AVG-Certificering

14 december 2018

Ed Ridderbeekx

Nu de storm rond de invoering van de Algemene Verordening Gegevensbescherming (AVG) na 25 mei wat is gaan liggen, richten organisaties zich logischerwijs op de borging van alle inspanningen die ze hebben gedaan om aan de nieuwe privacywetgeving te voldoen. Daarbij komt automatisch de vraag naar voren: hoe laten we zien dat we aantoonbaar 'in control' zijn?

Uiteraard wordt die aantoonbaarheid verbeterd door de maatregelen die een organisatie voor de AVG heeft genomen; denk aan het aanleggen van een verwerkingsregister, het opstellen van een privacystatement, en gedocumenteerde procedures om te voldoen aan de rechten van betrokkenen. Maar verwerkingsverantwoordelijken en verwerkers hebben daarnaast vaak behoefte aan een onafhankelijk oordeel over de beheersing van privacy. De vraag om zo'n audit of certificering die al dan niet leidt tot een keurmerk, wordt versterkt doordat de AVG zelf (de ontwikkeling van) certificeringsmechanismes aanmoedigt als middel om compliance met de wet aan te tonen. Dat doet ze met name in artikel 42. In artikel 43 AVG ('Certificeringsorganen') wordt ingegaan op de rolverdeling bij certificering.

Organisaties kijken naar deze artikelen uit de AVG en vragen zich af: hoe staat het daar nu mee? Aanbieders kijken naar dezelfde passages en aarzelen kennelijk soms niet om hun klanten een AVG-certificering of -keurmerk aan te bieden; de Autoriteit Persoonsgegevens (AP) heeft al gewaarschuwd voor 'misleidende AVG keurmerken'. Hieronder zetten we een aantal zaken op een rijtje.

EDPB conceptrichtlijnen

In de artikelen 42 en 43 spreekt de AVG slechts in algemene zin over certificering als ondersteuning bij aantoonbaarheid. In dat verband is het interessant een blik te werpen op de conceptrichtlijnen die de European Data Protection Board (EDPB, de opvolger van de Article 29 Working Party) heeft uitgebracht over certificering. Dit lezenswaardige document gaat onder andere in op:

- certificering als middel voor accountability/aantoonbaarheid;
- scope en betekenis van certificering in de betekenis van de AVG;
- de rol van toezichthouders bij certificering;
- te stellen eisen aan het certificeringsproces en in het bijzonder de certificatiecriteria.

De richtlijnen definiëren certificering als volgt:
'In the context of certification under Articles 42 and 43 of the GDPR, certification shall refer to third party attestation related to processing operations by controllers and processors.'

Voor wat betreft de betekenis van 'attestation' sluiten de richtlijnen aan bij de definitie van ISO:
'Attestation is an "issue of a statement", based on a decision following review, that fulfilment of specific requirements has been demonstrated.' (section 5.2, ISO 17000:2004)

Kortom: de richtlijnen van de EDPB sluiten aan bij de gebruikelijke opvatting over (de definitie van) certificering.

Rollen en verantwoordelijkheden

De richtlijnen noemen ook de traditionele rolverdeling bij certificering. Een certificerende instelling (CI) toetst organisaties op het naleven van een set beoordelingscriteria en verstrekt certificaten. De CI op haar beurt moet worden geaccrediteerd door een accreditatieinstelling, waarbij wordt vastgesteld of de CI over de noodzakelijke kwaliteit beschikt om te toetsen en certificaten uit te geven. Interessant is dat de richtlijnen verschillende mogelijkheden openlaten om die rolverdeling in te vullen. Dit raakt ook direct aan de rol van de toezichthouder:

- De toezichthouder kan CI zijn, waarbij hij de mogelijkheid heeft delen van het beoordelingsproces aan derde partijen uit te besteden.
- De toezichthouder kan partijen aanwijzen als CI.
- De toezichthouder kan het ontwikkelen en uitvoeren van certificeringsmechanismen overlaten aan de markt.

Wel geldt dat de toezichthouder op grond van de AVG te allen tijde de certificeringscriteria zal moeten goedkeuren en de EDPB hiervan op de hoogte dient te stellen. In de afsluitende paragraaf van dit artikel wordt ingegaan op de huidige Nederlandse situatie.

Criteria

Certificeringscriteria zijn het hart van ieder certificeringsschema. Ze zijn immers de norm waaraan wordt getoetst. De richtlijnen van de EDPB noemen op verschillende plaatsen een aantal eisen waaraan die criteria moeten voldoen, willen ze in aanmerking komen voor AVG-certificering. Hieronder hebben we de voornaamste eisen opgesomd:

De volgende compliance-aspecten moeten in de criteria worden betrokken:

- rechtmatigheid van de verwerking;
- de principes van verwerking van persoonsgegevens (artikel 5 AVG);
- de rechten van betrokkenen;
- de meldplicht van datalekken;
- Privacy by Design en Privacy by Default;
- DPIA's;
- technische en organisatorische maatregelen op basis van artikel 32 AVG.

