Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

# 34 993 Initiatiefnota van de leden Middendorp en Verhoeven: Online identiteit en regie op persoonsgegevens

**Nr. 2 HERDRUK**[1]

## INITIATIEFNOTA

### 1. Controle over je Identiteit en Persoonsgegevens bij de Digitale Overheid

*1.1. Aanleiding*

De samenleving digitaliseert. Sneller dan de overheid. Toch gaat ook de werkwijze van de overheid – en daarmee de levens van mensen voor wie de overheid werkt – door digitalisering radicaal veranderen.

De opslag van persoonsgegevens bij digitale overheidsdiensten gebeurt vaak dubbel en gefragmenteerd. Daarnaast is het is moeilijk voor mensen zicht te houden op de juistheid van de persoonsgegevens die van hen zijn opgeslagen en wie ze gebruikt. Door onjuiste gegevens ontstaat verwarring tussen overheidsinstanties, een ondoelmatige overheid en voor mensen die het betreft geeft het soms enorme kosten. Dat maakt mensen onzeker of hun persoonsgegevens veilig zijn bij de digitale overheid en of ze veilig online met de overheid zaken kunnen doen.

Voorbeelden van hoe fouten in persoonsgegevens bij digitale overheidsdiensten tot problemen voor mensen leiden zijn er te veel. Torenhoge belastingaanslagen omdat verhuizingen niet goed verwerkt zijn door gemeenten, AOW'ers die gekort worden omdat iemand anders foutief op hun woonadres wordt ingeschreven, aanmaningen van het waterschap door ketenbesluiten die brief op brief naar een online contactadres sturen dat de mensen die het betreft zelf niet inzien. Een overheidsdienst die bepaalde persoonsgegevens niet digitaal inzichtelijk maakt voor de persoon die het betreft terwijl een andere overheidsdienst dezelfde gegevens wel online inzichtelijk maakt. Het kan soms jaren doorgaan voordat fouten ontdekt worden waardoor mensen soms in nare en uitzichtloze situaties belanden.

[1] I.v.m. correctie in Kamerstuktitel

kst-34993-2-n1
ISSN 0921 - 7371
's-Gravenhage 2018

*1.2. Doel en strekking*

Iedere Nederlander krijgt één online identiteit voor het contact met de overheid online. Een online identiteit, waarmee je veilig bij overheidsdiensten *kan* laten zien wie je bent, je meer regie krijgt over je persoonsgegevens door middel van een individuele *digitale kluis* en de overheid mensen toch kan bereiken als fysieke post niet aankomt, doordat de overheid, ook een digitaal contactadres heeft. Met die online identiteit kunnen mensen de controle terugpakken over hun identiteit en persoonsgegevens bij de digitale overheid.

Wat is de *online identiteit* waar deze initiatiefnota over gaat? Identiteit krijgt pas betekenis als er iets achter ligt. Inloggen of online identificatie krijgt pas betekenis als je daarna toegang krijgt tot *iets*, zoals persoonsgegevens. Persoonsgegevens zijn een belangrijk onderdeel van je identiteit, ook online. Niet alleen inlogcodes zijn persoonlijk, ook de gegevens die daar achter liggen. Online identiteit is dus meer dan een goed en veilig inlogsysteem.

In de fysieke wereld geeft je identiteitsbewijs toegang tot je persoonsgegevens in de basisregistratie personen (BRP). Die bepalen samen met je woonadres je identiteit bij de overheid. Door bij de digitale overheid: (1) inloggen (bijvoorbeeld via DigiD); (2) het in een individuele digitale kluis opslaan van geselecteerde persoonsgegevens; en (3) een online contactadres in samenhang te bekijken, kan iedere Nederlander ook online een identiteit krijgen.

