ShoppingTomorrow

thuiswinkel.org

Flip the script: een outside-in perspectief op Consumentengedrag

happy horizon
CREATIVE DIGITAL AGENCY

mollie

Takeaways

1. **Vraag alleen gegevens uit die je nodig hebt**
   Gegevens van consumenten zijn kostbaar. Die bewustwording groeit. Daardoor verandert het consumentengedrag. Dat vraagt om een andere aanpak van bedrijven. Zij zullen moeten kunnen uitleggen waarom ze bepaalde gegevens uitvragen. En dus is onbeperkt gegevens verzamelen, zoals vroeger, er niet meer bij. Vraag alleen de gegevens uit die je nodig hebt om nieuwe klanten te trekken, huidige klanten te ondersteunen, je service optimaal te laten renderen en daarnaast ook financieel succesvol te zijn.

2. **Neem verantwoordelijkheid**
   Het is onmogelijk voor consumenten om leidend te zijn in de discussie over data delen en data-beheer. Soms komt men er niet onderuit om data te delen, zelfs als het niet goed voelt. En vaak gebeurt er zoveel achter de schermen waarvan de consument geen weet heeft en niet op kan reageren. Besef dat je als organisatie de verantwoordelijkheid hebt om acties begrijpelijk en gebruiksvriendelijk te houden en te waarborgen dat gebruikersdata worden beschermd.

3. **Blijf op de hoogte**
   De wereld van privacy en gegevensbeheer evolueert snel. Begrijp dat consumenten verschillende opties hebben, zoals Privacy by Design, Personal Digital Wallets en Single Sign-On. Er bestaat geen ‘one size fits all’-oplossing. Blijf op de hoogte van de ontwikkelingen in wetgeving en markttrends, omdat deze van invloed kunnen zijn op hoe jij moet handelen.

Inhoud

Inleiding

Consumentengedrag is binnen ieder bedrijf een belangrijk thema. Logisch. Het gedrag van de consument begrijpen, of nog beter: voorspellen, is de eerste stap van een strategische keuze. Jarenlang was het bedrijfsleven vrij om te doen met data wat het wilde. Maar dat is aan het veranderen. Men hoopt consumenten beter te beschermen tegen inbreuk op privacy door consumenten de regie over hun data weer terug te geven. Dat gebeurt onder andere aan de hand van nieuwe wet- en regelgeving.

De grote vraag is of en, zo ja, hoe het gedrag van consumenten gaat veranderen? Op welke manier kunnen zij de regie over hun data voeren? Pakken ze überhaupt de regie terug? En welke impact heeft dit op de relatie tussen consument en merk? We kiezen daarom voor een outside-in-benadering. We stellen niet het bedrijfsleven, maar de consument centraal. Flip the script noemen we dat. In deze bluepaper houden we de huidige markt en het consumentengedrag tegen het licht. We stellen scenario's op die, naar ons idee, de omgang met data gaan beïnvloeden en nemen je mee in de verwachtingen.

1 Juridische ontwikkelingen

Zoals gezegd gaat de wet- en regelgeving rondom datagebruik veranderen. Zowel op Europees als op nationaal niveau moeten bedrijven en consumenten rekening houden met vernieuwde regels. Met name de e-privacyverordening (ePV), Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), Data Act en Data Governance Act gaan invloed hebben op onze omgang met persoonsgegevens.

1. E-privacyverordening (Europese wetswijziging)

De e-privacyverordening is een aanvulling op de Algemene Verordening Gegevensbescherming (AVG) en focust zich op de bescherming van persoonsgegevens bij elektronische communicatie. Belangrijke punten zijn onder meer uitbreiding van privacyregels naar nieuwe spelers in elektronische communicatie, strengere regels voor gegevensbescherming, privacy voor communicatie-inhoud en metadata, nieuwe zakelijke kansen voor traditionele telecompartijen, eenvoudigere regels voor cookies en bescherming tegen spam.

De wet is nog in ontwikkeling en zal naar verwachting in de aanloop naar de Europese verkiezingen van 2024 nieuw leven in worden geblazen. Het is nog onduidelijk wanneer de verordening tot stand komt.

Meer lezen over deze wetswijziging? [Lees verder]

2. Uitvoeringswet Algemene Verordening Gegevensbescherming (nationale wetswijziging)

De Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) is de Nederlandse uitvoeringswet van de AVG. Deze wet wordt op dit moment tegen het licht gehouden door de Tweede Kamer. Men wil aanpassingen doen aan de definitie van strafrechtelijke persoonsgegevens en veranderingen doorvoeren in de toestemming voor gegevensverwerking voor jongeren van 12 tot 16 jaar.

Meer lezen over deze wetswijziging? [Lees verder]

3. Data Act (Europese wet)

De Data Act heeft als doel een eerlijkere digitale markt te creëren, een concurrerende datamarkt te bevorderen en meer toegankelijkheid van data mogelijk te maken. Consumenten krijgen meer controle over hun gegevens, omdat de datawet helpt toegang te krijgen tot eigen gegevens én het helpt deze gegevens op een verantwoorde manier te delen met derden. Daarnaast worden cloud-switching en interoperabiliteit bevorderd. Ook krijgt het recht op reparatie en datatoegang voor zowel B2B- als B2C-diensten extra aandacht.

Meer lezen over deze wet? [Lees verder]

4. Data Governance Act (Europese wet)

Met de Data Governance Act (DGA), die geldig is vanaf september 2023, hoopt men het vertrouwen in het delen van gegevens te vergroten, de beschikbaarheid van gegevens te versterken en technische obstakels voor het hergebruik van gegevens weg te nemen. Dat doet het door een veilige omgeving te scheppen waarin gegevens kunnen worden gedeeld. Dat zou het vertrouwen van consumenten in het delen van gegevens kunnen vergroten. Het doel? Het potentieel van de data-economie volledig benutten.

Meer lezen over deze wet? [Lees verder]

De bovenstaande nieuwe wetgeving geeft een discrepantie wat betreft datadeling en databescherming. Enerzijds legt men meer focus op de bescherming van (persoons)data, waarbij vooral de consument gebaat is. Maar anderzijds kijkt men hoe de dataverrijking en datadeling in de interne markt kan toenemen.

2 Ontwikkelingen op dit moment

Consumenten worden al jarenlang gevraagd keuzes te maken over hun online privacy. Maar sinds een aantal jaar groeit de aandacht voor dit thema. Bedrijven proberen steeds vaker bewustwording te creëren bij de consument over het delen van data.
Sterker nog: overheden, banken, techbedrijven en telecompartijen bieden tools of maatregelen om consumenten te helpen.

