ICT verdient AVG kwaliteitskeurmerk

EIPACC helpt passende technische AVG maatregelen aantonen

ICT-maatregelen zijn wel of niet passend in de zin van de Algemene Verordening Gegevensbescherming (AVG). EIPACC bevordert heldere, transparante en onderbouwde uitspraken over het wel of niet voldoen van technische (ICT-) maatregelen aan AVG vereisten van compliance en accountability.

Jonkheer Victor Alting van Geusau (links) is Vice-President EIPACC en Lid RvT Nederlands Privacy Klachten Instituut (NPKI)

Romeo Kadir is President EIPACC en Member International Board of Experts EuroPrivacy Certification (Luxembourg)

Alle CFO'S, CIO'S, DPO'S (FG'S), juristen, compliance officers en AVG (implementatie) projectleiders, Raden van Toezicht, Raden van Advies en andere rollen en functies in het kader van de AVG verdienen professionele ondersteuning en begeleiding bij verantwoorde certificeringsprocessen om afdoende garanties te bieden en passende maatregelen te treffen zoals vereist in de AVG. Dat is de overtuiging op basis waarvan het in Utrecht gevestigde European Institute for Privacy, Audit, Compliance & Certification (EIPACC) bedrijven en organisaties ondersteunt en begeleidt naar Nederlandse en Europese Privacy Keurmerken.

Garanties

De verwerker is verplicht om afdoende garanties 'met betrekking tot het toepassen van passende technische en organisatorische maatregelen' te bieden aan de verwerkingsverantwoordelijke. Sterker nog, volgens artikel 28 lid 1 van de AVG mag de verwerkingsverantwoordelijke uitsluitend met een verwerker zaken doen die 'afdoende garanties' biedt, oftewel 'comply or die'. Nadat de drempel is genomen, volgen over en weer nog zorgplichten waarvan de niet-naleving is gesanctioneerd. Met het niet-naleven van deze verplichtingen riskeert de organisatie een administratieve geldboete van € 10 miljoen of voor een onderneming tot 2 procent van de totale wereldwijde jaaromzet in het voorgaande boekjaar.

Meer dan alleen 'aantonen'

AVG accountability gaat in zekere zin verder dan alleen maar kunnen 'aantonen', het houdt onder andere ook in dat moet kunnen worden beargumenteerd ('demonstrated') waarom men heeft gekozen voor een bepaalde ict-maatregel of specifiek beveiligingsniveau of beveiligingsaanpak, aldus Romeo Kadir, President van EIPACC en Member/Liaison of the International Board of Experts van het eerste Europese AVG certificeringsschema van EuroPrivacy (Luxembourg) en Lid Raad van Experts van het Nederlands Privacy Keurmerk (NPK).

Passendheid

Alhoewel ICT van onmisbare waarde is voor het realiseren van compliance, accountability en effectuering van rechten van betrokkenen, wordt het als zodanig wel vaker aangeduid als 'waardenloos'. De koppeling van technische maatregelen naar beginselen inzake verwerking van persoonsgegevens wordt (beboetbaar) door de AVG gecodificeerd in art. 32 AVG via de bandbreedte van de 'passendheid' in het kader waarvoor de beginselen van verwerkingen in art. 5 AVG het startpunt zijn. Dit betekent bij het bepalen van de vraag of de ICT maatregelen 'passend' zijn in de zin van bijvoorbeeld art. 24 en/of 32 AVG moet kunnen worden aangetoond hoe wordt voldaan aan de beginselen van verwerking van persoonsgegevens, ook wel privacy fatsoensnormen genoemd. Voor een concrete benadering van hoe dit kan worden vormgegeven, zie EIPACC Whitepaper 'AVG Beginselen, PLASTICFAD', kosteloos te raadplegen op **www.eipacc.eu.**

Keurmerken

Zowel als 'te treffen organisatorische maatregel' als ter invulling van de AVG in het algemeen en de verplichting van 'privacy by design' in het bijzonder is het betrekken van voldoende kennis, expertise en praktijkervaring in een zo vroeg mogelijk stadium 'passend.' Senior expertise is in het bijzonder van belang om aan heldere, goed onderbouwde AVG logica gerelateerde aspecten te voldoen. Deze reiken verder dan slechts het voldoen aan bepaalde processen, zoals sommige (branche-) gedragscodes betogen. Uiteraard is een goede procesinrichting van belang als 'tussenstation in de reis naar AVG compliance en accountability'. Gedegen praktijkkennis en ervaring is daarbij noodzakelijk.
Diverse keurmerken, certificaten en zelfs sommige branchegedragscodes annex branchekeurmerken zijn opgezet op basis van een structuur die (ondanks alle goede bedoelingen) niet op alle onderdelen even goed lijken te voldoen aan de tekst, ratio en geest van verplichtingen uit hoofde van de AVG.

