



Understanding what makes people tick

Barrières van digitaal persoonsgegevens delen door middel van regietoepassingen

Rapportage van kwalitatief onderzoek

Projectnummer: 2022076 Referentienummer

Mens Centraal: 4266717

Amsterdam, 18 augustus 2022 – versie 2

Inhoudsopgave



Introductie	3
• Onderzoeksdoelstellingen	4
• Onderzoeksverantwoording	5
• Leeswijzer	6
Conclusies & aanbevelingen	8
• Conclusies	9
• SWOT regietoepassingen	11
• Typologie burgers en regietoepassingen	12
• Aanbevelingen	13
Resultaten	14
• Context	15
• Kennis // het delen van persoonsgegevens	16
• Gedrag // beschermen van (online) persoonsgegevens	17
• Typologie burgers en online privacy	19
• Drempels en drijfveren regietoepassingen	20
Bijlagen	22
• Stimulusmateriaal	23

Introductie

Onderzoeksdoelstellingen



Doel

Inzicht krijgen in de barrières om gebruik te maken van regietoepassingen waarmee persoonsgegevens worden gedeeld met derden en hoe deze (eventueel) te slechten onder hoofdzakelijk de doelgroep sceptici en minder digitaal vaardigen

Meer specifiek inzicht in:

- Huidige kennis, houding en gedrag ten aanzien van het delen van persoonsgegevens
- Gepercipieerde voor- en nadelen van het delen van persoonsgegevens, zowel digitaal als niet-digitaal
- Welke factoren en overwegingen weerhouden burgers om persoonsgegevens uit overheidsbronnen digitaal te delen met derden
- Verwachtingen, wensen en behoeften ten aanzien van manieren van persoonsgegevens delen via een regietoepassing
 - Op het vlak van: veiligheid, gemak, privacy, betrouwbaarheid etc.
- Randvoorwaarden om gebruik te maken van regietoepassingen
 - Wat is doorslaggevend?
 - Zijn er drempels te slechten?
 - Zijn er drempels die onoverkomelijk zijn?



Output

- Aanknopingspunten om barrières te slechten en het gebruik van regietoepassingen te bevorderen

Onderzoeksverantwoording

Veldwerk

Het onderzoek is op 7, 11, 12, 13, 20 en 21 juli 2022 uitgevoerd online via MS Teams én face-to-face bij MARE in Amsterdam.

Methode

Het onderzoek is uitgevoerd aan de hand van 19 single interviews en 3 duo-interviews van 60 minuten (8 interviews face-to-face, 14 interviews online).

Stimulusmateriaal

Er is gebruik gemaakt van 3 use cases: energietoeslag, huurwoning vrije sector en pensioeninzicht (zie bijlagen). Dit om de regietoepassingen te verduidelijken met voorbeelden en daarmee de drempels en barrières (nog) meer bloot te leggen.

Selectiecriteria

Voor alle respondenten geldt:

- Zijn in de leeftijd 21-66 jaar
- Zijn pragmatisch of sceptisch (op basis van stellingen)
 - Pragmatici zijn mensen die kunnen twifelen om hun persoonsgegevens (online) te delen (n=18).
 - Sceptici zijn mensen die bezorgd zijn over hun online privacy en niet bereid zijn om hun persoonsgegevens (online) te delen. (n=4).

Verder een spreiding op:

- Geslacht
- Leeftijd
- Woonplaats (heel NL, behalve de fysieke gesprekken)
- Opleidingsniveau en beroep
- Inkomen
- Huishoudsamenstelling (alleenwonend, samenwonend, wel/geen thuiswonende kinderen)
- Minder digitaal-vaardigen (op basis van stellingen) (n=7)
- Minder taal-vaardigen (op basis van stellingen) (n=5)
- Enkele mensen die kritisch zijn ten aanzien van de (online) overheid (n=6).

Leeswijzer | 1



Leeswijzer rapportage

Dit document bevat een weergave van de belangrijkste conclusies en nadere bevindingen. Het document is als volgt opgebouwd:

- Het inhoudelijke deel van de rapportage begint met de conclusies, gevolgd door de onderzoeksresultaten.
- De resultatensectie vangt aan met een slide met betrekking tot de context en de onderverdeling van de doelgroep.
- De resultatensectie gaat vervolgens dieper in op de inzichten met betrekking tot kennis en gedrag omtrent het delen van (online) persoonsgegevens en daarna worden de drempels en drijfveren voor het gebruik van regietoepassingen besproken.
- In de bijlage een impressie van de use cases die leidend waren in de gesprekken.

Disclaimer

Kwalitatief onderzoek is verkennend en inventariserend van aard. Uitkomsten van dergelijk onderzoek moeten dan ook in de eerste plaats worden gezien als indicatief en hypothesevormend en niet als (cijfermatig bewezen) feiten. Ter wille van de leesbaarheid wordt in deze rapportage de stellende vorm gebruikt.

