
ERNST-JAN VAN DE PAS | ADVOCAAT IE/ITRECHT DIRKZWAGER

HOGE BOETES LEGGEN URGENTIE BLOOT

# “Een verwerkersovereenkomst moet er gewoon zijn”

Hij bestaat al meer dan 16 jaar, maar nu de Autoriteit Persoonsgegevens forse geldboetes mag opleggen staat hij volop in de schijnwerpers: de bewerkersovereenkomst – binnenkort verwerkersovereenkomst geheten. Elke organisatie die persoonsgegevens door een derde partij laat verwerken, dient zo'n overeenkomst te sluiten. Een al bestaand contract tussen opdrachtgever en leverancier hoeft daartoe niet per se te worden opengebroken. Dat gebeurt vaker dan nodig is, signaleert Ernst-Jan van de Pas, vennoot en advocaat IE/IT-recht van Dirkzwager advocaten & notarissen in Arnhem.

Wat is er aan de hand? In de Wet bescherming persoonsgegevens, de algemene privacywet in Nederland, staat beschreven aan welke regels alle verwerkingen van persoonsgegevens moeten voldoen. Indien een organisatie persoonsgegevens door een derde partij (een bewerker zoals CRM Partners) laat verwerken, dan dient ze over die uitbesteding schriftelijke afspraken te maken in een bewerkersovereenkomst. Ook al staan de gegevens buiten de deur, als uitbestedende partij blijf je verantwoordelijk dat die overeenkomst aan de wettelijke eisen voldoet én voldoende waarborgen biedt, bijvoorbeeld tegen datalekken. Dit is zeker geen sinecure.

**820.000 euro**

Op het ontbreken van een bewerkersovereenkomst of het anderszins schenden van de privacyregels staat een maximale geldboete van 820.000 euro. Opdrachtgevers ervaren dat als een zwaard van Damocles dat boven hun hoofd hangt. En dat gevoel wordt versterkt nu een overtreding van de privacywetgeving als een bestuurdersverantwoordelijkheid wordt gezien. En nog erger, vanaf 25 mei 2018 geldt op ernstige overtredingen een geldboete van maximaal 20 miljoen euro, of 4 procent van de wereldwijde omzet!

**Kous af**

De dreiging van boetes en aansprakelijkheid maakt dat ondernemingen soms onbezonnen acties uithalen. Sommigen plukken in allerijl een willekeurig voorbeeld voor een bewerkersovereenkomst van internet, ondertekenen die voor hun gemoedsrust en hopen dat daarmee de kous af is. Maar ook ziet IT-advocaat Ernst-Jan van de Pas ondernemingen die de situatie aangrijpen om hoofdovereenkomsten open te breken, waarin beide partijen afspraken over risicotoedeling waren overeengekomen om er vervolgens ook de afspraken over de bewerkersovereenkomst in op te nemen. En dat gaat dan weer verder dan noodzakelijk is.

### WAT NU?!

*‘Een datalek, dat ik dat nog eens zou meemaken. Gegevens die op straat liggen. Paniek! Deugde de beveiliging niet? Zijn we mogelijk gehackt? Hoe dan ook: dit is verwijtbaar gedrag. Ik kan dus uitzien naar een boete. En wie krijgt de rekening gepresenteerd: ik als opdrachtgever en eigenaar van de gegevens? Of mijn leverancier die voor passende beveiliging moet zorgen? Maar wat is passend? Dat je patiëntgegevens of financiële gegevens zwaarder moet beveiligen dan de gegevens van de lokale sportvereniging, dat begrijp ik, maar daarmee weet ik nog niet wat te doen.’*

**Firewalls en gelimiteerde datatoegang**
"Het is een mythe dat je bij een datalek altijd een boete krijgt opgelegd. Concreet heb je een meldingsplicht en dien je de Autoriteit Persoonsgegevens binnen 72 uur te informeren via een formulier. Laat je dat na, dan krijg je een waarschuwing. Informeer je dan alsnog niet, dan ontvang je een boete. In de basis moet je met de juiste firewalls je beveiliging op orde hebben. Daarnaast dienen alleen degenen die werken met de data toegang tot die data te hebben. De werkwijze die je hiervoor inricht bij uitbesteding van gegevensverwerking veranker je in een bewerkersovereenkomst. Zo'n contract moet er gewoon zijn, niets meer en niets minder. Het is een evolutie die plaatsvindt, geen revolutie. Al vanaf de Tweede Wereldoorlog is een aantal Europese landen privacy heel belangrijk gaan vinden, waaronder Duitsland, Nederland en Scandinavië. We hebben destijds ervaren wat het doet als persoonsgegevens in de verkeerde handen komen."

