Beheer van ICT-risico's van derden (ICT-leveranciers)
- Uitwisseling van informatie

Meer weten over de regels? Lees dan verder in onze blog over de DORA.

Hoe nu verder?
De DORA is formeel aangenomen in Europa en moet nu door elke EU-lidstaat in wetgeving worden omgezet. Ook door Nederland.

Tegelijkertijd ontwikkelen de betrokken Europese toezichthoudende autoriteiten technische normen waaraan alle instellingen voor financiële diensten zich moeten houden. De nationale bevoegde autoriteiten zullen het toezicht vervolgens op zich nemen en de DORA vanaf januari 2025 handhaven.

Niet alleen voor financiële entiteiten, maar ook voor ICT-leveranciers is het zaak om de DORA goed te bestuderen. Niet alleen op het gebied van ICT-risicobeheersing, maar ook contractueel heeft de DORA bijvoorbeeld gevolgen. Zo moeten financiële entiteiten ervoor zorgen dat ze hun overeenkomst met een ICT-leverancier onder bepaalde omstandigheden kunnen beëindigen.

Artificial Intelligence Act

Europa werkt wereldwijd als eerste aan Artificial Intelligence (AI) wetgeving. Nu de technologische ontwikkelingen elkaar razendsnel opvolgen, maakt Europa ook vaart. Eind 2023 werd een voorlopig akkoord gesloten, waarin bijvoorbeeld ook ChatGPT is opgenomen.

De Artificial Intelligence Act in het kort

Steeds vaker denken computers voor ons en dat niet alleen. Met de komst van ChatGPT hebben we gezien dat AI-systemen ook zelf content kunnen creëren.

Europa wil graag dat haar inwoners op een veilige manier gebruik kunnen maken van nieuwe technologie. Daarvoor is vertrouwen en dus wetgeving nodig. De voorgestelde Artificial Intelligence Act bevat een risicogebaseerde aanpak en deelt systemen in 3 categorieën in:

- onaanvaardbaar risico;
- hoog risico;
- beperkt of minimaal risico.

Zoals de naam al verraadt, zijn AI-systemen in de categorie ‘onaanvaardbaar risico’ verboden. Dit zijn systemen die grondrechten schenden of een grote bedreiging vormen voor de samenleving. Denk aan manipulerende systemen die aansporen tot ongewenst gedrag.

AI-systemen met een hoog risico zijn toegestaan, maar wel onder strenge voorwaarden. Zo moet er onder meer passend menselijk toezicht zijn en moeten gebruikers duidelijk en adequaat geïnformeerd worden. Het gaat hier om systemen die als risicovol worden gezien en bijvoorbeeld gebruikt worden in het onderwijs, kritieke infrastructuurnetwerken of bij wetshandhaving.

Zijn de risico’s beperkt of minimaal (dat zal waarschijnlijk gelden voor het grootste deel van de AI-systemen), dan gelden volgens het huidige voorstel van de Artificial Intelligence Act enkel transparantieverplichtingen.

Meer weten over de Artficial Intelligence Act?
Lees dan online verder in de blogs:
Europa bereikt voorlopig akkoord over Artificial Intelligence Act
Eerste Artificial Intelligence Act in zicht: ook ChatGPT ontkomt er niet aan.

EU Data Act

Data is het nieuwe goud, wordt weleens gezegd. Daar wil Europa beter van kunnen profiteren door middel van de EU Data Act. Deze in 2023 aangenomen verordening geeft Europese bedrijven en consumenten meer controle over hun eigen data. Tegelijkertijd wordt de macht van Amerikaanse techbedrijven als Google, Microsoft en Amazon ingeperkt.

EU Data Act aangenomen

In februari van 2022 kwam Europa met het voorstel voor de EU Data Act. Dit voorjaar werd een tussentijds akkoord bereikt en op 9 november 2023 heeft het Europees Parlement de EU Data Act aangenomen.

Deze verordening bevat onder meer regels over het vereenvoudigen van de toegang tot data en het kunnen wisselen van cloudprovider voor gebruikers binnen de EU. Naar verwachting zal deze verordening een boost geven aan de data economie in Europa en zal het voordelen opleveren voor Europese bedrijven.

De Data Act geeft zowel personen als bedrijven meer controle over hun gegevens. Deze Europese wetgeving maakt duidelijk wie waarde kan creëren uit data en onder welke voorwaarden.

Wat zijn de belangrijkste regels uit de EU Data Act?

