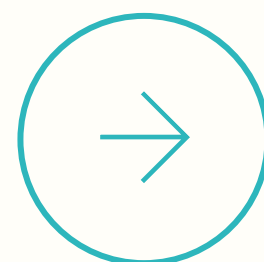




CUCCIBU'S INSIGHT OF THE WEEK

Een terugblik op het nieuws van de afgelopen week:

- Meertalige werkvloer vraagt om extra aandacht voor arbeidsveiligheid
- Boete van 530 miljoen euro voor Tiktok om doorgifte data naar China
- Cybersecurity prioriteit rond NAVO-top in Den Haag
- Winkels hangen foto's van vermeende dieven op
- AI-versie van vermoorde Amerikaan geeft verklaring in rechtszaak



Meertalige werkvloer vraagt om extra aandacht voor arbeidsveiligheid

29 april 2025 - Op basis van de Nationale Enquête Arbeidsomstandigheden (NEA) 2024 blijkt dat ruim een derde van de werknemers op meertalige werkplekken werkt. Hoewel 64% van hen aangeeft dat taalverschillen zelden tot misverstanden leiden, blijkt uit de cijfers dat dit in de sectoren bouw, landbouw en industrie in verhouding toch vaak voorkomt. Miscommunicatie kan leiden tot gevaarlijke situaties, bijvoorbeeld wanneer veiligheidsinstructies niet goed worden begrepen.

Preventie en goed beleid essentieel

Werkgevers zijn volgens de Arbowet verplicht te zorgen voor een veilige en gezonde werkplek, inclusief duidelijke communicatie. Dit kan onder andere door eenvoudige taal, visuele hulpmiddelen zoals afbeeldingen en het inzetten van meertalige collega's als vertalers. De Sociaal-Economische Raad (SER) heeft in 2019 een handreiking uitgebracht met praktische tips om taalbarrières te herkennen en te overbruggen.

Een goed arbobeleid houdt niet alleen rekening met fysieke en mentale risico's, maar ook met de diversiteit op de werkvloer — inclusief verschillen in taal en cultuur. Maak werkafspraken, instructies en protocollen die voor iedereen begrijpelijk zijn. Preventie en goed beleid zijn essentieel. Voorkomen is ten slotte beter dan genezen.



Boete van 530 miljoen euro voor TikTok doorgifte data naar China

2 mei 2025 - TikTok is door de Ierse Data Protection Commission (DPC) beboet met €530 miljoen vanwege schendingen van de AVG. De boete is het gevolg van het doorgeven van persoonsgegevens van Europese gebruikers naar China door moederbedrijf ByteDance, zonder adequate waarborging van privacy en de bescherming van persoonsgegevens.

Privacyrisico's van deze schending

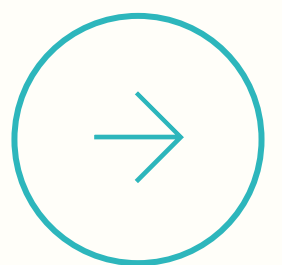
Deze schending brengt aanzienlijke privacyrisico's met zich mee:

- **Onvoldoende bescherming van persoonsgegevens:** de Chinese wetgeving maakt het mogelijk voor overheidsinstanties om toegang te krijgen tot gegevens die in China zijn opgeslagen, zonder de strikte privacy-eisen van de EU.
- **Gebrek aan transparantie:** gebruikers weten niet waar hun gegevens precies worden opgeslagen of wie er toegang toe heeft.
- **Risico's voor kwetsbare groepen:** veel jongeren maken gebruik van TikTok. Zij lopen het risico dat hun gegevens zonder toestemming gedeeld worden, wat kan leiden tot profilering en ongewenste beïnvloeding.

Bescherming van gebruikersgegevens

In reactie op de boete heeft TikTok "Project Clover" gelanceerd, waarbij datacenters in de EU zijn opgezet om gegevens binnen Europa te bewaren en toegang vanuit China te beperken. Dit is een stap richting betere dataveiligheid, maar de risico's blijven bestaan zolang Chinese wetgeving nog invloed kan uitoefenen.

De boete benadrukt de noodzaak voor strikte naleving van privacywetgeving, vooral bij bedrijven die wereldwijd opereren en grote hoeveelheden persoonsgegevens verwerken.



Cybersecurity prioriteit rond NAVO-top in Den Haag

6 mei 2025 - De NAVO-top op 24 en 25 juni 2025 in Den Haag wordt de grootste veiligheidsoperatie ooit in Nederland. De Nederlandse veiligheidsdiensten bereiden zich sinds 2023 voor op deze tweedaagse top. Er wordt rekening gehouden met diverse dreigingen, zoals cyberaanvallen, spionage, verstoringen in de digitale infrastructuur en maatschappelijke onrust. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) heeft zowel cybersecurity als het bestrijden van desinformatie benoemd als één van de prioriteiten.