Wat is digitale identiteit?

Je digitale identiteit bestaat uit al jouw persoonsgegevens. Je leeftijd, je geboorteplaats, de namen van je ouders enzovoort.
Op dit moment liggen deze stukken informatie over het hele internet verspreid. Thuisbezorgd kent bijvoorbeeld je favoriete maaltijd, Wehkamp je kledingmaat en Netflix je kijkgedrag.

Over welke data hebben we het dan eigenlijk?
We maken onderscheid in drie categorieën data:

- Inherent attributes (accrued data) zoals leeftijd, gender, biometrische gegevens en het gezondheidsdossier.
- Assigned attributes zoals burgerservicenummer (BSN), IP-adres, telefoonnummer, e-mailadres en je studentnummer.
- Accumulated attributes zoals locatiegegevens, surfgedrag, contactenlijsten, creditcardnummer en koopgedrag.

eID’s: middelen of manieren om je online te identificeren

Elektronische identificaties, oftewel eID's, zijn digitale hulpmiddelen voor online identificatie en authenticatie. Ze zijn van essentieel belang voor beveiliging, privacy en gemak in de digitale wereld. Elke sector heeft wel een eigen eID. Het zorgt ervoor dat wij onze persoonlijke informatie kunnen beveiligen, financiële transacties kunnen verrichten of snel toegang kunnen krijgen tot digitale diensten. Daarnaast zien we ook steeds meer commerciële aanbieders van eID’s.

Overheid
De meest bekende identity tool in Nederland is de DigiD. Iedere Nederlander heeft een DigiD om zich online veilig te identificeren. Voor de zakelijke markt kennen we eHerkenning. Bovendien bouwt de Europese overheid aan een Europees raamwerk voor id-wallets en een publieke voorbeeld-wallet[1].

Banken
In Nederland kwam een aantal jaar geleden iDIN op de markt. Met iDIN kunnen consumenten zich bij andere organisaties, via hun vertrouwde bank, online identificeren, inloggen, leeftijd bevestigen en documenten ondertekenen. In België is een soortgelijk programma ontworpen onder de naam itsme. Dit online-identificatieprogramma is opgezet door banken en telecompartijen en wordt ondersteund door de Belgische overheid.

Telecom
In de telecomsector heeft GSMA de service Mobile Connect in meer dan twintig landen op de markt gebracht. Hiermee kun je je als consument identificeren of inloggen met je telefoon.

1 https://www.digitaleoverheid.nl/achtergrondartikelen/de-europese-id-wallet-hoe-wat-en-waarom/

Browsers
De nieuwe regels rondom third-party-cookies dwingen browsers tot actie. Apple (Safari) en Mozilla (Firefox) stopten al met het delen van hun dataverzameling en ook Google (Chrome) gaat dit binnenkort doen.

Digitale kluizen
Partijen als YIVI, Datakeeper, Lastpass en PIM by KPN bieden digitale kluizen waarin je als consument jouw data opslaat. Wil je data delen, inloggen op een website of overeenkomsten ondertekenen? Dan kan dat via de kluis. Ook zijn er partijen die zich richten op het veilig doorgeven van data in plaats van ze op te slaan, zoals Ockto. Zij halen namens de consument data op bij verschillende databronnen en delen dit vervolgens met de vooraf aangegeven partij.

Ook Schluss is een mooi voorbeeld. Schluss werkt volgens het principe van een centrale gedistribueerde plek waar de originele documenten beschikbaar zijn. Partijen die de data nodig hebben kunnen inzage krijgen of via het ‘zero knowledge proof’-principe een bewijs verkrijgen van echtheid. Het idee van Schluss is om alle digitale data zo op te slaan, inclusief surfgedrag op websites en persoonlijke CRM-accountdata zoals die bij bedrijven bestaat. Er ontstaat zo een ‘digital self’ in de vorm van een database, waar de consument volledige controle over heeft.

Techbedrijven
De BigTech-organisaties (onder andere Google, Meta, Microsoft, Amazon en Apple) blijven niet achter. Hun toepassingen en wallets spelen een belangrijke rol in het dagelijks leven van gebruikers. Neem de Apple Wallet. In de Verenigde Staten kun je daar je betaalpas, rijbewijs én paspoort aan koppelen.

De mogelijkheden om je online te identificeren of data op te slaan zullen nog verder groeien. Er worden stappen gezet om controle en decentralisatie te bevorderen, bijvoorbeeld met:

- Blockchain, een sleutelcomponent in Web3. Web3 staat voor een decentraal internet met focus op privacy en autonomie. Hierbij blijven je gegevens en identiteit bij jou en zijn ze niet bereikbaar voor grote techbedrijven. Blockchain dient dan als register voor verklaringen, waartoe je alleen toegang hebt met unieke sleutelparen.
  [Lees verder]

- SSI, een Self-Sovereign Identity. Het draait hierbij om controle over je digitale persoonsgegevens. Jij bepaalt hoe jij je gegevens beheert.
  [Lees verder]

