Alexandra Boot
is partner bij Boot Advocaten en co-founder van Blue Building Institute. Ze is ruim 28 jaar gespecialiseerd in bouw- en vastgoed en aanbestedingsrecht. Sedert 6 jaar is zij tevens actief in het energierecht. Alexandra bekleedt diverse nevenposities onder meer als docent en toezichthouder en is vaste columnist bij diverse landelijke media.

De Algemene Verordening Gegevensbescherming

De bescherming van persoonsgegevens krijgt steeds meer aandacht. Technische ontwikkelingen maken interessante nieuwe bedrijfsmodellen en maatschappelijk relevante toepassingen met betrekking tot het gebruik van persoonsgegevens mogelijk. In slimme gebouwen (smart buildings) worden individuele gebouwbeheersystemen geïntegreerd met ICT-systemen en facilitaire bedrijfssystemen. De verzamelde data kunnen worden gebruikt om tot optimalisatie te komen van gebouw en werkomgeving. Ook op stedelijk niveau worden initiatieven ontwikkeld om op basis van de technologie en gegenereerde data oplossingen te vinden voor de steeds grotere druk op de publieke voorzieningen en infrastructuur. Het verzamelen van data en het delen van de informatie is niet zonder juridische gevolgen. De vraag is hoe het verzamelen van al deze data zich verhoudt tot onze persoonlijke levenssfeer.

De bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verwerken van persoonsgegevens is een aan de persoon gekoppeld grondrecht. Regels die deze bescherming normeren zijn vastgelegd in de algemene privacywet, de Wet bescherming persoonsgegevens(Wbp), en diverse specifieke wetten. Op 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG) in werking. Vanaf dat moment zal er nog maar één algemene privacywet gelden in de Europese Unie. De nieuwe regels hebben directe werking en hoeven dus niet apart te worden geïmplementeerd in nationale wetgeving. Decentrale overheden moeten direct voldoen aan de regels in de Verordening, en kunnen zich hier ook direct op beroepen. De AVG zal voor iedereen die zich bezig houdt met compliance veel betekenis krijgen. Op grond van huidige wetgeving dient er reeds vooraf toestemming te worden gevraagd voor het verzamelen, opslaan en gebruik van persoonsgegevens.

De AVG stelt strengere eisen aan deze toestemming. Zo bent u onder de nieuwe regels verplicht in kaart te brengen op basis van welke wettelijke grondslag u deze gegevens verwerkt, met welk doel u dit doet, met wie u ze deelt en hoe u ervoor zorgt dat u in lijn met de regelgeving handelt. Nieuw is onder meer dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken en dat het voor mensen net zo eenvoudig moet zijn om hun toestemming in te trekken als om die te geven.

Nieuw is ook de plicht om een Functionaris Gegevensbescherming te benoemen. Voor veel organisaties zal deze verplichting niet gelden, maar in ieder geval wel voor overheidsinstanties en organisaties die hoofdzakelijk zijn belast met verwerkingen die leiden tot regelmatige en stelselmatige grootschalige observatie van betrokkenen, verwerken van informatie of het op grote schaal verwerken van bijzondere gegevens.

Voorbeelden van deze vormen van observatie zijn profilering en locatietracering via een gezondheidsapp, of slimme apparatuur in auto's of woningen. Steeds meer gebruiksvoorwerpen worden verbonden met het internet. Men spreekt ook wel van 'the internet of things'. Dit leidt tot een exponentiële toename van de uitwisseling van data, waaronder ook persoonlijke gegevens. De AVG beoogt deze gegevens adequaat te beschermen. De vraag is of overheden en de betreffende ondernemingen gereed zijn om vanaf 25 mei 2018 deze bescherming ook te bieden. Een korte rondgang langs de velden leert dat dit nog lang niet het geval is. Nationale toezichthouders kunnen echter substantiële boetes opleggen met maxima tussen €10 en 20 miljoen of 2 tot 4% van de wereldwijde omzet voor overtredingen van bepalingen uit de AVG. Aan de slag met AVG compliance!