In gesprek met vertrekkend voorzitter Autoriteit Persoonsgegevens

Privacy moet 'chefsache' worden

Jacob Kohnstamm, (scheidend) voorzitter van de Autoriteit Persoonsgegevens (AP) in Den Haag, spreekt zacht en schuwt de kwinkslag niet. Hij is het vriendelijke gezicht van de waakhond die niet ervoor terugdeinst de tanden te laten zien, mocht dat nodig zijn.

Door Jac. Janssen

Ondanks de naamsverandering – het vroegere College bescherming persoonsgegevens heet sinds kort Autoriteit Persoonsgegevens – is het aspect van bescherming de kern gebleven, legt Kohnstamm uit. Maar omdat het voormalige College vanaf januari de bevoegdheid kreeg boetes op te leggen, veranderde het volgens de wet in een autoriteit. Vanwege pensioenverzekeraar ABP viel deze afkorting af. 'Privacy Autoriteit' werd het evenmin, want privacy is iets anders dan persoonsgegevens.
"De naam 'Autoriteit Persoonsgegevens' leek het niet te halen. Toenmalig staatssecretaris Fred Teeven was tegen, hij zei: ik ben niet voor autoriteit. Dat was mij nooit eerder opgevallen," grapt Kohnstamm. Hij trok Teeven over de streep met een praktisch argument. "De aanstaande verhuizing naar het oude pand van Economische Zaken, waar het CBP gaat samenwonen met het CPB, hielp hem over zijn weerzin tegen het woord autoriteit heen. '

Waarom is deze instantie nodig? Biedt de wet onvoldoende bescherming?
"Meer dan enig ander toezichthouder zijn wij steeds meer nodig. Als u iets koopt en u met geld betaalt, is dat eenmalig en zichtbaar. Koopt u iets tegen betaling met uw persoonsgegevens, dan is het niet altijd zichtbaar wat daarmee gebeurt. Neem bijvoorbeeld de apps op uw telefoon: waarschijnlijk vrijwel gratis, maar u moest er wel persoonsgegevens voor afstaan. En weet u eigenlijk wel zeker of deze gegevens niet ook voor een ander doel worden gebruikt? Het nieuwe geld, voornamelijk de economie rond de smartphone, is zo gecompliceerd dat bijna niemand het kan overzien. Daarvoor is goede wetgeving nodig, maar ook een goede toezichthouder om een crisis rond persoonsgegevens te voorkomen."

Bent u onafhankelijk of valt AP onder Justitie?
"Voor het beheer valt de Autoriteit Persoonsgegevens onder het ministerie van Justitie, maar verder zijn we onafhankelijk. De voorzitter van de AP is bijvoorbeeld even onafhankelijk als een rechter. Wij bestaan bij gratie van Europese regelgeving. De Wet gelijke behandeling en wetten rond de privacy, waarvan de Wet bescherming persoonsgegevens de voornaamste is, volgen uit Europese richtlijnen. Landelijke wetgeving hierover is gelijkgetrokken om te voorkomen dat verschillen concurrentievoordelen tussen de EU-lidstaten veroorzaken."

Wat verstaan we onder 'persoonsgegevens'?
"Het zijn de gegevens op basis waarvan je terecht kan komen bij een individu. Bijvoorbeeld: je burgerservicenummer, het IP-adres van je computer, je telefoonnummer, je MAC-adres (in de netwerk-adapter van je computer of mobiele telefoon) in combinatie met geolocatie. Het makkelijkst zijn je NAW-gegevens: naam, adres, woonplaats. Het gaat om alle gegevens op basis waarvan jij traceerbaar bent. Data over een persoon kunnen bij elkaar opgeteld een profiel vormen waardoor je anders kan worden behandeld door de samenleving. Bijvoorbeeld als je bepaalde informatie niet krijgt aangeboden op basis van je profiel. Als je macht koppelt aan persoonsgegevens, kan dat de vrije ontwikkeling van het individu in de weg staan.