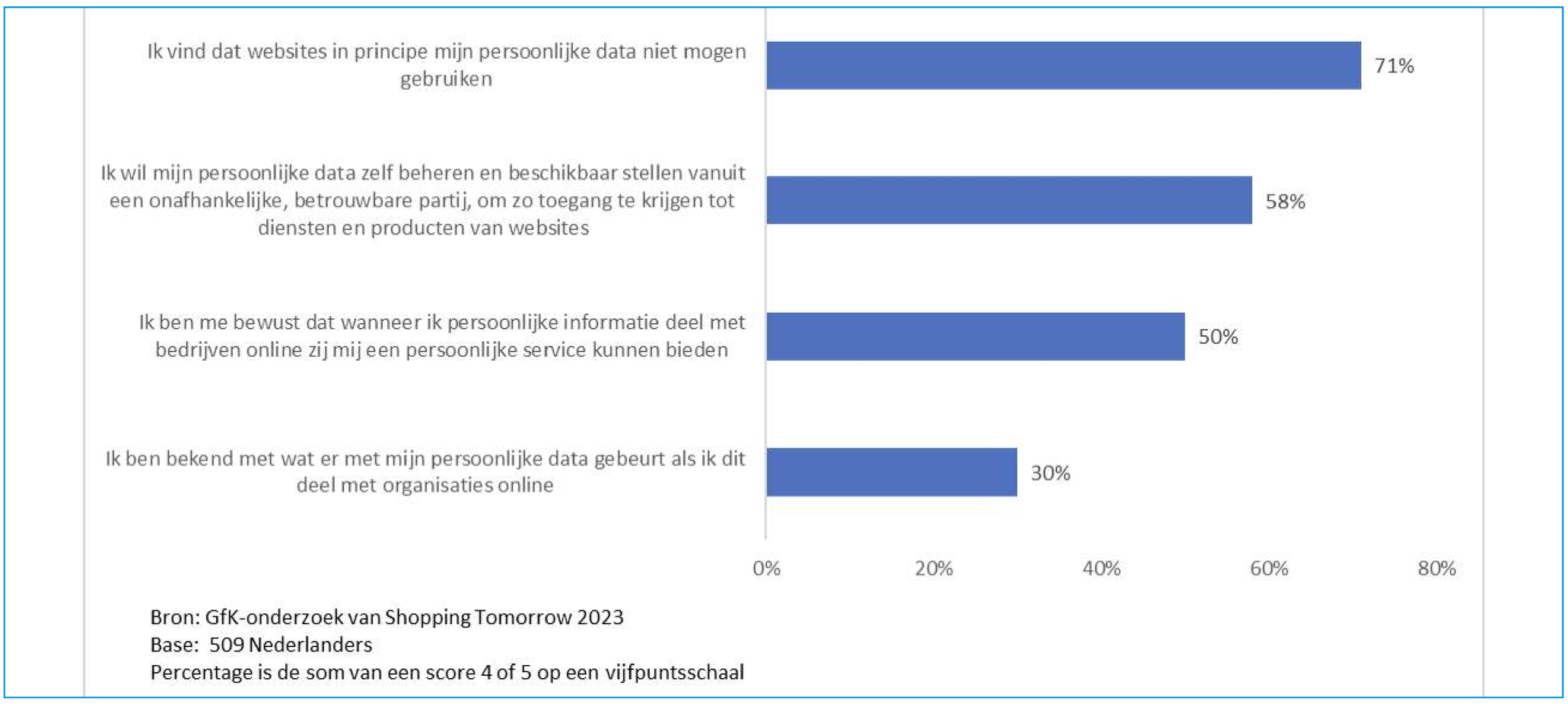
- DISP, een Digital Identy Service Provider. Dit zijn partijen die zich volledig focussen op digitale identiteit. Door een DISP hoeven bedrijven maar één technische aansluiting aan te sluiten en één overeenkomst te tekenen om tegelijkertijd meerdere eID’s toegankelijk te maken. Dankzij deze tool geeft men de consument (het gevoel van) meer controle.
  [Lees verder]

De belangrijkste vraag is misschien wel hoe dit allemaal van de grond kan komen. Het antwoord op deze vraag is gecompliceerd. De markt van digitale identiteiten is groeiend, waarbij het nog niet duidelijk is wat de standaard gaat worden. Is dat een identiteit georganiseerd door de overheid of gaat toch een commerciële aanbieder deze race winnen? Daarnaast staat de innovatie op het gebied van eID’s ook niet stil en dat zal blijven bijdragen aan een verbeterde online-ervaring. Als consument is het onmogelijk om leidend te zijn in deze discussie. Zolang er geen ‘one size fits all’- oplossing is, is het belangrijk om als organisatie op de hoogte te blijven van alle ontwikkelingen zodat je op het juiste moment kunt aanhaken.

3 Het huidige consumentengedrag

Om te onderzoeken hoe het gedrag van consumenten ten opzichte van hun privacy gaat veranderen, besloten we met behulp van een GfK-onderzoek en deskresearch het huidige consumentengedrag onder de loep te nemen. Hoe kijken Nederlanders op dit moment tegen online privacy aan?

Om met de deur in huis te vallen: uit ons onderzoek blijkt dat er een verschil is tussen wat consumenten zeggen en wat ze doen. Het GfK-onderzoek laat zien dat 71% van de Nederlanders vindt dat websites hun persoonlijke data niet mogen gebruiken. Van de respondenten zegt 59% minder bij een webshop te kopen, als (te) veel persoonlijke data moeten worden gedeeld. Toch is de meerderheid van Nederlanders bereid data te delen, zo blijkt uit de DDMA Privacy Monitor 2023. Dat doen ze soms omdat het moet, soms omdat het hen iets oplevert en soms omdat ze geen idee hebben wat er met hun data gebeurt. Slechts een klein deel van de Nederlanders is echt privacy-bewust en handelt daar ook naar.



Oorsprong pragmatische houding

De pragmatische houding van de meeste Nederlanders is vooral het gevolg van onwetendheid, onverschilligheid of een combinatie daarvan. Dat lichten we toe.

Onwetend of onkundig

Een aanzienlijk deel van de consumenten is nog steeds onwetend over de volledige omvang en complexiteit van privacykwesties. Veel mensen begrijpen niet goed welke gegevens er over hen worden verzameld, hoe deze worden gebruikt of met wie ze worden gedeeld. Een studie onder 2022 Nederlanders liet zien dat 80% van hen dacht dat cookies voor browsergeschiedenis worden gebruikt.

Bovendien denken consumenten bij persoonsgegevens primair aan het actief delen van gegevens, zoals een e-mailadres, NAW-gegevens of telefoonnummer in een bestelformulier. Ze denken niet aan het passief delen van gegevens, zoals browsegedrag, locatiegegevens of IP-adres.

Overigens wordt het consumenten ook niet makkelijk gemaakt. Privacyvoorwaarden en instellingen zijn vaak moeilijk te begrijpen. Daardoor is het voor consumenten lastig om keuzes te maken. Deze onwetendheid kan leiden tot een gebrek aan proactieve bescherming van persoonlijke gegevens en maakt consumenten kwetsbaar voor privacyrisico's.

Onverschillig

Veel Nederlanders zien het nut niet van het beschermen van hun privacy. Dat noemen we ‘privacy cynicism’. Consumenten zijn cynisch over de controle die ze hebben, omdat ze ervan uitgaan dat grote techbedrijven hun data hoe dan ook verzamelen en voor commerciële doeleinden gebruiken. Het delen van data voelt als onontkoombaar. Bovendien is het doorlezen van de voorwaarden te tijdrovend en te complex. Daardoor accepteert men voorwaarden zonder ze daadwerkelijk te lezen.

