De vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis van de Koning van de Eerste Kamer, heeft bij brief van 10 juli jl een aantal vragen gesteld ter voorbereiding op het op 22 september 2020 te houden voorbereidend onderzoek inzake het voorstel voor de Wet digitale overheid (Kamerstukken 34 972).

Deze vragen hebben betrekking op drie belangrijke thema's:

- *Open source*;
- *Privacy by design* zoals centrale opslag versus decentrale opslag;
- Het koppelen van data door commerciële partijen.

Bijgaand treft u de vragen alsmede de gevraagde nadere toelichting aan.

De commissie constateert dat, wanneer private partijen in de gelegenheid worden gesteld om eID aan te bieden, privacy en veiligheid de eerste zorgpunten zijn die naar voren komen. De commissie geeft aan dat diverse partijen dringend adviseerden om in de wet vast te leggen dat er een verplichting komt om de middelen open source aan te bieden ofwel de broncode van de aangeboden eID-systemen te publiceren, zodat de gebruiker kan controleren of de privacy en beveiliging goed zijn geregeld. De commissie verzoekt aan te geven waarom de regering ervoor gekozen heeft dit niet in de kaderwet op te nemen.

In reactie op het bovenstaande merk ik op, dat van groot belang is dat de werking van processen transparant is, zodat deze controleerbaar zijn. Daarnaast dient de veiligheid van de inlogmiddelen te worden geborgd. Een manier om transparantie te bewerkstelligen, is het gebruik maken van *open source*: software waarvan de broncode (sources) is gepubliceerd en vrij beschikbaar is. Transparantie kan echter ook worden gerealiseerd met gesloten software. Ten aanzien van veiligheid kennen beide voor- en nadelen: *open source* software wordt beveiligd door openheid, *closed source* software door het nemen van beschermende maatregelen.

Belangrijk is dat systemen transparant zijn in hun werking. Echter daarvoor is niet noodzakelijk dat middelen *open source* worden aangeboden. Dit kan ook met aanbieders van gesloten software worden afgesproken. Belangrijk is de veiligheid van de software. Deze moet gezien worden mede in verband met het onderhoud ervan en de garanties die kunnen worden geboden, bijvoorbeeld ten aanzien van continuïteit. Belangrijke processen zoals eID vergen overzichtelijke componenten. Dit betreft niet alleen de software zelf maar ook de totstandkoming en het onderhoud. Het enkel beschikbaar zijn van een open source pakket '*as is*', dus zonder enige garantie op kwaliteit, zekerheid of zonder een transparant servicepakket, biedt geen meerwaarde. Daarom is ervoor gekozen om *open source* niet te verplichten en de eisen inzake veiligheid en continuïteit centraal te stellen. Dit betekent niet dat de mogelijkheid om van open source gebruik te maken wordt uitgesloten. Zie inzake algemene overwegingen (dus: los van eID) om al dan niet gebruik te maken van *open source* de bijlage bij de kabinetsbrief van 17 april 2020.[1]

Ten aanzien van de veiligheid van *closed source* zullen met leveranciers afspraken gemaakt kunnen en moeten worden over het borgen van de veiligheid. Deze afspraken worden genomen op basis van het Besluit identificatiemiddelen voor burgers, welke AmvB u binnenkort in concept zal worden voorgelegd conform artikel 25 van het wetsvoorstel WDO (voorhangprocedure).

[1] Overwegingen bij "open, tenzij" en aanpak open source 2020-2021 (Bijlage bij Kamerstuk 26 643, nr. 676).

De commissie constateert dat er grote zorg is over de mogelijkheden die commerciële partijen krijgen door inloggegevens te koppelen en vervolgens gevoelige data te vergaren. De commissie refereert aan de privacy-visie eID die eind januari 2019 naar de Kamer is gestuurd, waarin wordt aangegeven dat het is verboden inlogregisters te gebruiken voor andere doeleinden dan de werking van het identificatiesysteem zelf. De commissie merkt op dat in het voorstel voor de Wet digitale overheid dat verbod ontbreekt en vraagt toe te lichten waarom de regering dit verbod niet heeft opgenomen.

