Wet bescherming persoonsgegevens vervangen door nieuwe Europese regelgeving. Wat zijn de gevolgen?

Op 25 mei 2016 is de Algemene verordening gegevensbescherming (AVG) in werking getreden. Het is Europese regelgeving. Vanaf 25 mei 2018 geldt deze verordening ook in Nederland en zal die de Wet bescherming persoonsgegevens vervangen (Wbp). Deze wijziging heeft ook gevolgen voor huurders, verhuurders, beheerders en makelaars. Wat zijn de gevolgen?

Waarom de AVG?

De richtlijn bescherming persoonsgegevens, bij ons vastgelegd in de Wbp, is afkomstig uit 1995. Sinds 1995 is er echter bijzonder veel veranderd, juist op het gebied van privacy. De enorme digitalisering en de opkomst van internet en ICT-technologie maakte het noodzakelijk om nieuwe regels te maken voor de bescherming van privacy en verwerking van persoonsgegevens. Al in 2012 stelde de Europese Commissie de AVG voor en in mei 2016 is de definitieve versie goedgekeurd.

Wat bepaalt de AVG?

<u>Definities</u>
De AVG bevat regels over de verwerking van persoonsgegevens. Deze verordening bevat een aantal termen die relevant zijn om te onthouden. Te beginnen met de term *persoonsgegevens*. Hieronder vallen onder andere gegevens zoals naam, adres, BSN-nummer, foto's en vingerafdrukken. Ook '*verwerken*' is een cruciale term. Een zeer ruim begrip. Alleen al het verzamelen en opslaan van persoonsgegevens is 'verwerking'. Kortom registratie van een nieuwe huurder of woningzoekende (en alle werkzaamheden die daarop volgen totdat de huurder is vertrokken en alle gegevens zijn gewist) valt onder verwerking van persoonsgegevens. Degene die de gegevens verwerkt is de 'verwerker'. Als een organisatie verantwoordelijk is voor de verwerking is dat de 'verwerkingsverantwoordelijke'. Dit kan bijvoorbeeld de organisatie zijn waar de verwerker in dienst is of een overkoepelende organisatie van de verwerkende organisatie. De natuurlijke persoon om wiens gegevens het gaat is de 'betrokkene'.

<u>Wat zijn de regels?</u>

1. *Gegevens verwerken*
   Persoonsgegevens mogen alleen worden verwerkt als daar een grondslag voor is en vervolgens alleen voor het doel waarvoor deze gegevens zijn verkregen.

   De grondslag kan gelegen zijn in de wet, maar de betrokken persoon kan ook toestemming geven voor de verwerking van de persoonsgegevens. Kort weergegeven is de verwerking van persoonsgegevens rechtsmatig als:
   - Er toestemming is van de betrokkene. Hier mag niet lichtzinnig over worden gedacht. De toestemming moet in eenvoudige, duidelijke en toegankelijke taal worden gevraagd en de toestemming kan te allen tijde weer worden ingetrokken;
   - De verwerking is noodzakelijk op grond van overeenkomst;
   - De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting;
   - De verwerking is noodzakelijk om de vitale belangen van betrokkene of andere natuurlijke personen te beschermen;
   - De verwerking is noodzakelijk ter vervulling van een taak van algemeen belang of openbaar gezag;
   - De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde.

Daarnaast is het transparantiebeginsel van groot belang. De betrokkene moet op de hoogte worden gesteld van het feit dat zijn gegevens worden verwerkt en wat het doel is. Het gaat om informatie over wanneer de gegevens bij betrokkene worden verzameld, wanneer deze zijn verkregen via derden en over de rechten van betrokkene. Op deze rechten zal ik later in dit artikel ingaan.

Verwerking van bijzondere persoonsgegevens is verboden, tenzij er een bijzondere uitzondering van toepassing is. Bijzondere persoonsgegevens zijn gegevens over ras, afkomst, politieke opvattingen, religieuze overtuiging, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens en gegevens over gezondheid, seksueel gedrag of seksuele gerichtheid.

