jaaroverzicht 2022

De meest besproken ontwikkelingen in ICT & recht:

Van privacy tot cyberaanvallen

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. 2022 was een veelbewogen jaar met nieuwe wetten en regels, diverse rechtszaken en veel heisa over het uitwisselen van data met Amerikaanse bedrijven.

Dat laatste is kenmerkend voor de periode sinds de nietigverklaring van het Privacy Shield in de zomer van 2020. Sindsdien struikelen Europese toezichthouders over het gebruik van Amerikaanse platforms, tooling en social media. Ook worden er rechtszaken gevoerd over de inzet van clouddiensten van Amerikaanse techbedrijven. Is het nog wel mogelijk om onder de AVG veilig persoonsgegevens uit te wisselen met de Verenigde Staten? En waar blijft de opvolger van het Privacy Shield? U vindt de antwoorden in dit jaaroverzicht.

Ook zoomen we in op diverse nieuwe Europese wetsvoorstellen die dit jaar zijn goedgekeurd. Denk aan de Digital Services Act, die geldt voor online tussenpersonen en onder meer bepaalt hoe wordt omgegaan met illegale of potentieel schadelijke online content en de rechten van gebruikers online beschermt. Een impactvolle wet, waarvan de overgangsperiode om de wet te implementeren nu al in werking is getreden. Op 17 februari 2024 is de wet in heel Europa van toepassing.

In dit jaaroverzicht lichten we ook verschillende rechtszaken uit, die van belang zijn voor de dagelijkse praktijk. Daarnaast bespreken we de enorme toename van datalekken door cyberaanvallen, waarvan opvallend genoeg steeds meer IT-leveranciers het slachtoffer zijn. Uiteraard vertellen we wat u kunt doen bij een datalek en hoe u de impact ervan verkleint.

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 2023.

Op een succesvol nieuw jaar!

Mr. Robert Grandia
Oprichter en eigenaar ICT-advocatenkantoor Legalz

1. Waar blijft de opvolger van het Privacy Shield?

Als het jaar 2022 één ding duidelijk heeft gemaakt, dan is het wel dat we snel een opvolger voor het Privacy Shield nodig hebben. Steeds meer IT-diensten en -oplossingen van Amerikaanse techbedrijven worden in twijfel getrokken, want wordt de privacy eigenlijk wel goed geborgd? Een lichtpuntje is de Executive Order voor veilige gegevensuitwisseling die de Amerikaanse president Biden in oktober tekende, hoewel het nog maar de vraag is of die wél AVG-proof is....

Amerikaanse clouddiensten onder vuur door strenge privacywetgeving

Het gebruik van clouddiensten van Amerikaanse bedrijven is niet AVG-proof, zo concludeert de toezichthoudende aanbestedingskamer in een Duitse deelstaat in augustus 2022. Daarom mogen deze techbedrijven gepasseerd worden bij aanbestedingen en mag hun aanbod bij inschrijving genegeerd worden. Deze Duitse uitspraak toont aan hoe wankel de gegevensoverdracht tussen Europa en Amerika momenteel is. De grote vraag is of en wanneer er drastische maatregelen genomen worden.....

Amerikaanse cloud providers uitgesloten bij Duitse aanbestedingen?

De openbare aanbestedingskamer van de deelstaat Baden-Württemberg heeft geconcludeerd dat het gebruik van de clouddienst van een Amerikaanse partij die meedeed aan een aanbestedingsprocedure in strijd is met de Europese privacywetgeving.

In deze zaak had een in de EU gevestigde dochteronderneming van een Amerikaanse aanbieder van server- en clouddiensten deelgenomen aan een aanbestedingsprocedure. Hoewel de servers die werden gebruikt om diensten te verlenen zich binnen de EU bevonden, vond de Kamer voor Overheidsopdrachten dat dit een inbreuk is op de AVG. Als gevolg van deze inbreuk moet een overeenkomstige inschrijving worden uitgesloten van de aanbestedingsprocedure, aldus de Kamer voor Overheidsopdrachten.

Deze uitspraak gaat specifiek in op een Amerikaanse partij die diensten aanbiedt via een dochteronderneming in Europa. Problematisch, want dat is dé oplossing die veel Amerikaanse techgiganten hebben gekozen om op Europees grondgebied hun diensten aan te kunnen blijven bieden ondanks de strenge privacywetgeving.

Volgens de Kamer volstaat de loutere mogelijkheid van toegang tot persoonsgegevens door de Amerikaanse moedermaatschappij om een doorgifte naar de VS te impliceren. Of zo'n datastroom daadwerkelijk plaatsvindt, is dus niet relevant. Alleen al de mogelijkheid is voldoende.
Het besluit is nog niet definitief, er is inmiddels hoger beroep aangetekend. Als dit besluit wordt gehandhaafd, dan worden grote cloudproviders zoals Microsoft, Amazon en Google uitgesloten van toekomstige samenwerking met de Duitse autoriteiten. Uiteraard heeft deze uitspraak dan ook een storm van protest ontketend.

Het gebruik van Amerikaanse entiteiten door Europese door Amerikaanse partijen

Ook in Nederland wordt nagedacht over de wijze waarop we gegevens kunnen blijven uitwisselen met Amerika. Zo verscheen deze zomer op de website van het Nationaal Cyber Security Centrum een memo over de reikwijdte van de Amerikaanse Clarifying Lawful Overseas Use of Data (CLOUD) Act.

Deze wet verschaft Amerikaanse inlichtingendiensten toegang tot Europese persoonsgegevens die verwerkt worden door Amerikaanse partijen.
De Nederlandse overheid heeft bij een internationale advocatenfirma advies hierover opgevraagd. Hoe zorgen Europese cloud providers en partijen (Europese entiteiten) dat ze niet geraakt worden door deze CLOUD Act?

