



Onderzoeksrapport

DDMA Privacy Monitor 2025

Hoe Nederlandse consumenten geïnformeerd willen en moeten worden over online privacy en data delen



Inhoudsopgave

Introductie	03
Managementsamenvatting	04
Hoofdconclusies DDMA Privacy Monitor 2025	09
Wet- en regelgeving rondom online privacy en het delen van data	22
Aanbevelingen	32
Onderzoeksverantwoording en colofon	33

Introductie

Uit de 2023-editie van de DDMA Privacy Monitor bleek dat de eerste reactie van Nederlandse consumenten is om de hakken in het zand te zetten als het gaat om online privacy en het delen van data. Maar bij meer uitleg, transparantie en duidelijkheid staan consumenten er zeker voor open om data met organisaties te delen en deze bereidheid groeit ook door de tijd.

Vanuit Nederlandse regel- en wetgeving is niet concreet gespecificeerd hoe organisaties consumenten het beste kunnen informeren over wat er met hun data gebeurt. De vernieuwde **Leidraad Bescherming Online Consument van Autoriteit Consument & Markt** (ACM, mei 2024) geeft iets meer richting, maar er is nog steeds veel ruimte voor eigen invulling vanuit organisaties. In deze nieuwe editie van de DDMA Privacy Monitor diepen we verder uit hoe consumenten het liefst geïnformeerd willen worden over hun online privacy en het delen van data, ook bij het gebruik voor AI. En aan de andere kant: hoe zij door organisatie geïnformeerd móeten worden vanuit Nederlandse regel- en wetgeving.

Hoe consumenten geïnformeerd willen worden

De DDMA Privacy Monitor bestaat dit jaar uit twee delen. In het eerste deel behandelen we inzichten afkomstig uit kwalitatief onderzoek uitgevoerd door middel van groepsgesprekken in verschillende focusgroepen, wat ons waardevolle inzichten heeft gegeven. Om deze inzichten cijfermatig te onderbouwen grijpen we af en toe terug op het meest recente kwantitatieve Global Privacy Monitor-onderzoek uit 2022.

We gaan onder meer in op vragen als: op welke manier willen consumenten geïnformeerd worden over wat er met hun data gebeurt, wat vinden zij belangrijk en duidelijk? Wat is het kennisniveau en sentiment van consumenten rondom AI en het gebruik van hun data daarvoor? Wanneer ervaren consumenten voldoende controle en wanneer wordt informeren nudging?

Hoe organisaties consumenten móeten informeren

Daartegenover zetten we in het tweede deel uiteen hoe organisaties consumenten móeten informeren over hun online privacy en het delen van data conform regel- en wetgeving. Met als doel om tot concrete adviezen te komen voor organisaties die zich bezighouden met data en marketing.

Managementsamenvatting



Transparante informatievoorziening loont en zet je (potentiële) klant centraal

Transparante informatievoorziening rondom online privacy en het delen van data is niet alleen een morele verantwoordelijkheid voor organisaties, maar ook een strategische kans om vertrouwen van (potentiële) klanten te winnen en de bereidheid om data te willen delen te vergroten.

Door inzicht te bieden in het hoe en waarom van data-verzameling, voordelen voor de consument duidelijk te maken en de communicatie af te stemmen op het kennisniveau van de doelgroep, versterk je als organisatie niet alleen de relatie met je klant, maar draag je ook bij aan eigen succes.

Huidige situatie toont gelaten acceptatie van consumenten rondom data delen

Consumenten hebben het gevoel dat ze geen echte keuze hebben als het gaat om het delen van data, het lijkt onvermijdelijk in het huidige digitale leven. Hoewel ze iets beter op de hoogte lijken te zijn over online privacy, blijft het gebrek aan diepgaand begrip en complexe cookiebanners en privacy-verklaringen een belemmering vormen. Dit zorgt ervoor dat negatieve associaties over online privacy en het delen van data blijven bestaan.

Meer kennis en begrip over wat er met hun data gebeurt en welke keuzes ze hebben, kan ervoor zorgen dat consumenten minder negatief tegenover het delen van data staan.

Meer consumentenbewustwording rondom de waarde van hun data ('consent or pay')

De voorkeur van consumenten voor betalen voor een online dienst, service of product of gratis gebruik in ruil voor het delen van data of vrijwillig doneren, wordt beïnvloed door het type dienst en de perceptie van rechtvaardigheid.

Hoewel bewustwording rondom het delen van data groeit, heeft een aantal consumenten nog altijd een gevoel van onrechtvaardigheid, vooral wanneer ze moeten betalen voor online diensten die voorheen gratis waren. Het vrijwillig doneren voor een online dienst staat men positiever tegenover, zoals voor journalistieke platformen of nieuwsmedia.

Cookiebanners worden veelal verstorend en complex gevonden

Consumenten willen graag bewuster omgaan met hun cookie-voorkeuren, maar worden hierin beperkt door de verstorende werking van cookiebanners en de complexe en vaak misleidende opzet ervan. Het gebrek aan kennis over de gevolgen van hun keuzes, en de nog altijd bestaande overtuiging dat websites zonder cookies niet of niet goed werken, zorgt voor een verminderd gevoel van controle.

Hoe zien consumenten cookiebanners het liefst?

Een gebruiksvriendelijke cookiebanner biedt duidelijke, beknopte informatie in één oogopslag over welke data wordt verzameld, hoe deze data wordt gebruikt, wat het voordeel is van het accepteren van cookies voor de consumenten en het mogelijke nadeel van weigeren. Daarnaast vinden consumenten het fijn als de configuratie en lay-out van de buttons eerlijk en eenvoudig zijn, waarbij gelijkwaardig vormgegeven keuzes worden getoond.

Wat werkt bij het informeren van consumenten over de privacyverklaring

Uit de groepsgesprekken blijkt dat veel consumenten geen privacyverklaringen lezen, voornamelijk vanwege de complexiteit en de onderbreking van hun gebruikservaring. Wanneer consumenten zich toch verdiepen in een privacyverklaring, zien ze het liefst een scanbare opzet met begrijpelijke taal en een betrouwbare toon. Het toevoegen van informatie over de voordelen van data-uitwisseling voor de consument kan ook bijdragen aan een positievere ervaring.

Verschillende verwachtingen voor verschillende organisaties

De verwachtingen en het vertrouwen van consumenten rondom online privacy verschilt per type organisatie. Bij grote en gevoelige organisaties liggen de verwachtingen hoger, terwijl consumenten buitenlandse – en dan met name Russische en Chinese – organisaties minder vertrouwen geven.

De klantrelatie speelt ook een belangrijke rol in hoe bereid consumenten zijn om hun data te delen. Loyaliteit en vertrouwen kunnen de bereidheid om gegevens te delen vergroten, terwijl een gebrek in vertrouwen dit juist kan verminderen.

De ideale omgang met online privacy volgens consumenten

Consumenten hechten veel waarde aan duidelijkheid en transparantie bij het omgaan met online privacy. De wens voor standaardisatie van cookiebanners en privacyverklaringen, betere consumentenvoorlichting over online privacy, en het gebruik van een keurmerk voor online privacy geven aan dat consumenten in zekere zin de verantwoordelijkheid ook willen delen met toezichhouders, branchevertegenwoordigers en/of organisaties. Het voldoen aan deze behoeften kan de marketing-sector helpen een betrouwbaarder imago op te bouwen bij hun consumenten.

Door onwetendheid stelt consument nog geen nieuwe eisen aan AI

Bij consumenten ontbreekt kennis over AI, de impact ervan op hun online privacy en mogelijke privacy risico's. Er is enthousiasme voor met name ChatGPT, maar consumenten staan nauwelijks stil bij wat er gebeurt met de data die ze delen en ook commerciële toepassingen van AI worden niet gezien. Dit gebrek aan kennis zorgt ervoor dat consumenten op dit moment niet het gevoel hebben dat AI nieuwe eisen stelt aan hoe om te gaan met hun online privacy.

Vertrouwen en bewustwording nodig voor verdere AI adoptie

AI bevindt zich nog in de adoptiefase van de early majority, wat betekent dat er nog veel kansen zijn voor verdere adoptie en integratie. Vertrouwen en bewustwording van consumenten zijn cruciaal om verdere adoptie te bevorderen.

Organisaties hebben hierbij een belangrijke rol, niet alleen door AI toe te passen, maar ook door transparant te zijn over hoe ze AI toepassen, welke gegevens ze verzamelen en welke risico's en voordelen voor consumenten dit met zich meebrengt.



Onderzoekstoelichting: Drie typen consumenten

Consumenten kunnen een pragmatische, onbezorgde of sceptische houding hebben ten aanzien van online privacy en het delen van data

In 2022 onderscheidde we al drie typen consumenten, kijkend naar enerzijds de zorgen rondom hun online privacy en anderzijds de bereidheid om data te delen: de pragmatici, de onbezorgden en de sceptici. In de bespreking van de hoofdconclusies gebruiken we deze groepen om de resultaten te duiden.



De **pragmatist** is iemand die behoorlijk bezorgd is (score >6) over diens online privacy, maar nog steeds redelijk bereid om gegevens te delen (score \geq 5).



