De woningcorporatie en de DPO / FG

Een noodzakelijk huwelijk of 'good practice'?

Sinds de introductie van de definitieve versie van de Algemene Verordening Gegevensbescherming (AVG) in april 2016 heeft de private en (semi-)publieke sector de tijd gehad om alle vereisten uit de AVG zorgvuldig te implementeren. Eén van de nieuwe vereisten van de AVG, is het onder specifieke omstandigheden verplicht of als 'good practice' aanstellen van een *Data Protection Officer* (DPO), in het Nederlands: een Functionaris Gegevensbescherming (FG).

Vanaf 25 mei 2018 wordt de AVG ook daadwerkelijk gehandhaafd door de Autoriteit Persoonsgegevens. In de overheidssector is de Autoriteit Persoonsgegevens afgelopen week al gestart met aanschrijven van overheden die nog geen FG hebben aangemeld.[1] De komende maanden zal zij ook in de private sector dergelijke controles gaan uitvoeren. Geen tijd te verliezen dus voor woningcorporaties die nog geen FG hebben aangesteld. Woningcorporaties blijken zich opmerkelijk genoeg in de praktijk echter lang niet altijd doordrongen van deze mogelijke verplichting.

Artikel 37 AVG

Een organisatie is op grond van artikel 37 lid 1 AVG verplicht om een FG aan te stellen, wanneer:

a) het een (semi)-publieke organisatie betreft,

b) de kernactiviteiten bestaan uit het op grote schaal monitoren van betrokkenen, of wanneer

c) zij op grond van haar kernactiviteiten op grote schaal bijzondere persoonsgegevens van betrokkenen verwerkt.

Deze voorwaarden zijn niet cumulatief. Op basis van deze voorwaarden is het direct duidelijk dat bijvoorbeeld gemeenten, verzekeraars en banken een DPO nodig hebben. In hoeverre zijn deze voorwaarden dan van toepassing op woningcorporaties?

Woningcorporaties

Op grond van bovengenoemde bepaling uit de AVG lijken de meeste woningcorporaties in beginsel niet onder de verplichting uit te kunnen komen om een FG aan te stellen. Dit verplicht aanstellen van een FG kan evenwel om begrijpelijke redenen niet altijd op evenveel sympathie rekenen. In januari 2014 heeft Aedes, de Vereniging van Woningcorporaties, zich uitgelaten over het toen voorliggende tekstvoorstel van de AVG en de gevolgen daarvan voor sociale verhuurders. Aedes was van mening dat van de verordening een risico-benadering zou uitgaan en men niet iedereen over één kam zou moeten scheren. Over de FG werd gesteld:

> *"Het concept voor de Europese Verordening zou onder bepaalde omstandigheden ook de aanstelling van een zogeheten Privacy Officer verplichten. Ook deze bepaling brengt de nodige extra kosten met zich mee. Dit terwijl organisaties ook op andere terreinen aan wetgeving moeten voldoen zonder dat er voorgeschreven medewerkers aangesteld moeten worden. Maatregelen die intern moeten worden*

[1] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-gestart-met-controles-functionarissen-voor-gegevensbescherming

genomen behoren niet afhankelijk te zijn van de omvang van de onderneming of de verweking van de persoonsgegevens, maar moeten beoordeeld worden op grond van de mogelijke risico's en activiteiten.''[2]

Vervolgens wordt door Aedes opgemerkt:

''3) Het instellen van een Data Protection Officer zorgt voor teveel administratieve lasten, met name voor het MKB. Ook hier moet een meer gedifferentieerde risicobenadering worden toegepast.''[3]

Deze opvatting wordt door Aedes nogmaals herhaald in de door hen ontwikkelde Handreiking Gegevensbescherming uit 2016:

"Woningcorporaties lijken niet te vallen onder een van deze organisaties en zijn daarom ook met ingang van de AVG niet verplicht om een FG aan te stellen. De AP kan echter vaststellen dat voor corporaties een FG verplicht is."[4]

Even verderop in het document wordt wel opgemerkt:

''Hoewel de AVG een FG niet verplicht stelt, kan het inzetten van een FG wel degelijk nuttig zijn om privacy compliant te blijven.'' [5]