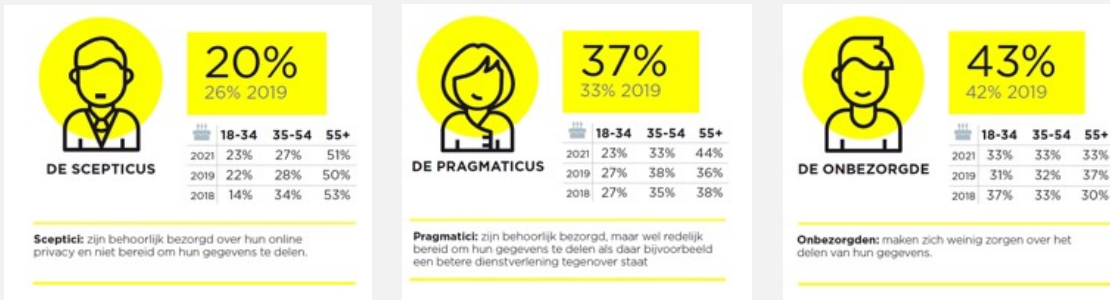
De bevindingen in de resultatensectie zijn gebaseerd op wat de respondenten tijdens dit onderzoek hebben gezegd of aangegeven.

MARE

MARE voert onderzoek uit binnen het kader van ISO 20252:2019 (kwaliteit onderzoek) en ISO 27001:2017 (informatiebeveiliging). MARE conformeert zich tevens aan de richtlijnen van brancheorganisatie MOA wat betreft persoonsgegevens. Daarnaast voldoet MARE aan de overheidsnorm Baseline Informatiebeveiliging Overheid (BIO).

Leeswijzer | 2

Doelgroep verschillen



De doelgroep is gebaseerd op eerder onderzoek van DDMA privacy monitor 2021 waarin een consumentensegmentatie (zie afbeeldingen) is beschreven. In dit huidige kwalitatieve onderzoek hebben we gestreefd om alleen sceptici en pragmatici te rekruteren. Tijdens het onderzoek bleek dat er een dunne scheidslijn is tussen de onbezorgde en pragmaticus. Uiteindelijk zijn daarom de drie verschillende types in de gesprekken voorbijgekomen. In het rapport hebben we, waar relevant, nuances per doelgroep weergegeven en de typologie verder aangevuld met inzichten uit ons onderzoek.

Regietoepassing

Over het algemeen zijn mensen niet bekend met regietoepassingen. Tijdens de gesprekken hebben we respondenten op weg geholpen met een korte omschrijving van regietoepassingen:

Een app waarin jouw persoonsgegevens van verschillende overheidsinstanties (UWV, Belastingdienst, basisregistratie persoonsgegevens, etc.) op een beveiligde manier per partij opgehaald kunnen worden en in afzonderlijke 'postvakjes' worden gestopt. De instantie heeft alleen toegang tot het eigen 'postvakje' en kan niet in andere delen van de app rondsnoeven. Als het ware een kluis waarvan de burger de bewaarder is en af en toe toestemming geeft om een kijkje te nemen in een 'postvakje'.

Inloggen gaat via DigiD waarna de burger op een persoonlijke pagina terecht komt. Vervolgens kan worden bepaald welke gegevens opgehaald moeten worden, ook hiervoor dient elke keer ingelogd te worden met DigiD, waarna vervolgens de gegevens worden verzameld. Hierna kan de burger aangeven met welke instantie (bijvoorbeeld een woningbouwvereniging) de gegevens gedeeld mogen worden.

De burger geeft hiervoor (eenmalig) toestemming voor een afgesproken periode en is zelf verantwoordelijk voor het beheer. Gegevens worden gedeeld aan de hand van certificaten/ dataminimalisatie (dus niet de exacte hoogte van het inkomen, maar alleen een indicatie of het inkomen boven/onder een bepaalde norm is).

Conclusies & aanbevelingen

Conclusies | 1



De belangrijkste leerpunten

- Iedereen heeft zijn administratie online geregeld, want per post komt immers ook weinig meer binnen. Dat dit online staat 'opgeslagen' werkt meestal naar tevredenheid; gegevens zijn eenvoudig terug te vinden. Toch overschatten mensen op andere gebieden hun eigen digitale vaardigheden. In de realiteit zijn ze onzeker over hun eigen digitale kunnen en houden ze zich daarom liever vast aan wat ze kennen en voor hen goed werkt.
- Over het algemeen is iedereen goed op de hoogte van de gevaren van (online) gegevens delen. Dit komt zowel door negatieve ervaringen (zelf of uit de omgeving) als de 'opvoeding' door banken, nieuwsberichten en televisieprogramma's.
- Vooral ouderen zijn voorzichtiger in het delen van hun 'feitelijke' data, zoals NAW-gegevens, bankrekeningnummer etc. Terwijl jongeren zich meer zorgen maken om hun online identiteit (content op social media en digitale sporen die je achterlaat).
- Mensen treffen verschillende maatregelen om hun gegevens te beschermen, denk aan cookies niet of deels accepteren, niet klikken op linkjes in de e-mail en wachtwoorden regelmatig veranderen. Daarbij zijn er een aantal indicatoren die duiden op een 'veilige' omgeving, zoals slotje in de webbrowser, bekende afzender en DigiD.
- Motivatie om (online) gegevens te delen is voornamelijk: 'ik heb niks te verbergen', 'je moet mee met de tijd' en gemak.
- De overheid wordt gezien als een betrouwbare bron om (online) gegevens mee te delen. Er is een groot vertrouwen, omdat de overheid geen commerciële belangen heeft en er wordt verwacht dat strenge AVG wet- en regelgeving geldt. En net zoals in voorgaande onderzoeken naar regie op gegevens, speelt DigiD ook een belangrijke rol in het vertrouwen.
- DigiD wordt gezien als heel veilig en betrouwbaar door de twee-stapverificatie, is landelijk al jaren in gebruik (met Corona ook veelvuldig gebruikt) en er zijn goede ervaringen met de toepassing. Kortom, DigiD is een 'heilige graal' voor veilig inloggen en persoonsgegevens delen.