Uit de memo blijkt het volgende: Europese entiteiten kunnen binnen het bereik van de CLOUD Act vallen, ook als ze buiten de Verenigde Staten zijn gevestigd. Om ervoor te zorgen dat deze entiteiten volledig buiten de reikwijdte van de CLOUD Act vallen moeten ze persoonsgegevens verwerken met behulp van een niet-Amerikaanse entiteit, die ofwel:

1. geen zakelijke relatie heeft met een bedrijf dat aanwezig is in de VS (zoals een Amerikaanse dochteronderneming) en die onvoldoende contacten heeft met de VS om Amerikaanse jurisdictie te laten gelden over de EU-entiteit/niet-Amerikaanse entiteit (dit omvat ook het niet verkopen van producten of diensten aan klanten in de VS); of;
2. als het wel een zakelijke relatie heeft met een bedrijf gevestigd in de VS, dan mag dit bedrijf de gegevens die zijn opgeslagen in de EU niet bezitten, opslaan of controleren.

Sowieso wordt in de memo gesteld dat een Europese entiteit absoluut geen Amerikaanse moedermaatschappij mag hebben, omdat deze in het 'bezit' is van de data. Daarnaast wordt geadviseerd om geen Amerikaanse staatsburgers in dienst te nemen die toegang hebben tot relevante data. Als het advies in deze memo opgevolgd wordt, heeft dit uiteraard grote impact op het gebruik van Amerikaanse clouddiensten.

Onzekere toekomst voor data-uitwisseling met de VS
Sinds de nietigverklaring van het Privacy Shield in 2020 worden vaker rechtszaken gevoerd en voorstellen gedaan om de gegevensuitwisseling met Amerikaanse partijen aan banden te leggen of zelfs te verbieden.

In 2022 berichtten we over een conceptbesluit van de Ierse privacytoezichthouder, die ervoor kan zorgen dat Facebook en Instagram binnenkort niet meer toegankelijk zijn voor Europeanen. De toezichthouder wil namelijk de overdracht van data van Europa naar de VS door moederbedrijf Meta blokkeren. Daarnaast oordeelde de Oostenrijkse privacy toezichthouder begin van 2022 dat het gebruik van Google Analytics in strijd is met de AVG.

Hoewel er steeds meer van dit soort uitspraken en besluiten in het nieuws komen, zijn er tot op heden geen drastische stappen gezet om data-uitwisseling met Amerika daadwerkelijk stop te zetten. De vraag is ook in hoeverre een verbod op het gebruik van Amerikaanse (cloud)diensten reëel is. Wij zijn als samenleving immers in grote mate afhankelijk van Amerikaanse techgiganten als Google en Microsoft.

Biden ondertekent Executive Order voor veilige gegevensuitwisseling: is deze wél AVG-proof?!

De Amerikaanse president Biden heeft op 7 oktober 2022 de Executive Order voor veilige gegevensuitwisseling ondertekend. Deze opvolger van het Privacy Shield moet de zorgen van Europa op het gebied van privacy wegnemen en veilige uitwisseling van persoonsgegeven waarborgen. Grote vraag is: doet het dat ook of stapt Schrems weer naar het Europese Hof van Justitie?

Van Privacy Shield naar Executive Order
Tot de zomer van 2020 vertrouwden we allemaal op het Privacy Shield als mechanisme om gegevens uit te wisselen tussen Europa en de Verenigde Staten.

Volgens de AVG mogen persoonsgegevens niet zomaar worden doorgegeven aan personen of organisaties buiten de Europese Economische Ruimte (EER). Dit is alleen toegestaan als er in het desbetreffende land sprake is van een passend beschermingsniveau. De Verenigde Staten bieden geen passend beschermingsniveau. Het Privacy Shield zorgde ervoor, in de vorm van juridisch bindende afspraken tussen de EER en de VS, dat doorgifte naar de VS toch toegestaan was

In de rechtszaak Schrems II werd het Privacy Shield echter nietig verklaard. Belangrijkste reden? De 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. Dit betreft dus niet alleen de strikt noodzakelijke gegevens, zoals in de EU. Dat is echter niet het enige probleem.

Het Amerikaanse ombudsman-mechanisme biedt onvoldoende bescherming aan EU-burgers met een klacht over de verwerking van hun persoonsgegevens in de VS. Betrokkenen hebben ook geen voor de rechter afdwingbare rechten tegenover de Amerikaanse autoriteiten. De Executive Order moet deze en andere zorgen wegnemen.

Wat houdt de Executive Order in?
De Executive Order moet het rechtsgeldige alternatief worden voor het Privacy Shield. Het zal dus de privacy van persoonsgegevens van Europese burgers moeten waarborgen. Op het eerste oog lijkt dit ook te gebeuren. De Executive Order:

- voegt aanvullende waarborgen toe voor activiteiten van Amerikaanse inlichtingendiensten, waaronder de eis dat dergelijke activiteiten alleen worden uitgevoerd om gedefinieerde nationale veiligheidsdoelstellingen na te streven. Hierbij wordt rekening gehouden met de privacy en de activiteiten moeten noodzakelijk en proportioneel zijn.

- eist van de Amerikaanse inlichtingendiensten om hun beleid en procedures bij te werken op basis van de aanvullende waarborgen.
- biedt een alternatief voor het ombusman-mechanisme, waarbij klachten en bezwaren van Europese inwoners en instellingen in 2 stappen onpartijdig en onafhankelijk worden behandeld. De klacht wordt allereerst bestudeerd en behandeld door een ambtenaar van de nationale inlichtingendienst en vervolgens wordt diens oordeel onder de loep genomen door een nog op te richten rechtbank voor gegevensbescherming (DPRC).

Wat vindt Schrems van de Executive Order?
Max Schrems heeft ervoor gezorgd dat het Privacy Shield werd nietig verklaard. Uiteraard heeft hij ook al gereageerd op deze Executive Order via de door hem opgerichte privacy organisatie NOYB. Zijn eerste reactie is niet positief en volgens hem houdt dit alternatief voor het Privacy Shield geen stand. Waarom niet?

