cuccibu

Reduce Risk, Create Value

CUCCIBU CONFERENCE

1 APRIL 2026 | KAS WOERDEN

CUCCIBU CONFERENCE 2026

Wat leuk dat je geïnteresseerd bent in de Cuccibu Conference 2026!

In deze informatiefolder nemen we je graag mee door het programma en ontdek je alles over de inspirerende kennissessies die onze experts en partners voor je hebben voorbereid.

HET PROGRAMMA

09.30 uur — **Opening door Tim Florack**

10.00 uur — **Plenaire keynote door Klaas Dijkhoff**

11.15 uur — **Ronde 1 - Kennissessies**

- Security 360: Van Bits tot Boardroom
- AI governance: van verantwoordelijkheid naar regie
- Wat als de stekker eruit gaat?

12.00 uur — *Lunchpauze*

13.15 uur — **Ronde 2 - Kennissessies**

- Open Source Intelligence en online veiligheid
- Motivatie binnen gedragsverandering
- De rol van FG in een crisissituatie

14.15 uur — **Ronde 3 - Kennissessies**

- Van ISO 27001 naar NIS2: wat moet je écht nog doen?
- De AI Act in de praktijk
- Online compliance & privacy

15.15 uur — **Afsluiting en dankwoord**

15.45 uur — *Borrel en netwerken*

Security 360: Van Bits tot Boardroom

Een verhaal waarin mens, proces en technologie samenkomen

Cybersecurity lijkt vaak een wirwar van termen en bij échte digitale weerbaarheid komt ook steeds meer kijken. In een interactieve sessie neemt Dennis de Hoog je mee in een verhaal waarin mens, proces en technologie samenkomen.

We starten met analyse: risico's scherp identificeren, je volledige aanvalsoppervlak kennen, inzicht krijgen in aanvallers en hun scenario's en begrijpen welke wet- en regelgeving zoals NIS2, AVG en DORA relevant is.

Daarna volgen maatregelen: het opzetten van een duurzaam securityprogramma met sterke basismaatregelen, security-awareness, kwetsbaarheden zien en snel reageren op aanvallen.

Tot slot kijken we naar verbeteren: hoe je security aantoonbaar maakt, voortdurend toetst en test en heel belangrijk blijft innoveren. In begrijpelijke taal en praktijkvoorbeelden laat Dennis zien hoe je van complexe begrippen concrete acties maakt.

In deze sessie ontdek je:

- Hoe je jouw digitale risico's scherp in kaart brengt.
- Hoe je een duurzaam securityprogramma met sterke maatregelen opbouwt.
- Hoe je security aantoonbaar maakt en continu verbetert.

Een breed publiek: van CISO's, CIO's en IT-managers tot andere professionals binnen Cyber Security.
Dit is geen diep technische sessie vol jargon of een stortvloed aan afkortingen. In plaats daarvan neemt Dennis je mee in begrijpelijke taal en met herkenbare praktijkvoorbeelden. Of je nu actief bent in de zorg, overheid, industrie of financiële sector - de principes van cybersecurity zijn overal hetzelfde: van analyse, naar maatregelen en eindigen bij verbeteren.

Dennis de Hoog
Business Manager Security bij Wortell

Deze sessie wordt verzorgd door onze partner Wortell.

wortell

Dennis is Business Manager Security bij Wortell. In deze rol brengt hij Microsoft-technologie, cybersecurity en mensen samen om organisaties veiliger en weerbaarder te maken. Van strategische uitdagingen tot concrete oplossingen. Hij gelooft in een balans tussen technologie, processen en de menselijke factor.

Daarnaast schrijf Dennis frequents blogs en LinkedIn artikelen, maak de podcast Cyberpraat, verzorgt webinars en keynotes. Ook is hij verbonden aan de Hogeschool Rotterdam als 2e examinator Business IT & Management opleiding. In zijn vrije tijd is hij een fanatieke fietser.

CUCCIBU CONFERENCE 2026

RONDE 1

AI governance: van verantwoordelijkheid naar regie

Waarom AI niet alleen een privacy of IT-vraagstuk is.

AI is in in korte tijd van experiment naar dagelijkse praktijk gegaan. Maar wie is eigenlijk verantwoordelijk voor het gebruik van AI in jouw organisatie? En hoe benut je de kansen van AI op een veilige en verantwoorde manier, zonder de controle te verliezen?

