

# PI Nieuws februari 2022

## **Boete Transavia: slechte beveiliging persoonsgegevens**

De Autoriteit Persoonsgegevens (AP) heeft Transavia een boete opgelegd van 400.000 euro vanwege een slechte beveiliging van persoonsgegevens. Door die slechte beveiliging kon een hacker in 2019 de systemen van Transavia binnendringen. Daarbij kreeg deze toegang tot systemen waarin hij gegevens van 25 miljoen mensen had kunnen inzien. Vastgesteld is dat de hacker persoonsgegevens van zo'n 83.000 personen downloadde.

De hacker kreeg deze toegang tot accounts van de IT-afdeling wel heel makkelijk. De beveiliging was namelijk op drie punten niet op orde:

- Het wachtwoord was makkelijk te raden. Het ging hierbij om een wachtwoord vergelijkbaar met '123456', 'Welkom' en 'Wachtwoord'.
- Alleen dat wachtwoord bleek voldoende om het systeem binnen te komen. Er was geen zogeheten meerfactorauthenticatie (2FA) door Transavia toegepast.
- Toen de hacker eenmaal de controle had over deze twee accounts, had hij ook toegang tot een groot aantal andere systemen van Transavia. De toegang van deze twee accounts was namelijk niet beperkt tot alleen de noodzakelijke systemen.

Meer informatie: [boetebesluit](#)

## **Website van de maand**

[gdprhub.eu](https://gdprhub.eu)

De GDPRhub is een initiatief van NOYB. Vrijwilligers houden op deze hub bij welke AVG beslissingen er in Europa genomen worden door toezichthouders en rechters. Hiermee houdt u makkelijk het overzicht zonder dat u vele websites in de gaten hoeft bij te houden. De informatie is bovendien per artikel doorzoekbaar. Ook kunt u zich hier abonneren op de nieuwsbrief. Een aanrader dus.

## **Het was me een ransomjaartje wel....**

Wat is de overeenkomst tussen: ANWB, UvA, Hof van Twente, Bakker/AH, Mandemakers, ROC Mondriaan, RTL Nederland, IJmond werkt, VDL en Media Markt?

Dat ze allemaal het afgelopen jaar getroffen zijn door cyberattacks. Criminelen verkrijgen toegang door gestolen wachtwoorden of gewoon door wachtwoorden te raden. Zijn ze eenmaal binnen dan dringen ze verder de systemen in, ze encrypten data, verwijderen backups, eisen losgeld en/of dreigen data openbaar te maken.

Vorig jaar keerden verzekeraars 21 miljard dollar uit aan bedrijven die getroffen zijn door cyber attacks en dan met name ransomware. Dit soort aanvallen op bedrijven zijn flink toegenomen. De verwachting is dat deze trend in 2022 verder doorzet.

Meer informatie: [Overzicht cyber attacks 2021](#)

## Security awareness trends 2022

Nog wat trends. Nu in het kader van awareness van medewerkers. De menselijke factor in informatiebeveiliging wordt alsmaar belangrijker. Wat kunnen we in 2022 allemaal verwachten? O.a. motiveren door gamification, het passwordless inloggen, de noodzaak tot het doorvoeren van maatwerk en het belang van meten van resultaten.

Lees verder in: [8 security awareness ontwikkelingen](#)

## Google analytics verboden

Her en der zijn er in Europa klachten ingediend bij toezichthouders over bedrijven die gebruik maken van Google Analytics (GA). Naar aanleiding van twee van die klachten hebben de toezichthouder van Oostenrijk en Frankrijk bepaald dat gebruik van GA niet rechtmatig is. In het kort komt het erop neer dat door GA te gebruiken er tot persoonsgegevens te herleiden data naar de VS gaan en dat is op grond van recente uitspraken van het Europese Hof verboden. Als je persoonsgegevens laat verwerken in de VS moet je maatregelen nemen om te voorkomen dat deze gegevens in handen komen van inlichtingendiensten. Deze maatregelen heeft GA onvoldoende genomen. De beslissingen zijn genomen in overleg met de overige toezichthouders. De AP heeft inmiddels laten weten dat ze er ook onderzoek naar doet en dat de kans reëel is dat zij eenzelfde besluit zal nemen.

Europese alternatieven voor Google Analytics zijn helaas schaars. In de link hieronder zijn er een aantal opgenomen.

Meer informatie: [Toelichting besluit CNIL & alternatieven](#)

## Wel vragen naar origineel ID bewijs, maar niet opslaan.

Het geschilleninstituut voor de banken heeft vastgesteld dat banken in het kader van anti witwaswetgeving verplicht zijn om ID bewijzen te controleren. Maar ook dat als ze deze willen opslaan ze rekening moeten houden met de AVG. In het kader van dataminimalisatie moeten banken de foto's blurren. Ook worden banken verplicht om misbruik tegen te gaan een watermerk aan te brengen. Slaat u een kopie ID bewijs op voor uw werknemer dan geldt overigens dat deze altijd een foto en BSN moet bevatten. Het ligt wel voor de hand dat u deze ID bewijzen voortaan een watermerk meegeeft als de werknemer dit zelf nog niet heeft gedaan.

Meer informatie: [Uitspraak Kifid](#)