Als er fouten zitten in persoonsgegevens kan dit, ook als er geen sprake is van fraude maar van een misverstand, tot flinke problemen leiden. Verkeerd geregistreerde woonadressen leveren bijvoorbeeld vaak problemen op.[2] Om meer zekerheid te krijgen dat overheidsdiensten met de juiste persoonsgegevens werken en om mensen meer zekerheid over de veiligheid en juistheid van hun persoonsgegevens te geven, is daarom de hier voorgestelde online identiteit nodig. Als iedereen in Nederland een online identiteit heeft, wordt de digitale overheid veiliger en wordt het makkelijker fraude te bestrijden. De digitale overheid wordt ook simpeler want er is minder kans op verwarring tussen overheidsinstellingen. Die digitale overheid wordt tot slot ook toegankelijker omdat overheidsinstellingen niet allemaal met een volledige set van persoonsgegevens hoeven te werken en het aantal «mijnomgevingen» gereduceerd kan worden.

Buiten de (semi)publieke sector wordt een individuele online identiteit en daaraan verbonden persoonlijk datamanagement razendsnel de standaard.[3] Kijk naar de toegenomen controle die mensen, mede dankzij de Algemene verordening gegevensbescherming (AVG), over hun eigen gegevens hebben bij de *social media* platformen, zoals Facebook waar mensen persoonlijke data die over hen is opgeslagen digitaal kunnen opvragen. Juist bij de overheid moeten mensen zicht hebben op hun persoonsgegevens en zoveel mogelijk kunnen inzien welke gegevens gebruikt en gedeeld worden. Immers het contact met de overheid kan je niet opzeggen, zoals dat wel kan bij commerciële bedrijven.

---

[2] Evaluatie Landelijke Aanpak Adreskwaliteit 2017, Kamerstuk, 17 050, nr. 540 (8 november 2017).
[3] Zie bijvoorbeeld https://www.wsj.com/articles/downloading-your-facebook-data-heres-what-to-look-for-1522341398 (29 maart 2018).

Het kabinet wenst in haar digitaliseringstrategie «de gebruiker centraal te stellen».[4] Omdat iedereen met de overheid te maken heeft gaat het bij de genoemde *gebruiker* om alle Nederlanders. Niet zelden blijkt, dat het centraal stellen van *de gebruiker* in de praktijk niet goed lukt.[5] Vaak komt dat doordat *de gebruiker* in de digitale wereld niet scherp is gedefinieerd. In het beste geval is de identiteit van een persoon online verdeeld over stukjes. In het slechtste geval zijn mensen in de digitale wereld identiteitloos. Het scherp bepalen van iemands identiteit online is daarom een belangrijke stap bij het centraal stellen van de *gebruiker* door de digitale overheid.

Kortom dit initiatief heeft als doel *iedere Nederlander online een identiteit en meer regie over zijn of haar persoonsgegevens te geven.*

*Wat is daarvoor nodig?*

- Het digitaal publiek domein toegankelijk met één online identiteit;
- Iedere Nederlander een digitaal contactadres dat de overheid kent;
- Persoonsgegevens zijn veilig en zoveel mogelijk onder controle van mensen zelf;
- «Eenbron» voor geselecteerde persoonsgegevens die het meeste gebruikt worden (zoals naam, leeftijd, huwelijkse staat, woonadres);
- Geselecteerde persoonsgegevens worden opgeslagen in een persoonlijke «digitale kluis». Dit wordt onderdeel van de basisregistratie personen
- Online identiteit wettelijk verankeren.

Je persoonlijke identiteit is kwetsbaar dus daar moet de overheid on- en offline met de grootste voorzichtigheid mee omgaan. Mensen willen zeker weten dat de gegevens die ze de overheid geven op papier of digitaal veilig zijn. Regelgeving en verantwoordelijkheid met betrekking tot de juistheid en beheer van persoonsgegevens moeten met de nieuwe mogelijkheden die een online identiteit geeft niet veranderen. De overheid moet daarnaast dezelfde rechten en mogelijkheden houden om justitioneel of veiligheidsonderzoek te doen. Kortom, de waarborgen die we in de fysieke wereld hebben rondom identiteitsbewijzen, persoonsgegevens en communicatie met de overheid moeten ook in de digitale wereld goed geregeld zijn. Daarom zijn de bestaande privacy- en Europese wetgeving, zoals eIDAS, om met het hoogste veiligheidsniveau bij de overheid in te kunnen loggen, cruciaal voor dit initiatief.