In veel organisaties komt AI automatisch op het bord van privacy officers, juristen of compliance specialisten terecht. Logisch misschien, maar is dat wel terecht? AI raakt immers niet alleen het thema privacy of security, maar de kern van hoe organisaties werken, besluiten nemen en diensten leveren. Daarmee is AI governance niet alleen een compliance-vraagstuk, maar een organisatiebrede én bestuurlijke verantwoordelijkheid.

AI governance gaat over het organiseren van eigenaarschap, verantwoordelijkheid en toezicht op het gebruik van AI. Niet als een eenmalig beleidsdocument, maar als een continu proces dat gedragen wordt door de hele organisatie - van bestuur tot uitvoering.

In deze sessie laten Leonie en Hayke zien wat AI governance écht betekent in 2026. Welke rollen zijn nodig? En welke principes helpen organisaties om AI veilig, verantwoord, transparant en beheersbaar in te zetten? Je krijgt inzicht in hoe je AI governance praktisch organiseert en hoe je zorgt dat het onderwerp op de juiste plek in de organisatie wordt belegd.

In deze sessie ontdek je:

- Wat AI governance inhoudt en waarom het verder gaat dan privacy, security of IT alleen.
- Welke rollen, verantwoordelijkheden en samenwerking nodig zijn om AI verantwoord te beheersen.
- Concrete governance-principes en praktische handvatten die je direct kunt toepassen binnen jouw organisatie.

Deze sessie is met name relevant voor professionals bij wie AI “op het bordje ligt” en die zich afvragen hoe dit goed georganiseerd kan worden binnen de organisatie.

Daarnaast is deze sessie waardevol voor iedereen die betrokken is bij de inzet, het toezicht of de besluitvorming van AI, zoals privacy officers, FG’s, CISO’s, IT-managers, beleidsmakers, bestuurders en directieleden.

Leonie Peters
Privacy & Legal Consultant Cuccibu

Hayke Jansma
Privacy & Legal Consultant Cuccibu

Leonie Peters en Hakye Jansma zijn privacy & legal consultants bij Cuccibu. Zij adviseren en begeleiden organisaties bij privacyvraagstukken, AI-governance en de implementatie van wet- en regelgeving zoals de AVG en de AI Act.

Vanuit hun dagelijkse praktijk zien zij hoe AI zich in hoog tempo ontwikkelt en welke vragen dat oproept over verantwoordelijkheid, compliance en governance. Zij helpen organisaties om AI op een verantwoorde en beheersbare manier in te zetten, door wetgeving, governance en praktijk met elkaar te verbinden. Zonder privacy uit het oog te verliezen.

CUCCIBU CONFERENCE 2026

RONDE 1

Wat als de stekker eruit gaat?

Ligt jouw bestuur wakker van geopolitieke risico's, en hoe groot is de kans dat dit écht gebeurt?

In deze sessie leggen we uit waarom digitale afhankelijkheid van hyperscalers, cloud-ecosystemen en grote technologieplatformen niet alleen een IT-vraagstuk is, maar een bestuurlijk risico dat thuishoort op boardniveau. We verbinden geopolitieke risico's en marktontwikkelingen aan privacy, security en compliance, waaronder de verplichtingen vanuit NIS2/Cyberbeveiligingswet (Cbw). Niet alleen de impact staat centraal, maar juist ook de waarschijnlijkheid: hoe reëel zijn deze scenario's, en hoe breng jij dat naar jouw bestuur? Daarnaast bieden wij praktische handvatten om deze thema's effectief op de bestuurlijke agenda te krijgen en écht impact te maken binnen jouw organisatie.

In deze sessie ontdek je:

- Welke digitale afhankelijkheden bestuurlijke risico's vormen en hoe je deze vertaalt naar bestuurlijke taal (risico, compliance, continuïteit).
- Drie praktische scenario's en gesprekspunten om bestuurlijke besluitvorming te stimuleren rondom digitale afhankelijkheid en vendor lock-in.
- Concrete handvatten om met bestuurders het gesprek aan te gaan en beweging te creëren, inclusief kernvragen en risico-kaders.

CISO's | Security Officers | Privacy Officers | Functionaris Gegevensbescherming | IT Managers
Wil je dat digitale risico's niet langer alleen een verantwoordelijkheid van de IT-afdeling zijn, maar ook bestuurlijk worden erkend en geadresseerd voor échte impact? Dan is deze sessie zeker interessant voor jou!