Conclusies | 2



Typen: scepticus, pragmaticus en onbezorgde

Er is een aantal belangrijke verschillen tussen de type burgers. Allereerst, maakt de onbezorgde zich letterlijk weinig zorgen om (online) privacy en beschermen van gegevens. De pragmaticus en scepticus maken zich, zoals verwacht, al meer 'zorgen'. De pragmaticus houdt zich vooral bezig met het beschermen van gegevens vanwege mogelijk diefstal en (identiteits-)fraude. Zodra de afzender betrouwbaar is, dan worden gegevens makkelijk gedeeld onder het mom van 'ik heb niks te verbergen'. Daarentegen is de scepticus meer op zijn hoede, omdat het zijn gegevens zijn, partijen commerciële belangen hebben (doorverkopen van data) en daarbij het gevoel van controle mist bij het delen van zijn eigen gegevens. Hierbij is men dus voornamelijk sceptisch tegenover commerciële partijen en sociale media en niet zozeer ten opzichte van de overheid.

Al met al geldt voor alle drie de typen dat teveel nadenken over het beschermen van gegevens ook het leven te moeilijk al dan niet onmogelijk maakt. Kortom, iedereen deelt wel (online) persoonsgegevens onder bepaalde voorwaarden.

Regietoepassingen

Mensen staan dan ook open voor het gebruik van regietoepassingen, maar er is wel een aantal drempels. De grootste drempel is het gebruik van een app.

Op de volgende twee slides gaan we dieper in op drempels en drijfveren van regietoepassingen. Als eerste staat dit weergegeven in een SWOT-analyse waarbij de toepassing van regiegegevens in een bredere context is geplaatst. Vervolgens wordt per type burger de drempels en drijfveren ten aanzien van regietoepassingen in kaart gebracht.

SWOT regietoepassingen



Sterkten

- Tijdbesparing ten opzichte van handmatig invullen
- Gemak ten opzichte van handmatig invullen
- Dataminimalisatie; geen onnodige informatie delen
- Toestemming geven voor tijdelijke/ eenmalige toegang
- Gebruik van DigiD
- Noodzaak van het regelen
- QR-code (gemak)

Zwakten

- Onbekende toepassing
- Er is nog veel uitleg nodig om het begrip van regietoepassingen te laten landen
- Een app als enige mogelijkheid om gebruik te maken van de toepassing
- Datacentralisatie; verhoogd risico alle belangrijke informatie bij elkaar
- Bewaartermijn van 90 dagen wordt ervaren als (te) lang
- QR-code (minder veilig/ onbekend)

Kansen

- Meer bekendheid van en uitleg over regietoepassingen; opvoeden burgers
- Positieve ervaringen van mensen uit de omgeving
- Overheidsbron als (mede-)afzender
- Alternatieven naast de app, zoals een webversie (in browser)
- Mogelijkheden tot (telefonisch) contact
- Routing richting regietoepassing: vanuit een bekende afzender/ omgeving (denk aan: website) doorgesluist worden; keuze voor het blijven in 'vertrouwde omgeving', zoals de webbrowser.

Bedreigingen

- Digitale- en leesvaardigheid van burgers: weinig zelfvertrouwen; angst om het fout te doen.
- Digitale apparaten niet compatible/ up-to-date: weinig geheugen voor apps
- Technologie is ongrijpbaar en daardoor minder gevoel van controle
- Negatieve publiciteit rondom het delen van (online) persoonsgegevens (hacken, phishing, programma's zoals Kassa etc.)
- Routing: onbekend afzender in combinatie met doorkliklinkjes in e-mail

Typologie burgers en regietoepassingen



Scepticus

Drempel

- Onbekende toepassing
- App (en geen web omgeving)
- Datacentralisatie
- Bewaartermijn
- Negatieve publiciteit

Drijfveer

- Betrouwbare afzender
- Gebruik DigiD
- Dataminimalisatie
- Toestemming verlenen voor tijdelijke/eenmalige toegang



Pragmaticus

Drempel

- Onbekende toepassing
- App (en geen web omgeving)
- QR-code
- Negatieve publiciteit