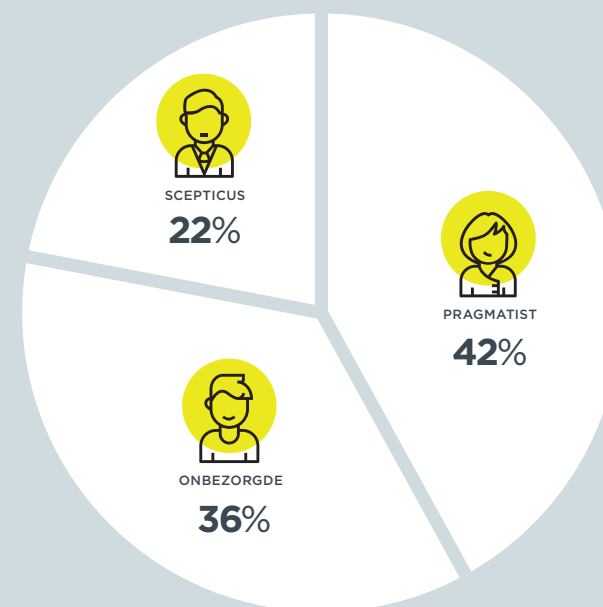
De **onbezorgde** maakt zich weinig zorgen over diens online privacy (score \leq 6).



De **scepticus** is behoorlijk bezorgd (score > 6) over diens online privacy en niet bereid om gegevens te delen (score < 5).

De Nederlandse samenleving bestaat vooral uit pragmatisten (42%) en onbezorgden (36%). 1 op de 5 Nederlanders (22%) staat sceptisch tegenover het delen van data. De uitgevoerde focusgroepen zijn gevormd op basis van deze groepen, met 1 groep alleen maar pragmatisten, 1 groep onbezorgden en 1 groep sceptici.

Houding t.a.v. online privacy en het delen van data



Bron: Global Privacy Monitor 2022, selectie: Nederland

Hoofdconclusies DDMA Privacy Monitor 2025

Hoe Nederlandse consumenten geïnformeerd willen worden over online privacy en het delen van data



Transparante informatievoorziening loont en zet je (potentiële) klant centraal

In een tijd waarin online interactie en dataverzameling alledaags is, groeit het belang van transparante informatievoorziening. 70% van de Nederlandse consumenten vindt het (zeer) belangrijk dat organisaties transparant zijn over hoe hun persoonlijke data wordt verzameld en gebruikt, bleek al uit de Global Privacy Monitor 2022. Dit vraagt om aandacht van organisaties: niet alleen om te voldoen aan verwachtingen van de consument, maar ook om eigen organisatiedoelen te ondersteunen.

Het belang van transparantie

Transparante informatievoorziening biedt consumenten een gevoel van controle over hun data. Dit heeft niet alleen een positief effect op hun vertrouwen, maar vergroot ook de bereidheid om persoonlijke gegevens te delen. De belangrijkste informatie die organisaties kunnen geven om de bereidheid te vergroten zijn:

- ▼ De reden voor dataverzameling (44%)
- ▼ Welke typen persoonsgegevens worden verzameld (36%)
- ▼ De voordelen voor de consument (35%)
- ▼ En of de data wordt gedeeld met derde partijen (35%)

Dit geldt voor zowel de pragmatisten als de onbezorgden. Voor de sceptici zijn extra details ook van belang, zoals de bewaartermijn van gegevens en de mogelijkheid om deze op verzoek te laten verwijderen.

Mijn bereidheid om mijn persoonlijke gegevens te delen is afhankelijk van...



Bron: Global Privacy Monitor 2022, selectie: Nederland

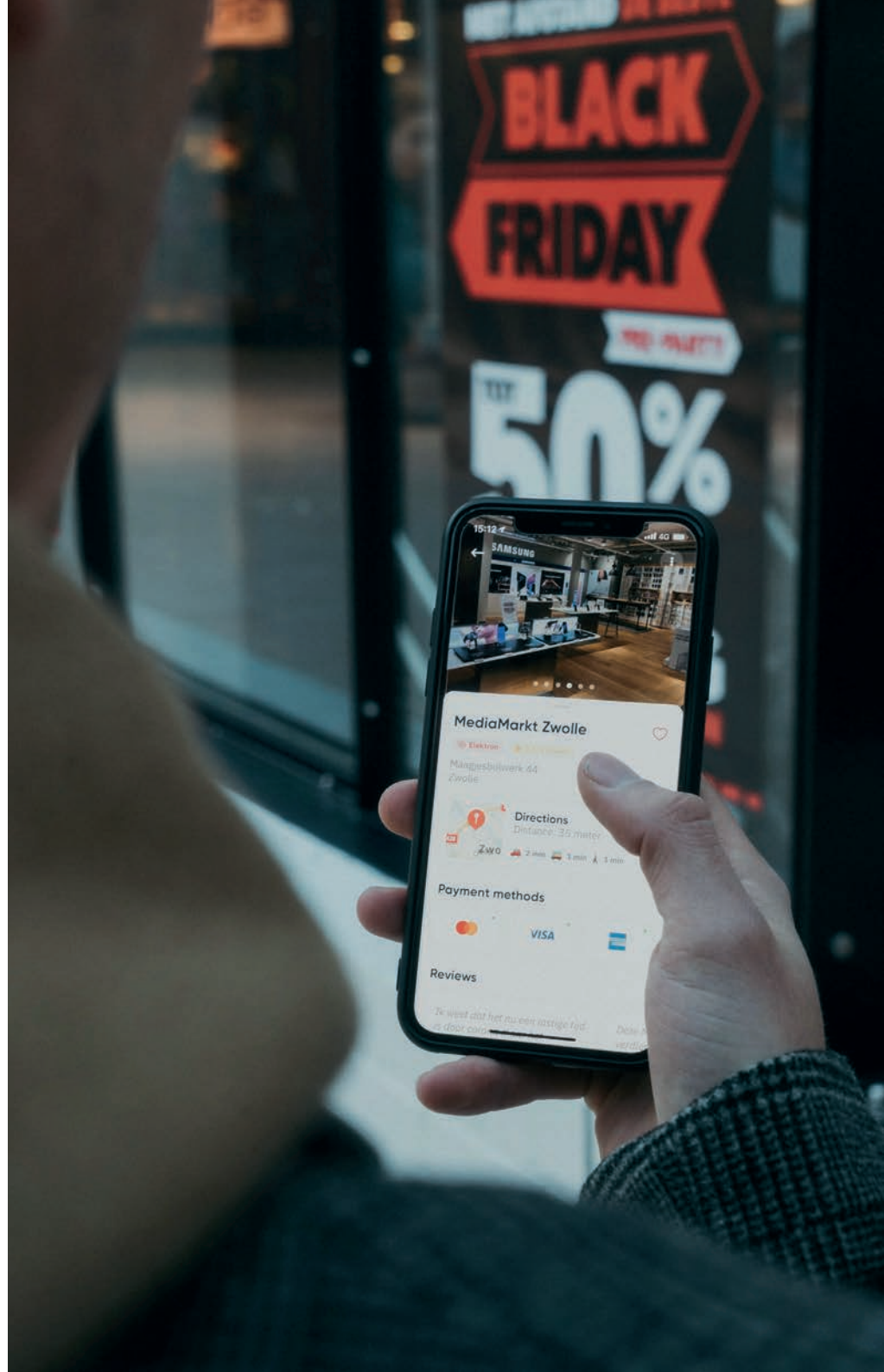
Vertrouwen als sleutel tot bereidheid om data te delen

Een centraal uitgangspunt voor consumenten is vertrouwen. Volgens de Global Privacy Monitor 2022 geeft 37% van de Nederlanders aan dat vertrouwen in een organisatie de belangrijkste voorwaarde is om persoonlijke gegevens te delen. Vertrouwen ontstaat niet alleen door transparantie, maar ook door het centraal stellen van de klant bij het formuleren van privacy- en cookiebeleid.

Tegelijkertijd bleek al uit de **DDMA Privacy Monitor 2023** dat de consument vooral uit eigen belang handelt bij het delen van data. Ze zijn bereid data te delen als ze daar direct voordeel van ervaren. Dit vraagt van organisaties om te achterhalen wat hun doelgroep als voordelen van data-uitwisseling met het desbetreffende product, dienst of service ziet.

Begrip bevordert acceptatie

Uit de recente groeps gesprekken voor deze editie van de Privacy Monitor met Nederlandse consumenten blijkt dat kennis bijdraagt aan een positievere houding ten opzichte van het delen van data. Daarom is het voor organisaties van belang om zich te verdiepen in het kennisniveau van de (potentiële) klant. Consumenten die begrijpen waarom gegevens worden verzameld, wat ermee wordt gedaan, en die controle ervaren, staan hier pragmatischer tegenover. Dit benadrukt het belang voor organisaties om niet alleen transparant te zijn, maar hun communicatie ook af te stemmen op het kennisniveau van hun doelgroep.



Huidige situatie toont gelaten acceptatie van consumenten rondom data delen

In de recente groepsgesprekken over online privacy en het delen van data, overheersten negatieve associaties bij consumenten. Veel consumenten ervaren een gevoel van gelaten acceptatie, omdat zij denken geen echte keuze te hebben. Ze zijn van mening dat volwaardig meedoen in de maatschappij, waar onder meer appen, social media en online aankopen doen een grote rol spelen, onvermijdelijk gepaard gaat met het delen van persoonlijke data.