Allereerst meent hij dat de formulering over de rechten van de Amerikaanse inlichtingendiensten weliswaar is aangepast, maar dat dit niet betekent dat Europa en de VS dezelfde interpretatie hierover hebben. Er zijn namelijk geen aanwijzingen dat de massasurveillance door de VS in de praktijk zal veranderen. Zo zal zogenaamde 'bulk surveillance' onder de nieuwe Executive Order blijven bestaan, terwijl dit door het Europese Hof van Justitie als niet evenredig is bestempeld. Dus hoewel de woorden zijn veranderd, lijken Europa en de VS geen overeenstemming te hebben bereikt over de juridische betekenis ervan.

Problematisch, aldus Schrems. Dat geldt ook voor de nieuw op te tuigen rechtbank voor gegevensbescherming. Volgens Schrems zal dit namelijk geen rechtbank zijn, zoals vermeld staat in de Amerikaanse grondwet. Het wordt een orgaan binnen de uitvoerende macht en daarmee volgens Schrems dus eigenlijk een veredelde vorm van het door het Europese Hof van Justitie afgekeurde ombudsman-mechanisme.

Tot slot staat er op de site van NOYB te lezen dat de organisatie de Executive Order nader gaat bestuderen en nog met een uitgebreide analyse komt. Max Schrems meldt wel alvast: "Op het eerste gezicht lijkt het erop dat de kernproblemen niet zijn opgelost en dat het vroeg of laat terug naar het Europese Hof van Justitie zal gaan."

In 2023 zullen we dus ongetwijfeld weer te maken krijgen met privacyvraagstukken rondom het gebruik van Amerikaanse IT-diensten.

2. Schrikbarende groei datalekken door cyberaanvallen + wat te doen?

Opvallende cijfers publiceerde de Autoriteit Persoonsgegevens afgelopen jaar. In 2021 zijn 88% meer meldingen gedaan van datalekken door cyberaanvallen. Opvallend is dat IT-leveranciers steeds vaker doelwit zijn. Wij nemen de cijfers met u door en bespreken wat u kunt doen om de risico's te verkleinen.

88% meer meldingen van datalekken door cyberaanvallen

In 2021 zijn er fors meer meldingen van datalekken door cyberaanvallen gemaakt dan in 2020, zo maakt de Autoriteit Persoonsgegevens bekend. Opvallend is dat steeds meer IT-leveranciers slachtoffer worden van cyberaanvallen. Deze partijen verwerken veel persoonsgegevens en zijn daarom een aantrekkelijk doelwit voor cybercriminelen.

Forse stijging datalekmeldingen door cyberaanvallen

De Autoriteit Persoonsgegevens (AP) bracht begin dit jaar haar jaarlijkse rapportage uitgebracht met betrekking tot de AVG-verplichting om datalekken te melden. In 2021 ontving de AP 24.866 datalekmeldingen. Een stijging van 4% ten opzichte van 2020. 2.210 datalekmeldingen waren het gevolg van cyberaanvallen, oftewel hacking, malware en phishing. Hoewel het aantal meldingen van datalekken door cyberaanvallen slechts 9% van het totaal bedraagt, maakt de AP zich zorgen. Het aantal datalekmeldingen door cyberaanvallen is namelijk gestegen met 88% ten opzichte van 2020.
Opvallend is dat vooral IT-leveranciers doelwit lijken te zijn, omdat ze veel persoonsgegevens verwerken.

IT-leveranciers gewild doelwit voor cyberaanvallen

IT-leveranciers treden vaak op als verwerker voor organisaties. Bijvoorbeeld door het faciliteren van digitale werkplekken, het leveren van op maat gemaakte software en de opslag van data. Doordat ze veel persoonsgegevens verwerken, zijn IT-leveranciers een aantrekkelijk doelwit voor criminelen en wordt er geregeld geprobeerd om hen af te persen.

In 2021 hebben 28 IT-leveranciers een datalek door een cyberaanval gemeld bij de AP. Daarop meldden 1800 getroffen organisaties zich en dat leverde uiteindelijk minimaal 7 miljoen slachtoffers op. Cyberaanvallen bij IT-organisaties zijn dus impactvol. Niet alle datalekken worden echter gemeld, waardoor het aantal slachtoffers vermoedelijk nog hoger is.

Afwachtende houding
Opvallend is dat IT-leveranciers vaak wachten met het melden van een datalek bij hun klanten. Uit angst voor reputatieschade of in afwachting van een uitgebreid onderzoek. Dat zijn volgens de AP geen goede redenen. Als een IT-leverancier als verwerker kan worden aangemerkt, dan is de leverancier volgens de AVG verplicht om een datalek zo snel mogelijk te melden bij de verwerkingsverantwoordelijken, oftewel de klanten.

De verwerkingsverantwoordelijke moet vervolgens de afweging maken of het lek ernstig genoeg is om te melden bij de AP en/of bij de betrokkenen.
De Autoriteit Persoonsgegevens benadrukt dat wanneer IT-leveranciers de verwerkingsverantwoordelijken niet direct en volledig informeren, dit ertoe kan leiden dat IT-leveranciers de AVG overtreden.

Acties bij een datalek
Wilt u weten welke acties u moet nemen bij een datalek? De Autoriteit Persoonsgegevens heeft hiervoor een handige actiepagina gemaakt.

Daarnaast kunt u onze blog lezen: 'Datalek melden? Hoe gaat dat precies in zijn werk?'

Datalek bij uw IT-leverancier? Zo verkleint u de impact ervan

Nu IT-leveranciers steeds vaker doelwit zijn van cyberaanvallen, neemt het risico voor u als afnemer ook toe. Als er bijvoorbeeld via malware of phishing persoonsgegevens buit worden gemaakt, dan hebt u als verwerkings-verantwoordelijke een probleem. Gelukkig zijn er maatregelen die u vooraf kunt treffen om de impact van een datalek bij de IT-leverancier te verkleinen.