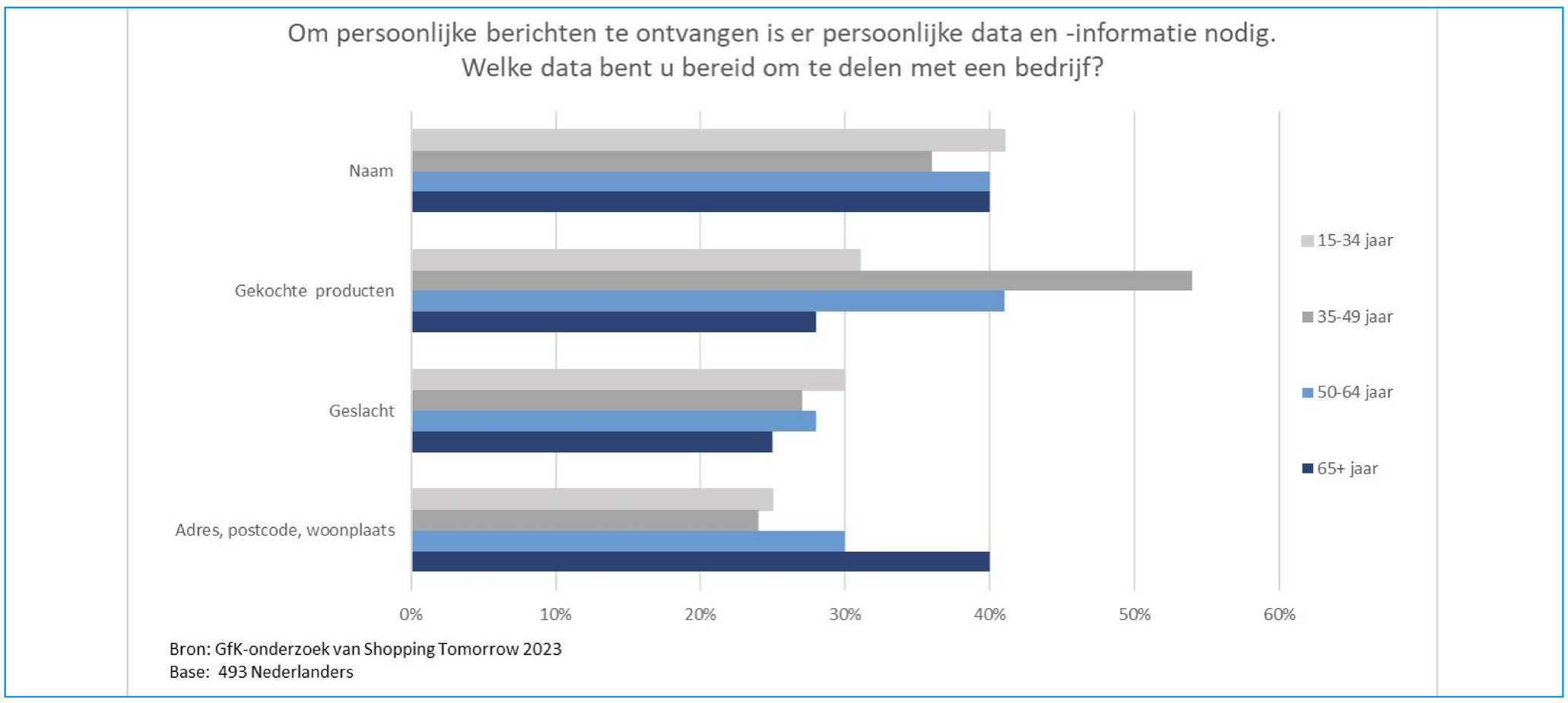
Bewust

Bewuste consumenten weten dat er data over hen worden verzameld en handelen voorzichtig. Zij gebruiken bijvoorbeeld een VPN-verbinding, incognitomodus of verschillende profielen of mailadressen. Veel consumenten noemen we onbewust onbekwaam. Er is nog te weinig kennis over welke data worden verzameld om onze houding te veranderen.

Houding ten opzichte van soorten data

Consumenten gaan niet met iedere soort data hetzelfde om. Uit onderzoek van DDMA Privacy Monitor 2023 blijkt dat Nederlanders hun financiële informatie (70%) en medische achtergrond (69%) als meest privé beschouwen. Demografische gegevens zoals leeftijd, geslacht en opleidingsniveau worden makkelijker gedeeld.

Dit zien we ook terug in onderstaande GfK-grafiek. Met name het verschil tussen de leeftijdsgroepen valt op. Zo hebben Nederlanders tussen de 35 en 64 jaar minder moeite met het delen van informatie over gekochte producten dan jongeren. En vinden 65+’ers het delen van het woonadres het minst bezwaarlijk.



Toch zijn consumenten in sommige gevallen bereid vertrouwelijke informatie te delen. Vooral het vertrouwen in een organisatie is een belangrijke voorwaarde. Maar ook relevantie en transparantie vanuit de organisatie heeft invloed.

Er is een grote verscheidenheid aan kennis, verwachtingen en behoeften van Nederlandse consumenten. Bedrijven hebben een flinke uitdaging als ze de privacybehoeften van hun klant centraal willen stellen. In het volgende hoofdstuk zijn een aantal scenario's ontwikkeld die hierbij kunnen helpen.

4 Drie mogelijke scenario's

Na een eerste onderzoek naar de huidige markt, privacyregelgeving en het huidige gedrag van consumenten met betrekking tot privacy, concludeerden we dat alle ontwikkelingen samen te vatten zijn in drie mogelijke scenario's. Die zijn gebaseerd op drie niveaus van betrokkenheid van de consument met betrekking tot privacy.

Scenario 1: Privacy by Design

Als consument kan het moeilijk zijn om controle te houden over persoonlijke data. Lastige termen en de hoeveelheid data die moeten worden afgegeven, maken het moeilijk om écht te snappen wat je deelt en waarom. Privacy by Design helpt consumenten daarbij. Het is een principe waarbij bedrijven al vanaf de ontwikkeling van producten, zoals een website, gegevensbescherming als uitgangspunt nemen. Zij leggen dan overal waar data worden afgevangen, uit waarom zij die data afvangen én geven de bezoeker de optie om ja of nee te kiezen. Ook hoef je niet altijd te kiezen tussen de twee extremen 'wel toestemming' of 'geen toestemming'. Je kunt aangeven welke gegevens wel of niet mogen worden vastgelegd. Belangrijk is wel dat de consument voldoende kennis heeft om de keuze te kunnen maken. Bedrijven die dit principe toepassen, gaan dus verder dan de gebruikelijke wetgeving. Niet-noodzakelijke data worden niet uitgevraagd of gepseudonimiseerd. Pseudonimiseren houdt in dat, anders dan bij anonimiseren, gegevens nog wel worden gezien als persoonsgegevens.

