cuccibu
Reduce Risk, Create Value

CUCCIBU'S
INSIGHT OF THE MONTH

Een terugblik op het nieuws van de afgelopen weken:

- AP: AI-impactbarometer kleurt rood. Compliance en handhaving blijven achter.
- Videodeurbellen: beelden worden te lang bewaard.
- DICTU lanceert tool voor het kiezen van clouddiensten.
- Gemeentesites delen data (zonder toestemming) met Big Tech.
- AP publiceert praktijkgids voor gezondheidsgegevens in de cloud.

Privacy

AP: AI-impactbarometer kleurt rood. Compliance en handhaving blijven achter.

5 maart 2026 - De Autoriteit Persoonsgegevens (AP) slaat alarm: de risico's van AI nemen sneller toe dan handhaving en beveiligingsmaatregelen kunnen bijhouden.

Twee keer per jaar publiceert de AP een rapportage over AI & Algoritmes in Nederland. Daarbij wordt gekeken naar de risico's en effecten. Inmiddels staan vier van de negen indicatoren op rood.

Er is te weinig voortgang op:

- Toezicht en handhaving
- Ontwikkeling van standaarden
- Registratie van algoritmes
- Inzicht in incidenten

Organisaties onderschatten risico's

Tegelijkertijd onderschatten organisaties de risico's en ontwijken zij hun verantwoordelijkheid voor veilige en verantwoorde inzet van AI. Dit brengt de bescherming van grondrechten en cyberveiligheid in gevaar. Vooral gezien het feit dat risico's exponentieel groeien. Deepfakes, AI-fraude en discriminatie neemt in hoog tempo toe.

Actie vereist

De komst van de AI-verordening zou betrouwenbare AI moeten bevorderen, met systemen die veilig zijn, grondrechten respecteren en tegelijkertijd innovatie mogelijk maken. Maar zonder duidelijke nationale implementatie (uitvoeringswet) en toezicht blijft dit achter.

Bron: Autoriteit Persoonsgegevens

Privacy

Videodeurbellen: beelden worden te lang bewaard

12 maart 2026 - Uit onderzoek van Omroep Gelderland blijkt dat 1 op de 3 videodeurbellen die de openbare weg filmen én zijn aangemeld bij een speciaal politieregister beelden langer bewaard dan toegestaan.

Volgens de Algemene verordening gegevensbescherming (AVG) mogen beelden niet langer opgeslagen worden dan ‘strikt noodzakelijk’. Meestal is dit maximaal 28 dagen. Uit het register ‘Camera in Beeld’ van de politie blijkt dat deze bewaartermijn veelal wordt overschreden. Daarmee komen privacyregels in het geding.

Bij wie ligt de verantwoordelijkheid?
In het register van de politie staan ruim 350.000 videodeurbellen geregistreerd. De eigenaren (niet alleen particulieren) stellen hun beelden beschikbaar voor het oplossen van misdrijven. De politie hanteert ook een maximum bewaartermijn voor deze beelden.

Het is onduidelijk bij wie deze verantwoordelijkheid ligt. Enerzijds wordt gezegd dat de politie de gebruikers moet attenderen op deze bewaartermijnen. Zij zeggen op hun beurt weer dat het toezicht op naleving van de AVG de verantwoordelijkheid is van de Autoriteit Persoonsgegevens (AP).

Bron: NOS.nl

Information Security

DICTU lanceert tool voor het kiezen van clouddiensten

16 maart 2026 - Hoe soeverein is jouw clouddienst? Met het nieuwe **Toetsingsinstrument Soevereiniteit Clouddiensten** biedt de Dienst ICT Uitvoering (DICTU) organisaties een praktische manier om de mate van soevereiniteit van hun (toekomstige) clouddiensten te bepalen.

Het instrument maakt gebruik van objectieve en transparante beoordelingscriteria en helpt overheden en publieke organisaties om weloverwogen keuzes te maken bij de selectie en evaluatie van cloudleveranciers. Daarbij wordt gekeken naar onderwerpen zoals datasoevereiniteit, wet- en regelgeving, autonomie en betrouwbaarheid.

Waarom is dit nodig?
Meer dan 70% van de wereldwijde cloud markt is in handen van grote Amerikaanse aanbieders (hyperscalers), zoals Microsoft en Google. Veel organisaties zijn afhankelijk van deze partijen. Deze afhankelijkheid brengt risico’s met zich mee, o.a. op het gebied van veiligheid, autonomie en onderhandelingspositie.

Met het toetsingsinstrument draagt DICTU bij aan een veilig, transparant en toekomstbestendig gebruik van clouddiensten binnen de overheid.

Bron: Security.nl & Dienst ICT Uitvoering

Privacy

Gemeentesites delen data (zonder toestemming) met Big Tech

16 maart 2026 - Bij ongeveer 61% van de gemeenten worden bezoekersgegevens, zoals IP-adressen, gebruikte apparaat en bezochte url, gedeeld met partijen als Google. Vaak zonder toestemming.

Deze combinatie van gegevens maakt het mogelijk om websitebezoekers te blijven volgen. In veel gevallen worden trackingdiensten al geladen vóórdat een gebruiker akkoord geeft. Dat is in strijd met de Algemene verordening gegevensbescherming (AVG).

Cookiebanners ontbreken
Dit is onder andere mogelijk doordat bij maar liefst 220 gemeenten een cookiebanner ontbreekt. Hierdoor wordt direct Google Analytics getriggerd.

Daarnaast is sprake van onbewuste datadeling, door het gebruik van standaardtools als YouTube en Google fonts. Dit lijkt onschuldig, maar deze tools starten vaak automatische tracking op. Veel gemeentes zijn zich daar niet bewust van.

Gebrek aan kennis
De oorzaak? Niet per se onwil, maar gebrek aan bewustzijn en technische kennis.

Bron: Security.nl

Privacy Information Security

AP publiceert praktijkgids voor gezondheidsgegevens in de cloud

23 maart 2026 - De Autoriteit Persoonsgegevens (AP) publiceert een nieuwe praktijkgids om organisaties te helpen bij het veilig verwerken van gezondheidsgegevens in de cloud.

De gids kijkt breder dan een eerdere gids over alleen patiëntgegevens en behandelt onder andere gegevens in medische dossiers, gegevens over gezondheid in relatie tot werk, testresultaten en gegevens uit digitale zorgtoepassingen. Daarbij wordt ook de rol van verschillende partijen in de keten belicht, zoals zorgaanbieders, arbodiensten, IT-leveranciers en andere ketenpartners.

De kernboodschap is duidelijk: **neem verantwoordelijkheid** voor de veilige en verantwoorde verwerking van gezondheidsgegevens.

De gids benadrukt het belang van:

- Duidelijke verantwoordelijkheden van de verwerkingsverantwoordelijke
- Inzicht in de rol van verwerkers en subverwerkers
- Structurele risicoanalyse
- Aandacht voor datasoevereiniteit en internationale doorgifte
- Het samenspel tussen AVG en NIS2

In de praktijk gaat het vaak mis door een gebrek aan inzicht in datastromen, betrokken partijen en van toepassing zijnde wetgeving.

Organisaties die gezondheidsgegevens in de cloud verwerken, blijven volledig verantwoordelijk. Die verantwoordelijkheid kun je niet uitbesteden aan een cloudleverancier. Cloudgebruik vraag om regie en inzicht.

Bron: Autoriteit Persoonsgegevens