Toenemende risico's voor verwerkingsverantwoordelijken
In 2021 werden opvallend veel IT-leveranciers slachtoffer van een cyberaanval. Doordat ze veel persoonsgegevens verwerken, zijn ze een aantrekkelijk doelwit voor cybercriminelen. Dit heeft ook gevolgen voor u als klant van een IT-leverancier in het geval u kunt worden aangemerkt als verwerkingsverantwoordelijke. Uw werknemers, klanten en cliënten vertrouwen hun persoonsgegevens aan u toe. Het feit dat u de verwerking van hun persoonsgegevens uitbesteedt aan een leverancier, verandert niets aan uw verantwoordelijkheid.

Bij een datalek bent u als verwerkingsverantwoordelijke volgens de AVG verplicht daadkrachtig op te treden. Het is zaak het incident zo snel mogelijk te beëindigen en de schade te beperken. Daarnaast kan het nodig zijn om het lek te melden bij de Autoriteit Persoonsgegevens en/of bij de betrokken personen.

Uiteraard heeft de verwerker ook verantwoordelijkheden bij een datalek. Zo moet deze het lek na ontdekking tijdig melden bij de verwerkings-verantwoordelijke en er grondig onderzoek naar doen. Zorgen dat u de meldplicht datalekken goed naleeft? Dan adviseert de Autoriteit Persoonsgegevens (AP) u:

6 maatregelen om vooraf te treffen
Naar aanleiding van de recente toename in cyberaanvallen op IT-leveranciers, heeft de AP 6 aanbevelingen gedaan voor maatregelen die u als verwerkingsverantwoordelijke kunt treffen. Daar zijn:

1. Focus op beveiliging

Het is misschien een open deur, maar u bent en blijft verantwoordelijk voor de beveiliging van persoonsgegevens. Ook als u de verwerking hiervan volledig uitbesteedt. Daarom is het belangrijk dat u alleen in zee gaat met een leverancier die aantoonbaar zorgt voor de juiste beveiligingsmaatregelen. Op technisch en organisatorisch vlak, zoals voorgeschreven door de AVG. Heeft een leverancier de benodigde certificeringen en/of zijn garanties af te dwingen in het contract?

2. Deel niet meer dan nodig
Let erop dat u niet meer persoonsgegevens deelt dan strikt noodzakelijk en controleer of de leverancier zich houdt aan de regels. Check bijvoorbeeld of gegevens na het verlopen van de bewaartermijn inderdaad gewist worden.

3. Maak duidelijke afspraken
Maak in de verwerkersovereenkomst goede afspraken over de hulp die de IT-leverancier geeft bij de naleving van de meldplicht datalekken. Hoe snel moet de leverancier het lek melden en welke acties verwacht u bij een datalek?

4. Controleer op naleving
Net als bij ieder ander contract geldt ook voor de verwerkersovereenkomst: controleer of deze ook echt wordt nageleefd. Zorg dat u dit periodiek inplant, zodat u niet voor nare verrassingen komt te staan bij een datalek.

5. Maak een actieplan
Als een datalek zich voordoet, bent u als verwerkingsverantwoordelijke verplicht snel te handelen. De leverancier (verwerker) moet u zo snel mogelijk inlichten, u maakt meestal melding bij de Autoriteit Persoonsgegevens (binnen 72 uur) en afhankelijk van de impact moeten ook de betrokkenen direct geïnformeerd worden. Zorg daarom dat u een gedegen actieplan op de plank heeft liggen.

6. Houd het verwerkingsregister bij
In veel gevallen bent u verplicht een verwerkingsregister bij te houden. Dit register bevat een overzicht van de verwerkingen van persoonsgegevens die binnen een organisatie plaatsvinden.

Het is essentieel dat u zorgt voor een goed verwerkingsregister, dat ook wordt bijgehouden. Zowel bij uzelf als bij de IT-leverancier. Dit register helpt bij het maken van een inschatting hoeveel en welk type persoonsgegevens zijn betrokken bij een datalek. Zo kan een organisatie eenvoudiger bepalen wat de gevolgen van het lek zijn voor de betrokkenen en welke acties vervolgens genomen moeten worden.

3. DSA, DMA en Data Governance Act goedgekeurd

In 2022 werden 3 belangrijke Europese wetsvoorstellen goedgekeurd. De monopoliepositie van online platforms wordt aangepakt, Europeanen worden beter beschermd tegen illegale of potentieel schadelijke online content en het moet eenvoudiger worden om data binnen Europa veilig te delen. Wij schetsen in het kort de Digital Services Act, Digital Markets Act en Data Governance Act. Ook blikken we kort voortuit op nieuwe Europese wetsvoorstellen.

Digital Services Act

Dit jaar is de Digital Services Act (DSA) goedgekeurd. De DSA vervangt de huidige Europese regels voor digitale diensten (de zogenaamde e-commerce richtlijn), die nog uit het jaar 2000 stammen en nogal verouderd zijn. Deze wetgeving biedt te weinig bescherming aan consumenten en kleinere spelers op de markt. Ook is er een enorme opmars aan illegale handel en schadelijke online content (waaronder nepnieuws), die Europa tegen wil houden. De Digital Services Act moet hiervoor gaan zorgen.

Voor wie geldt de DSA?
De DSA zal van toepassing zijn op alle online tussenpersonen die diensten verlenen in de EU. De DSA definieert duidelijke verantwoordelijkheden voor aanbieders van intermediaire diensten. Hoe groter een aanbieder, hoe strenger de regels voor die partij zullen zijn.