## 2. Voorstellen voor het creëren van een Online Identiteit

De initiatiefnemers beogen met deze nota een eerste stap te zetten naar een online identiteit door het combineren van: (1) een veilig inlogsysteem, (2) geselecteerde persoonsgegevens in een digitale kluis, (3) een digitaal contactadres. Met die drie componenten kan een online identiteit voor natuurlijke personen[6] bij de digitale overheid gecreëerd worden. Gebruikersgemak, dataveiligheid en privacy zijn daarbij cruciale randvoorwaarden. Uitvoerbaarheid evenzo.

---

[4] Zie het Algemeen Overleg Digitale Overheid van de Kamercommissie Binnenlandse Zaken (14 maart 2018).

[5] Het rapport *Hoezo MijnOverheid?* (6 september, 2017) van de Nationale ombudsman geeft van de kloof tussen de digitaliserende overheid en de Nederlander een voorbeeld.

[6] Deze initiatiefnota richt zich op natuurlijke personen. Rechtspersonen worden buiten beschouwing gelaten.

*2.1 Individuele Digitale Kluis*

Onderdeel van de online identiteit is om geselecteerde persoonsgegevens (niet alle dus) in een per Nederlander geïndividualiseerde digitale kluis op te slaan. Als geselecteerde persoonsgegevens één-op-één verbonden worden met de individuele online identiteit van individuen ontstaat voor deze specifieke persoonsgegevens één bron per individu. Omdat het om persoonsgegevens gaat moet deze individuele digitale kluis met het hoogste niveau beveiligd zijn.

Ook na de invoering van een individuele digitale kluis zullen veel gegevens, op dezelfde manier als nu bij overheidsdiensten geregistreerd worden. Denk bijvoorbeeld aan registratie van apotheekbezoek, dat opgeslagen wordt bij relevante instanties. Dat moet zo blijven. Maar door de meest gebruikte persoonsgegevens (zoals naam, leeftijd, huwelijkse staat, woonadres) in één bron (de digitale kluis)[7] op te slaan en te linken aan het individu kan veel gewonnen worden.

Een individuele digitale kluis voorkomt voor de geselecteerde persoonsgegevens dubbele opslag en fragmentatie van die gegevens. Het geeft overheidsdiensten de mogelijkheid persoonsgegevens veilig op te halen bij één bron (éénbron-gedachte) en voorkomt complexiteit die ontstaat bij het uitwisselen van de gegevens tussen overheden of het na gebruik weer centraliseren van gegevens op een centraal punt. Overheidsdiensten kunnen van dezelfde gegevens gebruik maken met meer zekerheid over de juistheid van die gegevens. De kans op fouten wordt kleiner en kosten om fouten te voorkomen of corrigeren lager.

Ten tweede wordt door de digitale kluis, in combinatie met de één-bron-gedachte, transparanter voor mensen welke persoonsgegevens (aan hem of haar gerelateerd maar door de overheid beheerd) door overheidsdiensten gebruikt worden. Het inzichtelijk maken – en zeker stellen dat overheidsdiensten deze ook gebruiken – maakt het zo makkelijker voor mensen om overheidsinstellingen op fouten te wijzen.

Buiten minder fouten, meer inzicht en makkelijker contact creëert de hier voorgestelde online identiteit en daaraan verbonden digitale kluis een mogelijkheid mensen meer regie te geven over hun persoonsgegevens. Doordat gegevensuitwisseling plaats vindt via de individuele digitale kluis – en dus via het individu zelf en niet via overheidsinstellingen onderling – maakt deze aanpak vormen van persoonlijk datamanagement mogelijk. Het wordt dan mogelijk bepaalde persoonsgegevens te selecteren en aan te geven wat wel en wat niet gedeeld wordt. Mensen zouden tot slot zelfs inzicht kunnen krijgen in welke overheidsfunctionaris welke gegevens heeft gebruikt of aan derden heeft verstrekt. Daarmee kan dus door geselecteerde persoonsgegevens in een digitale kluis bij het individu te houden worden voldaan aan eerdere verzoeken uit de Kamer om mensen de regie over hun persoonsgegevens terug te geven.[8]