## HET IS EEN EVOLUTIE DIE PLAATSVINDT, GEEN REVOLUTIE

**Audit én controle**
"Als uitbestedende partij wil je controle kunnen uitoefenen op de bewerkende partij. Daarvoor dien je de mogelijkheid te hebben om een audit en controle uit te oefenen. Als leverancier is het echter ondoenlijk om voor elke klant een afwijkende bewerkersovereenkomst te sluiten. Dat is niet reëel. Dat je een beveiligingsnorm moet naleven en dat je hierop mag worden gecontroleerd, is logisch. Maar dat dit op elk moment is toegestaan, gaat te ver."
"Stel je een leverancier voor die voor circa 100 klanten werkt, die zou dan per jaar 100 bezoeken tegemoet kunnen zien. Dat zou de organisatie van de leverancier onevenredig zwaar belasten, met alle kosten van dien. Kosten die dan aan de uitbestedende partijen zouden moeten worden doorbelast. Ter voorkoming hiervan kun je best wel realistische afspraken maken. Als leverancier heb je dus wel degelijk wat in te brengen over de inhoud van de bewerkersovereenkomst."

**Pas op 28 mei in 2018 wordt, op grond van Europese regelgeving, bij wet meer concreet vastgelegd wat er in een bewerkersovereenkomst dient te staan. Moeten we tot die tijd lijdzaam toezien?**
Geenszins, benadrukt de IT-advocaat.
"Maak het privacybeleid in je organisatie tot een *Chefsache*, want de risico's van aansprakelijkheid en imagoschade zijn groot. Anticipeer in de nu te sluiten bewerkersovereenkomsten al op die nieuwe regels. En zorg voor bewustwording en beleid in je eigen organisatie, zodat werknemers weten hoe ze met persoonsgegevens dienen om te gaan, wat je wel en wat je er niet mee mag doen. Juist in deze tijd waarin we het heel normaal vinden van alles voor iedereen zichtbaar op internet te plaatsen. Daar staat lijnrecht tegenover dat we het schandalig vinden indien allerlei overheden en bedrijven iets met onze eigen persoonsgegevens doen. Zie hier de paradox in ons denken en handelen."

**Reële overeenkomst**
"Als adviseur staan we een reële overeenkomst voor, waarin je de wettelijke verplichte afspraken vastlegt over het deugdelijk beveiligen en geheimhouden van de gegevens en de omgang met datalekken. Daarnaast is het verstandig afspraken te maken over zaken als de teruggave van de gegevens bij het einde van de overeenkomst en over het al dan niet mogen betrekken van derde partijen bij de dienstverlening. Het doel van een bewerkersovereenkomst is dat je als opdrachtgever in controle blijft over de persoonsgegevens waarvoor je verantwoordelijk bent. We zien dan ook liefst een model waarbij je als uitbestedende partij zelf verantwoordelijkheid draagt en niet alles bij de leverancier neerlegt. Bovendien kun je bepaalde risico's ook verzekeren."

**Een gewaarschuwd mens...**
De Wet bescherming persoonsgegevens (Wbp) geeft aan dat een persoonsgegeven elk gegeven is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is.
Iemands naam, adres en woonplaats zijn voor de hand liggende persoonsgegevens. Maar we onderscheiden er nog veel meer: een telefoon- of huisnummer, een postcode, een autokenteken, vaste en dynamische IP-adressen, een slimme koelkast....achter elk apparaat dat met moderne IT-technologie is uitgerust zit een individu met persoonsgegevens. En ook die hebben dus de aandacht van de Autoriteit Persoonsgegevens. Een gewaarschuwd mens telt voor twee.

### EEN GESCHIL AFWACHTEN?

*Eerder een jurist met de juiste expertise bij de zaken betrekken, kan veel problemen en hoge kosten voorkomen. Laat vooraf checken of de overeenkomst tussen partijen wel voldoende specifiek en meetbaar is. Want als een afspraak niet duidelijk is, kan het erg lastig zijn om later aan te tonen dat de wederpartij die afspraak heeft geschonden. Steeds meer organisaties wachten niet totdat een geschil hen noodzaakt een advocaat in te schakelen. Ze kiezen een strategisch partnership met een advocaat, immers: voorkomen is beter dan genezen. Zo heeft CRM Partners in Dirkzwager een partner gevonden in juridische dienstverlening. Vanwege zijn IT-achtergrond is Ernst-Jan van de Pas het eerste aanspreekpunt voor uiteenlopende zaken, variërend van IT-contracten, privacykwesties en intellectueel eigendom tot internationaal zakendoen.*