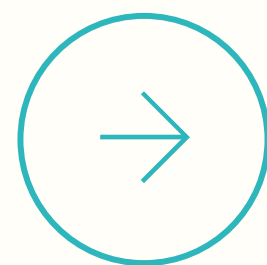




CUCCIBU'S INSIGHT OF THE MONTH

Een terugblik op het nieuws van de afgelopen weken:

- Cyberveilig gedrag van werknemers blijft achter
- AP zet volgende stap in toezicht AI
- Cyberaanvallen raken de levensmiddelensector
- Nieuwe EDPB-richtlijnen over samenspel DSA en AVG en privacyboetes
- AP onderzoekt websites vanwege misleidende cookiebanners
- Kritieke PHP-kwetsbaarheden leggen websites tijdelijk plat



Cyberveilig gedrag van werknemers blijft achter

1 oktober 2026 - Uit het Cybersecurity Gedragsonderzoek Alert Online 2026 blijkt dat werknemers nog onvoldoende cyberveilig handelen.

Slechts 32% gebruikt altijd tweefactorauthenticatie en 13% consequent een wachtwoordmanager voor zakelijke accounts. Daarnaast meldt slechts een derde altijd een zelfgemaakte beveiligingsfout en deelt 53% weleens persoonlijke documenten met AI-tools.

Volgens het NCSC spelen kennis, gebruiksgemak en een veilige meldcultuur een belangrijke rol bij het verbeteren van cyberveilig gedrag.

Het EAST-model biedt hiervoor vier uitgangspunten:

- **Easy:** maak veilig gedrag zo eenvoudig mogelijk.
- **Attractive:** maak veilig gedrag aantrekkelijk.
- **Social:** maak het gewenste gedrag zichtbaar (de sociale norm).
- **Timely:** stimuleer veilig gedrag op het juiste moment.

Technische beveiligingsmaatregelen alleen zijn dus niet voldoende. Organisaties moeten veilig gedrag stimuleren door maatregelen toegankelijk te maken, het goede voorbeeld te geven en een cultuur te creëren waarin medewerkers fouten durven te melden.

Cyberveiligheid is daarmee niet alleen een technische, maar ook een organisatorische verantwoordelijkheid.



AP zet volgende stap in toezicht op AI

9 oktober 2026 - De Autoriteit Persoonsgegevens (AP) heeft de nieuwe **directie Toezicht en Coördinatie AI/Algoritmes** (TCA) opgericht. Hiermee bereidt de AP zich voor op haar toekomstige toezichtrol onder de Europese AI-verordening (AI Act).

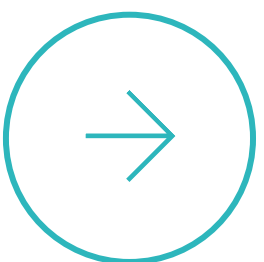
Samen met de Rijksinspectie Digitale Infrastructuur (RDI) werkt de AP aan een AI Coördinatiecentrum en een 'AI-sandbox', waarin organisaties onder begeleiding AI-systemen verantwoord kunnen ontwikkelen en testen.

Twee afdelingen richten zich op verschillende aspecten van AI-toezicht:

- **AI/Algoritmes Risicoanalyse & Coördinatie (ARC)**: onderzoekt de impact en risico's van AI en algoritmes voor mensen, grondrechten en de samenleving.
- **Markttoezicht AI (MTA)**: bereidt het toekomstige toezicht op de AI-verordening voor.

Hoewel de AP nog niet officieel is aangewezen als AI-markttoezichthouder, krijgt het Nederlandse AI-toezicht steeds concreter vorm. De AP krijgt deze bevoegdheden pas wanneer de Nederlandse Uitvoeringswet AI-verordening van kracht wordt. Ondertussen richt de toezichthouder zich al op samenwerking, voorlichting en het ondersteunen van verantwoorde innovatie.

Goed AI-toezicht draait niet alleen om handhaving, maar ook om duidelijkheid over wat wél mogelijk is. Voor organisaties onderstreept dit het belang van transparantie, risicobeheersing en verantwoord AI-gebruik. Door hier nu al aandacht aan te besteden, kunnen zij zich beter voorbereiden op toekomstige toezichtverplichtingen.



Cyberaanvallen raken de levensmiddelensector

13 oktober 2026 - In oktober werd de Europese levensmiddelensector getroffen door meerdere cyberincidenten.

Bij Ahold Delhaize, waaronder Albert Heijn en Etos, werden systemen uit voorzorg offline gehaald na een cyberincident. Dit leidde tot lege schappen, stilgelegde distributiecentra, problemen met thuisbezorgingen en dagenlange verstoringen van websites en apps.

In Frankrijk kregen hackers via verouderde software toegang tot koelsystemen van honderden supermarkten. Zij konden de temperatuurinstellingen op afstand aanpassen, waardoor voorraden verloren gingen en miljoenen euro's schade ontstond.

Het Nationaal Cyber Security Centrum (NCSC) benadrukt dat er vooralsnog geen aanwijzingen zijn dat de incidenten met elkaar verband houden.