Drijfveer

- Betrouwbare afzender
- Gebruik DigiD
- Gemak
- Tijdwinst
- Toestemming verlenen voor tijdelijke/eenmalige toegang
- Positieve ervaringen omgeving



Onbezorgde

Drempel

- Onbekende toepassing

Drijfveer

- Gemak
- Tijdwinst
- QR-code
- Positieve ervaringen omgeving

Aanbevelingen



Ondanks dat er meerdere drempels zijn die mensen momenteel ervaren om gebruik te maken van regietoepassingen, zijn er ook veel drijfveren. Daarbij denken wij dat de drempels wel zijn te slechten, met name door een betrouwbaar en veilig gevoel te geven. Hierdoor kan een grotere groep, met name minder digitaal vaardigen, geholpen worden om de stap te zetten richting het gebruik van regietoepassingen. Hieronder geven wij suggesties voor het slechten van de drempels. Deze zijn uiteraard niet dwingend, maar richtinggevend en ter inspiratie.

- Besef dat de doelgroep zijn eigen digitale kunnen overschat en vaak minder digitaal vaardig is dan in eerste instantie lijkt. Een eenvoudige en duidelijke uitleg, stapsgewijs is daarbij passend. Een voorbereidingslijst is ook handig ('dit moet je bij de hand hebben'). 'hoe makkelijker, hoe veiliger'.
- Kijk of er mogelijk alternatieven zijn voor het gebruik van een app. Denk aan een web versie in de browser. Hierdoor hoeven mensen de 'vertrouwde' omgeving niet te verlaten en kan dit ook op de laptop uitgevoerd worden. Dit geeft in ieder geval de minder digitaal vaardige meer vertrouwen om het te kunnen gebruiken en geeft een veilig(er) gevoel (niet op mobiel).
- Maak voor het gebruik van de regietoepassing duidelijk dat de gegevens worden opgehaald door middel van inloggen via DigiD. Dit geeft een veilig gevoel en voelt als betrouwbaar.
- Het is in de uitleg en communicatie rondom regietoepassingen belangrijk om duidelijk te maken dat toestemming wordt verleend voor tijdelijke toegang en dat partijen niet elkaars informatie kunnen inzien en gebruiken.
- Voor de scepticus kan meer informatie gegeven worden over dataminimalisatie (certificaten etc.). Besef wel dat voor de anderen dit potentieel juist verwarrend kan zijn (ongrijpbaar/ complex) bij een eerste keer gebruik van een regietoepassing.
- De voordelen van tijdswinst en gemak hoeven niet expliciet benoemd te worden. Dit kan juist voelen als bemoeizuchtig en een verkooppraatje, zoals sommigen zeiden 'ik bepaal dat zelf wel'. Een symbool met een klok en tijdindicatie zegt al genoeg.
- En de route naar de regietoepassing is ook belangrijk. Voorkom in ieder geval dat mensen een e-mail ontvangen van een onbekende afzender met een doorkliklink.

Resultaten

Context

Online administratie

Merendeel van de respondenten geeft aan alle administratieve regelzaken online te regelen en zich voldoende digitaal vaardig te achten. Vooral de doelgroep onbezorgde en pragmaticus hebben hun administratieve zaken verspreid opgeslagen, zoals ze 'binnenkomen' en stopt er weinig moeite in: het staat in hun e-mail inbox, opgeslagen op hun computer en in online portalen van bedrijven/ instanties. De scepticus heeft administratie meer georganiseerd in mapjes bij elkaar, zowel op computer als ook in een Cloud/ harde schijf.

Al pratend blijkt dat belangrijke (financiële) documenten nog steeds geprint worden door de meesten, met name als back-up en 'voor de zekerheid', denk aan jaaropgaven, Belastingaangifte, salarisstroken en contracten: *"stel dat er toch iets online gebeurt en je het kwijt bent."*

Overschatting van eigen digitale vaardigheden

Gedurende de gesprekken geeft een deel van de doelgroep aan, met name ouderen, zich niet voldoende vertrouwd te voelen met alle online aanpassingen en nog wennen aan de verandering van digitalisering. Hoewel de coronapandemie ervoor heeft gezorgd dat ook deze doelgroep meer gebruik maakt van online toepassingen (bijv. gebruik van DigiD voor testen en vaccinatie; minder contant geld en meer online bankieren; digitaal lesgeven/vergaderen, etc.), houden ze zich graag vast aan wat ze al kennen (ook op digitaal vlak) en voelen zich onzeker over het gebruik van nieuwe (online) toepassingen.

Daarentegen is er wel een verschil met jongeren die zijn opgegroeid met digitale oplossingen en ook niet anders kennen ('digital natives'). Voor hen voelt het gebruik van online omgeving niet als nieuw of een verandering en passen zich makkelijker aan in de digitale wereld.