2. *Rechten van de betrokkene*
Degene wiens gegevens worden verwerkt, heeft rechten ten aanzien van die gegevens. Niet alleen kan hij of zij toestemming geven en deze toestemming altijd weer intrekken, maar ook tijdens de verwerking heeft de betrokkene rechten. Het gaat om:

- Het recht op inzage;
  De betrokkene heeft het recht om te horen of de gegevens verwerkt worden en, als dat zo is, voor welk doel. Daarnaast heeft hij recht te weten aan wie de gegevens worden verstrekt, om welke gegevens het gaat, hoe lang de gegevens bewaard zullen worden en welke rechten de betrokkene nog meer heeft met betrekking tot de gegevens (zie hieronder).

- Het recht op rectificatie;
  De betrokkene mag onjuiste gegevens verbeteren. Dit moet zonder vertraging gebeuren.

- Het recht om vergeten te worden;
  Misschien een van de belangrijkste rechten van de betrokkene is dat hij ook weer vergeten mag worden. Een overheid moet aan dit verzoek in bepaalde gevallen voldoen. Bijvoorbeeld als de gegevens niet langer nodig zijn, als de toestemming is ingetrokken, als betrokkene bezwaar maakt tegen de verwerking en als de gegevens onrechtmatig worden verwerkt. Ook kopieën van de gegevens, koppeling naar de gegevens en reproducties van de gegevens moeten worden verwijderd en vernietigd. Een heel karwij in deze digitale tijd.

- Het recht op beperking van de verwerking
  De betrokkene kan bepalen dat niet alle gegevens worden verwerkt, bijvoorbeeld als hij de juistheid betwist of wanneer niet alle gegevens nodig zijn voor het beoogde doel.

- Een kennisgevingsplicht en het recht op overdraagbaarheid van de gegevens.
  De betrokkene moet de verwerker informeren als zijn gegevens zijn verbeterd, verwijderd of beperkt. Ook heeft betrokkene het recht om de gegevens die hem betreffen te verkrijgen en mag hij deze overdragen aan een andere verantwoordelijke.

3. *Verplichtingen van de verwerkingsverantwoordelijke*
Degene die de gegevens verwerkt heeft ook verplichtingen anders dan het uitvoerig informeren van de betrokkene. Een aantal belangrijke verplichtingen zijn:

- Aanwijzing van een functionaris voor de gegevensbescherming.
  Deze verplichting geldt alleen voor overheidsinstanties, organisaties die belast zijn met de verwerking van gegevens die regelmatige of stelselmatige observatie op grote schaal van betrokkenen vereisen of organisaties die belast zijn met grootschalige

verwerking van bijzondere persoonsgegevens of gegevens over strafbare feiten. Deze organisaties moeten zelf een functionaris aanwijzen voor de gegevensbescherming of samen met een aantal andere organisaties een functionaris aanwijzen. De functionaris moet informeren over de AVG en andere EU-regelgeving, toezien op de naleving ervan, het personeel van de organisatie opleiden en bewust maken op het gebied van gegevensbescherming en samenwerken met en als aanspreekpunt optreden voor de Autoriteit Persoonsgegevens.

- Meldplicht bij inbreuk in verband met persoonsgegevens
  Al deze regelgeving is erop gericht om persoonsgegevens te beschermen. Het is dan ook niet vreemd dat inbreuken op deze gegevens, zoals datalekken of andere vormen van diefstal voorkomen moeten worden en als het toch gebeurt direct moeten worden gemeld. Bij een inbreuk moet binnen 72 uur na ontdekking melding worden gedaan bij de Autoriteit Persoonsgegevens. Als de melding later is dan 72 uur na ontdekking, moet uitgelegd worden waarom dat het geval is.

  Bij de melding moet de verwerkingsverantwoordelijke open kaart spelen en alles rond de inbreuk meedelen aan de autoriteit: de aard van de inbreuk, de soort gegevens, het geschatte aantal betrokkenen, de gegevens van de functionaris (als die er is) zodat die meer uitleg kan geven, de waarschijnlijke gevolgen van de inbreuk, de maatregelen die zijn voorgesteld of genomen om de inbreuk aan te pakken en de nadelige gevolgen te beperken.