- Slimme producten en gerelateerde diensten die data verzamelen, moeten zodanig worden ontworpen en vervaardigd dat product- en gerelateerde dienstgegevens standaard toegankelijk zijn voor gebruikers.
- Op verzoek van een gebruiker moeten fabrikanten en andere gegevenshouders de data ook aan een derde partij ter beschikking stellen. Gebruikers zijn voor onderhoud en reparatie niet langer afhankelijk van de maker.
- De Data Act stelt klanten in staat om snel en efficiënt over te stappen van de ene cloudprovider naar de andere: geen ‘lock-in’ situaties meer.
- Er mogen geen oneerlijke contractvoorwaarden worden opgelegd door een partij met een veel sterkere onderhandelingspositie.
- In uitzonderlijke situaties moet het voor overheidsinstanties mogelijk zijn om toegang te krijgen tot en gebruik te maken van gegevens die in het bezit zijn van de particuliere sector.

Meer weten over de EU Data Act?

Lees dan verder in de blog: ‘Akkoord Europese Data Act’.

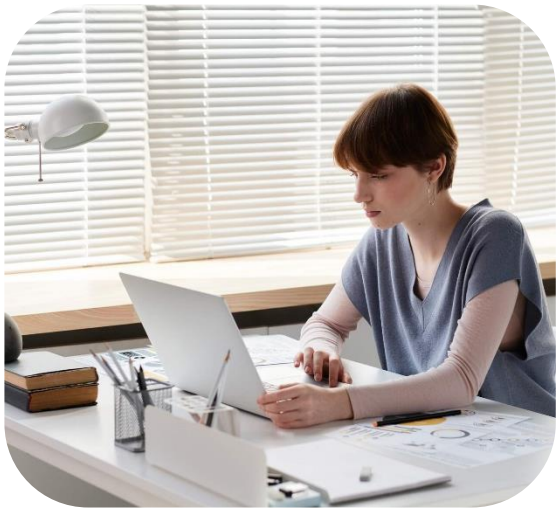
Richtlijn DAC7

Om belastingontduiking via digitale platforms op Europees niveau aan te pakken, werd in 2021 de nieuwe richtlijn DAC7 aangenomen. In 2024 zijn bepaalde digitale platforms voor het eerst verplicht om over het kalenderjaar 2023 te rapporteren. Ze moeten aan de Belastingdienst informatie verstrekken over verkopers en de via het digitale platform gegenereerde inkomsten.

Wat houdt de richtlijn DAC7 in?

In 2021 nam de Raad van de Europese Unie de richtlijn DAC7 aan. Deze richtlijn betreft de administratieve samenwerking tussen belastingdiensten in verschillende EU-lidstaten op het gebied van de digitale economie.

Waarom DAC7 is aangenomen?



Het komt geregeld voor dat verkopende partijen op digitale platforms hun belasting niet of in de verkeerde EU-lidstaat opgeven. Het doel van deze richtlijn is om deze bedoelde of onbedoelde belastingontduiking via digitale platforms te voorkomen.

Dankzij de DAC7 krijgen belastingautoriteiten binnen de hele EU toegang tot relevante belastinginformatie. Bepaalde digitale platforms zijn namelijk verplicht om informatie over verkopende partijen te verstrekken. De gedachte is dat er zo meer transparantie ontstaat met betrekking tot de activiteiten die via digitale platformen lopen. Inkomsten kunnen daardoor worden belast in de EU-lidstaat die daar recht op heeft.

DAC7 is in 2022 in Nederland geïmplementeerd met de Wet implementatie EU-richtlijn gegevensuitwisseling digitale platformeconomie.

Meer weten over de richtlijn DAC7?

Lees dan online verder in onze blog over de richtlijn DAC7.

European Accessibility Act

28 juni 2025 moeten bedrijven voldoen aan de European Accessibility Act. Het lijkt nog ver weg, maar dat is zeker geen reden voor uitstel. Het voor iedereen toegankelijk maken van uw digitale producten en diensten is misschien wel meer werk dan u denkt. Hieronder een toelichting op de richtlijn, de status ervan en hetgeen u kunt doen om eraan te voldoen.

Wat houdt de European Accessibility Act in?

De European Accessibility Act – in Nederland de Europese toegankelijkheidswet genoemd – moet het voor mensen met een beperking net zo goed mogelijk maken om digitale producten en diensten te gebruiken als voor mensen zonder beperking.