Dit gevoel wordt onderbouwd in de Global Privacy Monitor 2022, waarin 66% van de consumenten aangaf dat het delen van persoonsgegevens een steeds groter onderdeel uitmaakt van het moderne leven. Bij pragmatici is dit gevoel met 74% nog iets sterker dan bij sceptici (57%) en onbezorgden (63%).

“Het maakt mij niet zo veel uit hoe ze het communiceren. Ik heb het idee dat het toch wel moet gebeuren. Ik heb er nog nooit iets negatiefs over ervaren.”

Consument uit het kwalitatief onderzoek

Deze gelaten acceptatie ligt ook in het lage gevoel van controle, mede door de frequentie en complexiteit van cookiebanners en privacyverklaringen. Consumenten benoemen het ondoenlijk om deze bij iedere website of app die ze gebruiken goed door te nemen en voelen zich daardoor gedwongen om maar op ‘accepteren’ te klikken.

Kennisniveau blijft beperkt terwijl dit kan zorgen voor positievere perceptie

Hoewel het kennisniveau over online privacy lijkt te zijn toegenomen vergeleken met een aantal jaar geleden, ontbreekt vaak nog diepgaand begrip. Zo denken de consumenten bijvoorbeeld vaak nog dat een website niet of niet goed functioneert zonder cookies, wat de negatieve associaties rond online privacy en het delen van data in stand houdt.

Op verschillende punten in de groepsgesprekken met consumenten, zagen we terug dat meer kennis en bewustzijn rondom online privacy en het delen van data kan bijdragen aan positievere percepties. Consumenten die begrijpen hoe hun data wordt gebruikt en welke keuzes ze daadwerkelijk hebben, ervaren minder negatieve gevoelens over het delen van data.

Meer consumentenbewustwording rondom de waarde van hun data ('consent or pay')

Er lijkt ook iets meer bewustwording te ontstaan onder de consumenten rondom de werking van marketing en de waarde van hun persoonlijke data. De meesten realiseren zich dat het gebruik van gratis websites en app, zoals sociale media, nieuwsplatformen, het weer of spelletjes, vaak gepaard gaan met bewust of onbewust data delen en advertenties.

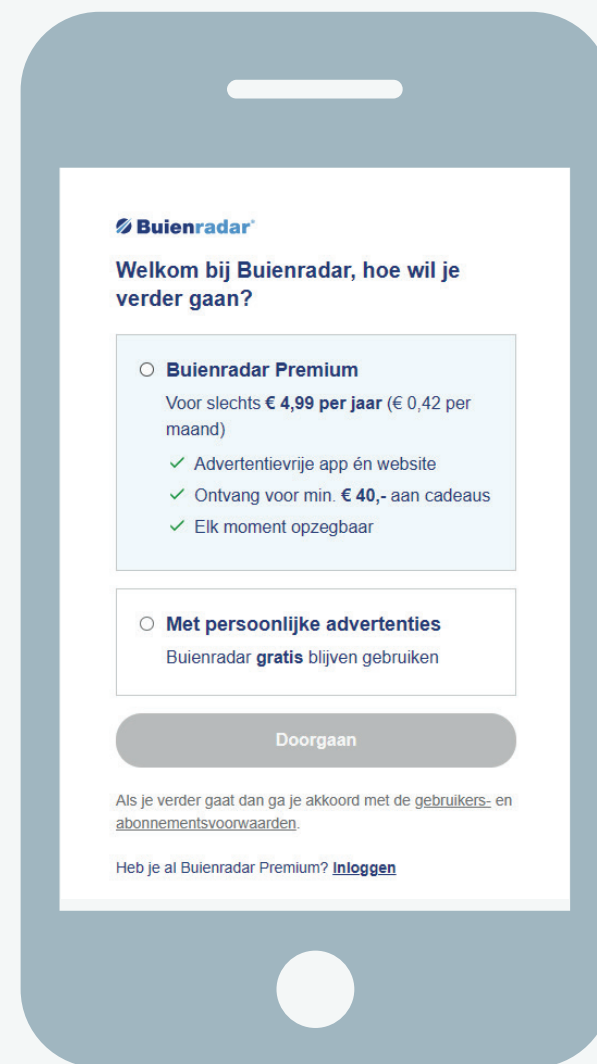
Dit bewustzijn brengt gemengde gevoelens met zich mee: een deel van de consumenten erkent dat ze afhankelijk zijn geworden van deze websites of apps, en begrijpen dat deze organisaties ook niet gratis kunnen opereren. Maar anderen zijn zo gewend geraakt dat bepaalde diensten gratis beschikbaar zijn op internet, dat de introductie van betaalopties, zoals bij het voorbeeld van Buienradar, tot gevoelens van onrechtvaardigheid leidt. Vooral de pragmatici en sceptici vinden zich hierover op.

**"Dat is toch de omgekeerde wereld!
Je wilt privacy en daar moet je voor betalen.
Dat is toch achterlijk?!"**

Consument uit het kwalitatief onderzoek

"Mensen met geld kunnen dan geen reclame krijgen. Het wordt een luxe. Het moet een recht zijn voor iedereen."

Consument uit het kwalitatief onderzoek



Bron: Cookiebanner Buienradar, oktober 2024

Voorkeuren voor data delen of betalen voor online diensten

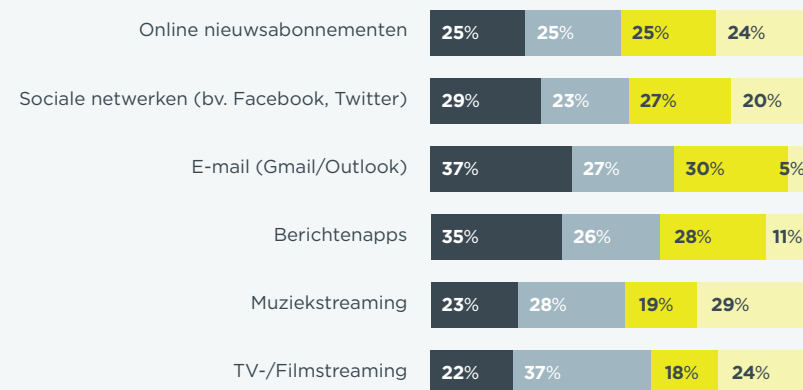
Uit de Global Privacy Monitor 2022 bleek al dat Nederlandse consumenten voorkeur geven aan betalen voor online diensten waarvoor bij introductie ook al betaald moest worden. Zo kiezen consumenten bij diensten als muziekstreaming (28%) en tv-/filmstreaming (37%) vaker voor betalen voor de dienst boven gratis gebruik in ruil voor het delen van data. Daarentegen geven consumenten bij sociale media (29%), e-mail (37%) en berichtenapps (35%) juist voorkeur aan gratis gebruik in ruil voor het delen van data.

Sceptici zijn wat terughoudender in de bereidheid om data te delen en geven vaker aan deze diensten helemaal niet te gebruiken. Onbezorgden geven daarentegen vaker de voorkeur voor gratis gebruik in ruil voor het delen van data.

Categorie 'bereidheid om te doneren' stemt mild

Een derde optie die, naast data delen of betalen voor online diensten, steeds gebruikelijker wordt is de bereidheid vragen om vrijwillig persoonlijke data of geld te doneren. Het vragen om een financiële donatie wordt onder andere gehanteerd door journalistieke platformen of nieuwsmedia (zie voorbeeld *The Guardian* op p. 15). Deze categorie roept minder weerstand op bij de consumenten, omdat het begrijpelijker voelt dat kwaliteitsjournalistiek geld kost en het doneren vrijwillig is.

Data delen of betalen voor online diensten




- Ik geef er de voorkeur aan om persoonlijke informatie met deze dienst te delen om deze gratis te gebruiken
- Ik geef er de voorkeur aan om voor deze dienst te betalen zodat ik geen persoonlijke informatie hoeft te delen
- Weet ik niet
- Niet van toepassing - ik zou deze dienst nooit gebruiken

Bron: Global Privacy Monitor 2022, selectie: Nederland

“The Guardian maakt het inzichtelijk op een heldere manier en je hebt zelf de regie.”

Consument uit het kwalitatief onderzoek

 **It's your choice**

When we make the Guardian available to you online, we and our partners may use cookies and similar technologies to help us to do this. Some are necessary to help our website work properly and can't be switched off, and some are optional but support the Guardian and your experience in other ways. To do this we work with a cross section of 156 [partners](#).

Cookies and other similar technologies may be used to access personal data, including page visits and your IP address. We use this information about you, your devices and your online interactions with us to provide, analyse and improve our services. Depending on your choice, we may also use your data to personalise content or advertising.

We use cookies and similar technologies for the following purposes:


- ✓ Store and/or access information on a device
- ✓ Personalised advertising and content, advertising and content measurement, audience research and services development

Learn more in our [privacy policy](#) and [cookie policy](#), and manage the choices available to you at any time by going to 'Privacy settings' at the bottom of any page.

