

Nieuwsbrief

Beste lezer,

De tropische temperaturen van juni maakte wel duidelijk dat de zomer in aantocht is. Maar de ontwikkelingen rond privacy en informatiebeveiliging lijken eerder te versnellen dan te vertragen.



Zo is de Verzamelwet gegevensbescherming aangenomen, wat concrete gevolgen kan hebben voor jouw organisatie. En de kansen en risico's van Artificial Intelligence (AI) roepen steeds nieuwe vraagstukken op.

In deze nieuwsbrief zetten we de need to knows voor je op een rij. Zodat je goed op de hoogte de zomerperiode in gaat.

We wensen je alvast een mooie en ontspannen zomer.

Team L2P

Omgaan met datalekken: hoe doe je dat als FG op de juiste manier?

Het UWV meldde in 2024 in totaal 1833 datalekken bij de Autoriteit Persoonsgegevens. Dat zijn dus bijna twintig incidenten per week.

De Functionaris Gegevensbescherming (FG) wordt volgens de Algemene verordening gegevensbescherming (AVG) "naar behoren en tijdig" betrokken bij alle aangelegenheden rond de bescherming van persoonsgegevens. Hoe werkt dat in de praktijk?



[Lees wat je te doen staat](#)

Kennisdag AI in control: grip op risico's in IB en P



Geen nieuw huis: Grip op AI met het fundament dat u al heeft.

Generatieve AI genereert oplossingen en werk. Maar nog geen grip.

Generatieve AI is in korte tijd elke organisatie binnengekomen, vaak sneller dan beleid en governance konden volgen.

Tegelijk werd zichtbaar hoe afhankelijk we zijn geworden van een handvol AI-leveranciers. Modellen die van de ene dag op de andere onder restricties vielen, voorwaarden die eenzijdig veranderen: het legde een ongemakkelijke waarheid bloot. We bouwen op een fundament dat niet van onszelf is.

Dat heet vendor lock-in, en het is geen incident maar de structuur. Wie de processen, data en workflows op één AI-leverancier baseert, levert regie in zonder het te merken. De vraag is niet óf die afhankelijkheid een risico vormt, maar of u er grip op hebt.

Twee reflexen, allebei duur.

Op die vraag reageren organisaties meestal op één van twee manieren. De eerste is verlamming: AI als onbeheersbare dreiging, dus alles op slot. Het gevolg is achterstand, terwijl de concurrent doorbouwt. De tweede is weggijken: AI als vrijblijvende hype, dus laten lopen. Het gevolg is ongecontroleerde schaduw-AI, met datalekken en onbeheerste verwerkingen tot gevolg. Beide reacties kosten geld en geen van beide levert grip.

De vraag of AI rendabel is of slechts hype, is daarmee de verkeerde vraag. De enige vraag die telt: heeft u grip? Wie grip heeft, beslist zelf wanneer AI rendeert en wanneer terughoudendheid verstandiger is.

AI is een bouwsteen, geen nieuw huis

Op onze kennisdag staat de vraag centraal die elke FG, privacy officer en securityprofessional bezighoudt: hoe houdt u grip terwijl de wereld draait? In zijn keynote laat Jean Paul van Schoonhoven zien dat het antwoord niet ligt in een nieuw AI-stelsel naast alles wat u al hebt opgebouwd. AI is een nieuwe bouwsteen op een bestaand fundament van risicomanagement,

PDCA en het Three Lines Model. De kunst zit niet in opnieuw beginnen, maar in slim inpassen.

Dat fundament werkt twee kanten op. Naar buiten richt u zich op het vendor management van uw AI-leveranciers: exitstrategie, dataportabiliteit, ketenrisico en heldere afspraken over modelwijzigingen. Naar binnen regelt u wat u als gebruikende organisatie niet kunt afschuiven, met dataclassificatie als voorwaarde vooraf. Want zonder classificatie beantwoordt niemand de simpele vraag of bepaalde data überhaupt naar een model mag. Juist hier komen privacy en informatiebeveiliging samen: de privacy officer beantwoordt die vraag niet zonder de CISO. De CISO is geen hindernis, maar de natuurlijke bondgenoot.

Van inzicht naar handelen

Daarna maken we het concreet. Een klant deelt zijn reis van chaos naar grip, met de nadruk op de hardere kant van goede informatiebeveiliging. En Niels den Ottelander, teamleider IB, en Linda Li, teamleider Privacy, geven u de toolkit mee waarmee u zelf aan de slag kunt: de AI-Quicksan om risico's en kansen in kaart te brengen, en het Traffic Light Protocol om AI-gebruik in uw organisatie hanteerbaar te maken.

We sluiten de dag interactief af en praten daarna met u na tijdens de netwerkborrel.

Generatieve AI genereert oplossingen en werk. Maar nog geen grip. Die haalt u op deze dag.

Het L2P-kennisevent vindt plaats op 24 september in Locatie78 in Bunnik. Deelname is gratis voor jou als nieuwsbrieflezers (maar een aanmelding is wel nodig).

[Direct aanmelden](#)

Zo maak je als Privacy Officer een succes van je werk



Hoe maak je als privacy officer daadwerkelijk een positieve impact? Je werkt praktisch én strategisch, maar er zijn ook taken en verantwoordelijkheden die thuishoren bij collega's.

