

Juridische aspecten Publiceren Ingekomen stukken op het Internet (in een notendop)

De raad heeft de wens om de ingekomen stukken voor de raad vanaf actief openbaar te maken door ze te publiceren op internet. Voor zover deze stukken persoonsgegevens bevatten moeten deze geanonimiseerd worden. In dit proces is sprake van het verwerken van persoonsgegevens. Daarmee is naast de Wob ook de Wbp (wordt vervangen door de AVG vanaf mei 2018) van toepassing.

In dit kader zijn dus van belang de Wet openbaarheid van bestuur (Wob) en de Wet bescherming persoonsgegevens (Wbp). Bij het verstrekken van overheidsinformatie in het kader van actieve openbaarmaking vindt er samenloop plaats tussen de Wob en de Wbp, wanneer de overheidsinformatie persoonsgegevens bevat.

Dit betekent ook dat er een spanningsveld kan ontstaan tussen het recht op toegang tot overheidsinformatie enerzijds en het recht op bescherming van persoonsgegevens anderzijds.

De Wob heeft als hoofdregel dat overheidsinformatie openbaar is. Het bevat ook het beginsel van actieve openbaarmaking, d.w.z. het verstrekken van informatie door een bestuursorgaan zonder dat daar aan een verzoek ten grondslag ligt. Bij actieve openbaarmaking is een bestuursorgaan gehouden aan de uitzonderingsgronden zoals genoemd in artikel 10 lid 1 en 2 van de Wob. Hierin is onder meer bepaald dat bijzondere persoonsgegevens zo wie so niet openbaar gemaakt mogen worden en dat informatieverstrekking eveneens achterwege blijft voor zover het belang niet opweegt tegen de eerbiediging van de persoonlijke levenssfeer. Gedoeld wordt hier op persoonsgegevens omdat deze deel uitmaken van de persoonlijke levenssfeer. In deze gevallen moet dus altijd een belangenafweging gemaakt worden voor dat overgegaan wordt tot actieve openbaarmaking. Tot op heden is aan de actieve openbaarmaking van ingekomen stukken uitvoering gegeven door ze ter inzage te leggen. Door het plaatsen van ingekomen stukken op internet gaat de raad een stapje verder.

De Wbp strekt er toe dat een ieder het recht heeft op bescherming tegen het ongebreideld verzamelen, bewerken, delen en verspreiden etc. van zijn persoonsgegevens. Deze wet geeft niet alleen aan wat de rechten zijn van iemand van wie de persoonsgegevens gebruikt worden, maar ook wat de plichten zijn van de organisatie die deze gegevens in hun bezit hebben en gebruiken. De wet benoemt deze organisaties expliciet als verantwoordelijke voor de bescherming van persoonsgegevens.

Van groot belang in dit kader is het feit dat de Wbp wordt vervangen door Europese wetgeving (de Algemene Verordening Gegevensbescherming hierna: **AVG**) per 25 mei 2018. Deze verordening heeft tot doel de bescherming van persoonsgegevens en is een aanscherping van voorgaande privacywetgeving. De AVG geeft de verantwoordelijke meer plichten en de betrokkene meer rechten. Zo introduceert de AVG een verantwoordingsplicht (zgn. accountability). Dit betekent dat een verantwoordelijke (het bestuursorgaan) verantwoordelijk is voor de naleving van de AVG privacyprincipes en die naleving moet kunnen aantonen. Die principes gaan over de gang van zaken bij gegevensverwerkingen.

Persoonsgegevens moeten door de verantwoordelijke verwerkt worden op een wijze die ten aanzien van betrokkenen rechtmatig en behoorlijk is. Iedere verwerking die onder de AVG valt moet gebaseerd zijn op één (of meerdere) van de zes grondslagen.

Dwz dat de verwerking nodig is om:

1. een overeenkomst met de betrokkene voor te bereiden of uit te voeren
2. aan een wettelijke verplichting te voldoen
3. voor iemand van levensbelang
4. om een overheidstaak goed te kunnen vervullen

5. is voor de verantwoordelijke van zodanig belang, dat dat zwaarder weegt dan de belangen van betrokkenen (belangenafweging);
òf
6. de betrokkene heeft toestemming gegeven voor de verwerking.

In de voorliggende kwestie (actieve openbaarmaking van ingekomen stukken door plaatsing op internet) is m.n. punt 5 aan te wijzen als grondslag voor de verwerking van persoonsgegevens. De AVG biedt de mogelijkheid tot deze grondslag onder twee voorwaarden:

- De verantwoordelijke heeft een gerechtvaardigd belang
- Dat belang weegt zwaarder dan de belangen van betrokkenen.

Hier moet dus een afweging gemaakt worden tussen de belangen van de organisatie en de belangen van degenen van wie de persoonsgegevens we de persoonsgegevens verwerken.

Het anonimiseren van gegevens is een privacy maatregel, maar dit is en blijft altijd mensenwerk. De kans op het per abuis plaatsen van persoonsgegevens op internet (datalek) is immers altijd aanwezig.

Een datalek doet zich voor wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden moeten hebben. Uit de statistieken blijkt dat veruit de meeste datalekken het gevolg zijn van menselijk handelen.

De gevolgen van zo'n datalek hebben in het slechtste geval een grote bestuurlijke impact (boete, imago schade, informeren betrokkene, schadevergoeding, verlies van vertrouwen) `en een persoonlijke impact voor de betrokkene (dit kan variëren van kleine ongemakken tot het risico op identiteitsfraude). Het anonimiseren is geen 100% garantie op het voorkomen van een datalek. Er blijft dus altijd een zeker restrisico over. Transparant moet worden gemaakt welke belangen zo zwaar wegen dat dit leidt tot acceptatie van dit rest risico ten koste van de belangen van betrokkenen (accountability).

Dit hoort in het nog op te stellen raadsvoorstel een besispunt te zijn.

Sinds 1 januari 2016 is de Meldplicht datalekken van toepassing hetgeen inhoudt dat deze onverwijld bij de Autoriteit Persoonsgegevens moeten worden gemeld. De AP kan dan nader onderzoek doen. Wanneer hieruit blijkt dat de privacyregels worden overtreden (omdat bijvoorbeeld sprake is van onrechtmatige verwerking), staat de AP een groot aantal corrigerende maatregelen ter beschikking. Hier kunnen genoemd worden een waarschuwing of berisping, een boete, gelaten dat de overtreding wordt opgelost, de verwerking verbieden etc.

Mr. Marijke Schep
Afdeling Juridische Zaken.