AUTORITEIT
PERSOONSGEGEVENS

Schriftelijke bijdrage aan de Eerste Kamer ten behoeve van deskundigenbijeenkomst 30 juni 2020

Aleid Wolfsen, voorzitter AP

Inleiding: Privacy is een grondrecht

- Onze samenleving is de afgelopen jaren wezenlijk veranderd door digitalisering en innovatie. Nederland loopt wereldwijd voorop in deze ontwikkelingen. In die wereld moet ook de overheid mee en dat doet ze ook.
- Dat biedt kansen: Nederlandse burgers ondervinden veel gemak van het online doen van belastingaangifte. En met een druk op de knop heeft een student inzicht in zijn studieschuld. En technologie maakt het ook mogelijk om zorgvuldig met persoonsgegevens om te gaan, bijvoorbeeld door deze te beveiligen tegen toegang door onbevoegden.
- Maar er zijn ook grote risico's: er wordt steeds meer over ons vastgelegd, ons leven wordt steeds beter gedocumenteerd zonder dat we precies weten wat er met die gegevens gebeurt en wie er toegang toe heeft. Dit maakt ons en onze democratische rechtstaat kwetsbaar.
- In deze digitale samenleving is de bescherming van persoonsgegevens (dataprotectie) essentieel. Daarom is het recht op gegevensbescherming opgenomen in het Handvest van de grondrechten van de Europese Unie. Omdat vrijwel alles data is, wordt dat grondrecht steeds meer een allesomvattend grondrecht. Het beschermt inmiddels feitelijk alle fundamenten van onze rechtsorde: vrijheid/grondrechten, gelijkheid/gelijkwaardigheid, democratie, rechtsstaat, solidariteit en de toegang tot vreedzame conflictbeslechting. Hiermee is dataprotectie geëmancipeerd tot een noodzakelijk en krachtig middel en wapen, een steunpilaar en hoeder van die fundamenten. Onzorgvuldig of onnadenkend omgaan met of spreken over gegevensbescherming tast ook die andere grondrechten aan. En leidt dus tot erosie van die fundamenten en daarmee van onze vrije wil en autonomie.

- De Autoriteit Persoonsgegevens (AP) heeft hierin een belangrijke taak. De AP is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt. Wij zijn onderdeel van een Europees samenwerkingsverband van toezichthouders. Ons toezichtveld is omvangrijk: nationale en internationale bedrijven en organisaties, de gehele overheid – inclusief politie en justitie – en ook verenigingen, scholen, stichtingen en individuele burgers. Dit doen we niet alleen in Nederland; data kennen immers geen grenzen. Het toezicht van de AP is daarom bij uitstek grensoverschrijdend.
- We varen – zeker ook sinds Corona – steeds scherper aan de wind. Alertheid en 'strengheid' van de AP zijn zeer gewenst.

De overheid en persoonsgegevens

- Overheden verwerken veel persoonsgegevens. Daarbij moeten we nog beter opletten: zij verwerken niet alleen veel, maar ook vaak gevoelige persoonsgegevens. Op basis van die informatie neemt de overheid dagelijks voor burgers ingrijpende besluiten.
- De taken en verantwoordelijkheden van overheden worden ook nog steeds uitgebreid. Overheidsinstellingen weten daardoor ook steeds meer over burgers, terwijl die instellingen zelf juist steeds ondoorzichtiger worden voor de burger, onder meer door het gebruik van algoritmes en AI. Belangrijk is dus dat burgers weten dat die informatie rechtmatig is verkregen, juist is en eerlijk en behoorlijk wordt verwerkt. Overheidsinstellingen moeten dus toetsbaar en transparant handelen en beslissen.
- Maar de overheid moet ook met de tijd mee, in haar dienstverlening richting burgers. En hier vindt de Wet digitale overheid (WDO) haar weg.
- De Wet digitale overheid heeft als doel het regelen van het veilig en betrouwbaar kunnen inloggen voor Nederlandse burgers en bedrijven bij de (semi-)overheid. Of zoals de website van de wet staat: 'Met veilig en betrouwbaar inloggen wordt bedoeld dat burgers elektronische identificatiemiddelen (eID) krijgen met een hogere mate van betrouwbaarheid dan het huidige Digid. Deze identificatiemiddelen geven publieke dienstverleners meer zekerheid over iemands identiteit.'
- De WDO gaat in feite om een aantal zaken:
  - Standaarden;
  - Informatiebeveiliging;

- Elektronische identificatiemiddelen.

De ankers van de AVG: Hoe beoordeelt de AP het wetsvoorstel?

Zoals gezegd, de AP vaart scherp aan de wind en kijkt kritisch naar voorstellen waar persoonsgegevens worden verwerkt. Daarin varen we op een aantal pijlers.

- In het toezicht bieden de beginselen van 'rechtmatigheid', 'transparantie' en 'behoorlijkheid' een goed aangrijpingspunt. De AVG bevat duidelijke normen over wanneer het rechtmatig is om persoonsgegevens te verwerken. Ook schrijft de wet voor dat verwerkingsverantwoordelijke organisaties transparant moeten zijn over welke persoonsgegevens zij verwerken, met welk doel en de wijze waarop die gegevens worden verwerkt.
- Dataminimalisatie: het verzamelen van data moet beperkt worden tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (minimale gegevensverwerking).
- Doelbinding: De overheid beschikt over veel bijzondere persoonsgegevens. In toenemende mate koppelen overheden bestanden. Hoewel de intenties goed zijn, kan het koppelen van bestanden een schending van het beginsel van 'doelbinding' vormen.