De DSA onderscheidt de volgende partijen:

- Online platforms, die verkopers en consumenten samenbrengen. Denk aan online marktplaatsen, appstores, platforms voor deeleconomie en sociale media platforms.
- Zeer grote online platforms en zoekmachines. Deze brengen bijzondere risico's met zich mee bij de verspreiding van illegale inhoud, die maatschappelijke schade oplevert. Er zijn specifieke regels opgenomen voor platforms die meer dan 10% van de 450 miljoen consumenten binnen Europa bereiken.
- Acces providers (ook wel ‘mere conduit’), die netwerkinfrastructuur aanbieden, providers van internettoegang en domeinnaamregistrators.
- Hostingservices, zoals cloud- en webhostingservices.

Wat zijn de belangrijkste nieuwe regels?
Onder de DSA zullen aanbieders van intermediaire diensten niet alleen transparanter moeten zijn, maar zullen ook verantwoordelijk worden gehouden voor hun rol bij het verspreiden van illegale en schadelijke inhoud.
De DSA:

- stelt speciale verplichtingen vast voor online marktplaatsen om de online verkoop van illegale producten en diensten te bestrijden;
- introduceert maatregelen om illegale online content tegen te gaan en verplichtingen voor platforms om snel te reageren, met inachtneming van de grondrechten;
- beschermt minderjarigen beter door platforms te verbieden gerichte advertenties in te zetten op basis van persoonsgegevens van minderjarigen;
- legt bepaalde beperkingen op aan de presentatie van advertenties en aan het gebruik van gevoelige persoonlijke gegevens voor gerichte advertenties, waaronder geslacht, ras en religie;
- verbiedt misleidende interfaces die bekend staan als 'dark patterns' en praktijken gericht op misleiding.

Hoe nu verder?
De DSA is in Europa definitief goedgekeurd en in werking getreden. De DSA zal 17 februari 2024 in de hele EU van toepassing zijn. Tot die tijd geldt een overgangsperiode, waarin platforms acties moeten ondernemen om zich te conformeren aan de DSA. Voor online platforms geldt bijvoorbeeld dat ze drie maanden de tijd (tot 17 februari 2023) hebben om het aantal actieve eindgebruikers op hun websites te melden. De Commissie nodigt alle online platforms ook uit om de bekendgemaakte aantallen bij haar te melden. Op basis van die gebruikersaantallen zal de Commissie dan bepalen of een platform als zeer groot online platform of zeer grote online zoekmachine moet worden aangewezen.

Wordt u als zeer grote zoekmachine of platform aangewezen?
Dan moet u binnen 4 maanden al voldoen aan de verplichtingen op grond van de DSA.

Meer weten over de DSA?
Lees onze blog: 'Wetsvoorstel Digital Services Act: grote impact + opvallende verplichtingen'

Digital Markets Act

Deze wetgeving legt duidelijke regels op aan grote online platforms. Zo moeten ook kleine spelers een kans krijgen op een markt die gedomineerd wordt door partijen als Microsoft, Apple en Google.

Strenge regels voor 'poortwachters'

De monopoliepositie van grote techbedrijven gaat op de schop voor een eerlijkere behandeling van concurrenten en gebruikers door de zogenaamde poortwachters. Wat zijn dan die poortwachters?

Dat zijn online platforms met:

- een jaaromzet van tenminste € 7,5 miljard in de EU in de laatste 3 jaar; en/of
- een beurswaardering van tenminste € 75 miljard; en
- tenminste 45 miljoen maandelijks actieve eindgebruikers en 10.000 professionele gebruikers die in de EU zijn gevestigd.

Daarnaast moet het platform in tenminste 3 lidstaten zeggenschap hebben over een of meer kernplatformdiensten. Denk aan marktplaatsen, zoekmachines, appstores, sociale netwerken, clouddiensten en webbrowser.

Poortwachters zijn onder meer Amazon, Apple, Google, Meta en Microsoft. Ook een platform als Booking.com wordt gezien als poortwachter.

Duidelijke regels met grote impact

Afgelopen jaren werden door Europa vele onderzoeken ingesteld naar techreuzen als Google, Meta en Microsoft. Soms met hoge boetes als gevolg, maar vaak pas na jarenlang onderzoek. De nieuwe verordening voorkomt dergelijke langslepende onderzoeken. De regels zijn nu duidelijk. We lichten er een paar uit.

<u>Interoperabiliteit messagingplatforms</u>

Messagingsplatforms als WhatsApp en iMessage moeten zorgen voor interoperabiliteit van hun basisfuncties. Hierdoor krijgen kleinere platforms ook een kans en kunnen eindgebruikers ieder messagingplatform gebruiken en toch berichten ontvangen vanuit de grote spelers.

Hergebruik persoonsgegevens enkel mét toestemming
Platforms mogen persoonsgegevens die ze verzameld hebben voor een bepaalde prestatie niet gebruiken voor een andere prestatie. Dit houdt bijvoorbeeld concreet in dat de data die Meta verzameld binnen Facebook niet gecombineerd of gebruikt mag worden binnen Instagram. In ieder geval niet zonder toestemming van de gebruiker.

Softwaretoepassingen standaard installeren uit den boze
Belangrijke software mag niet als standaardinstelling bij de installatie van het besturingssysteem verplicht worden. Google mag dus niet langer standaard de Chrome-browser instellen voor gebruikers. Ook wordt er anders omgegaan met vooraf geïnstalleerde apps op telefoons. Zo moet het altijd mogelijk zijn om die apps van de telefoon te kunnen verwijderen.

Meer ruimte voor app-ontwikkelaars
App-ontwikkelaars worden nu vaak nog verplicht om van bepaalde diensten gebruik te maken als ze hun app in een appstore willen aanbieden. Vaak gaat het om een betaalsysteem of een identiteitsaanbieder. Dat wordt verleden tijd. Gebruikers moeten rechtstreeks aan de ontwikkelaars kunnen betalen, aldus de DMA.

Alle regels lezen? Kijk dan op de site van de Europese Raad.

Data Governance Act

In 2023 treedt de Data Governance Act (DGA) in werking. Deze verordening maakt het mogelijk om data veilig en eenvoudig te delen binnen Europa. Hierdoor wordt een boost gegeven aan gegevensdeling en versterkt het de concurrentiepositie van Europa op het gebied van data. Ook voor bedrijven biedt de DGA kansen.