Are you happy to accept cookies?
To manage your cookie choices now, or to opt out where our partners rely on legitimate interests to use your information, [click on manage cookies](#).

Yes, I accept No, thank you Manage cookies

Bron: Cookiebanner The Guardian, oktober 2024

Rejection hurts ... 

You've chosen to reject third-party cookies while browsing our site. **Not being able to use third party cookies means we make less from selling adverts to fund our journalism.**





We believe that access to trustworthy, factual information is in the public good, which is why we keep our website open to all, without a paywall.

If you don't want to receive personalised ads but would still like to help the Guardian produce great journalism 24/7, please support us today. It only takes a minute. Thank you.

One-time **Monthly** Annual

€4 per month **€12 per month**

Other

Continue →    

Not ready to support today? [Remind me later](#)

The Guardian

Bron: [Cookiebanner The Guardian](#) na klikken op 'No, thank you', oktober 2024

Cookiebanners worden veelal verstorend en complex gevonden

Als we dieper ingaan op de controle die consumenten ervaren om hun online privacy te bewaken, benoemen ze in de groeps gesprekken het bewust omgaan met cookies als de meest voor de hand liggende manier. De consumenten geven aan dat je met cookiebanners eigenlijk heel bewust om zou moeten gaan, maar vinden dat in de praktijk lastig. Dat heeft enerzijds te maken met de onderbreking van hun online activiteiten, en anderzijds ervaren ze de informatie in een cookiebanner als te complex of misleidend. De Global Privacy Monitor 2022 liet al zien dat slechts 23% van de Nederlanders een gevoel van controle ervaart bij het instellen van privacy-instellingen. Dit percentage is het laagst onder sceptici (11%), terwijl pragmatici (33%) en onbezorgden (19%) zich iets meer in controle voelen.

“Ik heb er geen controle over en het is onoverzichtelijk. Maar ik lees me er niet constant over in. Je functioneert niet meer zonder cookies.”

Consument uit het kwalitatief onderzoek

Cookiebanner werkt verstorend

De consumenten benoemen dat cookiemeldingen hen afleiden van hun doel op een website, zoals informatie zoeken of iets kopen. Waarbij elke website weer een andere cookiebanner hanteert, wat leidt tot irritatie en tijdverlies. Dit zorgt ervoor dat gebruikers vaak blindelings de cookies accepteren en kiezen voor de meest opvallende button, zoals een gekleurde of bovenaan geplaatste optie, om snel verder te kunnen.

Cookiebanner is te complex en misleidend

Bovendien wordt de toelichtende tekst van cookiebanners vaak ook complex of misleidend gevonden. Consumenten missen vaak de marketingkennis om begrippen als ‘functionele cookies’ en ‘marketingcookies’ goed te begrijpen. En bijvoorbeeld bij de keuze tussen ‘alle cookies accepteren’ en ‘alleen vereiste cookies accepteren’, zijn veel consumenten onzeker over de gevolgen van hun keuze.

De misvatting heerst namelijk nog altijd dat websites niet of niet goed functioneren als cookies worden geweigerd. Hierdoor kiezen consumenten vaak voor ‘alles accepteren’, wat het gevoel van controle vermindert. Vooral de manier waarop de opties worden gepresenteerd, versterken dit patroon.

Hoe zien consumenten cookiebanners het liefst?

Korte, duidelijke informatie in één oogopslag...

Consumenten geven de voorkeur aan korte en begrijpelijke informatie in de cookiebanner. Ze willen in één oogopslag zien:

- ▼ **Welke gegevens** worden verzameld;
- ▼ **Hoe** deze gegevens worden **gebruikt**;
- ▼ Wat het **voordeel van het accepteren** van de cookies is voor de consument;
- ▼ En ook het uitleggen van het mogelijke **nadeel van niet accepteren** is belangrijk, bijvoorbeeld of de website dan nog goed werkt.

De informatie moet eenvoudig zijn en in één oogopslag zichtbaar zijn in de cookiebanner, waarbij ook direct de verwijzing naar de volledige privacyverklaring getoond wordt.



“Deze gebruikerservaring komt overeen met ons advies, net als dat van de Autoriteit Persoonsgegevens (AP): gebruik duidelijke woorden in de buttons zoals ‘accepteren’, ‘akkoord’ of ‘weigeren’ en zet verschillende keuzes zichtbaar op één laag. Website-bezoekers moeten net zo makkelijk kunnen weigeren als accepteren. Dat betekent dat iemand niet hoeft door te klikken om te weigeren, als dat voor (alles) accepteren ook niet hoeft. Ook is het verstandig om bij het gebruik van vinkjes en schuifjes deze niet automatisch aan te zetten. Lees meer hierover in het hoofdstuk ‘Cookies: met heldere communicatie smaken ze beter’”

Isa Nieuwstad, Legal Counsel bij DDMA

...dit geldt ook bij de buttonconfiguratie en -lay-out

Naast de informatie in de banner, speelt ook de opmaak van de keuze-opties een belangrijke rol voor een positievere gebruikerservaring:

- ▼ Consumenten willen graag **duidelijke, eerlijke keuzes** zien voor zowel de optie ‘accepteren’ als ‘weigeren’. De keuzes moeten **direct zichtbaar** zijn, zodat ze niet gedwongen worden door te klikken om verder te navigeren.

Slechts enkele consumenten die beter bekend zijn met de begrippen rondom cookies, zouden in sommige gevallen de mogelijkheid willen hebben om verschillende typen cookies aan en uit kunnen zetten, bij- voorbeeld via schuifknoppen. Voor de meerderheid van de consumenten wordt deze optie al snel als te complex en tijdrovend ervaren.

“Ligt aan hoe erg je ermee bezig bent. Als je het eng vindt wil je de meeste opties om het aan en uit te zetten. Als het je niet boeit vind je het prima.”

Consument uit het kwalitatief onderzoek

- ▼ Belangrijk hierbij is om voor de **consument begrijpelijke en consistente termen** te gebruiken bij de keuzes voor cookies.
- ▼ **Gelijkwaardig vormgegeven keuzes** worden positiever ervaren. Als bijvoorbeeld de button ‘alles accepteren’ een opvallendere kleur heeft, wordt dit gezien als misleiding.

Wat werkt bij het informeren van consumenten over de privacyverklaring?

De consumenten gaven toe dat ze privacyverklaringen zelden of nooit lezen. Hoewel sommigen in het verleden wel eens een privacyverklaring hebben doorgenomen, ervaren ze dit over het algemeen als te veel werk. Net als bij de cookiebanners geldt hier ook dat het moeten lezen van privacyverklaringen het initiële doel van website- of appbezoek verstoort en de materie wordt te complex en langdradig ervaren.

Als consumenten zich toch verdiepen in de privacyverklaring, zien ze het liefst dat:

- ▶ De tekst **snel scanbaar** is, bijvoorbeeld door het op te delen in duidelijke hoofdstukken en het gebruik van icoontjes om de informatie visueel te verduidelijken;
- ▶ Waarbij de tekst geschreven is in **eenvoudig en begrijpelijk taalgebruik**;
- ▶ Hierbij wordt het gewaardeerd als de tekst een **serieuze en betrouwbare toon** heeft. Een te jolige toon wordt ongepast gevonden voor een privacyverklaring;
- ▶ En een enkele consument merkte op dat privacyverklaringen vaak gericht zijn op wat de organisatie heeft aan de data, terwijl ze ook graag zien **wat de data-uitwisseling de consument oplevert**.

“Soms heb je ook een band met een bedrijf. Rituals mag alles van mij weten. Dat is geven en nemen.”

Consument uit het kwalitatief onderzoek

Verschillende privacyverwachtingen voor verschillende organisaties

Uit de groepsgesprekken blijkt dat consumenten verschillende verwachtingen hebben rondom de omgang met online privacy, afhankelijk van de grootte, sector en afkomst van de organisatie.

- ▶ Van **grote organisaties** wordt verwacht dat ze de online privacy goed op orde hebben met een degelijk en goed doordacht privacy beleid, mede vanwege het risico op imagoschade bij het onzorgvuldig omgaan met data. Bij **kleinere organisaties** stellen consumenten daar wat minder eisen aan.
- ▶ Bij **commerciële organisaties** spelen andere verwachtingen en eisen dan **gevoelige sectoren zoals banken, overheids- of zorginstellingen** vanwege andere belangen. Bij bijvoorbeeld banken, overheids- of zorginstellingen is er meer vertrouwen dat zij zorgvuldig met persoonsgegevens omgaan en deze goed beveiligen. Dit komt door het hogere risiconiveau dat gepaard gaat met de verwerking van gevoelige data in deze sectoren.
- ▶ Consumenten zijn over het algemeen minder geneigd om **buitenlandse organisaties** te vertrouwen, specifiek benoemd werden Russische en Chinese organisatie zoals Temu en AliExpress. Dit laat bovendien zien dat consumenten meer vertrouwen hebben in Nederlandse toezichthouders en wetgeving, en ervan uitgaan dat schandalen in de media aan het licht komen als organisaties zicht niet aan de regels houden.
- ▶ Daarnaast speelt de relatie die consumenten met een organisatie hebben ook een belangrijke rol in hun bereidheid om persoonlijke data te delen. Bij **loyale en geregeld terugkerende klanten** heb je een streepje op voor als organisatie, zij zijn vaak bereid om meer data te delen dan bij organisaties waar ze incidenteel terechtkomen.