Kennis | het delen van persoonsgegevens


Negatieve ervaringen

De doelgroep is zich ervan bewust dat ze iets met privacy en beschermen van (online) persoonsgegevens moeten doen. Dit besef wordt steeds groter mede doordat iedereen iemand van dichtbij kent of zelf weleens een negatieve ervaring heeft meegemaakt rondom phishing en fraude. Daarbij worden burgers tegenwoordig opgevoed door banken waar je op moet letten, maar ook programma's zoals Kassa en Opgelicht maken je bewuster van de 'gevaren' rondom het online delen van persoonsgegevens.

Privacy: online data vs. online identiteit

In de beleving van de burger bestaan online persoonsgegevens uit twee soorten data: enerzijds 'feitelijke' data, zoals NAW-gegevens, geboortedatum, e-mailadres, bankrekeningnummer, etc. Anderzijds gaat het om online identiteit en content die men post op sociale media en de digitale sporen die dit achterlaat, denk aan: een afgeschermd profiel op Instagram/ Facebook en niet zomaar iets delen qua foto's of filmpjes.

Opvallend is dat voornamelijk ouderen de privacy van online data belangrijk vinden: *"het is niet altijd nodig om alles in te vullen in een account."* Terwijl jongeren zich meer druk maken om hun online identiteit; het delen van 'feitelijke' data staan ze nauwelijks bij stil: *"Ik post geen foto's op Instagram, anders ziet mijn baas dat, maar heb geen moeite om ergens mijn adres en telefoonnummer achter te laten of een kopie van mijn paspoort te mailen".*



"Ik krijg mailtjes van mijn bank als er weer phishingmail rondgaat en waar ik op moet letten. Inmiddels ben ik daar zelf ook alert op."

"Ik ben wel bang voor fraude. Je hoort het zo vaak. Ik ben ook niet heel handig met computers. Als ik dan ook de programma's zoals Oplichting en Radar kijk, dan denk ik dat kan mij ook zo overkomen."

Gedrag | beschermen van persoonsgegevens 1



De drijfveer van mensen verschilt als het gaat om het beschermen van hun online persoonsgegevens en daarmee wel of niet hun persoonsgegevens (online) delen. Hierbij speelt de digitale- en leesvaardigheid ook een belangrijke rol: *"ik weet niet zo goed hoe ik mijn gegevens moet beschermen en of ik het kan vertrouwen"; "Als de gegevens op mijn telefoon of laptop staan, dan zijn ze toch van mij?"*

Belemmeringen

Niet iedereen is even alert (vooral pragmaticus en onbezorgde) om (online) persoonsgegevens te beschermen, omdat:

- *'Ik heb niks te verbergen'.*
- Het gevoel bestaat dat ze één van de velen zijn *'aan mijn gegevens hebben ze toch niks.'*
- *'ze weten toch wel alles van mij'.*
- Daarbij is ook gemak een reden om niet altijd alert te zijn: *"Ik vind het vervelend dat mijn zoekgedrag wordt bijgehouden en de gepersonaliseerde advertenties storen me, maar dat neem ik voor lief. Ik ga niet alle voorwaarden lezen of cookies uitzetten dat kost me teveel moeite."*
- En als laatste, is er het gevoel dat het onmogelijk is om altijd alert te zijn of vraagt, zowel de scepticus als pragmaticus/onbezorgde, zich af: moet je dat wel willen zijn: *"soms moet je het ook wel loslaten, anders heb je geen leven meer of maak het je het jezelf wel heel moeilijk."*

Drijfveren

Drijfveren om wel online persoonsgegevens te beschermen en voorzichtiger te zijn met het delen van (online) persoonsgegevens:

- Het zijn mijn gegevens: *"het is een stukje van mij, dat gaat een bedrijf niks aan."*
- Persoonlijke data wordt gebruikt in eigen belang van (commerciële) bedrijven, bijvoorbeeld het doorverkopen van data.
- Bang voor diefstal, (identiteit) fraude. Daarom zijn de meesten terughoudend met het delen van bankrekeningnummer, creditcardgegevens en BSN-nummer.
- Technologie is complex, ongrijpbaar en daardoor is er, in perceptie, ook minder gevoel van controle (in vergelijking met papier): *"je weet niet wat ermee gebeurt"; "ik snap niet zo goed hoe het werkt." ; "die gegevens zweven ergens rond."*

Gedrag | beschermen van persoonsgegevens 2



Onbekend maakt onbemind

Mensen gaan op zoek naar signalen en indicatoren die een veilig gevoel geven: een slotje in de webbrowser, een betrouwbare afzender en DigiD. Betrouwbare afzenders zijn met name grote en bekende bedrijven, zoals Bol.com, Amazon, Booking, banken, verzekeraars en de overheid. Een bedrijf is, naast bekend en groot, ook betrouwbaar als er een mogelijkheid is om contact met het bedrijf te hebben. Als het dan fout gaat, dan kan er altijd nog gebeld worden.

Vertrouwen in overheidsbronnen en gegevens delen

Er is een groot vertrouwen in de overheid als het gaat om zaken online regelen en gegevens delen via de overheid. Ondanks dat refereren sommigen wel aan de toeslagenaffaire. Het vertrouwen is groot, omdat de overheid geen commerciële belangen heeft én privacy wet- en regelgeving hanteert waar ze zich aan moeten houden. Tevens is met de komst en het gebruik van DigiD er een (nog) groter vertrouwen.