  Als de inbreuk bovendien een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, moet de verwerkingsverantwoordelijke dit niet alleen melden aan de autoriteit maar ook aan de betrokkenen. Deze mededeling mag niet in wollig taalgebruik worden verpakt, maar moet duidelijk en eenvoudig zijn waarbij ook wordt gemeld om welke gegevens het gaat en naar schatting de risico's en de gevolgen. De verwerkingsverantwoordelijke kan voorkomen dat hij bij de betrokkenen met de billen bloot moet, als hij de gegevens bijvoorbeeld versleuteld heeft, achteraf maatregelen heeft genomen om het risico voor de betrokkene dusdanig te beperken dat het zich niet meer zal voordoen of als de mededeling onevenredige inspanningen zou vergen (in dat geval moet een openbare mededeling worden gedaan).

  Momenteel geldt onder de Wbp ook al een meldplicht, namelijk de Meldplicht datalekken. Vanaf de inwerkingtreding van de AVG wordt deze meldplicht vervangen door de Meldplicht zoals hiervoor beschreven.

- Bij het ontwerpen en gebruiken van het informatiesysteem waarin de persoonsgegevens worden verwerkt moet rekening worden gehouden met privacy. Er moeten waarborgen zijn voor de bescherming van de persoonsgegevens. Dit kan bijvoorbeeld het psuedonimiseren van de gegevens zijn, maar ook het mogelijk maken dat de betrokkene zijn gegevens controleert. Hoe dit ingericht moet worden, zal van bedrijf tot bedrijf verschillen. Om aan te tonen dat aan deze eisen voldaan is, kan een bedrijf gebruik maken van een certificeringsmechanisme dat is goedgekeurd op grond van de AVG.

- Register van verwerkingsactiviteiten
  Iedere verwerkingsverantwoordelijke moet een register bijhouden van de verwerkingsactiviteiten. In dit register moeten de doelen van de verwerking, de categorieën van betrokkenen en gegevens, de categorieën van ontvangers van de gegevens, bewaartermijnen en een beschrijving van de beveiligingsmaatregelen worden opgenomen. Degene die daadwerkelijk verwerkt, moet ook een register bijhouden van zijn werkzaamheden. Een omvangrijke klus. De AVG bevat daarom een vrijstelling voor kleine organisaties. Ondernemingen of organisaties met minder

dan 250 personen in dienst hoeven geen registers bij te houden, tenzij de verwerking die zij verrichten grote risico's meebrengt, zij niet incidenteel gegevens verwerken of zij vooral bijzondere persoonsgegevens verwerken. Doorgaans is echter geen sprake van incidentele gegevensverwerking, maar van structurele gegevensverwerking. Bij het bijstaan van cliënten en verifiëren van hun identiteit voor de eigen dienstverlening is reeds sprake van structurele gegevensverwerking en is een verwerkingsregister dus verplicht, tenzij er wellicht sprake is van zeer weinig cliënten.

4. *DPIA: Data Protection Impact Assessment*
   Een laatste onderdeel waar een verwerkingsverantwoordelijke mee te maken kan krijgen, is de DPIA. In sommige gevallen moet de verantwoordelijke voorafgaand aan de verwerking de privacy risico's in kaart brengen. Dat is het geval als de verwerking een hoog risico voor de privacy van de betrokkenen oplevert. De AVG noemt drie situaties, namelijk (1) als een organisatie systematisch en uitvoerig persoonlijke aspecten evalueert (o.a. profiling), (2) op grote schaal bijzondere persoonsgegevens verwerkt en (3) op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (cameratoezicht). Dit zijn echter niet de enige denkbare situaties. De Europese privacy toezichthouders hebben in oktober 2017 richtlijnen opgesteld waarin zij 9 criteria hebben genoemd om te bepalen of een DPIA noodzakelijk is. Als uitgangspunt wordt gehanteerd dat een DPIA noodzakelijk is, als de verwerking aan 2 of meer van de 9 criteria voldoet. De criteria zijn:
   - Beoordeling van mensen op basis van persoonskenmerken (o.a. profiling/creditscoring);
   - Geautomatiseerde beslissing die (rechts)gevolgen hebben voor betrokken;
   - Stelselmatige of grootschalige monitoring (cameratoezicht);
   - Verwerking van bijzondere persoonsgegevens en gevoelige gegevens;
   - Grootschalige gegevensverwerking (beoordeeld naar aantal personen, hoeveelheid gegevens, tijdsduur van de verwerking en reikwijdte van de verwerking);
   - Gekoppelde databases;
   - Gegevens over kwetsbare personen (werknemers, patiënten, kinderen, andere personen die door een ongelijke machtsverhouding niet in vrijheid toestemming kunnen geven);
   - Gebruik van nieuwe technologieën;
   - Blokkering van recht, dienst of contract (zoals banken die controleren of iemand een lening kan krijgen).