Een AVG Certificaat heeft weliswaar grote praktische waarde bij het aantonen van AVG compliance richting stakeholders, tegelijkertijd moet de relatieve waarde in een juist perspectief worden geplaatst, waarschuwt EIPACC. Conform de AVG doet een AVG keurmerk niet af aan de AVG verantwoordelijkheid van de verwerkingsverantwoordelijke zelf.

Klachtbehandeling

ICT-maatregelen spelen niet alleen in het kader van datalekken een rol. Zo kan de betrokkene ingeval van het verwerken van persoonsgegevens voor geautomatiseerde besluitvorming ook gebruikmaken van het recht op nuttige informatie over de onderliggende logica en in dat kader een klacht indienen bij de Autoriteit Persoonsgegevens. Onder andere ter garandering van een professionele en objectieve behandeling van dergelijke klachten kan een organisatie – op basis van bijvoorbeeld algemene voorwaarden of verwerkersovereenkomsten – ervoor opteren om te voorzien in een 'extra rechtsgremium' door de klacht extern te laten behandelen door bijvoorbeeld het Nederlands Privacy Klachten Instituut (NPKI). Het NPKI streeft primair een minnelijke oplossing na waarbij 'de angel uit de klacht' wordt gehaald. Het voordeel hiervan is dat de formele klachtbehandelingsroute van de AP wellicht niet noodzakelijk blijkt. Uiteraard heeft de betrokkene te allen tijde het recht een formele klacht bij de AP in te dienen. Voor nadere informatie, zie **www.npki.nl.**

Generieke normen

Ter vermindering van de kans op hoge boeten en in verband met ketenaansprakelijkheid beginnen sommige goedwillende organisaties 'geblinddoekt' aan hun vaak kostbare reis naar AVG certificering ('certification urgency'). Het voldoen aan generieke normen zoals bijvoorbeeld ISO, NEN, ISAE en generieke branchegedragscodes betekent echter niet noodzakelijkerwijs dat wordt voldaan aan alle relevante verplichtingen uit hoofde van de AVG (ondanks 'GDPR mapping'). In een enkel geval verwijzen privacytoezichthouders naar dergelijke normen met als aanbeveling zich daar te beraden (op procesniveau) bij gebreke aan een specifieke AVG systematiek. Uiteindelijk moeten generieke normen worden ingevuld met specifieke AVG tekst, ratio en geest van relevante AVG verplichtingen. Branchegedragscodes zijn ex art. 40 AVG idealiter goedgekeurd door de Autoriteit Persoonsgegevens (AP). EIPACC zorgt hierbij voor begeleiding en ondersteuning.

Expert Key Note

Op 27 november 2018 verzorgt EIPACC een Expert Key Note over de meest actuele ontwikkelingen op het gebied van AVG keurmerken in Nederland (Mediaplaza Utrecht). Diverse certificeringsschema's worden besproken alsook het belang van interne AVG audits, rol van beleidsbepalers en de DPO (FG). Aanmelden is mogelijk via events@eipacc.eu.

Sparren met EIPACC

De senior privacy experts van EIPACC houden zich onder meer bezig met diverse kwaliteitsvraagstukken op het gebied privacy en dataprotectie. Zij delen hun kennis, expertise en praktijkervaring in diverse toezichts- en adviesgremia van bedrijven en organisaties. Indien nodig overleggen zij met de Autoriteit Persoonsgegevens (AP). Als ervaren senior certificeringsauditors zijn zij betrokken bij AVG certificaten voor diverse keurmerken zoals het Nederlands Privacy Keurmerk (NPK) en EuroPrivacy (Luxembourg). Misschien wilt u uw AVG inspanningen samen met EIPACC als gewaardeerde sparring partner tegen het licht houden. Desgewenst ondersteunt en begeleidt EIPACC u naar de volgende stap richting AVG-certificering.

Laat u vrijblijvend informeren.
Aandacht geeft daadkracht.
contact@eipacc.eu
www.privacyseals.eu

EIPACC