Tim Florack
Founder Cuccibu

Tim is oprichter van Cuccibu en heeft jarenlange ervaring in het verbinden van vraagstukken over privacy, informatiebeveiliging en risicomanagement met bestuur en compliance. Vanuit zijn achtergrond in risico- en IT-audit heeft hij organisaties geholpen om complexe digitale risico's inzichtelijk te maken en te vertalen naar bestuurlijke beslispunten. Cruciaal in een tijd waarin wetgeving zoals NIS2 de verantwoordelijkheid duidelijk bij governance en de board neerlegt. Volgens Tim zijn strategie, compliance en operationele risico's dan ook onlosmakelijk met elkaar verbonden.

Patrick Venderbos
Lead Consultant Cuccibu

Patrick heeft ruim een decennium lang ervaring met IT- en proces audits, risicomanagement, compliance en informatiebeveiliging bij uiteenlopende organisaties, zowel in de publieke als private sector. Hij ondersteunt organisaties bij het zichtbaar maken van risico's, optimaliseren van processen en het vergroten van bestuurlijke bewustwording. Patrick weet risico's te vertalen naar concrete beheersmaatregelen en, minstens zo belangrijk, adviseert bestuurders hoe zij hierop kunnen sturen. Dit doet hijdagelijks in zijn rol als Lead Consultant bij klanten, maar ook als CISO van Cuccibu.

CUCCIBU CONFERENCE 2026

RONDE 2

Open Source Intelligence en online veiligheid

Wat ligt er online voor het oprapen en wat kunnen hackers hiermee?

Tijdens deze interactieve OSINT-presentatie leer je hoe hackers met Open Source Intelligence openbare informatie verzamelen en inzetten voor phishing, social engineering en identiteitsmisbruik.

In praktische challenges ervaar je zelf hoe kwetsbaar digitale informatie kan zijn. Daarnaast krijg je inzicht in hoe je je digitale voetafdruk kunt verkleinen en je organisatie beter kunt beschermen tegen misbruik van openbare informatie.

In deze sessie ontdek je:

- Hoe hackers met OSINT openbare informatie verzamelen en analyseren.
- Hoe hackers OSINT gebruiken om jouw organisatie aan te vallen.
- Hoe je je organisatie beter kunt beschermen tegen misbruik van openbare informatie.

Deze sessie is interessant voor iedereen die wil begrijpen hoe hackers Open Source Intelligence inzetten en wil weten hoe je je organisatie beter beschermt tegen misbruik van openbare informatie.

Bas Cijsouw
Ethisch hacker
bij The S-Unit

Deze sessie wordt verzorgd door onze partner The S-Unit.

Bas Cijsouw is ethisch hacker bij The S-Unit en heeft een studieachtergrond in software development. Naast zijn OSCP-certificering heeft Bas ruime ervaring opgedaan met Bug Bounties, waarbij kwetsbaarheden in organisaties worden beloond op basis van het securityrisico. Zijn belangrijkste werkzaamheden zijn het uitvoeren van penetratietesten, maar hij verzorgt ook trainingen in OSINT en de OWASP Top 10 bij The S-Unit.

In zijn vrije tijd is Bas vaak in de sportschool te vinden, maar zijn echte passie ligt bij het zoeken. Waar hij zich professioneel richt op het opsporen van kwetsbaarheden in cybersecurity, speurt hij in zijn vrije tijd met zijn metaaldetector naar verborgen schatten in de grond. Voor hem draait het steeds om dezelfde spanning: het ontdekken van het onzichtbare, of dat nu digitale risico's zijn of gouden munten.

CUCCIBU CONFERENCE 2026

RONDE 2

Motivatie binnen gedragsverandering

Wetenschappelijk onderbouwde aanpak voor duurzame cultuurverandering

“Hoe krijg ik ze zover dat ze dit echt gaan doen?" Security- en Privacy-professionals zien intrinsieke motivatie vaak als de heilige graal bij bewustwordingstrajecten. Het idee: als medewerkers het 'uit zichzelf' doen, is het probleem opgelost. Maar hier ontstaat de paradox: intrinsieke motivatie kun je niet van buitenaf afdwingen. Sterker nog: hoe harder je duwt, hoe meer je datgene verliest wat je probeert te creëren.