Andere **maatregelen** die mensen treffen **om gegevens te beschermen** zijn:

- Antivirus software op de computer
- Niet klikken op linkjes in een e-mail én het e-mailadres checken van mailtjes van bedrijven/organisaties (potentieel phishing).
- Wachtwoorden regelmatig veranderen én de scepticus heeft verschillende wachtwoorden per account. De wachtwoorden worden meestal opgeschreven in een schriftje thuis. Een schrift kan niet gehackt worden, dus dat voelt veilig (pragmaticus). En sommigen van de sceptici maken gebruik van wachtwoordkluizen online.
- Cookies op websites niet accepteren of alleen de functionele cookies instellen.
- De scepticus maakt liever gebruik van gast-accounts of heeft weleens nep accounts om online bestellingen te doen, denk aan: vals telefoonnummer en geboortedatum invoeren. En een apart e-mailadres.

Typologie burgers en online privacy



DE SCEPTICUS

Scepticus

- Ziet zichzelf als voldoende digitaal vaardig en heeft zichzelf verklaard tot expert op het gebied van privacy en persoonsgegevens delen (boeken lezen, lezingen bijwonen; vanwege hun beroep/studie, zoals IT sector en filosofie)
- Voelt zichzelf online behoorlijk veilig.
- Is gedreven om voorzichtig te zijn met het delen van (online) persoonsgegevens: 'het zijn mijn gegevens', persoonlijke data wordt gebruikt in eigen belang van bedrijven en 'minder gevoel van controle over mijn gegevens'.
- Is sceptisch ten aanzien van commerciële websites en sociale media en past daar het gedrag op aan.
- Versoepelt bij overheidsorganisaties en zeker als DigiD gebruikt wordt.
- Is kritisch ten aanzien van de overheid op politiek-bestuurlijk en beleidsmatig vlak.



DE PRAGMATICUS

Pragmaticus

- Bijzonder heterogeen ten aanzien van de mate van digitaal vaardig, waarbij de ene heel handig is vergelijkbaar gedrag toont als de scepticus. En de ander in mindere mate digitaal vaardig is en vaak kiest voor het (online) delen van gegevens, omdat gemak prevaleert.
- Voelt zich online niet altijd veilig, maar denkt 'ik moet mee met digitale ontwikkelingen' en 'ik heb niets te verbergen'.
- Is gedreven om voorzichtiger te zijn in het delen van (online) persoonsgegevens, omdat hij/zij angstig is voor diefstal/ fraude, technologie is complex/ ongrijpbaar en weinig (zelf)vertrouwen in eigen digitale kunnen heeft.
- Heeft een groot vertrouwen in overheidsorganisaties en DigiD.
- Gebruikt voor DigiD vaker de web versie dan de app.



DE ONBEZORGDE

Onbezorgde

- Stelt gemak boven privacy.
- Voelt zich online veilig, omdat gedacht wordt 'wat kunnen ze nou met mijn gegevens' en 'dit is zoveel makkelijker en sneller'.
- Heeft een bijzonder groot vertrouwen in techniek, devices, overheidsorganisaties en DigiD.

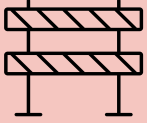
Regietoepassingen | drijfveren



Factoren die doorslaggevend zijn om gebruik te maken van regietoepassingen:

- Op spontaan niveau zijn de belangrijkste voordelen: **tijdbesparing** in vergelijking met handmatig invullen en **gemak**, namelijk niet alle papieren (digitaal) opzoeken, verzamelen en uploaden.
- **DigiD**. Dit wordt gezien als de 'heilige graal' van veilig inloggen door de twee-stapverificatie. En er is veel vertrouwen in DigiD, omdat het van de overheid is; landelijk gebruikt wordt; al jaren in gebruik is en er (bijna) geen slechte ervaringen zijn, ook niet van mensen in de omgeving of nieuwsberichten.
- **De route er naartoe (routing)**; vanuit welke context wordt de regietoepassing aangeboden en via welke site. Een e-mail van onbekende afzender met een doorkliklink kan mogelijk een afbreukrisico zijn (angst voor phishing mail). Terwijl een doorverwijzing vanuit de website van de gemeente, direct al betrouwbaar is.
- **De afzender**. Aansluitend op de route is de afzender ook van belang. Zoals eerder benoemd is er een groot vertrouwen in de overheid als het gaat om regelzaken, dus dat geldt ook voor de regietoepassingen. Zodra er een onbekende en potentieel commerciële partij betrokken is, dan een doorverwijzing via overheidsbron belangrijk (routing) in combinatie met inloggen via DigiD.
- Een andere belangrijke factor is het **zelf toestemming geven** voor wie, welke persoonsgegevens mag inzien. En daarmee ook het feit dat verschillende partijen niet elkaars data kunnen inzien, dat het 'aparte postvakjes' zijn, is belangrijk om te vermelden. Hoewel er het idee heerst dat overheidsbronnen elkaars gegevens kunnen inzien en delen met elkaar, is het een geruststelling en meer gevoel van controle dat dit in werkelijkheid niet kan.
- Enig gevoel van **noodzaak**, want het gaat vaak om zaken die je graag wilt hebben of doen: huis huren, kopen/ subsidietoeslag, inzicht in je pensioen. Dat er informatie tegenover staat om dat voor elkaar te krijgen, neemt men op de koop toe en is soms ook logisch: *"Ik snap wel dat ze mijn inkomen moeten checken om te kijken of ik recht heb op de toeslag."*; *"Jij wilt iets van hun en zij willen iets van jou terug in retour."*
- **Dataminimalisatie** door geen onnodige informatie te delen en het gebruik van certificaten is voornamelijk voor de scepticus belangrijk en mogelijk zelfs doorslaggevend.