*2.2 Veilig Inloggen*

Een betrouwbaar inlogmiddel om toegang tot je persoonlijke digitale kluis te krijgen, is cruciaal voor de veilige en betrouwbare werking daarvan. Hiertoe worden nu de nodige stappen gezet o.a. in het Wetsvoorstel

---

[7] Zie bijvoorbeeld Estland waar de éénbron systematiek ver is doorgevoerd: https://joinup.ec.europa.eu/sites/default/files/inline-files/eGovernment_in_Estonia_2018_0.pdf

[8] Motie van de leden De Caluwé en Koşer Kaya over *de eigen regie van burgers over hun gegevens*, Kamerstuk, 34 550 VII, nr. 20 (30 november 2016).

digitale overheid.[9] Er ligt in deze belangrijke randvoorwaarde ook een raakvlak met het identiteitsbewijs in de fysieke wereld omdat bij tweestaps-identificatie, dat voor veilig inloggen de minimumstandaard is,[10] bijvoorbeeld de chip op je paspoort de sleutel kan worden om toegang te krijgen tot je online identiteit. Ook kan gedacht kan worden aan systemen waarin je kan inloggen door je paspoort tegen je telefoon aan te houden.

*2.3 Digitaal Contactadres*

Veel mensen gebruiken de berichtenbox van de overheid mijnoverheid.nl niet. Dat hoeft ook niet want als je dat niet wilt krijg je, bijvoorbeeld van de belastingdienst, nog altijd een brief. Het bijhouden van een digitaal contactadres bij de persoonsgegevens in de basisregistratie personen en de koppeling met mijnoverheid.nl zou echter een belangrijke stap zijn naar een heldere online identiteit. Het geeft de overheid een extra mogelijkheid met Nederlanders in contact te treden anders dan door aan te bellen op hun huisadres.

*2.4 Wettelijk Verankeren Online Identiteit*

De hier voorgestelde online identiteit bestaat formeel niet, in die zin dat daar geen wettelijke basis voor is. Om de online identiteit binnen de context van bestaande wetgeving te laten functioneren zal die wettelijke basis wel gecreëerd moeten worden. Zoals ook in de fysieke wereld je identiteit wettelijk is vastgelegd, is het nodig het concept dat iedere Nederlander een online identiteit heeft en de fundamenten van die identiteit (geselecteerde persoonsgegevens in een individuele digitale kluis en het registreren van een digitaal contactadres voor iedere Nederlander), in wetgeving te verankeren. Of daar een nieuwe wet voor moet komen dan wel of er bestaande wetgeving voor moet worden gewijzigd, dan wel beide, zal moeten worden uitgewerkt.

## 3. De huidige stand van zaken en uitvoering

Door aan het Wetsvoorstel digitale overheid, de adviezen van de Digicommissaris[11] en overheidsinspanningen als BRP en mijnoverheid.nl een digitale kluis en een digitaal contactadres voor iedere Nederlander toe te voegen kan een online identiteit gecreëerd worden. Het gaat de initiatiefnemers om het creëren van een online identiteit met behulp van het bestaande, niet om een geheel nieuwe aanpak. Hieronder wordt het huidige wettelijk kader en de stand van zaken beschreven.

*3.1 Wettelijk Kader en Stand van Zaken*

Het op een veilige manier registreren van alle Nederlanders en deze van een identiteitsbewijs voorzien, zijn onderdeel van de kerntaken van de rijksoverheid. Registratie van persoonsgegevens, het identiteitsbewijs (zoals een paspoort) en woonadresregistratie zijn dan ook vastgelegd in wetgeving.

---

[9] Wetsvoorstel Digitale Overheid, Kamerstukken II, 34 972, nr. 2.