Waarom een Data Governance Act?
Onze samenleving is datagedreven en Europa wil in het dataspeelveld een grotere rol innemen. Met de DGA wordt het eenvoudiger om data binnen de EU te delen, waarbij ook de veiligheid wordt gegarandeerd. Hierdoor wordt innovatie gestimuleerd en de drempel voor het ontwikkelen van nieuwe producten en diensten verlaagd.

Niet alleen de economie moet op deze wijze gestimuleerd worden. Ook gezamenlijke maatschappelijke problemen als klimaatverandering kunnen op deze manier beter aangepakt worden. Data wordt dus ook beschikbaar gesteld voor algemeen maatschappelijk belang.

Daarom gelden deze regels niet alleen voor bedrijven, maar ook voor overheden en Europese burgers.

Overigens zal de nog aan te stellen 'European Data Innovation Board' toezien op de toepassing van de verordening in de EU en waar nodig advies geven.

Speerpunten van de DGA
De maatregelen in de verordening zijn te verdelen in vier belangrijke pijlers:

1. Hergebruik van overheidsinformatie faciliteren
Het gaat dan vooral om overheidsgegevens die niet openbaar beschikbaar kunnen worden gesteld, maar wel belangrijke kennis opleveren. Door het hergebruik van bijvoorbeeld gezondheidsdata binnen de EU te vergemakkelijken, kan het onderzoek naar genezing van bepaalde ziektes een boost krijgen.

2. Data delen voor het algemeen belang
Een ander doel van de DGA is om het delen van waardevolle data zonder winstoogmerk te stimuleren. Het moet burgers en bedrijven makkelijker worden gemaakt om geheel vrijwillig hun data beschikbaar te stellen ten behoeve van de samenleving.

3. Verplichtingen voor gegevensbemiddelaars
De data wordt gedeeld binnen gemeenschappelijke Europese dataruimten en dit verloopt via gegevensbemiddelingsdiensten. Deze neutrale bemiddelaars moeten aan strenge eisen voldoen om te waarborgen dat de gegevensuitwisseling op een betrouwbare en veilige manier georganiseerd wordt.

4. Vereenvoudigen van gegevensdeling
Het delen van data over sectoren en grenzen heen moet mogelijk gemaakt worden. Daarnaast moet het mogelijk zijn om snel en eenvoudig de juiste data voor het juiste doeleinde te vinden.

De DGA in de praktijk
De EU hoopt met de DGA datagedreven innovatie binnen Europa te stimuleren en zo nieuwe banen te creëren. Voor bedrijven moet de nieuwe verordening zakelijke kansen opleveren. Zij krijgen nu immers eenvoudig toegang tot data uit de hele EU. Door het toepassen van data uit verschillende lidstaten, is de verwachting dat bedrijven sneller nieuwe producten en diensten op de markt kunnen brengen.

Of dit in de praktijk ook echt zo uitpakt, moet de tijd leren. De DGA treedt in september 2023 officieel in werking.

Europese wetsvoorstellen: Cyber Resilience Act en Cryptowet MiCA

In 2022 zijn er ook nieuwe Europese wetsvoorstellen geïntroduceerd, waaronder de Cyber Resilience Act en de Cryptowet.

Cyber Resilience Act

De Cyber Resilience Act moet zorgen voor meer veiligheid van hardware en software. Niet alleen van tablets en computers, maar ook van slimme apparaten als auto's, wasmachines en robotstofzuigers. Gedurende de hele lifecycle zijn producenten verantwoordelijk voor de veiligheid.

Meer hierover vindt u hier: www.legalz.nl/blog/cyber-resilience-act

Crytowet MiCA

De cryptowereld is volop in ontwikkeling en trekt de aandacht van steeds meer beleggers. Qua wet- en regelgeving is het echter nog een onontgonnen gebied. Europa brengt daar verandering in door de introductie van een verordening inzake markten in crypto-activa (MiCA). De nieuwe cryptowet moet crypto-beleggers en consumenten beschermen tegen een aantal risico's rondom het beleggen in crypto-activa, denk aan marktmanipulatie, frauduleuze praktijken en handel met voorkennis. De Europese Raad en het Europees Parlement hebben deze zomer een voorlopig akkoord bereikt over de inhoud hiervan.

Meer hierover vindt u hier: www.legalz.nl/blog/cryptowet-mica

4. Interessante uitspraken in rechtszaken

Ook afgelopen jaar werden diverse rechtszaken over ICT-vraagstukken gevoerd. We lichten er een paar uit, die veel aandacht kregen. Zo stond Coolblue in de rechtbank tegenover een ex-werknemer in het kader van portretrecht en werd uitspraak gedaan over de vraag of gebruikers zelf de broncode van software mogen reconstrueren om fouten te stellen.

Coolblue gebruikt foto's van ex-werknemer op busjes: mag dat?

. Coolblue en een ex-werknemer stonden afgelopen jaar in de rechtbank. Reden? Coolblue gebruikt foto's met het portret van de ex-werknemer nog altijd op bestelbussen en in een promotievideo. Hij beroept zich op zijn portretrecht en de AVG. De rechter gaat hier niet in mee. De bussen van Coolblue mogen dus gewoon zo blijven rijden. Hoe zit dat?

Goed geregeld in de arbeidsovereenkomst

In 2017 tekende de inmiddels ex-werknemer een arbeidscontract voor 7 maanden. Daarin stond de volgende passage opgenomen:

"Jij bent ons gezicht. Daarom gebruiken we graag beeldmateriaal met jouw portret erop. Dat zetten we op onze website en op YouTube, in folders, boekjes, jaarverslagen en al onze andere uitingen. Dat vind jij leuk en je moeder ook. Vanzelfsprekend doe je afstand van het portretrecht, ook voor de periode na je dienstverband. Dan hebben we gelukkig de foto's nog…"

Het contract is nadien meermaals verlengd, tot er uiteindelijk sprake was van een dienstverband voor onbepaalde tijd. De voorwaarden zijn bij iedere verlenging ongewijzigd gebleven.

