cuccibu
Privacy & Information Security

CUCCIBU'S
INSIGHT OF THE MONTH

Een terugblik op het nieuws van de afgelopen weken:

- Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten vanaf 15 augustus 2026 van kracht.
- AI vergroot de gevaren van cyberaanvallen.
- AP helpt organisaties met nieuwe AVG-richtlijnen voor generatieve AI.
- EDPB komt met drie nieuwe richtlijnen over scraping, anonimiseren en blockchain.
- Nieuwe transparantieverplichtingen voor AI vanaf 2 augustus 2026.

Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten vanaf 15 augustus 2026 van kracht.

7 juli 2026 - Na meerdere keren uitstel is het nu definitief: vanaf 15 augustus 2026 treden de **Cyberbeveiligingswet** (Cbw) en de **Wet weerbaarheid kritieke entiteiten** (Wwke) in werking. Hiermee zet Nederland de Europese NIS2- en CER-richtlijnen om in nationale wetgeving. Ruim 8.000 organisaties krijgen te maken met nieuwe verplichtingen op het gebied van cyberweerbaarheid. Daarnaast vallen ongeveer 500 kritieke organisaties onder aanvullende eisen voor fysieke weerbaarheid.

Wat betekent de Cyberbeveiligingswet concreet voor organisaties?

- Registratieplicht: organisaties moeten zich registreren bij het NCSC.
- Zorgplicht: organisaties moeten een risicoanalyse uitvoeren en passende beveiligingsmaatregelen treffen om risico's te beheersen.
- Meldplicht: significante incidenten moeten binnen de wettelijke termijnen worden gemeld.
- Bestuurlijke verantwoordelijkheid: bestuurders worden expliciet verantwoordelijk voor cyberrisicobeheersing en moeten aantoonbare kennis van cybersecurity hebben.
- Toezicht: toezichthouders controleren of organisaties voldoen aan de verplichtingen uit de Cyberbeveiligingswet.

Let op! Ook organisaties die niet rechtstreeks onder de wet vallen, kunnen met deze verplichtingen te maken krijgen. De Cyberbeveiligingswet verwacht namelijk dat organisaties risico's in de toeleveringsketen actief meenemen in hun risicobeheer. Hierdoor kunnen ook leveranciers en dienstverleners indirect aan strengere eisen moeten voldoen.

Hoewel de aandacht vaak uitgaat naar compliance, draait deze wetgeving uiteindelijk om het versterken van de **digitale weerbaarheid**.

Bron: Nationaal Cyber Security Centrum

Information Security | Privacy

AI vergroot de gevaren van cyberaanvallen

8 juli 2026 - De autoriteit Persoonsgegevens (AP) waarschuwt in haar jaarlijkse datalekkenrapportage dat de snelle opkomst van AI cyberaanvallen gevaarlijker maakt. Cybercriminelen gebruiken AI om sneller en op grote schaal overtuigende phishingberichten te maken. Succesvolle phishingaanvallen leiden vervolgens steeds vaker tot datalekken en accountovernames.

Een e-mail met een geloofwaardige phishinglink kan leiden tot de overname van het account van een medewerker. Van daaruit kunnen cybercriminelen een grotere aanval op de organisatie uitvoeren. Daarnaast gebruiken zij gestolen gegevens om AI-modellen te voeden, waarmee nóg overtuigendere phishingberichten worden gegenereerd. Zo ontstaat een vicieuze cirkel waarin AI cyberaanvallen steeds effectiever maakt.

Een zorgelijke ontwikkeling: kant-en-klare phishing kits
Hierdoor hebben cybercriminelen steeds minder technische kennis nodig om geavanceerde aanvallen uit te voeren. AI verlaagt de drempel voor aanvallers, terwijl de impact voor organisaties juist groter wordt.

AI, cyberveiligheid en privacy zijn onlosmakelijk met elkaar verbonden
Je kunt er niet meer omheen: digitale weerbaarheid moet op de bestuursagenda staan. AI verandert niet alleen de manier waarop organisaties werken, maar ook de manier waarop cybercriminelen aanvallen uitvoeren. Investeren in technische beveiliging alleen is daarom niet langer voldoende.

Uiteindelijk draait het niet alleen om het voorkomen van cyberincidenten, maar ook om het beschermen van persoonsgegevens en het behouden van het vertrouwen van klanten, medewerkers en andere betrokkenen in een steeds digitalere samenleving.

Bron: Autoriteit Persoonsgegevens

Privacy

AP helpt organisaties met nieuwe AVG-richtlijnen voor generatieve AI

13 juli 2026 - Generatieve AI biedt enorme kansen voor innovatie en efficiëntie, maar brengt ook risico's met zich mee voor de bescherming van persoonsgegevens. Daarom heeft de Autoriteit Persoonsgegevens (AP) twee nieuwe documenten gepubliceerd om organisaties te helpen generatieve AI op een verantwoorde manier te ontwikkelen en in te zetten.

De handreiking voor ontwikkelaars van generatieve AI-modellen
De handreiking geeft uitleg over hoe organisaties binnen de kaders van de AVG generatieve AI kunnen ontwikkelen en gebruiken. Daarbij wordt onder andere ingegaan op de rechtmatige verwerking van persoonsgegevens, de benodigde verwerkingsgrondslagen, passende waarborgen en het beheren, opschonen, verrijken en bewaren van data.