Ideale omgang met online privacy volgens consumenten

Volgens de consumenten is de sleutel voor een succesvolle omgang met online privacy het bieden van duidelijkheid en transparantie. Ze benoemen hierbij een aantal sectorbrede oplossingen:

- Zo geven de consumenten aan dat ze het liefst zien dat er **standaardisatie van cookiebanners en privacyverklaringen** plaatsvindt. Zodat het informeren en toestemming vragen rondom online privacy en het delen van data altijd op dezelfde manier gebeurt en consumenten daardoor sneller en gemakkelijker begrijpen wat ze accepteren, zonder dat ze elk gebruiksmoment opnieuw deze informatie hoeven door te nemen.



“Veel organisaties implementeren cookiebanner generators (zoals Cookiebot), maar weten daarbij zelf ook niet exact wat het inhoudt en aan welke regels moet worden voldaan. Het gebruik van standaardbots is prima, maar wees wel kritisch op designkeuzes. Kiezen voor de optie ‘GDPR’ compliant, betekent niet automatisch de garantie voor een compliant cookiebanner. Volg altijd de vuistregels bij het ontwerpen van je cookiebanner, wat is terug te lezen in het hoofdstuk ‘Standaard cookiebanner-generators: waar let je op?’”

Isa Nieuwstad, Legal Counsel bij DDMA

- Een ander punt dat consumenten benoemen, is het **belang van consumentenvoorlichting** over de omgang met online privacy. Ze zouden graag meer informatie willen over wat zij zelf kunnen doen om hun privacy online te waarborgen. Dit zou onder andere moeten gaan over het lezen van privacyverklaringen, de verschillende soorten cookies en waar en waarom data wordt verzameld.



“De AP gaf eind 2024 een voorzet in haar publieks-campagne over privacy risico’s van cookies, waarmee de toezichthouder organisaties oproept hun cookie-beleid onder de loep te nemen.”

Isa Nieuwstad, Legal Counsel bij DDMA

- Tijdens de groepsgesprekken werd door alle drie de groepen spontaan **het voordeel van een keurmerk** genoemd. Dit keurmerk zou consumenten in één oogopslag laten zien of hun gegevens bij een bepaalde organisatie veilig worden behandeld. Ze gaven hierbij een aantal suggesties, zoals het tonen van privacylevels of stoplichtkleuren die het privacy-niveau aangeven.

DDMA Privacy Waarborg

Een voorbeeld van een dergelijk keurmerk is het DDMA Privacy Waarborg. Dit keurmerk kan via self audits intern bij organisaties voor de verwerking van persoonsgegevens voor marketingdoeleinden gebruikt worden. Het DDMA Privacy Waarborg biedt een interne privacy- en securitycheck waarmee organisaties consumenten en partners kunnen laten zien dat zij privacy respecteren en zorgvuldig en transparant omgaan met persoonsgegevens. Organisaties die het DDMA Privacy Waarborg voeren krijgen een betrouwbare uitstraling richting huidige en toekomstige consumenten en partijen om mee samen te werken. Alleen leden van DDMA komen in aanmerking voor het Privacy Waarborg. Voor meer informatie, zie: www.ddma.nl/privacy-waarborg

Door onwetendheid stelt consument nog geen nieuwe eisen aan AI

Er heerst onder consumenten nog veel onbekendheid rondom kunstmatige intelligentie (AI). Wanneer hen wordt gevraagd naar hun associaties met AI, denken ze vooral aan ChatGPT, een toepassing die inmiddels relatief bekend is. Andere toepassingen worden amper genoemd en over het algemeen is de kennis over de bredere inzet van AI beperkt.

Enthousiasme voor ChatGPT, maar onwetendheid over datagebruik en toekomstige ontwikkelingen

Desondanks is er bij consumenten enthousiasme over de mogelijkheden van ChatGPT. Ze gebruiken het voor werk of schoolopdrachten, het genereren van teksten en het krijgen van antwoorden op praktische vragen. Wat opvallend is, is dat consumenten nauwelijks stilstaan bij wat er gebeurt met de data die ze delen en of dit wenselijk is. Ze beschouwen de informatie die ze delen met ChatGPT vaak ook niet als privacygevoelig.

“Het verzamelt heel veel informatie. Hoe vaker ik het gebruik, hoe beter hij antwoord geeft voor mij.”

Consument uit het kwalitatief onderzoek

De beperkte kennis brengt alleen ook zorgen met zich mee. De consumenten vragen zich af waar de voortdurende ontwikkeling van AI uiteindelijk toe zal leiden, bijvoorbeeld of AI in de toekomst slimmer wordt dan de mens. Ook is er bezorgdheid over mogelijke misbruikscenario's, zoals deepfakes.

Ook commerciële toepassingen van AI worden niet gezien

Wat verder opviel, is dat mogelijke commerciële toepassingen van AI nauwelijks benoemd worden. De enige toepassing die genoemd werd, is de verwachting dat chatbots van organisaties in de toekomst steeds slimmer zullen worden. Consumenten gaan ervan uit dat de gegevens die ze met deze bots delen, op dezelfde manier worden behandeld als informatie die ze telefonisch delen met een klantenservice.

“Mij maakt het niet uit of het een robot of mens is. Mensen leren ook van de gesprekken die je voert. Daar hoeft je ook geen toestemming om te vragen.”

Consument uit het kwalitatief onderzoek

De rol van AI in het verwerken en analyseren van verzamelde data wordt in geen van de groepen spontaan benoemd. Zelfs als hier specifiek naar wordt gevraagd, blijkt dit voor de meeste respondenten een ongrijpbaar onderwerp te zijn. Door het gebrek aan kennis over hoe AI wordt toegepast door organisaties en op welke manier(en) hun gegevens ermee verwerkt worden, hebben consumenten op dit moment niet het gevoel dat AI nieuwe eisen stelt aan hoe om te gaan met hun online privacy.

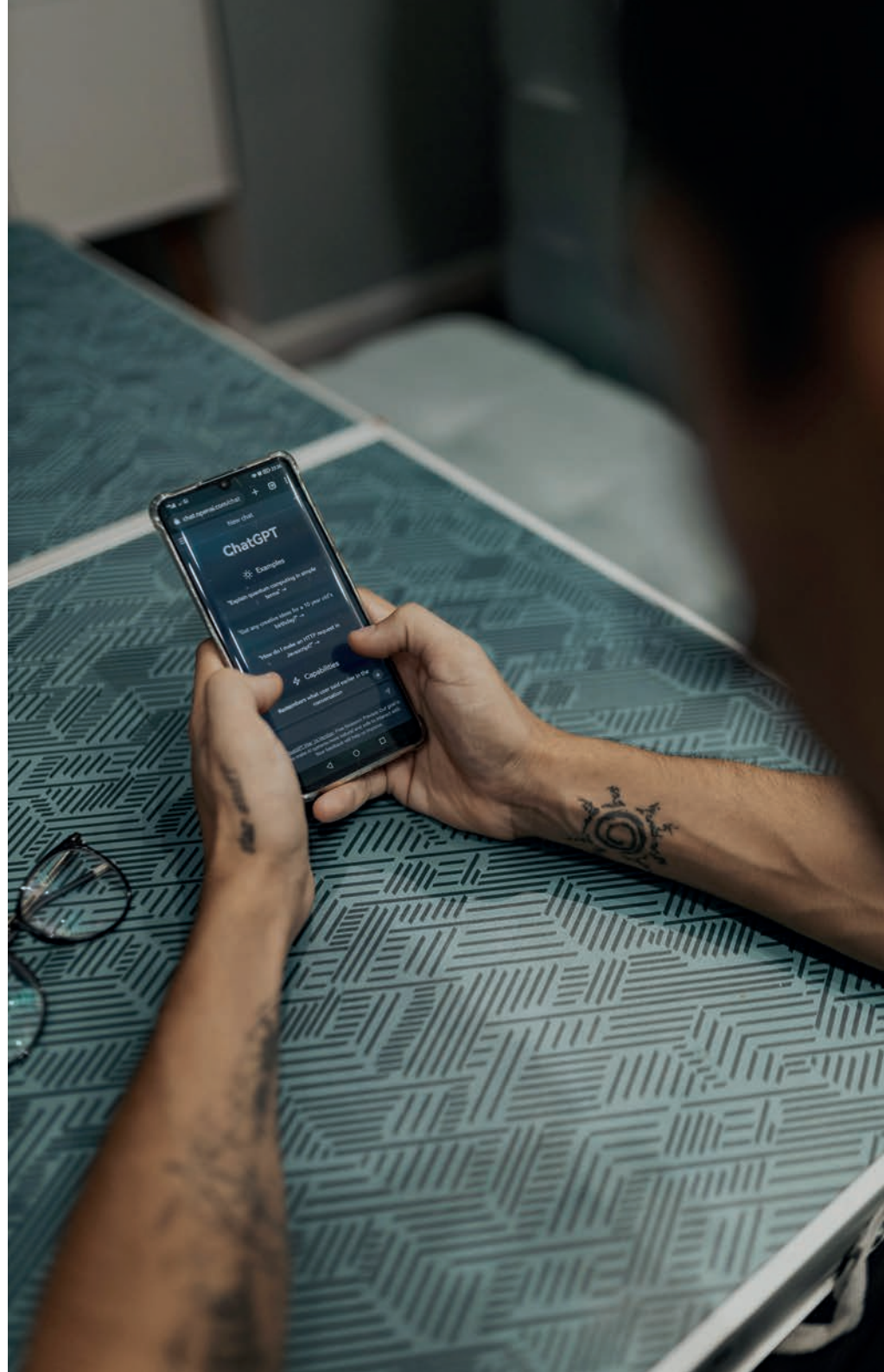
Vertrouwen en bewustwording nodig voor verdere AI adoptie