In deze kennissessie fileert Pascal Koelemij, Head of Research & Innovation bij Awareways, de mythe van de intrinsieke motivator. Hij laat zien waarom het najagen van deze illusie averechts werkt en biedt een krachtiger, realistisch alternatief. Geen korte gedragscampagnes of repressieve maatregelen, maar een wetenschappelijk onderbouwde aanpak voor duurzame cultuurverandering.

In deze sessie ontdek je:

- Hoe je mensen in beweging krijgt, zonder dat je intrinsieke motivatie als driver nodig hebt.
- Hoe je voorbij ‘belonen en straffen’ gaat en jouw programma aansluit bij de persoonlijke waarden van medewerkers.
- Hoe gewenst gedrag standhoudt, ook als de Security Officer even niet meekijkt.

Deze sessie is voor jou als:

- ...je een CISO, ISO, FG, Awareness Officer of Compliance Lead bent die verder wil gaan dan ‘vinkjes zetten’.
- ...je op weg bent naar een weerbare organisatie in een tijd van AI en complexe dreigingen.
- ...je de kracht van gedragsverandering- en motivatie-theorie in jouw organisatie wil gaan toepassen.

Pascal Koelemij
Psycholoog en Head of Research & Innovation bij Awareways

Deze sessie wordt verzorgd door onze partner Awareways.

AWAREWAYS

Pascal slaat de brug tussen complexe gedragswetenschap en de dagelijkse security- en privacy-praktijk. Met jarenlange ervaring bij diverse nationale en internationale organisaties (Nederlandse gemeenten, ministeries, zorginstellingen en financiële dienstverleners) biedt Awareways een beproefde methode om jouw organisatie digitaal weerbaar te maken.

Klaar voor de snel veranderende digitale toekomst.

CUCCIBU CONFERENCE 2026

RONDE 2

De rol van de FG in een crisissituatie

Over de hack bij TU/e

Begin januari 2025 werd de TU/e opgeschrikt door een hack. Dankzij snel en doortastend handelen bleef de schade beperkt en kon worden voorkomen dat ransomware werd geïnstalleerd. Maar wat gebeurt er achter de schermen op zo'n moment? En wat is de rol van de Functionaris Gegevensbescherming (FG) tijdens een crisis van deze omvang?

In deze sessie neemt Laura Hooijen – de Vries, Functionaris Gegevensbescherming bij de TU/e, je mee in haar ervaringen tijdens deze ingrijpende gebeurtenis. Vanuit haar positie maakte zij de hack van dichtbij mee en was ze nauw betrokken bij de opvolging. Ze laat zien wat er van een FG wordt verwacht in een crisissituatie, bij welke aspecten je betrokken bent en hoe je bijdraagt aan het beschermen van persoonsgegevens en het ondersteunen van de organisatie.

Aan de hand van een heldere tijdlijn krijg je inzicht in de verschillende fasen en de impact die de universiteit meemaakte tijdens het cyberincident. Laura bespreekt haar rol tijdens de hack en geeft een inkijkje in de samenwerking met belangrijke stakeholders zoals het privacyteam, de CISO, communicatie en het CvB. Je leert hoe cruciaal goede communicatie, samenwerking en snel schakelen zijn om de impact van een incident te beperken.

In deze sessie ontdek je:

- Welke stappen een organisatie doorloopt tijdens een hack.
- Hoe de rol van de Functionaris Gegevensbescherming eruitziet tijdens een crisis.
- Hoe je effectief samenwerkt met stakeholders om de impact van een incident te beperken.

Iedereen die wil weten hoe een organisatie handelt in tijden van crisis. In het bijzonder voor Functionarissen Gegevensbescherming, maar ook voor alle professionals die betrokken zijn bij datamanagement, privacy, informatiebeveiliging, IT of crisismanagement.

Laura Hooijen - de Vries
Functionaris Gegevensbescherming (FG) bij TU/e

Deze sessie wordt verzorgd door:

TU/e

Laura Hooijen - de Vries is Functionaris Gegevensbescherming bij de TU/e en maakte in deze rol de hack van dichtbij mee. Naast haar huidige rol als FG heeft zij brede kennis en ervaring op het gebied van privacy en gegevensbescherming. Zo vervulde zij ruim vijf jaar de rol van Privacy & Legal Consultant bij Cuccibu. In deze functie hielp zij organisaties bij het implementeren van de AVG en andere wetgeving, het vergroten van privacybewustzijn binnen organisaties en het vertalen van wet- en regelgeving naar pragmatische en werkbare oplossingen. Dankzij haar combinatie van inhoudelijke expertise en praktijkervaring weet Laura als geen ander hoe gegevensbescherming tot zijn recht komt, juist wanneer het er écht toe doet.