Privacy by Default

Sommige bedrijven gaan nog een stapje verder. Op een website waar Privacy by Default wordt toegepast, worden in eerste instantie geen data afgevangen. Dat gebeurt pas als een bezoeker uitdrukkelijk toestemming geeft. Om dit principe goed toe te passen moet een organisatie niet alleen technische, maar ook organisatorische maatregelen nemen. Zo moeten ook afdelingen onderling zorgvuldig omgaan met data van klanten.

Marktontwikkelingen

Privacy by Design zie je vaker terug. Bijvoorbeeld de website van Ikea[2]. Via een korte video vertellen deze bedrijven welke gegevens ze nodig hebben van de consument, wat ze daarmee doen en hoe de consument daarin keuzes kan maken. Toch is er nog een slag te slaan. Privacy by Design is nog erg vaag en weinig bedrijven omarmen het principe volledig. Eenduidige normen of best practices zouden de ontwikkeling helpen.

Voor- en nadelen

Kies je voor het scenario Privacy by Design, dan komen daar voor- en nadelen bij kijken. Denk bijvoorbeeld aan:

Voordelen

- Consumenten ontvangen wat ze al lang denken te krijgen.
- Voor bedrijven zorgt het voor schonere data en minder risico bij datalekken.

Nadelen

- Het is nog vaag wat Privacy by Design werkelijk inhoudt.
- De goede intenties van Privacy by Design vallen niet altijd op bij consumenten. Alleen privacybewuste consumenten zullen ervaren dat ze (een stuk) regie over hun data terugkrijgen.
- Het houden aan Privacy by Design is een besluit met veel gevolgen. Het moet passen in de missie van het bedrijf en worden uitgevoerd in alle geledingen van de organisatie.

Bedrijven zoeken vaak naar oplossingen waarin heel duidelijk is waar ze zich aan moeten houden. Privacy by Design is nog heel erg in ontwikkeling en blijft daarom vaag. Desondanks zien wij grote kansen voor bedrijven die kiezen voor dit scenario. Wij verwachten namelijk dat consumenten transparantie en openheid omtrent data enorm gaan belonen door het tonen van loyaliteit richting het bedrijf.

2 https://www.youtube.com/watch?v=j1MsEl9cTRc

Scenario 2: Personal Digital Wallet

Nu digitale diensten zich uitbreiden naar allerlei apparaten en omgevingen, zijn nieuwe aanpakken voor identiteitsbeheer nodig. Die moeten zorgen voor sterke beveiliging (on- en offline) en voor meer controle. Een veelbelovende oplossing is de Personal Digital Wallet. Dit is een digitale identiteitsportemonnee die je digitale identiteit opslaat. Daarna kun je data delen, valideren of één keer laten inzien door bedrijven. Ook kun je ervoor kiezen gedeelde data later weer in te trekken.

Delen, valideren en eenmalig inzien

Delen: Je deelt je bezorgadres met Wehkamp. Zij slaan jouw gegevens op bij jouw order totdat je besluit je gedeelde gegevens in te trekken of te wijzigen.
Valideren: Een autoverhuurbedrijf stuurt een aanvraag naar je datakluis om te checken of je een rijbewijs hebt. Het bedrijf krijgt geen inzage in de gegevens zelf.
Eenmalig inzien: Je deelt je biometrische gegevens zoals je slaappatroon voor een offerte voor een matras op maat. Het bedrijf kan de gedeelde gegevens dan maar één keer inzien.

Een Personal Digital Wallet is zeer gebruiksvriendelijk. Je kunt jezelf identificeren, informatie uitwisselen tussen diensten en gevoelige gegevens met een sterke versleuteling beschermen. Ook kunnen handige functies worden gekoppeld, zoals geavanceerdere gegevensuitwisseling, beheer van persoonlijke informatie en zelfs koppelingen met betalingssystemen.

Persoonlijke data space
Binnen dit speelveld is er een verschil tussen een digitale wallet en persoonlijke data space. Een digitale wallet is je digitale visitekaartje met al je persoonlijke gegevens. In een persoonlijke data space beheer en bescherm je grotere sets persoonlijke data. Het gaat dan over data als koopgedrag, biometrische gegevens of zelfs je medisch dossier.

Keuzeniveaus voor gebruikers

De verwachting is dat in de toekomst een vrije marktwerking zal ontstaan en dat, afhankelijk van welke functionaliteiten diverse kluizen bieden, de consument zelf op basis van voorkeur één zal selecteren.

Op dit moment zijn drie branches uitgebreid bezig met de uitrol van identiteitsportemonnees:

1. BigTech
Zij breiden hun platformmogelijkheden uit met identity wallets, zoals Apple met Apple Wallet. Aan deze wallets kunnen inmiddels betaalpassen, ID-kaart en rijbewijs worden toegevoegd.

2. De publieke sector, zoals de Europese Unie en haar lidstaten
Zij herzien hun digitale identiteitsaanpak met wetgeving en nationale portemonneediensten. De Nederlandse overheid heeft al aangekondigd de ID Wallet[3] te introduceren.

3. Onafhankelijke aanbieders van portemonnees
Zij bieden een marktgedreven en open benadering met zowel gratis als commerciële diensten. Dit kunnen bestaande partijen zijn als telecomproviders of banken, maar ook nieuwe initiatieven, zoals Schluss en Yivy.app.

Marktontwikkelingen
Zowel overheid, grote commerciële partijen en individuele initiatieven investeren flink in de ontwikkeling van digitale kluizen. Hoewel de adoptie bij de consumenten nog laag is op dit moment, kan dit snel omslaan als grote webshops of instellingen deze manier van identificatie en authenticatie in hun platform opnemen. Deze trend is al zichtbaar in de financiële markt, bij sommige hypotheekverstrekkers en verzekeraars die het gebruik verplichten.

3 https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/identiteit/id-wallet/

Voor- en nadelen
Kies je voor het scenario Personal Digital Wallet dan zijn er enkele overwegingen waar je rekening mee moet houden. Denk bijvoorbeeld aan:

Voordelen
- Consument heeft regie. Hij kan per situatie keuzes maken.
- Als meerdere aanbieders zich in deze markt begeven, ontstaat er een vrije marktwerking.

Nadelen
- Er is een risico dat adoptie traag op gang komt en de consument dit pas gebruikt wanneer het verplicht wordt gesteld.
- Een Personal Digital Wallet staat niet op zichzelf. De andere scenario's zijn nodig om de juiste voorwaarden te scheppen om succesvol te zijn, zoals Privacy by Design en een strakke wet-en regelgeving.