De adoptie van AI volgt het patroon van de innovatie-adoptiecurve van Rogers¹, die vijf fasen van technologie-adoptie beschrijft. Momenteel is AI nog niet volledig geïntegreerd bij de meerderheid van de gebruikers, maar verschillende groepen bevinden zich in uiteenlopende stadia van de adoptie:

- ▼ **Innovators:** de eerste groep gebruikers heeft AI volledig omarmd en verder ontwikkeld. Zij speelden een cruciale rol in het toegankelijk maken van gebruiksvriendelijke AI-tools en zijn vaak de voortrekkers in het verkennen van nieuwe technologieën.
- ▼ Ook de **pioniers** (ook wel de *early adopters*), vaak individuen en organisaties die geïnteresseerd zijn in nieuwe technologieën, zien de voordelen van AI en zijn inmiddels actief begonnen deze toe te passen, bijvoorbeeld in het gebruik van generatieve AI en automatiseringsmogelijkheden.
- ▼ De **early majority** toont groeiende interesse en begint interesse te tonen vooral voor praktische en toegankelijke toepassingen. Deze bredere groep consumenten en organisaties begint zich open te stellen voor AI, maar er zijn nog drempels, zoals het gebrek aan kennis en zorgen over privacy en ethiek, die bredere adoptie kunnen belemmeren.

Om de acceptatie van AI verder te bevorderen, ligt er een belangrijke taak voor organisaties om vertrouwen en bewustwording te creëren bij consumenten. Dit kan door transparant te zijn over hoe AI wordt toegepast, welke gegevens worden verzameld en welke risico's en voordelen voor consumenten dit met zich meebrengt.

¹ Rogers, E. M. (1962). *Diffusion of innovations*. Free Press of Glencoe.



Wet- en regelgeving rondom online privacy en het delen van data

Hoe organisaties consumenten
hierover móeten informeren
van data



Introductie

Een boete van 4,75 miljoen euro voor **Netflix**. Het klinkt als een opvallend nieuwsbericht, maar het is tegelijkertijd een duidelijke waarschuwing voor iedere organisatie die persoonsgegevens verwerkt. De Autoriteit Persoonsgegevens (AP) heeft deze boete opgelegd, omdat Netflix niet voldeed aan de wettelijke informatieplicht uit de Algemene Verordening Gegevensbescherming (AVG). De striktere aanpak van de toezichthouder benadrukt hoe belangrijk het is om zorgvuldig om te gaan met privacy en de communicatie hierover richting consumenten.

Sinds 2018 is de AVG van toepassing en zijn organisaties verplicht om transparant te zijn over het gebruik van persoonsgegevens. Of je nu e-mailadressen verzamelt voor een nieuwsbrief of data inzet om je doelgroep beter te begrijpen: de regels van de AVG zijn van toepassing. Het bieden van heldere en toegankelijke informatie over hoe je gegevens verwerkt, is niet alleen een wettelijk vereiste, maar ook een manier om het vertrouwen van consumenten te winnen en te behouden.

Als verantwoordelijke organisatie – of ‘verwerkingsverantwoordelijke’ in termen van de AVG – draag je de verantwoordelijkheid om bezoekers van je website inzicht en controle te geven over hun gegevens. Dit vraagt om duidelijke communicatie, zodat consumenten een weloverwogen keuze kunnen maken over het gebruik van hun persoonsgegevens.

In dit hoofdstuk bespreken we de belangrijkste juridische vereisten en bieden we praktische richtlijnen voor hoe je consumenten effectief kunt informeren. Met deze aanbevelingen bieden we bedrijven niet alleen handvatten voor de naleving van de wet, maar dragen we ook bij aan het bevorderen van transparantie, vertrouwen en een ethische benadering van communicatie.

Wat is de informatieplicht van organisaties?

Volgens de AVG moeten organisaties consumenten op een **duidelijke en toegankelijke** manier informeren over het gebruik van hun persoonsgegevens (artikelen 12 en 13 AVG). Deze verplichting start **voordat** gegevens worden verwerkt en vormt de basis voor een transparante en eerlijke omgang met data. Het betekent dat je proactief en helder communiceert over welke gegevens je verzamelt, waarom je dat doet, op welke juridische grondslag dit is gebaseerd en welke rechten consumenten hebben.

Deze informatie moet gemakkelijk te vinden zijn, bijvoorbeeld via een zichtbare link op de website naar een **privacyverklaring**. Dit document dient als een centraal punt waar consumenten terecht kunnen voor antwoorden op hun vragen over gegevensverwerking. Belangrijk is dat de taal en opmaak van de verklaring aansluiten bij de doelgroep, zodat de inhoud zowel correct als begrijpelijk is.

Voor marketingdoeleinden zijn toestemming en gerechtvaardigd belang de meest gangbare grondslagen voor verwerking

Als je werkt op basis van toestemming, die het meest als deze op de juiste manier is verkregen, zorg er dan voor dat deze vrijwillig, specifiek, ondubbelzinnig en aantoonbaar wordt gegeven. Het proces hiervoor moet eenvoudig en transparant zijn, zodat consumenten precies begrijpen waarvoor ze akkoord geven. Gerechtvaardigd belang biedt meer flexibiliteit en kan in de praktijk meer voordelen opleveren voor marketingdoeleinden, maar het vereist een zorgvuldige afweging tussen de belangen van de organisatie en de privacy van betrokkenen. Het is essentieel om deze afweging goed te documenteren en de consument duidelijk te informeren over de gehanteerde grondslag.

Meer weten?

Lees ons artikel over het [gerechtvaardigd belang](#).

Sommige gegevensverwerkingen, zoals het leveren van een dienst die door de consument is aangevraagd, kunnen gebaseerd zijn op de **grondslag van een overeenkomst**. Houd er rekening mee dat deze grondslag beperkt is tot wat strikt noodzakelijk is voor de levering van die specifieke dienst. Bij marketingactiviteiten kan een verwerking noodzakelijk zijn voor een overeenkomst, maar in de praktijk komt dit zelden voor, omdat het vaak lastig is om dit overtuigend te onderbouwen.



Ongeacht de grondslag: onthoud dat je consumenten altijd een opt-out moet aanbieden en actief moet informeren.

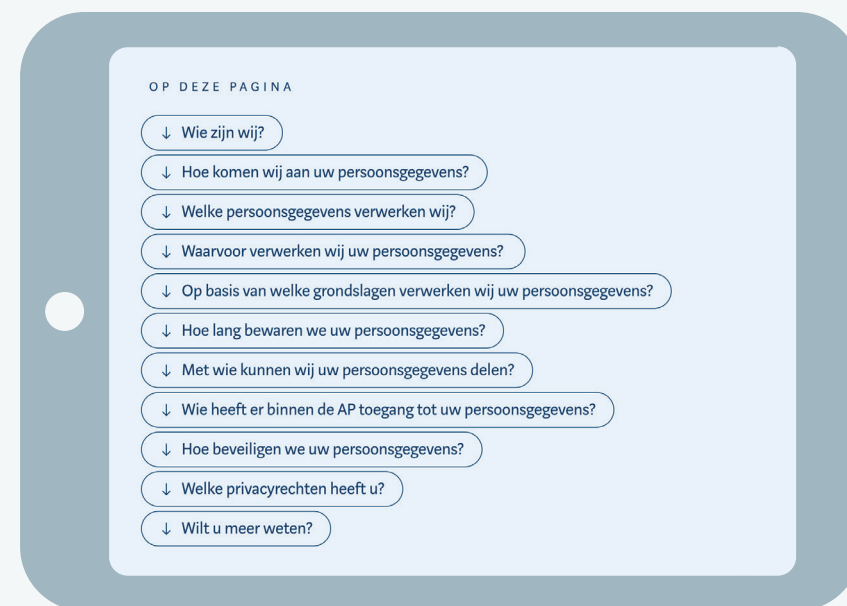
Hoe informeer je de consument over het verwerken van de persoonsgegevens?

Het is dus belangrijk om consumenten te informeren over wat er met hun gegevens gebeurt, waar ook de EDPB (Europese Privacykoepel van toezichthouders) op wijst. Het kan zelfs zo zijn dat sprake is van een oneerlijke handelspraktijk wanneer consumenten niet juist worden geïnformeerd over het gebruik van hun gegevens door een organisatie, **zo legde de ACM uit**. Maar hoe doe je dit?