CUCCIBU CONFERENCE 2026

RONDE 3

Van ISO 27001 naar NIS2: wat moet je écht nog doen?

Inzicht in de overeenkomsten, verschillen en aanvullende stappen

Veel organisaties beschikken al over een Information Security Management System (ISMS) conform ISO 27001 en vragen zich af of zij daarmee automatisch voldoen aan de NIS2-richtlijn en de aankomende Cyberbeveiligingswet. Het korte antwoord is: nee, maar je hebt wél een sterke basis.

In deze sessie duik je samen met Max in de relatie tussen de internationale norm ISO/IEC 27001 en de Nederlandse Cyberbeveiligingswet, die voortkomt uit de Europese NIS2-richtlijn. Je krijgt helder inzicht in wat je met een ISO 27001-certificering al hebt afgedekt en waar de aanvullende eisen en verantwoordelijkheden liggen. We maken concreet welke onderdelen overlappen, waar de belangrijkste verschillen zitten en welke aanvullende stappen nodig zijn om aantoonbaar te voldoen aan de Cyberbeveiligingswet.

In deze sessie ontdek je:

- Of, en in hoeverre, je met een ISO 27001 certificering al voldoet aan de eisen van de NIS2/Cyberbeveiligingswet.
- Wat de belangrijkste verschillen zijn tussen de ISO 27001 en de eisen uit NIS2.
- Hoe groot de stap écht is van ISO 27001 naar NIS2 en welke concrete stappen je nog moet zetten.

Organisaties die direct of indirect met de NIS2-richtlijn te maken krijgen en willen weten wat dit concreet betekent voor hun informatiebeveiliging. Werk jij als **ISO**, **CISO**, **IT-manager**, **security**- of **compliance officer** binnen zo’n organisatie? En wordt er naar jou gekeken zodra de term NIS2 valt? Dan is deze sessie voor jou! Je krijgt helder inzicht in wat NIS2 van je vraagt en waarom ISO 27001 een sterke basis is of kan zijn.

Max Aarts
Information Security Consultant & Lead Auditor bij Cuccibu

Max Aarts is Information Security Consultant en Lead Auditor ISO 27001 bij Cuccibu. Hij heeft brede ervaring als consultant, CISO en (externe) auditor op het gebied van informatiebeveiliging. Binnen Cuccibu heeft hij bijgedragen aan de ontwikkeling van een NIS2-scan en ondersteunt hij organisaties bij hun voorbereiding op de NIS2-richtlijn, onder andere binnen gemeentelijke organisaties. Daarnaast beoordeelt hij als externe auditor vanuit een gecertificeerde instelling in hoeverre organisaties voldoen aan ISO 27001 en de NIS2-eisen.

Dankzij deze combinatie van advies- en auditervaring weet Max als geen ander wat organisaties nodig hebben om de stap van ISO 27001 naar NIS2 succesvol te maken.

CUCCIBU CONFERENCE 2026

RONDE 3

De AI Act in de praktijk

Van wetgeving naar concrete actie in jouw organisatie

De Europese AI Act is de eerste wet ter wereld die specifiek regels stelt aan het gebruik van AI. Deze wet treedt gefaseerd inwerking en is op 2 augustus 2027 volledig van kracht. Organisaties moeten nu al stappen zetten om hun AI-gebruik in kaart te brengen en te zorgen dat toepassingen veilig, transparant en verantwoord worden ingezet.

Maar wat betekent deze wet concreet voor jouw organisatie? Wanneer valt een AI-toepassing onder de AI Act? En wat moet je dan daadwerkelijk doen?

In deze praktische én interactieve sessie neemt Leonie je mee in de kern van de AI Act: hoe de wet is opgebouwd, welke risicocategorieën er zijn en welke verplichtingen daarbij horen. Daarna maken we direct de praktische vertaalslag. Aan de hand van een herkenbare praktijksituatie analyseren we:

- Hoe AI wordt gebruikt;
- Welke risico's daarbij horen;
- Onder welke risicocategorie de toepassing valt;
- En wat de AI Act in dat geval concreet van je organisatie vraagt.