Aedes lijkt er aldus ons inziens een (te) enge lezing van de AVG op na te houden. Het argument dat een FG administratieve lasten en kosten met zich meebrengt weegt naar onze mening niet op tegen de 'good practice' die van de aanstelling van een FG uitgaat. In onze visie is het aanstellen van een FG door een woningcorporatie, zowel als 'good practice' als op grond van de AVG, in beginsel onontkoombaar. Dat blijkt uit het navolgende:

Semi-publieke sector

Ad a) een (semi)-publieke organisatie

Omdat de AVG geen absolute definitie van een '(semi)-publieke organisatie' bevat, dient er gekeken te worden naar andere gezaghebbende documenten. Eén van de belangrijkste bronnen zijn de zogeheten *Guidelines on Data Protection Officers* van de 'Werkgroep 29'.

> De Werkgroep 29 (per 25 mei 2018 vervangen door de European Data Protection Board (EDPB)) is hét onafhankelijke en gezaghebbende privacyadviesorgaan bestaande uit vertegenwoordigers van de Europese privacytoezichthouders, de Europees Toezichthouder voor gegevensbescherming en de Europese Commissie. Haar doelstellingen zijn het adviseren van de Lidstaten op het gebied van gegevensbescherming, het aanmoedigen van uniforme interpretatie van de AVG, het adviseren van de Europese Commissie en om aanbevelingen te publiceren met betrekking tot het verwerken van persoonsgegevens en privacy in de Europese Unie. De Werkgroep 29 bood ter uitvoering van haar doelstellingen *Guidelines* aan, dit zijn handvatten voor het interpreteren van de rechten en plichten uit de AVG. Het gezag in de juridische gemeenschap ten aanzien van deze *Guidelines* is groot en deze worden dan ook door de rechterlijke macht gebruikt als bron van wetsuitleg en invulling. Een deel van de *Guidelines* van de Werkgroep 29 is door de EDPB bekrachtigd en daardoor nog steeds actueel en relevant voor de praktijk.

---

[2] Aedes, Voorstellen EU Privacy Verordening bezien door woningcorporaties, januari 2014, p. 1: https://www.bof.nl/static/lobby-tomie-documenten/VENJ/20140100-022-vereniging-woningcorporaties.pdf
[3] Aedes, Voorstellen EU Privacy Verordening bezien door woningcorporaties, januari 2014, p. 2: https://www.bof.nl/static/lobby-tomie-documenten/VENJ/20140100-022-vereniging-woningcorporaties.pdf
[4] Aedes, Handreiking Gegevensbescherming, december 2016, p. 24: https://dkvwg750av2j6.cloudfront.net/m/5e173f7b37f5a6a8/original/20161103-Handboek-GegevensbeschermingV-6.pdf
[5] Aedes, Handreiking Gegevensbescherming, december 2016, p. 25: https://dkvwg750av2j6.cloudfront.net/m/5e173f7b37f5a6a8/original/20161103-Handboek-GegevensbeschermingV-6.pdf

In de *Guidelines on Data Protection Officers* van de Werkgroep 29, die bovendien door de EDPB zijn bekrachtigd, staat een aantal handvatten beschreven om te beoordelen of een woningcorporatie aangemerkt kan worden als (semi-)publiek, waardoor een woningcorporatie alleen al op basis van deze grondslag automatisch verplicht is tot het aanstellen van een FG:

> *"A public task may be carried out, and public authority may be exercised not only by public authorities or bodies but also by other natural or legal persons governed by public or private law, in sectors such as, according to national regulation of each Member State, public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing or disciplinary bodies for regulated professions.''*[6]

Uit deze niet-limitatieve opsomming blijkt dat privaatrechtelijke rechtspersonen die een maatschappelijke doelstelling behartigen, waaronder het faciliteren van sociale woningbouw kunnen worden gelijkgesteld met een (semi-)publieke organisatie. Woningcorporaties hebben op grond van de Woningwet 2015 de wettelijke taak om onder meer sociale woningbouw te faciliteren, te verhuren en te beheren. Aedes zegt hierover bijvoorbeeld:

> *"Woningcorporaties zorgen dat ruim 2,4 miljoen huishoudens in Nederland goed kunnen wonen en dragen bij aan leefbare buurten, wijken en regio's. (…) Wij maken ons sterk voor optimale omstandigheden waaronder zij als maatschappelijke ondernemingen hun werk kunnen doen."*[7]