Neem een ziekmelding. Jij moet figuurlijk met de billen bloot; de bedrijfsarts krijgt medische gegevens die niet bij de werkgever terecht mogen komen. De bedrijfsarts mag wel zijn advies doorgeven, bijvoorbeeld een betere bureaustoel, maar niet wat de klachten zijn.Wij hebben bijvoorbeeld een geprivatiseerde arbodienst aangepakt die de werkgever toegang gaf tot een verzuimsysteem waarin allerlei medische gegevens van werknemers waren te zien. Zieke werknemers kunnen daardoor anders worden behandeld dan collega's. Medische gegevens zijn in de zin van de wet bijzondere persoonsgegevens, waarmee helemaal voorzichtig moet worden omgegaan."

Bedrijven leggen graag veel gegevens vast van medewerkers, klanten en leveranciers. Welke regels gelden daarvoor?
"Daarvoor geldt een aantal wettelijke bepalingen. Zorgvuldige omgang met de gegevens is het belangrijkste. Eerst moet je een rechtsgrond hebben om gegevens te verzamelen en te verwerken. Van je werknemers heb je naam, bankrekeningnummer en adres nodig, dat volgt logisch uit het contract. Zo zijn er zes rechtsgronden. Organisaties moeten zich altijd afvragen: heb ik een rechtsgrond? Soms is nadrukkelijke goedkeuring van de individuele werknemer nodig. Deze moet dit expliciet gevraagd krijgen en hij moet zijn toestemming expliciet geven. Dit wordt een probleem bij een ongelijke machtsverhouding, wanneer je bijvoorbeeld niet in redelijkheid 'nee' kunt zeggen. Bureau Jeugdzorg in Noord-Brabant verplichtte bijvoorbeeld al haar medewerkers tot een psychologisch assessment, op straffe van ontslag. Dit voorstel was goedgekeurd door de or, maar ook al geeft de or zijn in-

stemming aan een bepaalde verwerking van gegevens, de toestemming van de individuele medewerker blijft noodzakelijk.
Het individu kan nog steeds bij ons een tip indienen als hij denkt dat er iets niet klopt op privacygebied. Verzuimregistratie, personeelsdossier, salarisinformatie, managementsystemen, prikklokken, dat zijn allemaal voorbeelden van privacyzaken waarbij de or geraadpleegd moet worden. De Wet op de ondernemingsraden(WOR) zegt hier meer over. Er moet altijd een rechtsgrond zijn om zulke maatregelen door te voeren."

Een or heeft op basis van de WOR instemmingsrecht wat betreft bescherming van gegevens van medewerkers en bij voorzieningen gericht op waarneming of controle van medewerkers. Wat zijn daarbij aandachtspunten voor een or?
"Ga bij zulke zaken na: is dit noodzakelijk? Zo ja, kan het ook met minder ingrijpende middelen (ofwel: is het proportioneel)? De Wet bescherming persoonsgegevens doet een beroep op fatsoen: doe het fatsoenlijk en met mate. Verzamel en bewaar gegevens alleen voor de duur die nodig is. En alleen voor het aangegeven doel. Als je dan toch gegevens verzamelt: beveilig ze zo goed mogelijk. Daarop moet de or letten.
Een transportbedrijf installeerde twee camera's in de cabine van vrachtwagenchauffeurs, één naar buiten gericht en één op de chauffeur. Het doel was op zichzelf prima: meer verkeersveiligheid, minder ongelukken. Maar hun middel beoordeelden wij als disproportioneel. Er bestaan namelijk middelen die de privacy van de chauffeur minder schenden. Dat is essentieel: is het gekozen middel noodzakelijk of kan het wat minder wat inbreuk op de privacy betreft."

Kan een ondernemingsraad een zaak bij u onder de aandacht brengen?
"Zeker. Wij krijgen vaak signalen van een or of een vakbond, op grond waarvan wij een zaak kunnen oppakken en in contact treden met de betreffende organisatie. Soms ook met branchevertegenwoordigers om na te gaan of het een wijder verspreid fenomeen is. Als wij uitspraak doen over een zaak, wordt vaak de hele branche wakker. Een voorbeeld. Hotels slaan verplicht de naw-gegevens van hun gasten op. In een politieregio kreeg de politie dagelijks die gegevens van enkele hotels. Dat is onzinnig: het zou alleen moeten gebeuren wanneer de politie met een reden daarom vraagt. Wij hebben één politieregio hierop aangesproken, vervolgens is de werkwijze van de politie op nationaal niveau aangepast."