Zo ervaar je zelf hoe je AI-toepassingen kunt beoordelen en beheersen conform de AI Act.

In deze sessie ontdek je:

- De kern van de AI Act: wat zegt deze richtlijn?
- Welke impact de AI Act heeft op jouw organisatie: wat moet echt?
- Hoe je de AI Act vertaalt naar de praktijk.

Deze sessie is met name relevant voor professionals die betrokken zijn bij de inzet, het toezicht of de beheersing van AI en zich afvragen wat de AI Act concreet van hen en hun organisatie vraagt.

Denk aan privacy officers, FG’s, juristen, CISO’s, IT-managers, compliance professionals, beleidsmakers, bestuurders en directieleden. Er is geen juridische of technische voorkennis vereist.

Leonie Peters
Privacy & Legal Consultant Cuccibu

Leonie Peters is privacy & legal consultants bij Cuccibu. Zij adviseert en begeleidt organisaties bij privacyvraagstukken, AI-governance en de implementatie van wet- en regelgeving zoals de AVG en de AI Act.

Vanuit de dagelijkse praktijk helpt zij organisaties om AI op een verantwoorde en beheersbare manier toe te passen. Zij vertaalt complexe wetgeving naar concrete stappen en praktische handvatten, zodat organisaties niet alleen begrijpen wat er moet gebeuren, maar ook hoe dit in de praktijk kan worden georganiseerd.

Online compliance & privacy

De nieuwste ontwikkelingen en wat dit betekent voor jouw organisatie

In deze kennissessie neemt Jitty van Doodewaard je mee in de meest actuele ontwikkelingen op het gebied van online compliance en privacy. Deze sessie is sterk praktijkgericht en gaat in op nieuwe wet- en regelgeving én toezicht. Zo bereid je je als organisatie goed voor om hier zorgvuldig en toekomstbestendig mee om te gaan.

In deze sessie ontdek je:

- De aankomende Digitale Omnibus en wat dit betekent voor organisaties.
- Het verscherpte toezicht van de Autoriteit Persoonsgegevens op cookies.
- Online tracking en gedragsmodellering (profilering, targeting en retargeting).
- De afhankelijkheid van de online infrastructuur van Amerikaanse aanbieders en wat dit betekent voor internationale doorgifte van persoonsgegevens (VS).
- Hoe een goede en geldige opt-in eruit ziet, mede in het licht van recente handhaving - zoals de CNIL-boete van €3,5 miljoen voor het onrechtmatig delen van loyaliteitsdata voor social media advertising.
- En vooral: wat deze ontwikkelingen concreet betekenen voor organisaties in de praktijk.

Deze sessie is relevant voor iedereen die zich bezighoudt met online communicatie, marketing, fondsenwerving, digitale dienstverlening en datagedreven contact met klanten, leden, donateurs of burgers, zoals:

- (online) Marketeers
- Fondsenwervers en relatiemanagers
- CRM-, database- en dataspecialisten
- Beleidsadviseurs communicatie
- Communicatieadviseurs en voorlichtingsprofessionals
- Webredacteuren, contentspecialisten en digital product owners
- Professionals betrokken bij digitale dienstverlening en burgercommunicatie
- Privacy officers, juristen en compliance professionals

Kortom: voor iedereen die online communiceert met klanten, leden, donateurs én burgers en daarbij zorgvuldig wil omgaan met privacy, toezicht en regelgeving.

Jitty van Doodewaerd
Directeur Privacy
bij DMCC Group

Deze sessie wordt verzorgd door DMCC Group
(sinds 2024 onderdeel van Cuccibu)

Jitty van Doodewaerd is directeur privacy bij de DMCC Group. In deze functie ondersteunt zij opdrachtgevers uit velerlei maatschappelijke sectoren bij privacyvraagstukken.

Jitty was onderdeel van de Big Data expertgroep van het ministerie van Economische Zaken en was verantwoordelijk voor de belangenbehartiging van marketingbrancheverenigingen DDMA. Zij was lid van de Legal Affairs Committee van de Federation for European Direct and Interactive Marketing (FEDMA) en de Privacy Commissie van VNO-NCW.