ANJA DEKHUIJZEN is advocaat en partner bij Whitebridge Advocatuur. Zij is gespecialiseerd in IT, Sourcing en GDPR, en jurylid van de Sourcing Awards.

ICT-INDUSTRIE INTRODUCEERT GEDRAGSCODE GDPR

GOED INITIATIEF MET ADDER ONDER HET GRAS

NLDigital, voorheen ICT Nederland (en voor de *diehards* onder u: voorheen de FENIT) heeft als een van de eerste in Nederland een gedragscode opgesteld, die naar verwachting binnenkort zal worden uitgerold in Nederland. De GDPR geeft brancheorganisaties de mogelijkheid om dergelijke gedragscodes in te voeren. Daartoe dient een traject te worden afgelegd waarbij de Autoriteit Persoonsgegevens goedkeuring geeft aan de tekst. De beoogde gedragscode heeft als fraaie naam Data Pro Code.

Wat heeft de markt hieraan? Op zichzelf is dit initiatief van IT-leveranciers toe te juichen. De GDPR vereist het nodige van bedrijven en andere organisaties wanneer men persoonsgegevens verwerkt. Wanneer u vervolgens deze verwerking uitbesteedt aan een IT-leverancier is dit uw zogeheten verwerker. De Data Pro Code beoogt dat verwerkers inzichtelijk moeten maken waaraan zij zich houden, met name op beveiligingsgebied. Doel is dat u met een gerust hart kunt kiezen voor een IT-leverancier die aldus is geaccrediteerd.

Maar is dit werkelijk het geval? Wanneer een aangesloten IT-leverancier zich niet aan de code houdt, staat deze onder toezicht van de zogeheten Data Pro Toezichthouder en kan deze in het ergste geval de accreditering verliezen. Bovendien komt een code tot stand na overleg met en goedkeuring door de Autoriteit Persoonsgegevens. Dit wekt de indruk dat de code een zekere standing heeft. Inderdaad zeggen de recent in juni verschenen Guidelines on code of conduct van de EDPB (de verzameling van alle Europese toezichthouders op privacygebied) dat ingeval van een inbreuk op de GDPR er wellicht minder reden is voor het opleggen van een boete wanneer er sprake is van een goedgekeurde code: "In case of a breach of one of the provisions of the Regulation (GDPR, AED), adherence to an approved code of conduct might be indicative of how comprehensive the need is to intervene with an effective, proportionate, dissuasive administrative fine or other corrective measure from the supervisory authority."

Er zit echter een adder onder het gras. De Guidelines van de EDPB zien uitsluitend toe op de wijze van accreditering en de inhoud van de code zelf. De Data Pro Code gaat een aanzienlijke stap verder. De code omvat volgens de website van NLDigital tevens een zogeheten "neutrale" verwerkersovereenkomst in de vorm van standaardclausules, om tegenwicht te bieden aan de contracten die controllers opleggen aan de verwerkers. Echter, zo neutraal zijn de standaardclausules niet. De standaardclausules verraden wel degelijk de maker. Zo staat er vermeld dat de verwerker er slechts naar hoeft te "streven" dat de beveiliging passend is. De verwerker staat er bovendien niet voor in dat de beveiligingsmaatregelen doeltreffend zijn onder alle omstandigheden.

Concluderend kan men vaststellen dat het goed is dat brancheorganisaties codes introduceren voor haar leden, zodat deze beveiligingsmaatregelen nemen. Echter, de onderhavige code schiet haar doel voorbij. Belangrijk voor u is dat de code op vrijwillige basis door IT-leveranciers zal worden gehanteerd. Het staat u vrij om het gedeelte betreffende de verwerkersovereenkomst in de code te vervangen door afspraken die recht doen aan uw beider belangen. ✖