Een privacyverklaring is een van de meest gebruikte middelen om deze informatie te verstrekken. Hoewel er geen strikte vormvereisten zijn, moeten de inhoud en structuur wel voldoen aan de uitgangspunten van toegankelijkheid en volledigheid. Het gebruik van een *gelaagde structuur* wordt daarbij aanbevolen, waarbij je de belangrijkste informatie, zoals de identiteit van de organisatie en de kernpunten van gegevensverwerking, in ieder geval op de eerste laag presenteert.

Een zorgvuldig opgestelde privacyverklaring kan helpen om consumenten duidelijkheid te bieden over hoe hun gegevens worden verwerkt. **Maar let op: deze verklaring moet gemakkelijk vindbaar zijn**, bijvoorbeeld via een prominente link op de homepage van je website of in je communicatie-uitingen. Zo creëer je niet alleen transparantie, maar zorg je er ook voor dat consumenten zich gehoord en serieus genomen voelen.

Dat zou er dan als volgt uit kunnen zien:



Bron: *Privacyverklaring AP | Autoriteit Persoonsgegevens*

Hoe ziet een privacyverklaring eruit? Welke onderdelen neem je erin op?

Deze zaken mag je niet vergeten in je privacyverklaring:

- ▶ De identiteit en contactgegevens van de organisatie
- ▶ De contactgegevens van een eventuele functionaris gegevensbescherming (FG)
- ▶ Voor welke doeleinde persoonsgegevens worden verwerkt en op basis van welke grondslag dat gebeurt. Wanneer de grondslag gerechtvaardigd belang is, zorg dan dat ook vermeld is wélk belang (bijvoorbeeld commercieel belang) dat is.
- ▶ De (categorieën van) ontvangers van de persoonsgegevens.
- ▶ Of je van plan bent de persoonsgegevens door te geven buiten de Europese Economische Ruimte (EER) of aan een internationale organisatie. En zo ja, op welke juridische grond dit gebeurt.

Privacyverklaring, privacystatement, of privacybeleid: wat is het verschil?

Privacyverklaring en -statement zijn hetzelfde. Privacybeleid is voor **intern** gebruik: door de regels en richtlijnen in het beleid weten medewerkers hoe zij om moeten gaan met alle persoonsgegevens die worden verzameld door een organisatie.

Privacyverklaring of algemene voorwaarden?

In een privacyverklaring legt een organisatie uit welke persoonsgegevens worden verzameld, voor welke doeleinden, hoe deze worden beschermd en welke rechten betrokkenen hebben. In de algemene voorwaarden vind je de rechten en plichten van zowel de organisatie als de klant, zoals aansprakelijkheid en betalingsvoorwaarden, maar ook meer informatie gerelateerd aan de bedrijfsactiviteiten.

Daarnaast is het goed om onder andere de bewaartermijn van de gegevens en rechten van de betrokkenen te vermelden.

Een voorbeeld

Stel, jouw organisatie wil transparant zijn over het opbouwen van klantprofielen, waarin vermeld je dit?

- ▶ Privacyverklaring: hierin informeer je over het combineren van data om een profiel op te bouwen. Hierin vermeld je dan het volgende:
 - Dat de organisatie klantprofielen opbouwt.
 - Het doel en de rechtsgrondslag hiervoor (zoals gerechtvaardigd belang).
 - Hoe klanten bezwaar kunnen maken (opt-out).
- ▶ Algemene voorwaarden: als profilering een essentieel onderdeel is van de diensten van je organisatie, kan je hierover ook informatie opnemen in de algemene voorwaarden.



Cookies: met heldere communicatie smaken ze beter

En wat nu als je ook cookies gebruikt? Naast de privacy-verklaring, is het ook noodzakelijk consumenten te informeren van dit gebruik in een **cookiebanner** en een **cookieverklaring**.

Een cookiebanner informeert consumenten specifiek over het gebruik van cookies en andere trackingtechnologieën. Cookies verzamelen vaak persoonsgegevens, zoals IP-adressen of surfgedrag en kunnen dus invloed hebben op de privacy van de bezoeker van je webpagina. Volgens de 'Cookiewet' (artikel 11.7a van de Telecommunicatiewet) is **toestemming van de bezoeker noodzakelijk** voor het plaatsen van niet-essentiële cookies.

Wist je dat in Nederland (bepaalde) analytische cookies ook als essentieel worden gezien? Dat betekent dat je voor privacyvriendelijke analytische cookies **geen** toestemming nodig hebt, wat handig kan zijn als je het gebruik van een website wil analyseren met een tool als Google Analytics. [Lees hier meer over het gebruik van cookies.](#)

Ook moeten bezoekers de mogelijkheid hebben om niet-essentiële cookies te weigeren, **zonder nadelige gevolgen**. Dat betekent dus dat een webpagina ten alle tijde beschikbaar moet zijn voor bezoekers, ook wanneer ze de cookies weigeren.

Het is belangrijk om misleidende methoden, ook wel '**dark patterns**' genoemd, te vermijden bij het verkrijgen van toestemming voor cookies. Denk hierbij aan het minder opvallend maken van bepaalde knoppen: daardoor kunnen bezoekers geen weloverwogen keuze maken. Naast dat het wettelijk verplicht is, zien we ook een trend van strengere handhaving door de AP. Bovendien neemt het consumentenvertrouwen in een organisatie toe door eerlijke en duidelijke communicatie. Dit begint bij de eerste blik op de website: de cookiebanner.

Belangrijk om te weten:

De volgende technieken zijn ook onderhevig aan de regels voor cookies: het plaatsen van niet-essentiële gegevens op het apparaat van de gebruiker, bijvoorbeeld via local storage, trackingpixels, web beacons en fingerprinting.

Hoe richt je zo'n cookiebanner nu goed in?

De AP gaf daar haar advies over als volgt:

- ▼ Geef informatie over het doel
- ▼ Zet vinkjes niet automatisch aan
- ▼ Gebruik duidelijke tekst
- ▼ Zet verschillende keuzes op één laag
- ▼ Verberg bepaalde keuzes niet
- ▼ Laat iemand niet extra klikken
- ▼ Gebruik geen onopvallende link in de tekst
- ▼ Wees helder over het intrekken van toestemming
- ▼ Verwar toestemming niet met gerechtvaardigd belang

Bron: [Heldere en misleidende cookiebanners](#) | [Autoriteit Persoonsgegevens](#)

Zelf een compliant cookiebanner opstellen?
Bekijk dan hier onze [Cookiebanner checklist](#).

Vergeet ook niet in de cookiebanner te verwijzen naar de cookie- of privacyverklaring!

Standaard cookiebanner-generators: waar let je op?

Cookiebot, ConsentManager of Onetrust: als je wel eens een cookiebanner hebt gemaakt, ken je deze platforms ongekend. Ze faciliteren de beschikbaarheid van toestemming voor gecategoriseerde cookies (marketing, analytics, functioneel etc.). Ondanks dat dit zeer nuttige tools zijn met veel potentie om een goede cookiebanner te maken, zien we vaak dat dit soort cookiebanners niet altijd correct zijn ingesteld. Daarom adviseren wij altijd om zelf het standaarddesign van een 'GDPR-compliant' cookiebanner te checken, wanneer je besluit gebruik te maken van een CMP (Consent Management Platform). Dit doe je door bovenstaande vuistregels langs te gaan.

Meer over weten?
Lees hier ons artikel over [CMP's](#).

Kijk ook eens naar de [cookieverklaring van Coolblue](#), waarin de nadruk duidelijk ligt op de voordelen voor de consument.

DA maakt gebruik van cookies

We gebruiken cookies om content en advertenties te personaliseren, om functies voor social media te bieden en om ons websiteverkeer te analyseren. Ook delen we informatie over uw gebruik van onze site met onze partners voor social media, adverteerders en analyse. Deze partners kunnen deze gegevens combineren met andere informatie die u aan ze heeft verstrekt of die ze hebben verzameld op basis van uw gebruik van hun services.

 Noodzakelijk Voorkeuren Statistieken Marketing [Details tonen](#) >

[Alle cookies toestaan](#)

[Selectie toestaan](#)

[Alleen noodzakelijke cookies](#)


Bron: [DA.nl](#) | [Persoonlijk gezondheidsadvies voor jou](#)

Deze website gebruikt cookies

We gebruiken cookies om inhoud en advertenties te personaliseren, om functies voor sociale media aan te bieden en om ons verkeer te analyseren. We delen ook informatie over uw gebruik van onze site met onze partners op het gebied van sociale media, reclame en analyse, die deze informatie kunnen combineren met andere informatie die u aan hen hebt verstrekt of die zij hebben verzameld via uw gebruik van hun diensten. U kunt deze accepteren, wijzigen of weigeren. Hier vindt u [Google's privacybeleid](#) en [LOAVIES privacybeleid](#).

[ALLES ACCEPTEREN](#)

Bron: [LOAVIES](#) | [Shop Fashion Online](#)



Consent **Details** **About**

This website uses cookies

DDMA wants to make your visit to the website as easy and personalized as possible. To achieve this, we use cookies and similar technologies. This ensures that you see relevant DDMA advertisements on other websites, that we can create lookalikes on social media, and that we can map out behavior on our website. Prefer not to? In that case, we will only place essential and statistical cookies. These cookies do not collect any data about you as an individual. By clicking the 'clip' icon in the bottom left corner of the webpage you're visiting, it is possible to withdraw (or change) your consent. Want to know more? Then read our [Privacy Statement here](#).