[10] Motie van het lid van Engelshoven over *bevorderen dat mensen met tweestaps-identificatie inloggen via DigiD*, Kamerstuk, 34 725 VII, nr. 9 (21 juni 2017).

[11] Digicommissaris B. Eenhoorn was van 2014 tot begin 2018 aangesteld om de regie te voeren op de (door)ontwikkeling van de Generieke Digitale infrastructuur. Zie Digiprogramma 2015, 2016/17 en 2018.

### *Digitaal contact*

In de Wet elektronisch berichtenverkeer Belastingdienst (artikel X, lid 1) staat:
«*Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties draagt zorg voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing alsmede van voorzieningen voor elektronische authenticatie en elektronische registratie van machtigingen.*» Mijnoverheid.nl speelt een centrale rol in het digitaal contact tussen overheden en mensen. Via deze website sturen overheidsinstellingen berichten naar natuurlijke personen. Op mijnoverheid.nl is voor alle Nederlanders boven de veertien een emailinbox aangemaakt. Deze inboxen die in feite een digitaal contactadres kunnen zijn, zijn niet gekoppeld aan de basisregistratie personen.

### *Basisregistratie Personen en AVG*

In de Wet basisregistratie personen (artikel 1.3, lid 1 en 2) staat:
«*De basisregistratie heeft tot doel overheidsorganen te voorzien van de in de registratie opgenomen gegevens, voor zover deze gegevens noodzakelijk zijn voor de vervulling van hun taak*». En tevens «*De basisregistratie heeft mede tot doel derden te voorzien van de in de registratie opgenomen gegevens, in bij of krachtens deze wet aangewezen gevallen.*» Persoonsgegevens worden bij gemeenten verzameld en digitaal opgeslagen. Op een centrale plek worden deze gebundeld waarna ze onder strenge voorwaarden en voor specifieke taken door afnemers, zoals de Sociale Verzekeringsbank, worden gebruikt.

In de Algemene verordening gegevensbescherming[12] (artikel 15 en 16) wordt het recht van inzage en recht om te wijzigen van persoonsgegevens bepaald. Verder worden in de AVG het recht om in te zien, recht om vergeten te worden, recht om gegevens over te dragen en recht op informatie vastgelegd. Het recht op inzage is de laatste tijd sterk verbeterd doordat op MijnOverheid.nl mensen kunnen inzien welke persoonsgegevens in de basisregistratie personen staan. Zij kunnen daar niet zien welke instellingen zich daarop baseren. Op www.wiekrijgtmijngegevens.nl kan een algemene beschrijving gevonden worden van welke overheidsorganisaties welke persoonsgegevens gebruiken. De combinatie – welke individuele gegevens door welke overheidsdienst worden gebruikt – is dus niet inzichtelijk op een centraal punt. Er zijn verschillende manieren om dit inzichtelijk te maken.

Naar aanleiding van verzoeken van de Kamer om mensen meer regie over hun persoonsgegevens te geven zijn onderzoeken gedaan naar de mogelijkheden daartoe. Daarbij was het uitgangspunt vaak informatie-uitwisseling buiten het individu over wie de gegevens gingen om. Hier wordt echter gepleit voor meer informatie-uitwisseling via het individu. De commissie Snellen keek juist wel naar een meer centrale positie voor het individu door voor te stellen persoonsgegevens aan het individu te koppelen. Zij adviseerde al in 2001 om een individuele digitale kluis onderdeel van de modernisering van de basisregistratie te laten zijn.[13] Dat is niet gebeurd en het langdurige project om de basisregistratie te

---

[12] Verordening (EU) nr. 2016/679 (27 april 2016) betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

[13] Commissie Modernisering GBA, GBA in de Toekomst. *Gemeentelijke Basis Administratie persoonsgegevens als spil voor de toekomstige identiteits-infrastructuur* (Commissie Snellen, maart 2001).

moderniseren is in juli 2017 gestopt.[14] Er wordt gewerkt aan een nieuw langetermijn plan voor de toekomst van de basisregistratie personen.[15]

