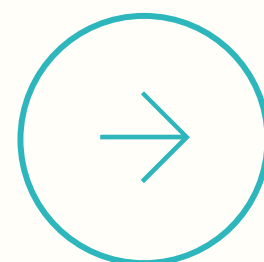




CUCCIBU'S INSIGHT OF THE WEEK

Een terugblik op het nieuws van de afgelopen week:

- Het OM meldt: minder cybercrime, meer gedigitaliseerde criminaliteit
- AP start inspecties bij gemeenten: privacy onder de loep
- Luchtvaart: meer aandacht voor cyberdreigingen en klimaatverandering
- Lancering Nederlands Register voor Functionarissen
Gegevensbescherming



Het OM meldt: minder cybercrime, meer gedigitaliseerde criminaliteit

12 mei 2025 - Uit het Jaarbericht 2024 van het Openbaar Ministerie (OM) blijkt een opvallende verschuiving in de aard van digitale criminaliteit in Nederland. Het aantal geregistreeerde cybercrimezaken, zoals hacks en ransomware-aanvallen, daalde vorig jaar met 42%. Tegelijkertijd steeg de gedigitaliseerde criminaliteit, waaronder online oplichting via nepshops en belfraude, met 22%. Gezamenlijk leidde dit tot een totale toename van 11% in online criminaliteit.

Deze verschuiving wordt deels toegeschreven aan verbeterde registratiemogelijkheden bij de politie, waardoor verschillende vormen van gedigitaliseerde criminaliteit beter worden vastgelegd. Toch blijft de instroom van dit soort zaken bij het OM beperkt: slechts 1,2% van alle strafzaken betreft cybercrime of online fraude. In 2024 resulteerde dit in 59 veroordelingen tot gevangenisstraf.

Het OM onderstreept dat de dreiging, omvang en impact van digitale misdaad snel groeit, mede door de internationalisering en steeds geraffineerdere werkwijze van cybercriminelen. Daarom wordt flink geïnvesteerd in capaciteit, kennis en kunde om cybercrime en gedigitaliseerde criminaliteit te bestrijden.

Wat betekent dit voor organisaties?

Deze cijfers tonen aan dat digitale dreiging niet afneemt, maar verandert. Organisaties lopen niet alleen risico op technische hacks, maar ook op social engineering en digitale fraude via menselijke interactie en manipulatie.

Cybersecurity vraagt daarom om een brede aanpak: niet alleen focus op technische beveiliging, maar ook structurele aandacht voor bewustwording onder de medewerkers en een stevige samenwerking in de (digitale) keten.



AP start inspecties bij gemeenten: privacy onder de loep

13 mei 2025 - De Autoriteit Persoonsgegevens (AP) kondigt aan de komende maanden steekproefsgewijs gemeenten te inspecteren om te beoordelen hoe zij omgaan met de persoonsgegevens en privacy van burgers.

Gemeenten verwerken dagelijks grote hoeveelheden persoonsgegevens – van het registeren van de geboorte van je kind tot het verlengen van je rijbewijs – en burgers moeten erop kunnen vertrouwen dat die op veilige en verantwoorde wijze gebeurt.

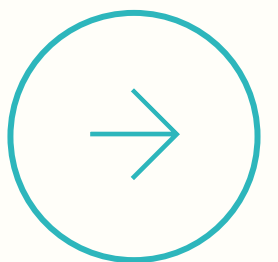
Tijdens de inspectie wordt er onder andere gekeken naar:

1. **Actuele verwerkingsregisters:** Heeft de gemeente een volledig en actueel overzicht van alle verwerkingen van persoonsgegevens?
2. **Privacy risicoanalyses:** Worden potentiële privacyrisico's voorafgaand aan gegevensverwerkingen adequaat in kaart gebracht?
3. **Functionaris Gegevensbescherming (FG):** Is er een onafhankelijke FG aangesteld die effectief toezicht houdt op de naleving van privacyregels?

Volgens AP-vicevoorzitter Monique Verdier is het doel van deze inspecties niet om te bestraffen, maar om gemeenten te ondersteunen bij het verbeteren van hun privacypraktijken. De AP deelt na afloop de bevindingen en geeft waar nodig aanwijzingen om processen te verbeteren.