Criteria dienen:

- uniform en verifieerbaar te zijn;
- auditeerbaar te zijn;
- relevant te zijn in relatie tot het beoogde publiek;
- rekening te houden en aan te sluiten met andere standaarden;
- flexibel en schaalbaar te zijn zodat certificering op verschillende typen organisaties toepasbaar is.

Andere belangrijke aspecten die in de richtlijnen worden genoemd hebben betrekking op de scope en het object van de certificering. De scope wordt beperkt tot *processing operation or set(s) of operations* van persoonsgegevens (kort gezegd: verwerkingen van persoonsgegevens). Een 'processing operation' bestaat volgens de richtlijnen uit technische systemen, processen en procedures. Hiermee wordt certificering van personen (bijvoorbeeld Functionarissen Gegevensbescherming) uitgesloten. Als object ('target of evaluation, ToE') benadrukken de richtlijnen het belang van een (zeer) precieze omschrijving: 'At any instance, a reliable, meaningful assessment of conformity can take place only if the individual object of a certification project is described precisely. It must be described clearly which processing operations are included in the object of certification and then the core components, i.e. which data, processes and technical infrastructure, will be assessed and which will not.'

Stand van zaken

In de Nederlandse situatie zien we dat de AP kiest voor een model waarbij de ontwikkeling van certificeringsschema's en criteria aan de markt wordt overgelaten. Voor accreditatie verwijst zij potentiële CI's expliciet naar de Raad voor Accreditatie (RvA) (hierbij gelden richtlijnen die de EDPB recent heeft goedgekeurd). Organisaties die geïnteresseerd zijn in het verwerven van een certificaat, wordt aanbevolen contact op te nemen met geaccrediteerde CI's. Maar de AP wijst er op haar website ook meteen op dat er op dit moment nog geen geaccrediteerde CI's zijn. Pas als accreditatie door de RvA én goedkeuring van de certificeringscriteria door de AP hebben plaatsgevonden, is certificering in de betekenis van de AVG dus mogelijk. Althans, zo lijkt het.

Het is in dit verband interessant te kijken naar de ontwikkelingen in een ander land dat te maken heeft met de GDPR/AVG: Luxemburg. Daar kiest de lokale toezichthouder (Commission Nationale pour la Protection des Données, CNPD) voor een geheel ander model. Samen met marktpartijen ontwikkelt de CNPD een certificeringsmechanisme waarvan zij zelf de schemabeheerder wordt én waarvoor zij zelf CI's accrediteert. De beoogde CI's zijn 'independent professional audit firms' en een certificaat kan alleen worden afgegeven op basis van een assurancerapport conform ISAE 3000. De criteria die bij de beoordeling dienen te worden gehanteerd zijn de 'GDPR-certified assurance report based processing activities' (GDPR-CARPA). Het is niet ondenkbaar dat internationale auditorganisaties, op basis van een accreditatie door de Luxemburgse toezichthouder, te zijner tijd ook in Nederland CARPA-certificaten zullen afgeven. In dat geval lijkt het moeilijk vol te houden dat een dergelijk certificaat niet past in de eisen die artikel 42 en 43 van de AVG worden gesteld.

In april 2018 heeft de NOREA het Privacy Control Framework (PCF) gepubliceerd. Het PCF is een normatief raamwerk dat bedoeld is om auditors te ondersteunen bij het uitvoeren van privacy audits in de context van de AVG. Het PCF kan worden gebruikt als verzameling criteria (bestaande uit beheersdoelstellingen en -maatregelen) bij een op Richtlijn 3000 gebaseerde assurance-opdracht. Daarnaast voert de NOREA een privacykeurmerk onder de naam Privacy Audit Proof. Dit mag door organisaties worden gevoerd na een toetsing van een bevoegde privacy-auditor op basis van Richtlijn 3000 en het door de NOREA opgestelde PCF. Een assurancerapport op basis van het PCF (eventueel aangevuld met een Privacy Audit Proof keurmerk) kan een heel belangrijke rol spelen in de aantoonbaarheid van compliance met de privacywetgeving. Strikt genomen echter geldt het niet als AVG-certificering in enge zin, aangezien de criteria uit het PCF formeel (nog) niet zijn goedgekeurd door de AP (hetgeen de AVG wel vereist). Op dit moment overlegt de NOREA met de AP hierover. Het PCF voldoet in ieder geval aan alle eisen die de richtlijnen van de EDPB, zoals hierboven genoemd, aan de certificeringscriteria stellen. Het is nu aan de AP om dit te bevestigen en daarmee duidelijkheid aan de markt te geven.

E. (Ed) Ridderbeekx | Zelfstandig IT-auditor en privacy professional

Ed Ridderbeekx is zelfstandig IT-auditor en privacy professional. Hij is een van de samenstellers van het Privacy Control Framework en lid van de Kennisgroep Privacy van de NOREA.