   Het kan dus per verwerking verschillen of een DPIA noodzakelijk is. Wellicht is de DPIA voor de verwerking van interne gegevens wel vereist, maar voor externe gegevens niet, of andersom.

De naleving van de AVG zal worden gecontroleerd door de autoriteit persoonsgegevens (AP). De AP kan boetes opleggen als organisaties de regels niet naleven. Deze boetes kunnen oplopen tot maar liefst € 20 miljoen.

Hulpmiddelen van de AP

Op de website van de Autoriteit persoonsgegevens staat een aantal hulpmiddelen om u zich zo goed mogelijk te laten voorbereiden op de inwerkingtreding van de AVG. Onder andere een stappenplan en 'De AVG in een notendop'. Deze informatie vindt u hier:

- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/avg_in_een_notendop.pdf
- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2017-11_stappenplan_avg_online_v2.pdf

Conclusie: Waar moet u als verhuurder, beheerder en makelaar rekening mee houden?

Verhuurders, beheerders en makelaars verwerken persoonsgegevens. De AVG is dus ook van toepassing op de werkzaamheden van deze partijen. Dit betekent dat het in ieder geval noodzakelijk is om na te gaan om welke wijze uw organisatie persoonsgegevens verwerkt.

Uit het voorgaande blijkt dat er een aantal onderdelen is dat voor iedere verwerker van persoonsgegevens geldt. Iedere verwerker (en dus verhuurder, makelaar en beheerder) moet nagaan of hij of zij in de gegevens omstandigheden wel persoonsgegevens mag verwerken. Met name in de beginfase is er nog geen overeenkomst of plicht waar aan voldaan moet worden. Toch wordt de aspirant-huurder doorgaans gevraagd zijn persoonsgegevens achter te laten als hij geïnteresseerd is in een woning. Dit zou onder het kopje 'toestemming' kunnen vallen, maar de AVG bepaalt dat de persoon al uitgebreid geïnformeerd moet worden over zijn rechten voordat hij toestemming geeft. Een simpele invuloefening op een website volstaat dus niet.

Vervolgens moet de verwerker de rechten van de betrokken natuurlijke persoon goed in zijn oren knopen. De huurder mag altijd vragen om inzage in zijn gegevens, om rectificatie daarvan en uiteindelijk om vernietiging daarvan. Een klantenbestand met oude gegevens is straks dus wellicht niet meer mogelijk. Daarnaast geldt altijd de meldplicht bij inbreuken en de voorzorgsmaatregelen die genomen moeten worden. Persoonsgegevens mogen niet zomaar toegankelijk zijn en niet zonder menselijke tussenkomst voor derden bereikbaar. Een niet vergrendelde computer waar iemand in heeft gekeken, een verloren dossier of een USB-stick zijn een inbreuk in verband met persoonsgegevens die gemeld moet worden. In dat soort gevallen zijn de gevolgen bovendien niet te overzien.

Daarnaast zijn er nog de verplichtingen die mogelijk voor uw organisatie geldt, zoals het register voor verwerkingsactiviteiten, het aanstellen van een functionaris voor gegevens bescherming en het uitvoeren van een DPIA. Deze maatregelen kunnen per organisatie en zelfs per verwerking verschillen. Ga dus goed na op welke wijze u gegevens verwerkt.

Als u er niet uitkomt, kunt u de Autoriteit Persoonsgegevens bellen. Ook geeft de autoriteit op uitnodiging voorlichting. Meer informatie kunt u vinden op https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/voorbereiding-op-de-avg. Uiteraard staan wij ook tot uw beschikking voor overleg.

Marjolein Scheeper