Geen expliciete toestemming?

Tijdens zijn dienstverband heeft de inmiddels ex-werknemer meegewerkt aan promotiemateriaal voor Coolblue. Zijn gezicht is te zien op bestelbussen en in een promotievideo. Na zijn ontslag op staande voet in 2020, eist hij dat zijn portret wordt verwijderd en offline wordt gehaald. Daarbij eist hij ook een schadevergoeding van € 25.000,-.

Hij beweert daarbij dat zijn contract telkens stilzwijgend is verlengd en dat hij geen expliciete toestemming heeft gegeven voor het gebruik van zijn portret. Daar is de rechter het niet mee eens. De ex-werknemer heeft meerdere brieven ontvangen over de verlengingen, dus stilzwijgend waren de verleningen niet. In die brieven staat tevens dat de arbeidsvoorwaarden ongewijzigd en van toepassing blijven. Daarnaast heeft Coolblue in briefings vastgelegd op welke manier het gemaakte beeldmateriaal gebruikt wordt. De inmiddels ex-werknemer heeft nooit bezwaar hiertegen gemaakt.

De toestemming voor het gebruik van het portret is dus wel degelijk goed geregeld. Expliciete toestemming is niet noodzakelijk voor het gebruik van een portret. Als een geportretteerde geacht wordt impliciet te hebben ingestemd, dan geldt dit ook als toestemming.

Beroep op de AVG

De ex-werknemer stelt dat hij op grond van de Algemene verordening gegevensbescherming (AVG) om hernieuwde toestemming voor publicatie van zijn portret had moeten worden gevraagd. Daarnaast vindt hij dat Coolblue hem op zijn rechten en plichten op het gebied van privacy had moeten wijzen. In het kader van de AVG heeft hij het recht om de toestemming voor de verwerking van persoonsgegevens in te trekken. Daarbij speelt belangenafweging echter een grote rol.

Wat is belangrijker?

De inbreuk die het gebruik van het portret maakt op de persoonlijke levenssfeer van de ex-werknemer. Of het commerciële belang van Coolblue, die (onredelijk) hoge kosten moet maken om alle bestelbussen aan te passen. Daarbij moet gezegd worden dat Coolblue aan de eisen van de ex-werknemer tegemoet komt. In die zin dat de 36 bestelbussen worden uitgefaseerd en zijn portret niet op nieuwe uitingen wordt gebruikt. De betreffende promotievideo is al offline gehaald. De rechter oordeelt dan ook dat de (eventuele) inbreuk op de persoonlijke levenssfeer van de ex-werknemer in dit geval te rechtvaardigen is.

Coolblue handelt dus niet in strijd met het portretrecht of de AVG.

Het belang van goede documentatie

Uit deze casus blijkt maar weer hoe belangrijk het is om goede voorwaarden op te stellen. Door het portretrecht expliciet op te nemen in de arbeidsvoorwaarden heeft Coolblue een heel sterke zaak. Ook is het verstandig om iedere keer vast te leggen waarvoor u een portret van een medewerker wilt gebruiken en die informatie ook te delen met de betreffende persoon. Goede documentatie en voorwaarden zorgen ervoor dat u sterk staat bij een geschil.

Rechter: security & back-ups maken onderdeel uit van ICT-totaalpakket

Een groothandel sleept haar ICT-leverancier voor de rechter, nadat alle bedrijfsdata versleuteld wordt door malware. Back-ups ontbreken, waardoor de schade enorm is. De leverancier meent echter dat er geen specifieke afspraken zijn gemaakt over beveiliging en back-ups. Dit meningsverschil leidt tot een rechtszaak.

Wat is de casus?

Eind 2016 sloot de groothandel een koopovereenkomst met de ICT-leverancier voor de levering van software, hardware en een koppeling. Ook sluiten ze een dienstverleningsovereenkomst voor support en onderhoud hiervan, waaronder ook hosting door een derde partij valt.

In 2020 wordt de server van de groothandel gehackt en raken alle bedrijfsdata door middel van ransomware versleuteld. Er blijken geen back-ups van de FTP-server te zijn, waardoor duizenden product- en sfeerfoto's van artikelen uit het assortiment verloren gaan.

De vraag die partijen verdeeld houdt, is of ook de beveiliging van het netwerk deel uitmaakte van het overeengekomen totaalpakket. Ze hebben de afspraken niet (volledig) op papier gesteld, wat de zaken bemoeilijkt.

Rechtszaak: van zorgplicht tot back-ups

De partijen komen onderling niet tot een oplossing en daarom stapt de groothandel naar de rechter. Het verwijt? De leverancier is toerekenbaar tekort geschoten in haar verplichtingen, doordat zij geen back-ups heeft gemaakt. Zelfs als de uiteindelijke fout bij de hostingprovider ligt, is de leverancier in de ogen van de groothandel aansprakelijk.

Volgens de groothandel wist de ICT-leverancier dat een adequate beveiliging van groot belang voor haar is en is zij volledig afgegaan op de deskundigheid en adviezen van de leverancier. Kortom, er is volgens de groothandel sprake van een gebrekkige zorgplicht.

De reactie van de leverancier?

De overeenkomsten bevatten geen enkele bepaling over een correcte uitvoering van de hosting, ondersteuning en beveiliging. Ook betwist de leverancier dat sprake is van een bijzondere zorgplicht, laat staan dat zij die heeft geschonden. Als er wel sprake is van een zorgplicht, dan zou die bij de hostingprovider liggen.