Cyberdreigingen een risico

In deze tijd van geopolitieke spanning, zijn cyberaanvallen en desinformatie de wat minder zichtbare dreigingen. Toch kan dit grote impact hebben op de veiligheid. Hoewel Nederland relatief goed beveiligd is, benadrukt Pieter-Jaap Aalbersberg, nationaal coördinator van de NCTV, het belang van voorbereiding op crisissituaties. Hij wijst op eerdere NAVO-toppen in de VS en Litouwen, waar cyberaanvallen en desinformatiecampagnes al voorkwamen. Het is cruciaal dat de veiligheidsdiensten snel kunnen reageren als een incident zich voordoet.

Momenteel in fase van oefenen en trainen

Aalbersberg geeft aan dat er niet te veel details gedeeld kunnen worden over de specifieke vormen van beveiliging. De voorbereidingen omvatten onder andere het instellen van extra veiligheidsrisicogebieden rond Den Haag en Schiphol, waar de politie meer bevoegdheden heeft om preventief op te treden. Daarnaast worden er beperkingen opgelegd aan het vliegverkeer en het gebruik van drones in de regio. Momenteel bevinden de veiligheidsdiensten zich in de fase van oefenen en trainen, waarbij alle mogelijke scenario's worden doorgenomen en geoefend om snel en effectief te kunnen reageren op incidenten.



Diverse winkels hangen foto aan de muur bij diefstal

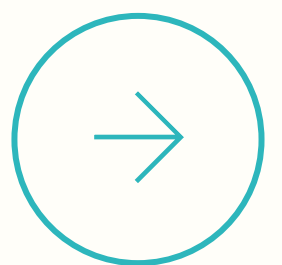
9 mei 2025 - In diverse Nederlandse winkels, waaronder Plus in Almere, Intratuin in Duiven en Slijterij Groningen, worden foto's van vermeende winkeldieven opgehangen met teksten als "Deze dame moet nog 23 blikken afrekenen". Hoewel deze 'wall of shame' bedoeld is om diefstal te ontmoedigen, roept het vragen op over de naleving van de Algemene verordening gegevensbescherming (AVG).

De politie heeft aangegeven dat het plaatsen van dergelijke foto's in strijd is met de privacywetgeving. Ze adviseren winkels om alternatieve methoden te overwegen om diefstal te voorkomen, zoals een collectief winkelverbod.

In strijd met de AVG

De Autoriteit Persoonsgegevens heeft in het verleden al gewaarschuwd tegen het gebruik van gezichtsherkenning en het openbaar maken van foto's van verdachten zonder hun toestemming. Zij benadrukt dat bedrijven zorgvuldig moeten omgaan met persoonsgegevens en deze alleen mogen verwerken in uitzonderlijke gevallen met een duidelijke wettelijke grondslag. De huidige praktijken, zoals het ophangen van foto's, worden beschouwd als een schending van de privacywetgeving.

Hoewel het begrijpelijk is dat winkels maatregelen willen nemen tegen diefstal, moeten ze ervoor zorgen dat ze handelen binnen de kaders van de AVG om onterecht schade aan de reputatie van individuen te voorkomen.



AI-versie van vermoorde Amerikaan geeft verklaring in rechtszaak

9 mei 2025 - In een rechtszaak in Phoenix, Arizona, werd voor het eerst een AI-avatar ingezet om het slachtoffer, Christopher Pelkey, te vertegenwoordigen. Pelkey werd in 2021 doodgeschoten tijdens een verkeersruzie. Zijn zus schreef een script en liet haar man een AI-versie van haar broer maken, die vervolgens in de rechtszaal werd getoond. In de video sprak de AI-versie van Pelkey de dader aan en bood hij vergeving aan. De rechter was onder de indruk en gaf aan dat het aannemelijk was dat Pelkey zo zou hebben gereageerd. De dader werd veroordeeld tot 10,5 jaar gevangenisstraf. De advocaat van de dader heeft echter aangegeven in hoger beroep te gaan, omdat hij vindt dat de rechter te veel waarde heeft gehecht aan de AI-getuigenis.

Ethische en juridische overwegingen

Het gebruik van AI in de rechtszaal roept verschillende ethische en juridische vragen op. Hoe betrouwbaar en representatief is een AI-gegenereerde verklaring? Hoe kan men er zeker van zijn dat de AI-getuigenis overeenkomt met wat de overledene daadwerkelijk zou hebben gezegd? En kan een AI-getuigenis überhaupt als bewijs worden geaccepteerd in de rechtszaal? Het is essentieel dat het gebruik van AI in juridische processen zorgvuldig wordt overwogen en gereguleerd om misbruik en ongewenste gevolgen te voorkomen.

Tot nu toe werd AI in de Amerikaanse rechtspraak voornamelijk gebruikt voor administratieve taken, onderzoek en het voorbereiden van zaken. Echter, een lid van het Hooggerechtshof in Arizona erkent dat de populariteit van AI binnen de rechtspraak toeneemt. Daarom is er een commissie ingesteld die moet toezien op de verantwoorde inzet van AI, zodat alles volgens de regels verloopt.