[No thanks](#) [I agree](#)

Bron: [DDMA](#)

AI & Privacy

Anno 2025 zijn tools als ChatGPT onmisbaar geworden in ons dagelijks leven. Of het nu gaat om het opstellen van een contentplan of het schrijven van een nieuwsbrief: met een paar eenvoudige prompts tover je in no-time een complete tekst tevoorschijn, vaak sneller en beter dan je zelf in die tijd had kunnen doen.

Maar laat je niet misleiden door het gemak van deze tools. Wat op het eerste gezicht een onschuldige toepassing lijkt, kan grote risico's met zich meebrengen. Neem bijvoorbeeld de gratis versie van ChatGPT. Alles wat je invoert, wordt opgeslagen en kan worden gebruikt voor verdere training van de tool. Dit betekent dat er persoonsgegevens kunnen worden verwerkt. En daar zitten belangrijke verplichtingen aan vast, zoals het hebben van een rechtsgrond en het voldoen aan de informatieplicht voordat je gegevens verwerkt.

Met andere woorden: deze tools zijn krachtig, maar zeker niet zonder risico's. Als organisatie is het cruciaal om hier bewust mee om te gaan en zorgvuldig na te denken over hoe je dergelijke technologie inzet, zeker als je met klantdata werkt.

Wanneer je toch besluit persoonsgegevens te gebruiken in een tool als ChatGPT, dan zijn daarbij dit onze tips:

- ▼ Zorg voor een geldige grondslag, zoals toestemming of gerechtvaardigd belang
- ▼ Vermijd het gebruik van gevoelige gegevens, zoals medische gegevens. Bedenk bovendien: zou ik dit prompt ook op een openbaar platform posten? Is het antwoord nee? Schrijf het dan ook niet op in een prompt.
- ▼ Check goed de voorwaarden van de tool. De gratis versie van ChatGPT gebruikt automatisch verzonden gegevens voor trainingsdoeleinden, terwijl de zakelijke versie, zoals ChatGPT Enterprise, dit standaard niet doet om de privacy te waarborgen.

Meer weten over het verantwoord inzetten van AI in de marketingstrategieën van je organisatie?
Bekijk dan hier de [Marketinggids Responsible AI](#).

Rechten van consumenten: waar moet je op letten?

Een van de kernprincipes van privacywetgeving, zoals de AVG, is het versterken van de controle die consumenten hebben over hun persoonsgegevens. Dat gevoel van controle komt, zoals ook volgde uit de groepsgesprekken met consumenten voor het onderzoek, naar voren op twee momenten: bij het geven van de juiste informatie door de organisatie in een privacyverklaring of cookiebanner, maar ook wanneer consumenten actief hun rechten kunnen uitoefenen. Transparantie en het bieden van echte keuze staan hierbij centraal. Dit zijn de belangrijkste rechten die consumenten volgens de AVG hebben.

Consumenten hebben ten eerste het **recht op inzage** in hun gegevens. Zij kunnen een verzoek indienen om te achterhalen welke gegevens een organisatie van hen verwerkt, met welk doel dit gebeurt en met wie deze gegevens worden gedeeld. Daarnaast hebben zij het **recht op rectificatie**, waarmee zij kunnen verzoeken om onjuiste of onvolledige gegevens te corrigeren. Ook hebben consumenten het **recht op verwijdering** van hun gegevens, bijvoorbeeld wanneer deze niet langer nodig zijn voor het oorspronkelijke doel of als toestemming is ingetrokken. Verder biedt de AVG consumenten het **recht op dataportabiliteit**, zodat zij hun gegevens in een gestructureerd, gangbaar formaat kunnen ontvangen en overdragen aan een andere dienstverlener. Tot slot hebben consumenten het **recht om bezwaar te maken** tegen specifieke verwerkingen van hun gegevens, zoals voor direct marketing, waarbij organisaties deze verwerking altijd (!) moeten stopzetten.

Organisaties zijn verplicht binnen één maand gehoor te geven aan bovenstaande verzoeken. Ook mag niet vergeten worden consumenten 'uiterlijk op het moment van eerste contact' hierover te informeren, wat in het privacyverklaring moet worden opgenomen.



Aanbevelingen

- ▶ **Informeer de consument:** communiceer helder in een privacyverklaring over het gebruik van gegevens door je organisatie. Maak gebruik van de aanbevolen 'lagen-structuur', waarbij je ervoor zorgt dat de meest belangrijke informatie op de eerste laag staat. Maak een privacyverklaring zo eenvoudig mogelijk voor de consument door gebruik te maken van iconen, symbolen en uitklapbare secties.
- ▶ Door **transparant te zijn over cookies, smaken ze beter** voor de consument: wees kritisch op standaard cookiebanners, zoals de standaardversie van cookiebanner generators. Informeer consumenten in begrijpelijke taal en wees volledig in je uitleg, maar vermijd een overdaad aan informatie.
- ▶ Een cliché, maar **klant is koning**: zorg dat naast de mogelijke risico's van het delen van gegevens ook de voordelen voor de consument duidelijk uit de informatie naar voren komen. Op die manier ben je volledig, maar spreek je de consument ook sneller aan om wel gegevens te delen.
- ▶ **Verdiep je in het kennisniveau van je klant:** geef potentiële klanten een gevoel van controle. Uit het onderzoek blijkt dat consumenten bereid zijn meer te delen bij duidelijke communicatie.
- ▶ Denk aan de **algehele uitstraling en branding** van je organisatie: uit het onderzoek blijkt ook dat consumenten meer geneigd zijn om informatie te delen of sneller te betalen wanneer zij vertrouwen hebben in een organisatie en zich aangetrokken voelen tot de charme van een bedrijf.
- ▶ **Geen onnodige drempels opwerpen:** consumenten mogen niet worden ontmoedigd om hun rechten uit te oefenen, bijvoorbeeld door ingewikkelde processen of kosten. Handel daarnaast snel: de wet vereist dat privacyverzoeken door consumenten betreffende hun rechten binnen een maand moeten worden opgevolgd.
- ▶ **Blijf op de hoogte van de nieuwste ontwikkelingen:** bij DDMA organiseren we regelmatig events, zoals de maandelijkse Legal Member Meetup en schrijven we artikelen die jou op de hoogte houden van de laatste trends en updates op privacygebied. Leden weten ons daarnaast te vinden via onze Legal Helpdesk, waar alle privacy- en reclamerechtelijke vragen snel voorzien worden van een praktisch advies. Ook op de hoogte blijven? [Schrijf je hier in voor onze legal nieuwsbrief.](#)

Onderzoeksverantwoording



Het rapport bevat resultaten van 2 onderzoeken:

1. Groepsgesprekken met Nederlandse consumenten

Methode

Kwalitatief onderzoek, uitgevoerd door middel van focusgroepen.

Onderzoeksbureau

Uitvoering en analyse in samenwerking met kwalitatief onderzoeksbureau CO-efficiënt.

Doelgroep en steekproef

De groepsgesprekken vonden plaats in de vorm van 3 focusgroepen op locatie: 1 groep pragmatici, 1 groep onbezorgden, 1 groep sceptici - in totaal 24 respondenten.

Veldwerkperiode

November 2024

2. Global Privacy Monitor

Methode

Kwantitatief onderzoek, uitgevoerd door middel van een online enquête.

Onderzoeksbureau

Uitvoering door de GDMA (de koepelorganisatie van DDMA) in samenwerking met Foresight Factory.

Doelgroep en steekproef

Voor de Global Privacy Monitor 2022 zijn 20.626 respondenten ondervraagd, afkomstig uit 16 landen. Waaronder 1.039 Nederlandse respondenten, representatief voor de Nederlandse bevolking 18+ jaar (achteraf gewogen op geslacht, leeftijd en regio).

Veldwerkperiode

December 2021

Colofon

Uitgever

DDMA
WG-plein 185
1054 SC Amsterdam
T: 020 452 8413
E: info@ddma.nl
W: www.ddma.nl

Auteurs

Nanda Appelman (Market Insights Specialist, DDMA)
Allisha Hosli (Legal Counsel, DDMA)
Isa Nieuwstad (Legal Counsel, DDMA)

Eindredactie

Bob Younge (Content- en Communicatiespecialist, DDMA)

Heb je vragen of opmerkingen over dit onderzoek?
Stuur dan een e-mail naar info@ddma.nl.

OVER DDMA

DDMA is de grootste branchevereniging voor marketing en data. Wij zijn een netwerk van ruim 360 merken, non-profits, uitgevers, bureaus en tech-leveranciers die data succesvol en verantwoord willen inzetten voor marketingdoeleinden. Wij duiden ontwikkelingen op het gebied van technologie, regelgeving en ethiek en brengen marketeers, dataspecialisten en juristen bij elkaar om hen te helpen groeien in hun vak. Ook bevorderen we zelfregulering en zijn we gesprekspartner van beleidsmakers en toezichthouders.

Ga voor alle DDMA-onderzoeken naar: ddma.nl/research-insights