Regietoepassingen | drempels



Er zijn ook drempels om gebruik te maken van regietoepassingen:

- De belangrijkste is de vorm: **een app**. Er zijn verschillende redenen waarom een app een drempel is.
 - Voor minder digitaal vaardigen en de pragmatici is het gebruik van een app voor deze zaken **nieuw en een onbekende route**: *"ik doe deze dingen altijd via een website en op mijn laptop."*; Daarbij voelt een mobiel **minder veilig** in vergelijking met een laptop/computer: *"Een mobiel heb je altijd bij je en kan makkelijker worden gestolen"; "op mijn computer staat anti-virus software, op mijn mobiel niet."* En meer praktisch van aard: het is een klein scherm om belangrijke zaken op te regelen: *"dat doe ik liever niet op mijn mobiel."*
 - Voornamelijk de scepticus vindt het een drempel, omdat de informatie van meerdere partijen, in perceptie, op één centrale plek staat (**datacentralisatie**). Dat wordt gezien als een verhoogd risico.
- Hoewel een deel van de doelgroep (vooral onbezorgde) het scannen van een **QR-code** als gemakkelijk ervaart (een snelweg naar de app toe), kan een QR-code potentieel ook een drempel zijn, want 'hoe werkt dat' en 'je weet niet waar je uitkomt', 'is het wel te vertrouwen'.
- Volledig **eigen beheer van en verantwoordelijkheid over** de persoonsgegevens gaat vaak te ver en is geen (latente) behoefte aan (zeker niet bij minder digitaal vaardigen): *"het is toch informatie die ik uit de overheidsbronnen haal, dan moeten zij dat toch ook bijwerken? Waarom moet ik dat doen?"*. De scepticus heeft hier wel iets meer behoefte aan, omdat dit een gevoel van controle geeft over zijn of haar eigen persoonsgegevens.
- De **bewaartermijn** van 90 dagen lijkt in perceptie erg lang: *"dat is dan toch 3 aanden dat ze bij je gegevens kunnen."* Voornamelijk de scepticus krijgt wantrouwen ten aanzien van de betrokken partij en wil graag weten waarom er zo'n lange termijn nodig is: *"bij zo'n energietoeslag hoeven ze toch alleen je inkomen te checken. Waarom moet dat 3 maanden duren?"; "ik krijg het gevoel dat ze dan je gegevens voor iets anders gebruiken of delen met anderen."*



Bijlagen: impressie use cases

Use case energietoeslag

Energietoeslag

De energieprijzen lopen op en de energiekosten worden steeds duurder.

Meneer de Jong heeft van familie gehoord over een energietoeslag.

En meneer de Jong wil weten of hij ook in aanmerking komt voor de energietoeslag.

Hij gaat op zoek naar informatie en komt via de gemeentewebsite uit op een organisatie waar hij kan uitrekenen of hij recht heeft op toeslag.

Om in aanmerking te komen voor de energietoeslag moet meneer de Jong een inkomenscheck doen met behulp van een mobiele app.

Wat zou u doen?

The image shows two screenshots of a mobile application interface. The top screenshot is titled "Heb je alles bij de hand?" and contains a series of questions with "Ja" and "Nee" buttons. The questions are: "Ik heb mijn DigID inlog-gegevens bij de hand.", "Ik heb 'controle via sms' bij DigID aan staan.", "Ik heb eerder ingelogd bij MijnOverheid.", and "Ik heb mijn telefoon bij de hand." Below these questions is an orange button labeled "Aan de slag!". The bottom screenshot is titled "Heb jij recht op energietoeslag?" and features a form with input fields for "Postcode", "Huisnummer", and "Huisnummertoevoeging". It also includes a dropdown menu for "Wat is jouw leeftijd?" (set to "21 tot pensioengerechtigde leeftijd"), and three yes/no questions: "Ben je getrouwd of samenwonend?", "Woon er een kind onder de 18 jaar bij jou in huis?", and "Is het (geomet) netto maandinkomen minder dan € 1.256,07?". A green banner at the bottom of the form states "Je komt mogelijk in aanmerking voor energietoeslag." and an orange button labeled "Ga verder" is at the bottom right.