AP Wetgevingsadvies over de WDO

- Het wetgevingsadvies van de AP op de WDO dateert van oktober 2017. In deze tijden van razendsnelle ontwikkelingen lijkt dat lichtjaren geleden. Dat is ook het eerste punt om mee te geven aan de Eerste Kamer:
- **Standaarden**: Zorg voor actuele standaarden. Het lijkt erop dat de WDO leunt op een site die verouderde informatie bevat en waarvan het lijkt dat deze niet (voldoende) actueel gehouden wordt terwijl dat uiteraard essentieel is.
- **Informatiebeveiliging:** Voor de AP is informatiebeveiliging een van de aandachtspunten voor de komende periode, zoals ook beschreven in het visiedocument *Focus AP 2020-2023*. De beveiliging van persoonsgegevens bij de overheid laat nog vaak te wensen over. Slechte beveiliging kan leiden tot een datalek. De impact van datalekken bij de overheid kan erg groot zijn, omdat het vaak gaat om enorme hoeveelheden bijzondere of gevoelige persoonsgegevens. Het is daarom belangrijk dat overheidsorganisaties aandacht hebben voor de beveiliging van gegevens.

- Op dit moment zijn we afhankelijk van het inloggen met een publiekmiddel: Digid. Het is begrijpelijk dat er wordt gezocht naar een back-up, voor een terugval optie voor als Digid niet bereikbaar of beschikbaar is. Het afhankelijk zijn van een systeem waar zoveel mensen zo vaak met zulke belangrijke gegevens gebruik van maken verdient een terugvaloptie. Het wetsvoorstel digitale overheid biedt de optie voor private partijen om identificatiemiddelen te maken. Met als voordeel dat burgers kunnen kiezen.
- Informatiebeveiliging wordt traditioneel bekeken vanuit de BIV-driehoek: Beschikbaarheid, Integriteit en Vertrouwelijkheid.
- Door meer identificatiemiddelen aan te bieden wordt de Beschikbaarheid inderdaad minder kwetsbaar. De Vertrouwelijkheid wordt echter wel kwetsbaarder doordat het 'aanvalsoppervlak' groter wordt. Om een vergelijking te maken: vroeger beschermden we een kasteel door een kasteelmuur met één enkele ophaalbrug en een enkele toegangspoort. In het geval van de WDO maken we in de toekomst gebruik van meerdere ophaalbruggen en toegangspoorten.
- Dit betekent uiteraard meer onderhoud van meer verschillende systemen. Met de kans op meer (menselijke) fouten die kunnen leiden tot kwetsbaarheden of een niet goed genoeg onderhouden systeem. De Minister zal hierin goed een afweging moeten maken bij het accepteren van nieuwe identificatiemiddelen. Waarbij hij ook moet letten op dat sommige burgers een inlogmiddel voor alle diensten gaan gebruiken. Hierdoor wordt dat ene inlogmiddel een mogelijke toegang voor een kwaadwillende tot bijna alle persoonsgegevens van de desbetreffende persoon.
- De AP wijst er dus graag op dat het verstandig is om na te denken over een back up, maar dat door een oneindig (?) aantal partijen, waaronder private partijen zoals de grote techbedrijven, toe te staan zich te melden, maken we ons ook kwetsbaar. De Beschikbaarheid is dan geen probleem meer, maar de Vertrouwelijkheid kan lelijke schade oplopen.
- **Uitwisseling van gegevens**: Een belangrijk startpunt in de wet is ook de term 'koppelvlakken'. Waarmee wordt bedoeld om gegevens makkelijk te kunnen delen. En dat is ook handig, maar we moeten ervoor waken dat 'handig' niet de overhand krijgt. De grens tussen 'wat fantastisch en knap dat dit kan' en 'levensgevaarlijk wat hier gebeurt' is nog nooit zo dun geweest. Verkeerd of onnadenkend gebruik kan ook gemakkelijk en structureel leiden tot bijvoorbeeld ongelijke behandeling.
- **De punten van proportionaliteit en subsidiariteit** zijn nu grotendeels verwerkt in de AMVB. Besteed voldoende aandacht aan deze onderwerpen in de wet zelf.

Afsluiting

Met de WDO laat de overheid zien mee te gaan in de gedigitaliseerde samenleving. Goed toezicht op de bescherming van persoonsgegevens is hierin essentieel. Zeker omdat het over grote hoeveelheden en veelal bijzondere persoonsgegevens gaat. De AP staat hiervoor. Daarbij moet gezegd worden dat er inmiddels verschillende knelpunten bij de AP zichtbaar zijn. Er loopt inmiddels een onderzoek in opdracht van het ministerie van Justitie en Veiligheid en de AP naar het toekomstbestendigheid van de AP zodat ook wij het toezicht op de digitale overheid efficiënt en effectief kunnen blijven uitvoeren.