De Werkgroep 29 merkt vervolgens over deze privaatrechtelijke rechtspersonen die een maatschappelijke doelstelling behartigen op:

> *''In these cases, data subjects may be in a very similar situation to when their data are processed by a public authority or body. In particular, data can be processed for similar purposes and individuals often have similarly little or no choice over whether and how their data will be processed and may thus require the additional protection that the designation of a DPO can bring.*
>
> *Even though there is no obligation in such cases, the WP 29 recommends, as good practice, that private organisations carrying out public tasks or exercising public authority designate a DPO (..).''*[8]

Hoewel strikt genomen dus niet verplicht, zal een woningcorporatie op grond van deze Guidelines van de Werkgroep 29 worden gelijkgesteld met een semi-publiekrechtelijke organisatie zoals bedoeld in de AVG, waardoor zij als 'good practice' toch (!) een FG dient aan te stellen.

Ad c) als kernactiviteit bijzondere persoonsgegevens verwerken

Het behoeft geen discussie dat woningcorporaties een scala aan persoonsgegevens van hun huurders verwerken. Dit betreffen zowel 'gewone persoonsgegevens', 'bijzondere persoonsgegevens' als 'gevoelige persoonsgegevens'. Gewone persoonsgegevens zijn bijvoorbeeld NAW-gegevens, telefoonnummers en e-mailadressen. Bijzondere persoonsgegevens zijn persoonsgegevens van (zeer) gevoelige aard. Voorbeelden van bijzondere persoonsgegevens die (veelal) verwerkt worden door woningcorporaties zijn medische gegevens met betrekking tot het aanbrengen van medisch noodzakelijke voorzieningen aan de woning, vluchtelingen status. Een ietwat ongewisse status hierin

---

[6] Guidelines on Data Protection Officers ('DPOs'), 13 december 2016, p. 6.
http://ec.europa.eu/newsroom/document.cfm?doc_id=43823

[7] Aedes, Voorstellen EU Privacy Verordening bezien door woningcorporaties, januari 2014, p. 2:
https://www.bof.nl/static/lobby-tomie-documenten/VENJ/20140100-022-vereniging-woningcorporaties.pdf

[8] Guidelines on Data Protection Officers ('DPOs'), 13 december 2016, p. 6.
http://ec.europa.eu/newsroom/document.cfm?doc_id=43823

heeft het BSN dat formeel niet langer tot deze categorie behoort maar nog altijd enkel op basis van een wettelijke grondslag mag worden verwerkt. BSN-nummers (bijvoorbeeld op salarisspecificaties) of een kopie van het paspoort of de identiteitskaart van de huurder worden ook vaak op grote schaal verwerkt. Daarnaast worden grote hoeveelheden gevoelige persoonsgegevens verwerkt. Gevoelige persoonsgegevens, zoals bankrekeningnummers, huurtoeslag- en belastinggegevens en gegevens over eventuele betalingsachterstanden, zijn geen aparte categorie persoonsgegevens. Toch moeten deze gevoelige gegevens gelijk worden behandeld als bijzondere persoonsgegevens. In de *Guidelines on Personal data breach notification* van Werkgroep 29 worden de criteria wanneer een datalek gemeld moet worden uitgewerkt. Wanneer bijzondere persoonsgegevens, zoals medische gegevens, onderdeel zijn van een datalek, moet een dergelijk datalek altijd gemeld worden aan de nationale toezichthouder, in Nederland de Autoriteit Persoonsgegevens. Financiële gegevens zijn (zeer) gevoelig van aard en zeker in combinatie met andere (bijzondere) persoonsgegevens te gebruiken voor identiteitsfraude. De Werkgroep 29 stelt in de *Guidelines on Personal data breach* dan ook dat wanneer dergelijke gegevens bij een datalek betrokken zijn, er een aanzienlijke kans bestaat dat het datalek een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen, zodat het datelek zowel aan de privacy toezichthouder als aan de betrokkenen moet worden gemeld.[9] Wij zijn vanwege deze uitleg van Werkgroep 29 van oordeel dat financiële gegevens, vanwege de gevoelige aard en de beschermingsgedachte van de AVG, in dit licht bezien gelijkgesteld moeten worden aan bijzondere persoonsgegevens en dienovereenkomstig moeten worden behandeld.