***eID/Inloggen***

In Nederland kunnen alleen Inlog- of identificatiesystemen die behoren tot een door de Europese Commissie aangemeld en goedgekeurd stelsel in de wet opgenomen worden. In 2004 heeft de EU de lidstaten verplicht een chip in het paspoort op te nemen.[16] Er is nieuwe Europese wetgeving op komst over beveiliging van identiteitskaarten en verblijfsdocumenten. In de digitale wereld is in Europa de Europese verordening eIDAS leidend. Daarin worden standaarden vastgesteld voor inlogprocedures. Lidstaten mogen binnen de standaarden van eIDAS bepalen hoe het systeem vorm te geven.

Inlog- of identificatiesystemen staan in Nederland onder toezicht van het Agentschap Telecom. In het wetsvoorstel digitale overheid (artikel 9 lid 1) staat: «*Onze Minister wijst publieke identificatiemiddelen aan als toegelaten identificatiemiddelen op de betrouwbaarheidsniveau's substantieel of hoog indien deze identificatiemiddelen naar zijn oordeel in voldoende mate voldoen aan de krachtens de eIDAS-verordening vastgestelde technische specificaties en procedures.*»

Het huidige inlogsysteem dat door de overheid onderhouden wordt (DigiD), wordt nu op het veiligheidsniveau «substantieel» gebruikt. De ambitie is dat dit naar niveau «hoog» gaat. Daarmee zou het ook geschikt kunnen worden voor zeer gevoelige informatie (zoals persoonsgegevens). Het kabinet heeft de Kamer toegezegd dat het niveau «hoog» er snel komt als onderdeel van de multimiddelenstrategie.[17] [18] [19]

*3.2 Uitvoering*

Dit initiatief is bedoeld als toevoeging aan de huidige inspanningen een digitale overheid te bouwen maar kan in die huidige inspanningen een belangrijke rode draad worden. Er wordt hier gepleit om naar de verbanden tussen eID, BRP en mijnoverheid.nl te kijken en daar een individuele digitale kluis en een online contactadres aan toe te voegen. Door het project klein te houden, in stappen uit te voeren en vooral in te passen in het bestaande kan de hier voorgestelde online identiteit succesvol concreet gemaakt worden.

De rijksoverheid hoeft niet alles zelf te doen. Zij moet wel standaarden en waarborgen creëren. Waar dat niet anders kan, of waar operationele betrokkenheid belangrijke kennis oplevert, kan de overheid zelf de benodigde toepassingen ontwikkelen. Dat moet zoveel mogelijk techniek-neutraal. Het project mensen een online identiteit te geven kan de overheid ook veel kennis en kunde opleveren. Hierbij zullen wel soms

---

[14] Motie van het lid Middendorp c.s.: *onderzoeken hoe de operatie BRP op een ordentelijke wijze kan worden beëindigd,* Kamerstuk, 27 859, nr. 106 (6 juli 2017).

[15] Motie van het lid Middendorp over *de basisregistratie personen toekomstvast maken*, Kamerstuk, 34 775 VII, nr. 13 (16 november 2017) en Aanpak toekomst BRP stelsel, Kamerstuk, 2018Z1387 (10 juli 2018).

[16] Verordening (EG) nr. 2252/2004 (13 december 2004) betreffende normen voor de veiligheids-kenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten.

[17] Zie hiervoor het Algemeen Overleg Basisregistratie Personen (BRP) en programma eID van de vaste Kamercommissie Binnenlandse Zaken (5 Juli 2017).

[18] Zie brief van de regering «Impuls eID» Kamerstuk, 26 643, nr. 419 (25, augustus 2016).

[19] Motie van het lid de Caluwé over *in ieder geval één publiek authenticatiemiddel introduceren in 2017*, Kamerstuk, 26 643, nr. 376 (8 december 2015).

bestaande belangen van gevestigde partijen binnen de rijksoverheid en ICT toeleveranciers en de soms bestaande «doe-het-zelf-cultuur» doorbroken moeten worden.