Wat oordeelt de rechter?
De rechter oordeelt dat het moeilijk voorstelbaar is dat bij de overeenkomst van een totaalpakket de bijbehorende beveiliging niet is inbegrepen. Zeker ook omdat de groothandel nadrukkelijk het belang hiervan vermeld heeft. De ICT-leverancier mocht er dus niet zomaar van uitgaan dat de groothandel geen prijs stelde op adequate beveiliging en back-upsystemen.

Volgens de rechter had de leverancier de verantwoordelijkheid om ofwel (adequate) beveiliging onderdeel van het totaalpakket te maken, of anders met de groothandel uitdrukkelijk te bespreken dat zij daar juist niet voor zou zorgen. Dat is niet gebeurd en daarom mocht de groothandel er in deze casus van uitgaan dat de beveiliging en het back-upsysteem adequaat ingericht waren.
Hoe zit het met de verantwoordelijkheid van de hostingprovider?

Volgens de rechter is de ICT-leverancier voor de gedragingen van de hosting provider op gelijke wijze aansprakelijk als voor eigen gedragingen.
Er zijn tussen de leverancier en de provider geen contractuele afspraken gemaakt over de beveiliging van de FTP-server, waarop de product- en sfeerfoto's van de groothandel werden opgeslagen. De hostingprovider was dus niet verplicht om back-ups te maken. De rechter concludeert daarom dat de ICT-leverancier toerekenbaar is tekortgeschoten in haar verplichtingen tegenover de groothandel en een schadevergoeding moet betalen.

Mogen gebruikers de broncode van software zelf reconstrueren om fouten te herstellen?

Een interessante zaak! Een gebruiker en softwareleverancier komen niet tot een oplossing om fouten in de software te herstellen. De gebruiker besluit vervolgens zélf tot foutherstel over te gaan. Hoe? Door de broncode te reconstrueren, oftewel door het decompileren van software. De leverancier ziet dit als inbreuk op zijn auteursrecht en spant een zaak aan. Diverse rechters buigen zich erover, tot aan het Hof van Justitie van de Europese Unie aan toe.

Wat is het decompileren van software?
Software wordt geprogrammeerd in broncode. Vervolgens wordt die broncode omgezet naar objectcode, zodat de computer het kan lezen. Dit proces wordt de code compileren genoemd. Decompileren is het omgekeerde proces. Dus het reconstrueren van de broncode aan de hand van de objectcode. Door de objectcode te decompileren krijg je niet precies de oorspronkelijke broncode, maar wel een code die erop lijkt. Deze code wordt de quasibroncode genoemd.

De gebruiker van software heeft meestal slechts de objectcode. De broncode blijft bij de ontwikkelaar, tenzij er afspraken zijn gemaakt over de afgifte van de broncode. Wil een gebruiker zelf fouten herstellen? Dan heeft hij vaak de broncode nodig. De vraag is in hoeverre een gebruiker de objectcode mag decompileren om zo problemen op te lossen. De softwareleverancier in deze zaak vindt in ieder geval van niet.

De casus
Een Belgische softwareleverancier heeft op verzoek van een instelling uit België verschillende toepassingen ontwikkeld. Het gaat om standaardsoftware met op maat gemaakte aanpassingen. Voor het gebruik heeft de instelling een licentie gekregen. Op een gegeven moment ontstaan er verschillende problemen met de software. De partijen komen samen niet tot een oplossing voor de problemen. Daarop laat de Belgische instelling een derde partij de software decompileren, om zo de fouten in de software te herstellen. De leverancier noemt dit auteursrechtinbreuk. De Belgische rechter zegt van niet.

In hoger beroep oordeelt het Belgische Hof dat het niet weet of er wel of geen sprake is van inbreuk onder de Europese Softwarerichtlijn. Er worden vragen gesteld aan het Hof van Justitie van de Europese Unie...

De Europese softwarerichtlijn en de uitspraak van het Europese Hof
Het Hof van Justitie van de Europese Unie stelt vast dat decompileren een handeling is waarbij software (gedeeltelijk) wordt gereproduceerd en vertaald. Daar is op grond van artikel 4 van de Softwarerichtlijn in principe toestemming voor nodig van de rechthebbende. In artikel 5 en 6 van de Softwarerichtlijn zijn echter uitzonderingen opgenomen.

Artikel 5 gaat over uitzonderingen in het kader van reproductie- en wijzigingshandelingen. Voor deze handelingen is geen toestemming nodig, als deze voor de gebruiker noodzakelijk zijn om de software te kunnen gebruiken voor het beoogde doel. Bijvoorbeeld om fouten te verbeteren. In dit artikel staat decompileren niet specifiek genoemd.

Artikel 6 noemt wel uitdrukkelijk decompileren. Decompileren zonder toestemming van de rechthebbende is onder bepaalde voorwaarden toegestaan om de compatibiliteit met andere software tot stand te brengen. In dit artikel wordt alleen weer niet gesproken over foutherstel.

Het Hof oordeelt dat artikel 5 geldt: decompileren moet noodzakelijk zijn om de software te kunnen gebruiken voor het beoogde doel, waaronder foutherstel. Noodzakelijk wil volgens het Hof zeggen dat de gebruiker slechts mag decompileren als de broncode niet contractueel of wettelijk beschikbaar voor hem is. Is deze wel beschikbaar? Dan is decompileren niet noodzakelijk.

Daarnaast moet het echt alleen gaan om foutherstel. Het resultaat van het decompileren mag niet worden gebruikt voor andere doeleinden. Dus bijvoorbeeld niet worden verspreid of worden gebruikt om andere (concurrerende) software mee te ontwikkelen.

Let op!

Het Hof bepaalt nog iets belangrijks. Volgens het Hof mag niet iedere mogelijkheid van de gebruiker om fouten te herstellen via decompileren in een overeenkomst worden uitgesloten. Wel kunnen partijen afspraken maken over de wijze waarop dit mag plaatsvinden.

Niks missen in 2023?

Dit waren de belangrijkste ontwikkelingen in ICT & recht in 2022. Wilt u ook in 2023 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