Praktisch hulpmiddel voor organisaties die AI willen implementeren
Daarnaast heeft de AP een praktische checklist gepubliceerd voor organisaties die generatieve AI willen aanschaffen, implementeren of gebruiken. De checklist helpt organisaties te bepalen of zij generatieve AI willen, kunnen én mogen inzetten. Het hulpmiddel geeft inzicht in welke AVG-verplichtingen van toepassing zijn en welke technische en organisatorische maatregelen nodig zijn om generatieve AI verantwoord te gebruiken.

De AP adviseert daarbij om eerst te onderzoeken of AI kan worden ingezet zonder persoonsgegevens te verwerken. Is verwerking van persoonsgegevens toch noodzakelijk, dan helpt de checklist organisaties om privacy vanaf het begin mee te nemen in het ontwerp, de implementatie en het gebruik van AI.

AI vraagt om meer dan alleen innovatie
De publicatie van deze richtlijnen laat zien dat verantwoord AI-gebruik niet begint bij techniek, maar bij governance. Door privacy by design toe te passen en privacy al vanaf de ontwerpfase mee te nemen, kunnen organisaties generatieve AI verantwoord inzetten én voldoen aan de eisen van de AVG.

Bron: Autoriteit Persoonsgegevens

Privacy

EDPB komt met drie nieuwe richtlijnen over scraping, anonimiseren en blockchain

15 juli 2026 - De European Data Protection Board (EDPB) heeft drie nieuwe richtlijnen gepubliceerd over onderwerpen die steeds belangrijker worden in de digitale praktijk: scraping, anonimiseren en blockchain. Met deze richtlijnen krijgen organisaties meer duidelijkheid over hoe zij verantwoord omgaan met persoonsgegevens bij het gebruik van deze technologieën.

Het scrapen van data voor het trainen van generatieve AI
Veel generatieve AI-modellen worden getraind met gegevens die automatisch van websites worden verzameld (scraping). De EDPB benadrukt dat het feit dat gegevens openbaar beschikbaar zijn, niet automatisch betekent dat deze ook zonder meer mogen worden gebruikt voor AI-training. De richtlijn geeft o.a. uitleg over hoe scraping-processen werken en de AVG-beginselen, grondslagen en verplichtingen die daarbij komen kijken. De richtlijn is nog in consultatie.

Het anonimiseren van data
Deze richtlijn beschrijft hoe organisaties ervoor kunnen zorgen dat persoonsgegevens écht anoniem zijn. Gegevens zijn pas anoniem als ze op geen enkele manier herleidbaar zijn naar een natuurlijk persoon. Ook deze richtlijn is nog in consultatie.

Het gebruik van blockchaintechnologie
Deze richtlijn beschrijft hoe blockchaintechnologie werkt en welke privacy-uitdagingen ontstaan wanneer persoonsgegevens op een blockchain worden verwerkt. De EDPB benadrukt het belang van privacy by design, dataminimalisatie en het uitvoeren van een Data Protection Impact Assessment (DPIA) voordat persoonsgegevens via blockchain worden verwerkt. Deze richtlijn is definitief vastgesteld.

Innovatie vraag om duidelijke kaders
De drie richtlijnen laten zien dat organisaties niet alleen moeten kijken naar wat technisch mogelijk is, maar ook naar wat juridisch is toegestaan.

Bron: Autoriteit Persoonsgegevens

Privacy

Nieuwe transparantieverplichtingen voor AI vanaf 2 augustus 2026

31 juli 2026 - Vanaf 2 augustus 2026 gelden nieuwe transparantieverplichtingen uit de Europese **AI Act**. Organisaties die bepaalde AI-systemen ontwikkelen of gebruiken, moeten voortaan duidelijk maken wanneer mensen te maken hebben met AI of met door AI gegenereerde content.

De nieuwe Europese regels helpen gebruikers beter te herkennen wat echt is, wat door AI is gemaakt en wanneer zij met een AI-systeem communiceren. Het doel is om misleiding, nepnieuws, identiteitsfraude en oplichting tegen te gaan. Transparantie wordt daarmee een belangrijk onderdeel van verantwoord AI-gebruik.

Welke transparantieverplichtingen gaan gelden?
Voor alle verplichtingen geldt dat de informatie beschikbaar moet zijn uiterlijk vóór de eerste interactie met of blootstelling aan de content. Concreet betekent dit dat:

- AI-systemen, zoals chatbots, duidelijk moeten maken dat gebruikers met AI praten.
- Door AI gegenereerde content herkenbaar moet zijn door een digitale markering.
- Het moet duidelijk zijn als mensen worden blootgesteld aan AI-systemen die emoties herkennen of biometrische kenmerken analyseren.
- Video's, afbeeldingen en geluidsfragmenten die met AI zijn gemaakt of bewerkt en daardoor niet van echt te onderscheiden zijn (deepfakes), moeten worden gelabeld.

Praktijkcode helpt organisaties op weg
Om organisaties hierbij te ondersteunen heeft de Europese Commissie een vrijwillige praktijkcode voor AI gepubliceerd. De Autoriteit Persoonsgegevens (AP) adviseert aanbieders van AI-modellen deze praktijkcode te ondertekenen. Organisaties die dit doen, laten zien dat zij zich inzetten voor het verantwoord ontwikkelen en gebruiken van AI en krijgen tegelijkertijd praktische handvatten om aan de transparantieverplichtingen uit de AI Act te voldoen.

Transparantie creëert vertrouwen
De nieuwe regels laten zien dat organisaties niet alleen moeten nadenken over wat AI kan, maar ook over hoe zij gebruikers duidelijk informeren wanneer AI wordt ingezet. Transparantie is daarmee niet alleen een wettelijke verplichting, maar ook een manier om vertrouwen op te bouwen bij klanten, medewerkers en andere betrokkenen.

Bron: Autoriteit Persoonsgegevens