In reactie op het bovenstaande merk ik op dat het principe van doelbinding, onder meer in relatie tot private partijen, wel degelijk is opgenomen in het wetsvoorstel, namelijk in artikel 16, eerste, tweede en derde lid. Reden hiervoor is dat het van groot belang is dat gegevens die van burgers worden verkregen bij het inloggen bij de overheid alleen gebruikt worden voor het doel waarvoor ze verstrekt worden en niet anderszins, bijvoorbeeld als handelswaar. Het voorgaande is, conform artikel 16, vierde lid, van het wetsvoorstel, uitgewerkt in de artikelen 5 tot en met 5 e van het Besluit digitale overheid. Voorts wordt het verplicht om gegevens over gebruikers en gebruik gescheiden op te slaan. Daardoor is een nadere handeling nodig om het gebruik door een burger in te zien, hetgeen nodig kan zijn om misbruik te kunnen aanpakken. Deze eis zal worden opgenomen in het Besluit identificatiemiddelen voor burgers.

De commissie merkt op dat het bovenstaande kan voorkomen worden wanneer in de kaderwet privacy by design wordt opgenomen. Wanneer privacy by design wordt geëist via de wetgeving kan vooraf getoetst worden of daaraan is voldaan. De commissie stelt dat, zoals nu de wet wordt voorgesteld, alleen de Autoriteit Persoonsgegevens achteraf kan ingrijpen, maar dan is het leed al geschied. De commissie vraagt zich daarom af waarom privacy by design niet is meegenomen in de wet.

In reactie hierop merk ik op dat het feit, dat *privacy by design* niet in het wetsvoorstel is opgenomen, niet betekent dat dit niet geldt voor eID en de aanbieders van inlogmiddelen. Dit beginsel, dat inhoudt dat er reeds bij het ontwerpen van producten en diensten voor wordt gezorgd dat persoonsgegevens goed worden beschermd, is namelijk vastgelegd in de Algemene Verordening Gegevensbescherming (AVG) en geldt per definitie voor verwerkingen van persoonsgegevens. EU-verordeningen zijn rechtstreeks toepasselijk in de lidstaten van de Europese Unie. Dat betekent dat zij niet hoeven en ook niet mogen worden omgezet in nationale regelgeving (overschrijfverbod). De – publieke en private – partijen die deel uitmaken van het eID-stelsel moeten derhalve zorgen dat zij aan de AVG voldoen. De wijze waarop dit gebeurt en de regelgeving die daarbij in acht moet worden genomen, zijn beschreven in de privacy-visie eID, waaraan de commissie eerder refereerde. *Privacy by design* maakt daarvan onderdeel uit. In dit verband merk ik nog op, dat de naleving hiervan een verantwoordelijkheid is van verwerkingsverantwoordelijken. De Autoriteit Persoonsgegevens toetst daarop niet vooraf. Uiteraard geldt dat alvorens aanbieders van inlogmiddelen tot het eID-stelsel worden toegelaten, zij aantoonbaar moeten voldoen aan de voor hen geldende eisen zoals opgenomen in de desbetreffende AMvB's en ministeriele regeling. Ook moeten zij aan de bepalingen van het Besluit digitale overheid voldoen.

De commissie merkt op dat verschillende sprekers op de op 30 juni jl. gehouden deskundigenbijeenkomst in verband met privacy en security pleitten voor een decentraal systeem en voor het werken met attributen. De commissie vraagt zich af waarom de regering niet heeft gekozen voor het opnemen van een decentraal systeem en waarom er in de kaderwet niet de mogelijkheid is opgenomen om, waar mogelijk, met attributen te werken.

In reactie op het bovenstaande merk ik op, dat in het wetsvoorstel is gekozen voor een centraal noch een decentraal systeem. Uitgangspunt is adequate privacybescherming op grond van de AVG en derhalve een goede afweging van alle privacybeginselen.

De vraagstelling centraal - decentraal ziet op een specifiek deelaspect van bescherming van persoonsgegevens, namelijk opslag van gegevens. Hiertoe worden op basis van het wetsvoorstel eisen gesteld aan alle bij het eID-stelsel betrokken – publieke en private, centraal en decentraal opererende – partijen. Uitgangspunt is: eisen stellen waar, bij wie en voor zover dit nodig is. In dit verband wordt binnen het eID-stelsel ook de mogelijkheid geboden om met attributen (gegevenssets, zie artikel 1 van het wetsvoorstel) te werken.