Jacob Kohnstamm, scheidend voorzitter van de Autoriteit Persoonsgegevens

Wat kan de Autoriteit Persoonsgegevens doen, behalve haar afkeuring uitspreken?
"Wij zijn bevoegd om 'met zwaailichten' bij een organisatie binnen te komen. Deze organisatie móet meewerken. Blijken ze het niet zo nauw te nemen met de wet, dan kunnen wij een last onder dwangsom opleggen als het ongewijzigd blijft. Bij een opzettelijke overtreding of in geval van ernstig verwijtbare nalatigheid kunnen wij een boete opleggen tot 820.000 euro per vergrijp. Vanaf 1 januari 2017 wordt dit fors hoger, namelijk maximaal twintig miljoen euro of 4 procent van de wereldwijde jaaromzet. Verder kunnen we snelle interventies plegen op basis van signalen over organisaties. Negen van de tien overtredingen gebeuren niet doelbewust, maar doordat er niet goed over is nagedacht. Zoals, vermoed ik, ziekenhuizen die hun autorisatie niet goed regelen en iedereen dezelfde inlogcodes geven. Of het VU Medisch Centrum dat toestemming gaf te filmen op de Eerste Hulp. Dit had ik graag beboet, want dat hadden ze best kunnen weten. Bij recidive kunnen we gemakkelijker ingrijpen. Een boete kan een

bedrijf een slechte naam bezorgen of zelfs het eind ervan betekenen. Privacy moet een 'chefsache' worden, waarover op CEO-niveau wordt beslist."

Wat verandert straks met de nieuwe Europese Dataverordening, wat gaat deze betekenen voor ondernemingsraden?

"De nieuwe Europese verordening, die binnen ongeveer twee jaar gaat gelden, werkt anders dan de huidige richtlijn. Een richtlijn krijgt een vertaling in nationale wetgeving, die daardoor per land kan verschillen. Dat is onhandig bij grensoverschrijdende branches en bijvoorbeeld internethandel. Die internationale verschillen vallen straks weg met deze Europese Verordening omdat die directe werking heeft. Voor organisaties in overtreding gaan hogere boetes gelden. Er komt meer verantwoordelijkheid te liggen bij de organisaties zelf; de bewijslast wordt als het ware omgekeerd. Er komt meer aandacht voor ongelijke machtsverhoudingen en de individuele burgers krijgen meer rechten.
De rol van de or verandert waarschijnlijk niet veel. Een belangrijke nieuwigheid is wel dat organisaties verplicht worden een interne privacywaakhond aan te stellen. Deze

Wij hopen op intensieve samenwerking met privacy-officers en or's

kan uitgroeien tot een vraagbaak wat betreft bescherming van persoonsgegevens. Ik zou zeggen: ondernemingsraad, overleg periodiek met deze nieuwe functionaris gegevensbescherming om elkaar te versterken. Jullie hebben een vergelijkbare rechtspositie; beide mogen jullie kritiek leveren op het beleid zonder daarvoor ontslagen te kunnen worden."

Per 1 januari is de Wet meldplicht datalekken van kracht. Wat betekent die voor een or?

"Zodra een organisatie persoonsgegevens van personeel lekt, is dat een zaak voor de ondernemingsraad. Niet bij klantgegevens overigens; alleen indirect, als de continuïteit van de werkgelegenheid erdoor in gevaar komt. De Autoriteit Persoonsgegevens hoopt op een intensieve samenwerking met de nieuwe privacyfunctionarissen en ondernemingsraden. Wij kunnen het niet alleen. Uiteraard kunnen wij besluiten direct in te grijpen bij structurele of ernstige overtredingen waarbij de privacy van veel mensen in het geding is. Ondernemingsraden kunnen, schriftelijk of tijdens ons telefonische spreekuur, dagelijks van 9.30 tot12.30 uur op 0900-2001201, zaken bij ons melden. Dat kan ook in vertrouwelijkheid."