In een interview met [Outvie](#) vertelt Jean Paul van Schoonhoven van L2P over de trends, uitdagingen en best practices. Je leest bijvoorbeeld wat veranderende wet- en regelgeving en de opmars van AI voor betekenen het dagelijkse werk en de interne positie van de privacy officer.

[Check hier het interview en ontdek alle inzichten](#)

Opleidingen & trainingen

Ben je een professional die verantwoordelijkheid draagt voor privacy en/of informatiebeveiliging? Dan is continue professionele ontwikkeling een must. Je houdt je expertise en skills altijd op peil met de praktijkgerichte trainingen van L2P.

L2P verzorgt verschillende eendaagse IAPP-trainingen, die je voorbereiden op het examen voor deze toonaangevende privacycertificering:

AIGP
[9 juli 2026](#), online

CIPT
[3 september 2026](#), online

CIPP/E
[17 september 2026](#), online

CIPM
[15 oktober 2026](#), online

Experts van L2P zijn docenten van diverse Outvie-trainingen, die speciaal zijn ontwikkeld voor privacy professionals:



de tiendaagse opleiding Certified Data Protection Officer (CDPO)
[vanaf 24 september 2026](#), Amsterdam

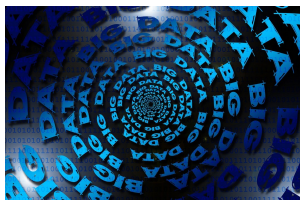
2 daagse praktijktraining AI Fundamentals voor privacy & compliance professionals
[vanaf 28 september 2026](#), Amsterdam en online

5 daagse training Senior Privacy Professional
[Vanaf 29 oktober 2026](#), Amsterdam en online

4 daagse training Privacy Professional 2.0
[vanaf 3 november](#), Amsterdam en online

Meer informatie over alle opleidingen & trainingen?

Verzamelwet gegevensbescherming, de belangrijkste wijzigingen



In mei heeft de Eerste Kamer [de Verzamelwet gegevensbescherming](#) aangenomen. De wet gaat over onder andere de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG). De wijzigingen kunnen concrete gevolgen hebben voor een groot aantal organisaties, waaronder financiële instellingen en accountants.

Het is daarom raadzaam om na te gaan of de werkwijze van je organisatie nog aansluit bij de nieuwe wettelijke kaders. Bijvoorbeeld wat betreft de interne processen en het privacybeleid. De privacy-experts van L2P denken mee over de gevolgen van de Verzamelwet gegevensbescherming voor jouw specifieke situatie. We adviseren ook over de acties die nodig zijn om straks aan de wet te voldoen.

Ik wil graag meer informatie



... miljoenen zonnepanelen in Nederland kwetsbaar zijn voor cyberaanvallen? Hackers zijn in toenemende mate in staat om toegang te krijgen tot zonnepaneleninstallaties die zijn verbonden met internet. Een goede beveiliging van het internetsysteem is noodzakelijk om te voorkomen dat gevoelige (persoons)gegevens worden gelekt.

... de integratie van zogenoemde threat intelligence een plek verdient in een Information Security Management System (ISMS)? Threat intelligence is gebaseerd op geautomatiseerde feeds en analyses die actuele dreigingsinformatie leveren. Met name over de motieven en aanvalsmethoden van kwaadwillende actoren. Volgens ISO 27001 helpt threat intelligence om nieuwe risico's tijdig te signaleren. Zodat je organisatie sneller en effectiever reageert.

... een cyberaanval op een wachtwoord met acht karakters doorgaans slechts enkele minuten duurt? Een wachtwoord dat bestaat uit minimaal twaalf tekens, waaronder letters, cijfers én symbolen, is aanzienlijk lastiger te kraken. [Aandacht voor sterke wachtwoorden is dan ook onmisbaar voor elke organisatie.](#)

Meer weten over privacy, security of compliance?
[Stel ons gerust je vraag.](#)



De nieuwe quiz test jouw kennis van Informatiebeveiliging.

Wat is het verschil tussen 'explainable AI' (XAI) en traditionele AI-methoden?

A) XAI kan beslissingen transparanter maken en verklaren, terwijl traditionele AI vaak een 'black box' is

B) XAI is sneller in verwerking dan traditionele AI

- C) Traditionele AI maakt altijd gebruik van regels, XAI niet
- D) XAI werkt alleen met gestructureerde data

Mail ons je antwoord **uiterlijk 17 juli** en maak kans op een notitiewaardige L2P-prijs.
[Mijn antwoord is](#)

De quizvraag in de vorige nieuwsbrief ging over de AVG.

De vraag was: Wat betekenen de principes van accountability in de AVG voor de manier waarop je als organisatie aantoont dat je zorgvuldig omgaat met persoonsgegevens?

Het juiste antwoord was antwoord B. Organisaties moeten expliciet aantonen dat ze - met passende maatregelen - voldoen aan de vereisten van de AVG. Dat gebeurt bijvoorbeeld met DPIA's, verwerkersovereenkomsten en audits

De winnaar heeft ondertussen bericht ontvangen.

L2P
Stadsplateau 7
3521 AZ Utrecht
www.l2p.nl



LinkedIn

Stel je vraag aan ons.