Nooit meer je paspoort laten kopiëren bij een hotel met de hoop dat de kopie later wordt weggegooid. De Personal Digital Wallet kan direct worden gebruikt door bepaalde sectoren zoals de reisbranche. Genoeg voordelen voor de consument, maar durven bedrijven het aan dat bepaalde gegevens ineens niet meer in te zien zijn?

Scenario 3: Single Sign-On

Voor sommige consumenten is niets belangrijker dan gebruiksgemak. Hoe minder je hoeft te doen om in te loggen, gegevens te delen of iets anders, hoe beter. Single Sign-On (SSO) is een technische benadering die gebruikers in staat stelt om met één set inloggegevens toegang te krijgen tot meerdere systemen, platformen of services. In plaats van aparte inloggegevens voor elk afzonderlijk systeem, kunnen gebruikers met SSO één keer inloggen om toegang te krijgen tot verschillende services.

SSO, eventueel in combinatie met een digitale kluis en Privacy by Design, stelt gebruikers in staat om controle te behouden over hun persoonlijke gegevens, terwijl ze profiteren van het gebruiksgemak van één enkele aanmelding.

Keuzeniveaus voor gebruikers
De keuze tussen SSO's wordt in principe bepaald door de gebruiker. Daarbij moet wel de kanttekening worden gemaakt dat de gebruiker alleen kan kiezen uit de mogelijkheden die worden aangeboden door de organisatie waarmee men zakendoet. Op dit moment zijn de opties beperkt tot Google, Apple en Meta in het commerciële domein en DigiD voor overheidsgerelateerde activiteiten.

Marktontwikkelingen
De adoptie van SSO is positief. Meer dan 80% van de organisaties gebruikt ten minste één vorm van SSO, bijvoorbeeld via een Google- of Facebookaccount. En de markt blijft evolueren, met organisaties die werken aan verbeteringen van functionaliteit, beveiliging en gebruikerservaring.

De vraag is in welke vorm SSO in de toekomst verder zal ontwikkelen en of de consument SSO via BigTech-aanbieders een betrouwbare oplossing vindt voor de lange termijn.

Voor- en nadelen
Bij de keuze voor het scenario Single Sign-On is het belangrijk om te bedenken dat daar ook voor- en nadelen aan zitten zoals:

Voordelen
- Gemakkelijke toegang.
- Tijdsbesparing.
- Minder wachtwoorden.
- Verbeterde gebruikservaring.

Nadelen
- Afhankelijkheid van een vendor.
- Geen overzicht over gebruik en opslag van je gegevens.
- Geen inzicht hoe je als consument je eigen data kunt beheren of intrekken.

We zien een situatie voor ons die lijkt op het huidige betaallandschap. Daar is inmiddels een overvloed aan opties met bijvoorbeeld iDeal, PayPal en achteraf betalen.

5 Het toekomstperspectief

De een vindt data maar gedoe, de ander wil koste wat kost in controle blijven. Hoe het consumentengedrag ten opzichte van data gaat veranderen, is daarom niet in één zin te vatten. Om een helder beeld te scheppen, delen we de consument op in vier persona's.

1. De privacy onbewusten
Delen hun data omdat ze niet beter weten of omdat het hun niet kan schelen.

2. De privacy onbekommerden
Zijn zich bewust van privacyissues rondom persoonsdata, maar delen (te) makkelijk hun (gedrags-) data om toegang tot diensten of platformen te krijgen.

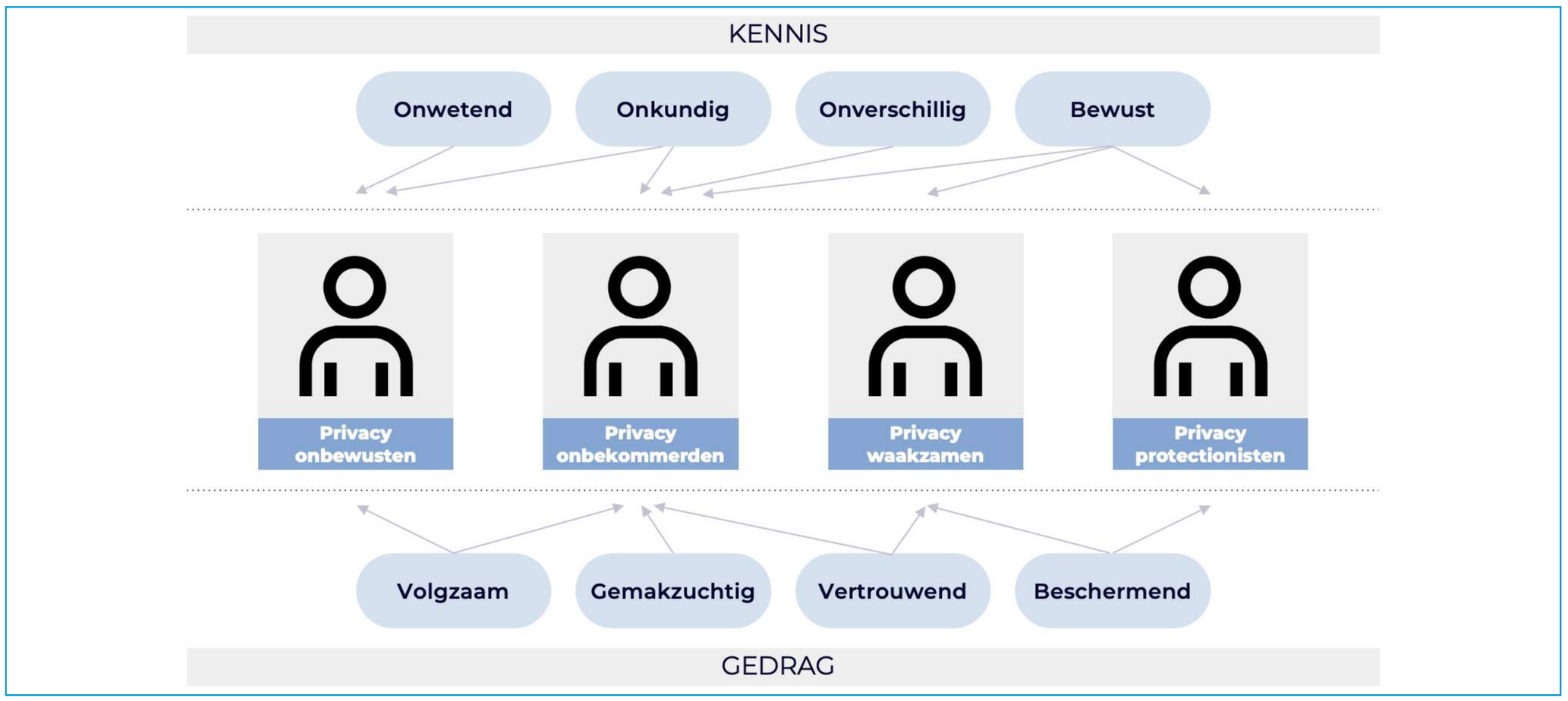
3. De privacy waakzamen
Zijn bewuste consumenten die weloverwogen keuzes maken tussen privacy en gemak. Ze kiezen per situatie welke data te delen met wie.