Het verwerken van al deze bijzondere en gevoelige persoonsgegevens is naar onze overtuiging bovendien te beschouwen als een kernactiviteit van woningcorporaties, al was het maar omdat het beheren en faciliteren van sociale woningbouw één (van de) belangrijkste activiteiten van woningcorporaties is. Het faciliteren, verhuren en beheren van sociale woningen kan immers uitsluitend plaatsvinden door een aanzienlijke hoeveelheid (bijzondere en gevoelige) persoonsgegevens te verwerken. Door deze verwerkingen zijn woningcorporaties in staat om hun taken op goede wijze uit te voeren.

Ter illustratie, door dergelijke verwerkingen kunnen bijvoorbeeld nieuwe huurders worden geselecteerd op grond van de hoogte van hun inkomen, asielzoekers worden geplaatst en begeleid, en kan de huur van bestaande huurders geïnd worden. Daarnaast bieden woningcorporaties aan huurders met fysieke beperkingen veelal extra zorgdiensten aan en kunnen woningen worden voorzien van (medische) hulpmiddelen.

Daarbij komt dat de Autoriteit Persoonsgegevens al snel van mening is dat er sprake is van een grootschalige gegevens verwerking. Voor huisartsenpraktijken en instellingen voor medisch specialistische zorg, niet zijnde ziekenhuizen, geldt dat een verwerking al grootschalig is als a) die praktijk of instelling meer dan 10.000 patiënten heeft ingeschreven óf als die gemiddeld meer dan 10.000 patiënten per jaar behandelt én b) de gegevens van deze patiënten in één informatiesysteem staan.[10] De verwerking van patiëntgegevens door ziekenhuizen, zorggroepen, huisartsenposten en apotheken (behalve als er sprake is van een solistisch werkende zorgverlener) is altijd grootschalig.

De gegevensverwerking door woningcorporaties van bijzondere en/of gevoelige persoonsgegevens is evengoed grootschalig. Gelet op de beschermingsgedachte van de AVG brengt een redelijke uitleg van artikel 37 lid 1 sub c AVG dan ook mee dat woningcorporaties verplicht zijn om een FG aan te stellen.

Conclusie

[9] Guidelines on Personal Data brech notification, 6 februari 2018, p. 24. Deze guidelines zijn door de EPDB eveneens bekrachtigd. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

[10] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-uitleg-over-grootschalige-gegevensverwerking-de-zorg

Wat ons betreft is het, gelet op de door de EDPB bekrachtigde *Guidelines on Data Protection Officers* van de Werkgroep 29 en (een redelijke) uitleg van de AVG door de Autoriteit Persoonsgegevens, onvermijdelijk dat op woningcorporaties in beginsel de verplichting rust tot het aanstellen van een FG. Zelfs als het naar de strikte letter van de AVG geen verplichting zou zijn, dan nog zouden woningcorporaties een FG moeten omarmen als 'good practice' en is het dus alsnog een verplichting. Ondanks de administratieve beslommeringen die dit meebrengt, adviseren wij woningcorporaties om zo snel mogelijk de nodige organisatorische maatregelen te nemen en een FG aan te stellen. Het correct interpreteren en vervolgens implementeren van de AVG in het algemeen en het aanstellen en inbedden van een FG in het bijzonder blijkt in de praktijk geen sinecure. Nu bekend is dat de aanstelling van een FG (en registratie daarvan bij de AP) een van de eerste AVG onderdelen is die door de AP krachtig zal worden gehandhaafd, is bovendien enige spoed geboden.

Mocht u meer over de DPO willen weten, dan kunnen wij u voorzien van deskundig en pragmatisch advies. Het aanstellen van een DPO is slechts één van de verplichtingen uit de AVG die op u als woningcorporatie rust. Wij kunnen u daarnaast ook adviseren over het opstellen van DPIA's op basis van zelf ontwikkelde standaarden, datalekprotocollen, verwerkingsregisters en verwerkersovereenkomsten. Daarnaast bieden wij (inhouse) trainingen aan.

Wilt u zelf een eerste inschatting doen of uw organisatie een DPO nodig heeft? Vul onze gratis DPO self-assessment in via www.dponodig.nl en ontvang direct een eerste vrijblijvend advies.

Olaf van Haperen, managing partner en sectiehoofd IE/IT

Sarah Zadeh, juridisch medewerker IT, Privacy & Data Security