De incidenten laten zien hoe cyberaanvallen niet alleen digitale systemen, maar ook fysieke bedrijfsprocessen en de voedselvoorziening kunnen verstoren. Dit onderstreept het belang van digitale weerbaarheid in de levensmiddelensector. Niet voor niets valt de sector 'Productie, verwerking en distributie van levensmiddelen' onder de **Cyberbeveiligingswet**, voor zover organisaties aan de toepasselijke criteria voldoen.

Voor organisaties zijn goed kwetsbaarhedenbeheer, incidentrespons en aandacht voor bedrijfscontinuïteit daarom essentieel. Cybersecurity moet een integraal onderdeel zijn van het bredere risicomanagement.



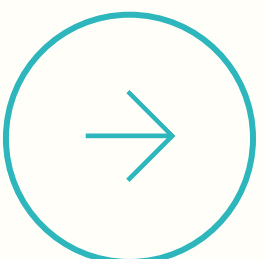
Nieuwe EDPB-richtlijnen over samenspel DSA en AVG en privacyboetes

14 oktober 2026 - De European Data Protection Board (EDPB) heeft twee nieuwe conceptrichtlijnen gepubliceerd, voornamelijk gericht op toezichthouders. Beide liggen tot 13 november 2026 ter publieke consultatie.

De eerste richtlijn verduidelijkt hoe de **Digital Services Act** (DSA) en de **Algemene verordening gegevensbescherming** (AVG) samen moeten worden toegepast. Omdat aanbieders van online diensten en platforms vaak persoonsgegevens verwerken, zijn beide verordeningen regelmatig van toepassing. De richtlijn helpt toezichthouders deze regels op een consistente manier toe te passen.

De tweede richtlijn richt zich op de procedure voor het **opleggen van AVG-boetes**. De EDPB introduceert hiervoor een vaste vijfstappenprocedure, zodat toezichthouders overtredingen en boetes op basis van actuele wetgeving en rechtspraak eenduidiger kunnen beoordelen.

Hoewel de richtlijnen primair bedoeld zijn voor toezichthouders, zijn ze ook relevant voor organisaties. Ze bieden meer duidelijkheid over de samenloop van Europese regelgeving en de handhaving van privacyregels. Voor organisaties, met name aanbieders van online diensten, onderstreept dit het belang van een samenhangende aanpak van privacy en compliance.



AP onderzoekt websites vanwege misleidende cookiebanners

16 oktober 2026 - De Autoriteit Persoonsgegevens (AP) onderzoekt twee organisaties die ondanks eerdere uitleg en waarschuwingen misleidende cookiebanners blijven gebruiken. Op hun websites ontbreekt een direct zichtbare mogelijkheid om trackingcookies te weigeren, terwijl accepteren wel eenvoudig is.

De AP waarschuwde eerder ongeveer honderd organisaties voor onjuiste cookiebanners. Zij kregen de kans om orde op zaken te stellen. De AP heeft daarbij handvatten voor een goed cookiebeleid en vuistregels voor heldere cookiebanners gedeeld. Circa 70% heeft de cookiebanner inmiddels aangepast. Organisaties die niet aan de regels voldoen, riskeren nader onderzoek en mogelijke boetes.

Volgens de AP moet het weigeren van trackingcookies net zo eenvoudig zijn als het accepteren ervan. Daarnaast moeten organisaties transparant zijn over welke persoonsgegevens zij verzamelen, voor welke doeleinden en met wie deze worden gedeeld.

De onderzoeken benadrukken dat de AP actief toeziet op correcte toestemming voor trackingcookies. Organisaties moeten bezoekers duidelijk informeren en een vrije keuze bieden.

Een transparante cookiebanner is niet alleen belangrijk voor naleving van de privacywetgeving, maar draagt ook bij aan het vertrouwen van gebruikers.



Kritieke PHP-kwetsbaarheden leggen websites tijdelijk plat

21 oktober 2026 - Het Nationaal Cyber Security Centrum (NCSC) waarschuwde voor twee kritieke kwetsbaarheden in PHP, een veelgebruikte programmeertaal voor websites en webapplicaties.

Misbruik van deze kwetsbaarheden kan aanvallers in staat stellen om op afstand systemen over te nemen. Uit voorzorg werden verschillende websites, waaronder DigiD en MijnOverheid, tijdelijk offline gehaald.

Hoewel het NCSC aangeeft dat grootschalig misbruik minder waarschijnlijk is dan aanvankelijk gedacht, blijft het advies om kwetsbare systemen zo snel mogelijk te updaten.

De situatie laat zien hoe beveiligingslekken in veelgebruikte software de continuïteit van digitale dienstverlening kunnen bedreigen.

Voor organisaties onderstreept dit het belang van inzicht in gebruikte software, tijdig patchmanagement en een goed voorbereid incidentresponsproces. Zo kunnen risico's worden beperkt en verstoringen van de dienstverlening zoveel mogelijk worden voorkomen.