Ook zullen burgerorganisaties en belangengroepen bij de verschillende stappen in de uitvoering van dit plan betrokken moeten worden. Het is cruciaal om niet alleen technische oplossingen te zoeken, maar ook zorgen die leven bij het operationaliseren van de online identiteit concreet te adresseren. Ten eerste, dataveiligheid. Juist omdat dataveiligheid voor de digitale overheid cruciaal is, is het hier voorgestelde nodig. De manier waarop banken zich online hebben georganiseerd is een interessant voorbeeld. Door individueel onzorgvuldig omgaan met pinpassen en pincodes kunnen incidenten ontstaan, maar er is vertrouwen in het systeem als geheel en veel mensen zijn na een initiële aarzeling overgestapt naar online bankieren. Door gebrek aan een veilige online identiteit sturen mensen nu vaak een gescand identiteitsbewijs of uittreksel uit de basisregistratie personen per *email*. Dit terwijl email een onveilig medium is.[20] Het is belangrijk steeds de voordelen van vernieuwing concreet te maken maar mensen tegelijkertijd de tijd geven te wennen en ze waar nodig te ondersteunen. Tot slot, kunnen sommige mensen niet mee in de digitale wereld. Daarom moet steeds uitgegaan worden van mensen en niet het «systeem». Mensen die digitaal niet mee kunnen moeten de mogelijkheid hebben om op de oude manier met de overheid te blijven communiceren.

## 4. Financiële consequenties

Onderzoek naar internationale voorbeelden kan met het bestaande apparaat. Kosten voor ontwikkeling en om de samenhang van het project te waarborgen moeten bij bestaande projecten kunnen worden ondergebracht. Er kan naar verwachting van de initiatiefnemers grotendeels gebruik worden gemaakt van de bestaande infrastructuur, plannen en budgetten voor de ontwikkeling van eID, DigiD, de basisregistratie personen en mijnoverheid.nl. Nieuwe kosten voor het ontwikkelen van de digitale kluis, kosten om de samenhang te waarborgen en de extra onderhoudskosten op lange termijn zullen naar verwachting laag zijn ten opzichte van gebudgetteerde kosten voor de ontwikkeling van de digitale overheid.

## 5. Beslispunten

Moet de overheid zich wel bemoeien met dit soort ingewikkelde vraagstukken in de digitale wereld? Ja, de overheid heeft bij het garanderen van een veilige identiteit online een rol. Net als in de fysieke wereld. Het alternatief is niet aantrekkelijk. Met *big data* (digitale data-analysetechnieken) is het inmiddels mogelijk om, op elk moment, een identiteit van iemand op te bouwen op basis van op het internet aanwezige informatie. Als de rijksoverheid niets doet, kan het zo maar zijn dat in de toekomst de grote internetplatformen je identiteit in de digitale wereld beter kunnen vaststellen dan de overheid.

Daarom vragen de initiatiefnemers de Kamer in te stemmen met zijn verzoek aan het kabinet hier een apart project voor op te zetten en concreet uit te werken om zo *iedere Nederlander online een identiteit en meer regie over zijn of haar persoonsgegevens te geven*, door middel van:

---

[20] De overheid verstrekt speciale hoesjes om BSN nummers af te schermen. Zie: https://www.binnenlandsbestuur.nl/bestuur-en-organisatie/nieuws/gemeenten-delen-id-hoesjes-uit.9097733.lynkx

*Wat is daarvoor nodig?*

– Het digitaal publiek domein toegankelijk met één online identiteit;
– Iedere Nederlander een digitaal contactadres dat de overheid kent;
– Persoonsgegevens zijn veilig en zoveel mogelijk onder controle van mensen zelf;
– «Eenbron» voor geselecteerde persoonsgegevens die het meeste gebruikt worden (zoals naam, leeftijd, huwelijkse staat, woonadres);
– Geselecteerde persoonsgegevens worden opgeslagen in een individuele «digitale kluis». Dit wordt onderdeel van de basisregistratie personen;
– Online identiteit wettelijk verankeren.

Middendorp
Verhoeven