Nederland telt miljoenen mensen met een (vorm van) functiebeperking, zoals slechtziendheid, doofheid, (kleuren)blindheid, autisme en laaggeletterdheid. Door de toenemende vergrijzing zal dit aantal de komende jaren naar verwachting verder oplopen.

Op welke producten en diensten is deze wetgeving van toepassing?

Het is essentieel dat mensen met een beperking gewoon kunnen blijven meedoen in de huidige, digitale maatschappij. Daarom moet onder meer online bankieren, reizen met trein, bus of metro en winkelen via webshops voor iedereen goed mogelijk zijn. De nieuwe wetgeving wordt van toepassing op onder meer:

- computers en besturingssystemen;
- e-commerce diensten (websites, -shops en apps);
- audiovisuele mediadiensten;
- e-books;
- smartphones, tables en tv-apparatuur;
- geldautomaten, ticket- en inchecksystemen;
- diensten van vervoersbedrijven, zoals kaartjesautomaten, apps en websites;
- financiële diensten, zoals internetbankieren.

Hele kleine organisaties (minder dan 10 werknemers) zijn uitgezonderd van deze wetgeving en hoeven niet te voldoen aan de bijkomende verplichtingen. Websites en apps van Nederlandse overheidsinstellingen moeten al sinds de zomer van 2018 voor iedereen toegankelijk zijn. Dit is vastgelegd in het Tijdelijk besluit digitale toegankelijkheid overheid.

Meer weten over de European Accessibility Act?

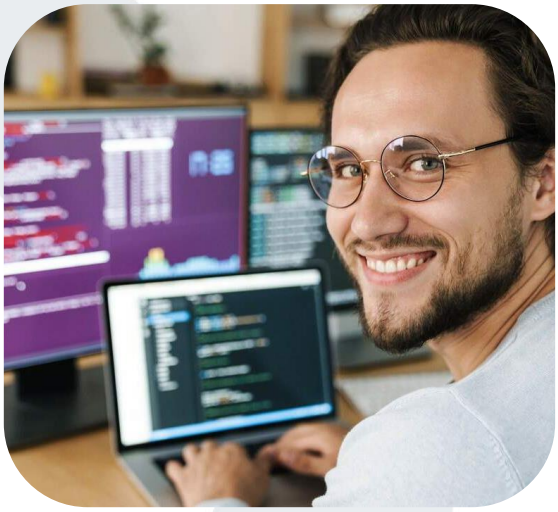
Lees dan verder in onze blog '[Hoe digitaal toegankelijk is uw bedrijf?]'.

Niks missen in 2024?

Dit waren de belangrijkste ontwikkelingen in ICT & recht in 2023. Wilt u ook in 2024 op de hoogte blijven van nieuwe wetsvoorstellen, belangrijke uitspraken, de opvolger van het Privacy Shield en nog veel meer? Abonneert u zich dan op onze maandelijkse nieuwsbrief en ontvang onze blogs automatisch in uw mailbox.

Over Legalz

ICT-advocatenkantoor Legalz in Rotterdam is gespecialiseerd in de juridische zaken rond de ontwikkeling, levering en exploitatie van ICT-producten en -diensten. Zo helpen wij al jarenlang ontwikkelaars, leveranciers en afnemers van apps, platforms en software bij de totstandbrenging van de contracten en het oplossen van geschillen. Ook staan wij opdrachtgevers bij die over dezelfde kennis en ervaring willen beschikken bij het sluiten van contracten of oplossen van geschillen met leveranciers.



ICT-advocatenkantoor Legalz werd in 2011 opgericht door ICT-advocaat Robert Grandia. Hij en zijn team werken vanuit de filosofie dat zaken op het terrein van ICT-recht expertise vergen van een ICT-advocaat of ICT-jurist die over kennis van beide domeinen beschikt.

Wilt u meer weten over de juridische aspecten van het inkopen van IT? Kijk dan eens op onze website of neem contact met ons op via contact@legalz.nl of door te bellen naar 010 2290 646.

Over Legalz Opleidingen

Legalz Opleidingen is de opleidingstak van ICT-advocatenkantoor Legalz. Lastige topics als cloud-contracten, Service Level Agreements en contractmanagement maken wij toegankelijk. In uw eigen taal, praktisch toepasbaar en gericht op juridische ICT-topics.

Onze trainingen zijn voor iedereen die met ICT-contracten te maken krijgt. Van inkoper tot contractmanager en van sales manager tot directeur.

Legalz Opleidingen biedt verschillende trainingen op het gebied van ICT-contracten en contractmanagement. Kijk voor onze trainingen op www.legalz-opleidingen.nl