4. De privacy protectionisten
Delen alleen noodzakelijke data en alleen wanneer ze zelf volledig in controle kunnen blijven.

Om tot deze vier persona's te komen, baseren we ons op eerdere onderzoeken van Strategy&, onderdeel van PWC. We hebben dit aangevuld met de bevindingen uit onze GfK-enquête.

Kenmerken van de persona's

Onderstaande afbeelding toont direct het verschil tussen de vier persona's. Zo is de privacy onbewuste consument volgzaam maar onwetend. Grote kans dat deze consument gedachteloos cookies accepteert. Terwijl de privacy protectionisten heel beschermend en bewust zijn van alle verzamelde data. Zo erg dat deze consument er bijna paranoïde van wordt.



Oplossing per persona

Als we de persona's combineren met de eerder geschetste scenario's dan ontstaat een matrix waarin de behoefte van consumenten aan mogelijke oplossingen wordt gelinkt.

Persona's	Scenario's		
	Privacy by Design	**Personal Digital Wallet**	**Single Sign-On** als norm in de markt voor identificatie en autorisatie
Privacy onbewusten	X		X
Privacy onbekommerden	X		X
Privacy waakzamen		X	X
Privacy protectionisten		X	X

Het is wachten op een externe prikkel of motivatie voor de scenario's om het huidige consumentengedrag te doorbreken.
De nieuwe wet- en regelgeving zal een zet in de nieuwe richting geven. En zodra er een uniforme én makkelijke manier is om jezelf met een ID-wallet te identificeren, en wanneer een groot aandeel van de platformen die als standaard implementeert, zal de adoptie bij consumenten écht een vlucht nemen.

Op welke manier gaan consumenten de regie over hun data voeren?

Hoewel iedere consument de regie over zijn data op zijn eigen manier zal voeren, is de Single Sign-On via een ID-wallet de eerste stap.
Men hoeft dan geen identiteitsgegevens te delen, maar kan deze beschermd laten valideren om toegang te krijgen tot platformen.
Zodra dit vanuit Europa de norm wordt, zal de adoptie snel stijgen.

Parallel daaraan ligt een rol voor het bedrijfsleven. Het bedrijfsleven zal consumenten tegemoet moeten komen aan de groeiende behoefte aan privacyopties, bijvoorbeeld door Privacy by Design.

"Er gebeurt heel veel en ze (consumenten) hebben geen idee wat er met hun data wordt gedaan. Wat wordt er extra verzameld, geanalyseerd, gepersonaliseerd, aan derden gegeven? Wordt de consent van andere sites binnen hetzelfde concern misbruikt?
Er is een heel grote onbekende wat een bedrijf allemaal met consumentendata doet. Wat brengt het de bedrijven om daarin iets te veranderen?"

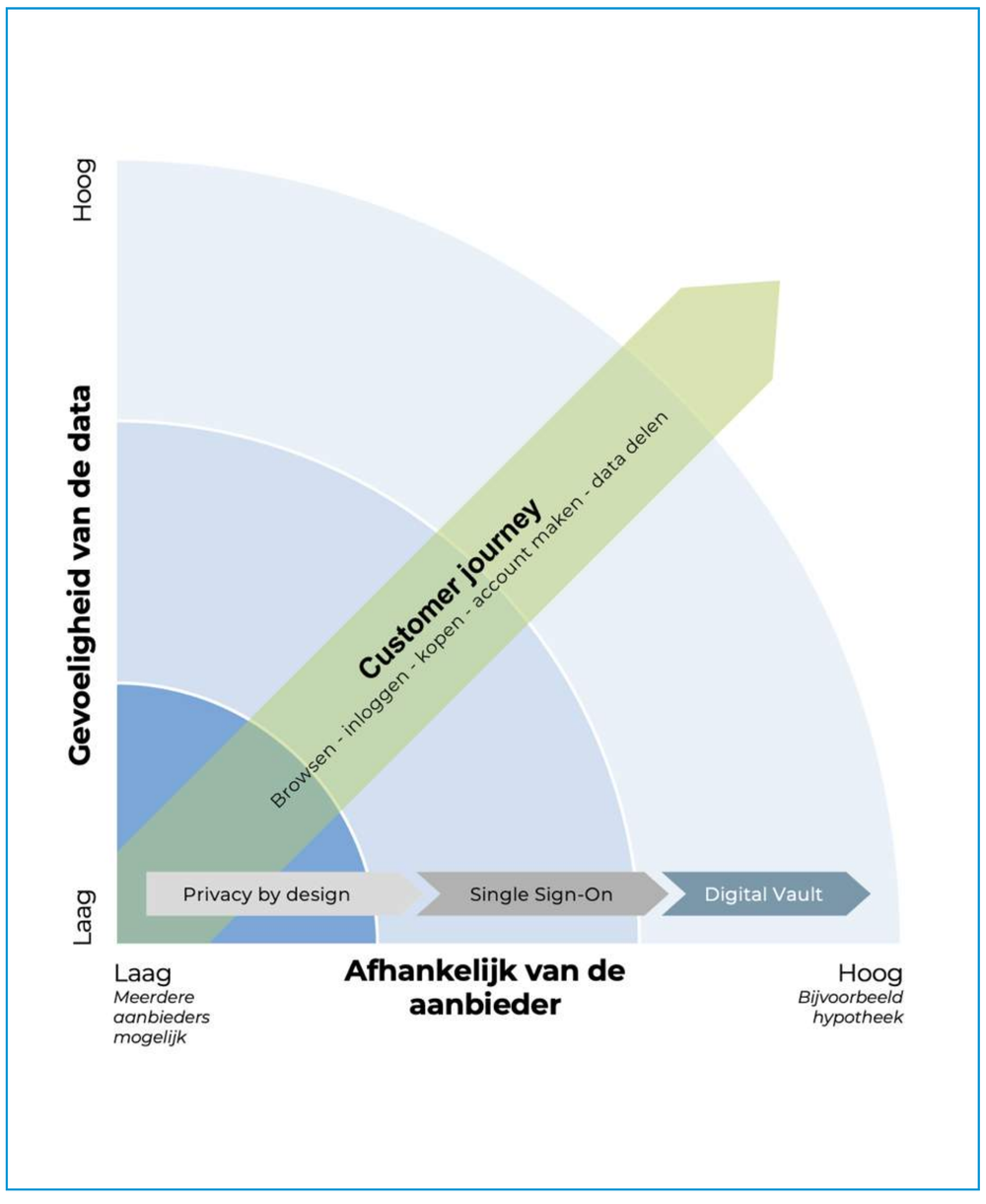
Het is een typische reactie op ons verhaal als we het hebben over de rol van het bedrijfsleven op het gebied van dataverzameling.
Voor het bedrijfsleven liggen de kansen voor het oprapen als ze juist aan de slag gaan met de verschillende privacyopties. We weten immers dat de klantloyaliteit stijgt bij een transparante manier van communiceren over data. Iets waar steeds meer bedrijven naar streven.
Als die opties worden geboden, krijgen de verschillende type persona's de mogelijkheid om weer iets meer regie terug te pakken. En daar heeft niet alleen de consument profijt van, maar ook het bedrijf zelf.