Use case pensioeninzicht

Pensioeninzicht

Afgelopen week las meneer de Jong in het nieuws dat de pensioenen worden verhoogd. Hierdoor is hij benieuwd geworden en vraagt zich af hoe hij er zelf voor staat.

Toevallig heeft hij net een e-mail ontvangen van zijn pensioenuitvoerder PFZW met de uitnodiging om in te loggen op het persoonlijke portaal.

Dit portaal biedt ook informatie om zelf tot financieel inzicht te komen over zijn pensioen nu en in de toekomst, genaamd de 'Toekomstverkenner'.

Wat zou u doen?

Op welke vraag wilt u antwoord?

Ontdek direct wat het voor uw situatie betekent

<p>Hoe ziet mijn financiële situatie eruit nu en tijdens mijn pensioen?</p> <p>Start</p> <p>Meer informatie</p>	<p>Wat als ik minder ga werken?</p> <p>Start</p> <p>Meer informatie</p>	<p>Wat als ik eerder stop met werken?</p> <p>Start</p> <p>Meer informatie</p>
<p>Wat als wij samen met pensioen gaan?</p> <p>Start</p> <p>Meer informatie</p>	<p>Kan ik tijdens mijn pensioen in mijn huidige woning blijven wonen?</p> <p>Start</p> <p>Meer informatie</p>	<p>Wat als ik mijn baan kwijt raak door ontslag?</p> <p>Start</p> <p>Meer informatie</p>

Pensioenfonds **Zorg & Welzijn** 42%

1 Start 2 **Gewenste situatie** 3 Gegevens ophalen 4 Inzicht

Stap 2: Gewenste situatie bepalen

Hallo, ik ben Penny, uw virtuele assistent.

U wilt graag antwoord op de vraag:
'Hoe ziet mijn financiële situatie eruit nu en tijdens mijn pensioen?'.
Indien dit klopt, dan kunt u doorgaan naar **stap 3**.

Door naar gegevens ophalen

Wat vindt u?

Pensioenfonds **Zorg & Welzijn** 76%

1 Start 2 Gewenste situatie 3 **Gegevens ophalen** 4 Inzicht

10 minuten

Gegevens automatisch ophalen met de Gegevens aanlever app

- ✓ **Veilig**, via uw vertrouwde DigiD omgeving
- ✓ **Nauwkeurig**, uw financiële overzicht dus ook
- ✓ **Aanpasbaar**, u kunt later alles zelf aanpassen

Bekijk hoe het werkt

Minimaal 45 minuten

Alles handmatig invullen

U zoekt zelf alle gegevens bij elkaar en vult deze handmatig in. Gegevens die we nodig hebben zijn onder andere: NAW-gegevens, woon-informatie, loongegevens, uitkeringen, pensioenoverzicht, belastinginformatie, eigen vermogen, effecten, (studie-)schulden en pensioeninformatie.

Kies voor handmatig

Wat vindt u?

Use case huurwoning vrije sector

Inschrijven huurwoning

Meneer de Jong is op zoek naar een kleinere huurwoning en heeft zijn oog laten vallen op een nieuwbouwproject in Utrecht.

Hij meldt zich aan op de website en vult zijn algemene gegevens in.

Om in aanmerking te komen voor de huurwoning (vrije sector) is een inkomenstoets nodig om vast te stellen of de woning passend is en/ of meneer de Jong de huur kan betalen.

Per e-mail ontvangt hij een uitnodiging om alle andere gegevens aan te leveren.

Wat zou u doen?



ACTUALITEIT
25 april 2022

Makkelijk en veilig je gegevens delen Inschrijven met de Gegevens aanlever app

Lees meer

START INSCHRIJVING

Snel, makkelijk en veilig je gegevens delen

Voor de definitieve inschrijving van nieuwbouw project [De Groene Steegjes - Betaalbare huur](#) vragen we je om (financiële) gegevens aan te leveren. Vaak gaat het dan om documenten en gegevens die je niet zo 1, 2, 3 klaar hebt liggen. Al die gegevens verzamelen vergt het nodige zoekwerk. Niet ideaal om in allerlei ordners en online portalen te moeten duiken om al deze informatie te verzamelen.

Makkelijk en snel aanleveren met de Gegevens aanlever app

Met de [Gegevens aanlever app](#) deel je eenvoudig en op [een veilige manier](#) je persoonlijke gegevens met Van Wanrooij Projectontwikkeling B.V.. Zo verzamel je met de app informatie vanuit MijnOverheid, de Belastingdienst, het UWV, de Basisregistratie Personen en Mijnpensioenoverzicht.nl. Deze informatie deel je vervolgens veilig met Van Wanrooij Projectontwikkeling B.V. die je om die gegevens heeft gevraagd. [Met de Gegevens aanlever app zit je zelf aan het stuur en bepaal je of de opgehaalde informatie wordt gedeeld.](#)



Understanding what makes people tick

Quarter Plaza
Transformatorweg 74
1014 AK Amsterdam
T +31 (0)20 670 50 20
info@mare.amsterdam
www.mare.amsterdam

MARE werkt volgens
ISO 20252:2019 &
ISO 27001:2017