Niet alleen relevant voor gemeenten

Hoewel deze actie zich op gemeenten richt, geldt de boodschap voor alle organisaties: een robuust privacybeleid, dat voldoet aan de eisen van de Algemene verordening gegevensbescherming (AVG) is essentieel.



Luchtvaart: meer aandacht voor cyberdreigingen en klimaatverandering

14 mei 2025 - De Inspectie Leefomgeving en Transport (ILT) publiceerde de Staat van de Luchtvaart 2025. Conclusie: Vliegen blijft één van de veiligste vormen van transport, maar nieuwe risico's maken versterkte weerbaarheid noodzakelijk. Onderwerpen zoals de groeiende cyberdreiging en klimaatverandering, staan nu hoog op de agenda.

Geopolitieke ontwikkelingen vragen om meer cyberweerbaarheid

De luchtvaart wordt steeds digitaler – en daarmee kwetsbaarder. Geopolitieke spanningen en technologische afhankelijkheid vergroten het risico op cyberaanvallen. Van aanvallen op individuele systemen tot grootschalige, gecoördineerde aanvallen op de infrastructuur. Met directe gevolgen voor de fysieke veiligheid, economie, reputatie en bedrijfscontinuïteit. Verhogen van cyberweerbaarheid is dan ook geen optie, maar noodzaak. De NIS2-richtlijn – van toepassing op luchthavens en luchtvaartmaatschappijen – biedt hiervoor een stevig kader.

Klimaatverandering vraagt om aanpassing

Door de klimaatverandering neemt de frequentie en intensiteit van extreme weersomstandigheden toe. En daarmee een groeiend risico voor de veiligheid en operationele continuïteit. ILT roept op tot aanpassing van veiligheidsprotocollen en infrastructuur. Denk aan hittebestendige startbanen, robuustere waterafvoer en betere voorbereiding van bemanningen.

Naast veiligheid krijgt ook duurzaamheid meer prioriteit. De luchtvaart levert een belangrijke economische bijdrage, maar zorgt ook voor geluidsoverlast en schadelijke uitstoot. Verdere verduurzaming van de sector is dan ook cruciaal.

De luchtvaartsector moet blijven investeren in weerbaarheid – zowel digitaal als fysiek – om een veilige, verantwoorde en duurzame toekomst te kunnen garanderen.



Lancering Nederlands Register voor Functionarissen Gegevensbescherming

15 mei 2025 - Op 15 mei 2025 is het Nederlands Register voor Functionarissen voor Gegevensbescherming (NRFG) officieel gelanceerd. Met dit onafhankelijke en openbare register kunnen Functionarissen voor Gegevensbescherming (FG's) zich registreren en aantonen dat zij beschikken over de vereiste vakbekwaamheid en professionele integriteit.

Het NRFG is opgericht om de kwaliteit en positie van FG's te versterken. Het draagt bij aan:

- Versterking van de kwaliteit en onafhankelijkheid van de FG;
- Duidelijkheid over functie-eisen, gebaseerd op de regels van de AVG;
- Transparantie en toezicht over wie als FG actief is, inclusief hun ervaring en expertise.

Beheer door onafhankelijke stichting

Het NRFG wordt beheerd door een onafhankelijke stichting. Deze stichting is onder andere verantwoordelijk voor het registreren en beheren van gegevens, het vaststellen van opleidingseisen en ethische normen, het accrediteren van opleidingen en het toezicht houden op de naleving van regelgeving.

Wanneer is een FG verplicht?

Een FG houdt binnen organisaties toezicht op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG). Volgens de Autoriteit Persoonsgegevens zijn er in Nederland inmiddels zo'n 10.000 FG's actief. Voor bepaalde organisaties is het aanstellen van een FG wettelijk verplicht, zoals:

- Overheidsinstanties en publieke organisaties;
- Organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen of hun activiteiten in kaart brengen;
- Organisaties die op grote schaal bijzondere persoonsgegevens verwerken en waarvan dit een kernactiviteit is;
- Organisaties die strafrechtelijke eisen verwerken.

Het register biedt niet alleen voordelen voor FG's, maar ook voor organisaties. Het kan helpen bij het vinden van een gekwalificeerde FG en draagt bij aan de professionalisering van het privacyvakgebied.