Met name voor BigTech ligt er een uitdaging. Kunnen deze grote en bijna onmisbare bedrijven met al hun data en 'macht' een positieve invloed uitoefenen op het vertrouwen van de consument en het gevoel van controle? Uniforme en gebruiksvriendelijke tools, zoals een Personal Digital Vault, kunnen het laatste zetje betekenen. Als consumenten naar eigen inzicht hun data kunnen beheren of delen, zijn zij in staat om de regie écht weer over te nemen.

Welke impact heeft dit op de relatie tussen consument en merk?
De veranderingen in consumentengedrag veranderen ook de relatie tussen consument en merk. Enerzijds zullen met name bedrijven die gevoelige data nodig hebben een manier moeten aanbieden die voldoende vertrouwen wekt om gevoelige data te delen. We hebben het dan over financiële informatie, medische achtergrond en gezichtsprofielen. Een Personal Digital Vault kan hierbij helpen.

Anderzijds is het belangrijk hoe afhankelijk een consument is van een aanbieder. Kan een consument niet zonder een dienst of platform, zal hij meer druk voelen om data te delen. Bij een zorgverzekeraar moet je persoonlijke data wel delen, bij een meubelleverancier niet. Zo kan een consument alleen zijn naam en adres willen afgeven als hij online bij HEMA ondergoed bestelt en daarna zonder bezwaren zijn persoonlijke gegevens, inclusief BSN, afstaan voor een zorgverzekering bij dezelfde HEMA.

In de visualisatie is te zien hoe spelers in de e-commercemarkt met de drie scenario's aan de slag kunnen om in te spelen op de behoefte van hun klanten.



Overigens speelt ook de fase in de customer journey en de relatie met het bedrijf mee. Als een consument zich oriënteert, zal hij minder bereid zijn data te delen. Voor privacy waakzamen en privacy protectionisten kan een toestemmingspop-up met een overdaad aan partners en technische opties daarom een reden zijn om naar een andere website over te gaan. Daarentegen is Privacy by Design een goede manier om vertrouwen te wekken. Maar als consumenten een product willen kopen of wanneer ze van een bepaalde dienst willen gebruikmaken, zijn opties als SSO of Digital Vault een goed alternatief.

6 Conclusie

Gedreven door nieuwe wet- en regelgeving, toenemende bewustwording en/of (commerciële) partijen die inspelen op de veranderende behoefte zal de consument de regie weer overnemen over zijn eigen online persoonsgegevens. Met Privacy by Design, Personal Digital Wallet en Single Sign-On zijn technologische opties voorhanden, maar het succes zal grotendeels afhangen van externe prikkels. Denk aan nieuwe wetgeving, de handhaving daarvan en de adoptie door grote platformen en organisaties. Als de juiste omstandigheden zijn gecreëerd, kunnen deze scenario's bijdragen aan een verandering in consumentengedrag met betrekking tot privacy en de relatie tussen consumenten en merken versterken.

Op dit moment zijn er nog te veel afhankelijkheden en onduidelijkheden voor de consument. Over hun rechten, over welke opties ze hebben enzovoort. Zeker consumenten die niet voldoende kennis hebben over online privacy, of zij die gemak belangrijker vinden dan online veiligheid, moeten voorlichting krijgen over de risico's van het delen van hun persoonlijke data. Maar ook over welke opties er zijn om deze data te beschermen. Hoe zal over 15 jaar met onze privacy worden omgegaan? Is het nog steeds een groot issue? Gaan we te maken krijgen met grote schandalen? Kunnen we niet meer terug omdat we zo afhankelijk zijn geworden van data en het ons enorm veel gemak brengt of hebben we een nieuwe vorm van dataverzameling gevonden waar alle partijen voordeel uit kunnen halen? Het onderzoek Flip the script staat nog aan het begin van deze zoektocht.

Hosts & voorzitter

Ilse Büter

Propositie Manager
Happy Horizon

Michiel Baart

Manager Business Relations
Happy Horizon

Simone van Diemen

Senior Partner Manager
Digital Agencies
Mollie

Chantal Schinkels

E-commerce Specialist
De IT girl

Leden expertgroep

Annabel van Dingenen

Conceptontwikkelaar
Jumbo Retail Media
Jumbo Supermarkten

Britt Timmerman

Customer Journey
Expert
ING bank

Charles van der Schot

Consumer journey
datamanager Western
Europe
**BSH
Huishoudapparaten**

Denise Visser - Koot

Product Manager
Experimentation
Bol.com

Djim Segers

Adviseur Public Affairs
Thuiswinkel.org

Emiel Fokker

Ondernemer
Startups & Scale-ups

Heidi Anthonis

Chief Innovation
Officer
Happy Horizon

Joanna Strycharz

Assistant Professor
**Universiteit van
Amsterdam**

Jordy Smit

Sr. Client Director
Microsoft

Leah Griffioen-Van Putten

Project Manager Data
Science
TNO

Nanda Appelman

Market Insights
Specialist
DDMA

Paul Maijers

Managing Director
Boxplosive

Ragild Raupp

CRM Specialist
G-Star Raw

Reineke Reitsma

Head of Data and
Technology
Ipsos

Thea van Oosterhout

Consultant Payments,
Identity & Data
Mariposa

Deze bluepaper is mede mogelijk gemaakt door ShoppingTomorrow – Thuiswinkel.org en