cuccibu
Privacy & Information Security



CUCCIBU'S
INSIGHT OF THE MONTH

Een terugblik op het nieuws van de afgelopen weken:

- Cyberdreigingen nemen toe, digitale weerbaarheid blijft achter.
- EDPB publiceert definitieve richtlijnen over gerechtvaardigd belang.
- Belastingdienst moet gegevensbescherming verbeteren.
- AP constateert privacy- en veiligheidsrisico's bij AI-camerabrillen.

Cyberdreigingen nemen toe, digitale weerbaarheid blijft achter

6 november 2026 - Uit het Cybersecurity Cybersecuritybeeld Nederland (CSBN) 2026 blijkt dat de cyberdreiging verder toeneemt, terwijl de digitale weerbaarheid van Nederlandse organisaties achterblijft. Volgens de NCTV vormt de groeiende kloof tussen dreiging en weerbaarheid een ernstig risico voor de nationale veiligheid.

Een belangrijke ontwikkeling is de inzet van kunstmatige intelligentie (AI) door cybercriminelen en statelijke actoren. Volgens het CSBN zetten kwaadwillenden AI aantoonbaar in tijdens alle fasen van cyberaanvallen, onder meer om aanvallen te automatiseren, malware te ontwikkelen en overtuigendere phishingberichten te maken. Hierdoor nemen de snelheid en schaal van aanvallen toe.

Tegelijkertijd hebben veel organisaties hun digitale basisbeveiliging onvoldoende op orde, met name mkb. Het NCSC en de NCTV benadrukken daarom het belang van het op orde krijgen van de digitale basisbeveiliging, waaronder tijdige patchmanagement, back-ups, logging en monitoring.

De toenemende dreiging vraagt echter om meer dan technische maatregelen. Door de grote afhankelijkheid van digitale systemen en de onderlinge verwevenheid van organisaties is cybersecurity niet langer uitsluitend de verantwoordelijkheid van CISO's en IT-afdelingen. Ook bestuurders moeten digitale veiligheid prioriteit geven, met aandacht voor risicobeheersing, bedrijfscontinuïteit en de risico's van AI.

Voor organisaties onderstreept dit het belang van een samenhangend cybersecuritybeleid, waarin zowel bestaande kwetsbaarheden als nieuwe dreigingen door AI worden meegenomen. Zo kunnen zij hun digitale weerbaarheid versterken en beter inspelen op het veranderende dreigingslandschap.

Bron: NCSC, NCTV en security.nl

Privacy

EDPB publiceert definitieve richtlijnen over gerechtvaardigd belang

11 november 2026 - De European Data Protection Board (EDPB) heeft definitieve richtlijnen gepubliceerd over het verwerken van persoonsgegevens op basis van een gerechtvaardigd belang. Dit is een van de zes wettelijke grondslagen uit de Algemene verordening gegevensbescherming (AVG). De richtlijnen verduidelijken wanneer organisaties deze grondslag mogen gebruiken en hoe zij dit moeten onderbouwen.

Om persoonsgegevens op basis van een gerechtvaardigd belang te mogen verwerken, moeten organisaties aan drie bestaande voorwaarden voldoen: er moet sprake zijn van een gerechtvaardigd belang, de verwerking moet noodzakelijk zijn en de belangen van de organisatie moeten zorgvuldig worden afgewogen tegen de rechten en belangen van betrokkenen.

De richtlijnen bieden verdere uitleg over de toepassing van deze voorwaarden en bevatten praktijkvoorbeelden, onder meer over fraudepreventie, netwerkbeveiliging en direct marketing. Ook verduidelijken ze welke rechten betrokkenen hebben en hoe organisaties rekening moeten houden met de mogelijke gevolgen van gegevensverwerkingen.

Voor organisaties bieden de richtlijnen meer duidelijkheid over het gebruik van gerechtvaardigd belang als verwerkingsgrondslag. Ze onderstrepen het belang van een zorgvuldige en aantoonbare beoordeling, waarbij organisaties de noodzaak van de verwerking onderbouwen, de gevolgen voor betrokkenen meewegen en hun afwegingen vastleggen.

Bron: Autoriteit Persoonsgegevens, EDPB

Privacy

Belastingdienst moet gegevensbescherming verbeteren

11 november 2026 - De Autoriteit Persoonsgegevens (AP) concludeert dat de Belastingdienst persoonsgegevens van Nederlanders nog onvoldoende beschermt en te langzaam verbeteringen doorvoert. De Belastingdienst staat sinds 2024 onder geïntensiveerd toezicht van de AP. Uit het rapport Staat van de gegevensbescherming bij de Belastingdienst blijkt dat de organisatie bij tien van de twaalf onderzochte onderwerpen nog niet aan de privacywetgeving voldoet.

De tekortkomingen hebben onder meer betrekking op onvoldoende onderbouwde selectiealgoritmes, gebrekkige beveiliging van persoonsgegevens en onvoldoende controle op de toegang tot gegevens. Ook voldoen bepaalde lokaal ontwikkelde applicaties niet aantoonbaar aan de geldende wet- en regelgeving, waaronder de AVG en de BIO. Wel constateert de AP vooruitgang: bij het melden van datalekken en het uitvoeren van privacytoetsen (DPIA's) voldoet de Belastingdienst inmiddels aan de wettelijke eisen.

Staatssecretaris Eerenberg erkent dat de naleving van de AVG nog niet op orde is en wil verbeteringen versnellen. Daarbij ligt de nadruk op het versterken van autorisatiebeheer, logging en de controle daarop. Ook moet er in het eerste kwartaal van 2027 een centraal overzicht zijn van lokaal ontwikkelde applicaties. Het doel is om in 2027 op alle onderdelen aantoonbare vooruitgang te boeken.

De bevindingen onderstrepen dat naleving van de AVG meer vraagt dan afzonderlijke technische maatregelen. Organisaties moeten structureel aandacht besteden aan gegevensbescherming, duidelijke verantwoordelijkheden vastleggen en verbetermaatregelen daadwerkelijk uitvoeren en controleren. Ook bij complexe IT-omgevingen blijft aantoonbare naleving van privacywetgeving essentieel.

Bron: Autoriteit Persoonsgegevens en Security.nl

Privacy Information Security

AP constateert privacy- en veiligheidsrisico's bij AI-camerabrillen

19 november 2026 - De Autoriteit Persoonsgegevens (AP) heeft zes AI-camerabrillen onderzocht en constateert ernstige tekortkomingen op het gebied van privacy, informatiebeveiliging en veiligheid.

Uit het onderzoek blijkt dat opnamelampjes vaak slecht zichtbaar en eenvoudig af te plakken zijn, terwijl de brillen blijven filmen. Ook is onvoldoende duidelijk waar opgenomen beeld- en geluidsgegevens terechtkomen en welke partijen deze verwerken. Daarnaast ontdekte de AP beveiligingsproblemen waardoor onbevoegden mogelijk toegang kunnen krijgen tot opnames of de camera kunnen bedienen.

Naast privacy- en beveiligingsrisico's constateerde de AP problemen met de betrouwbaarheid van AI. Tijdens een nagebootste noodsituatie gaf een camerabril bijvoorbeeld ten onrechte aan dat er al een ambulance onderweg was. Ook bij de bescherming van minderjarigen en het interpreteren van veiligheidswaarschuwingen bleken de AI-systemen tekort te schieten.

De AP roept fabrikanten en ontwikkelaars daarom op om privacy, veiligheid en relevante wetgeving vanaf het ontwerp van hun producten mee te nemen. Daarbij zijn de volgende aandachtspunten belangrijk:

- Omstanders moeten duidelijk kunnen zien wanneer zij worden gefilmd.
- Gebruikers moeten weten waar hun gegevens terechtkomen, wie deze verwerkt en waarvoor ze worden gebruikt.
- AI-systemen moeten voldoende betrouwbaar zijn, zeker wanneer hun adviezen gevolgen kunnen hebben voor de gezondheid of veiligheid van mensen.
- Fabrikanten moeten hun producten goed beveiligen en aantoonbaar voldoen aan toepasselijke Europese regelgeving, waaronder de AI-verordening.

Het onderzoek onderstreept het belang van verantwoord AI-gebruik. Voor organisaties die AI-producten ontwikkelen of aanbieden, is het essentieel om risico's voor gebruikers en omstanders vroegtijdig te identificeren en passende maatregelen te nemen. Zo worden privacy, informatiebeveiliging en veiligheid integraal onderdeel van productontwikkeling.

Bron: Autoriteit Persoonsgegevens