Consumenten over Privacy, AI en Online Veiligheid

Consumentenperspectief naar vertrouwen rond gegevensbescherming, algoritmen en sociale media



Cyber & TechLaw
Oktober 2026

KPMG. Make the difference.

Inleiding

In 2026 is privacy geen randvoorwaarde meer, maar door de verregaande digitalisering een vast onderdeel van het dagelijks leven. Nederlanders bewegen zich door een digitale wereld waarin risico's zichtbaarder worden, diensten steeds meer datagedreven zijn en nieuwe technologie continu invloed heeft op hoe we werken, communiceren en beslissingen nemen. Daardoor groeit niet alleen het bewustzijn, maar vooral de behoefte aan duidelijkheid: wat gebeurt er met mijn gegevens, wie heeft toegang, en welke keuzes heb ik zelf?

Tegelijkertijd verandert de context snel. Kunstmatige intelligentie wordt op grote schaal geïntegreerd in apps, platforms en werkzaamheden, terwijl nieuwe Europese regels de lat voor transparantie en verantwoord gebruik verder verhogen. Deze ontwikkelingen zorgen voor vragen, verwachtingen en soms ook spanning: consumenten willen innovatie, maar wel onder voorwaarden die begrijpelijk, uitlegbaar en controleerbaar zijn.

Met dit consumentenonderzoek laten wij zien hoe Nederlanders privacy, dataveiligheid, AI en online platforms ervaren. De resultaten tonen waar zorgen toenemen, welke rol men ziet voor organisaties en overheid, en hoe verschillende generaties technologie anders benaderen.
Samen geven deze inzichten een helder beeld van wat nodig is om vertrouwen te behoudenin een samenleving die snel digitaliseert.

Met de bevraging van 500 consumenten in Nederland schetsen we een beeld over hoe de gemiddelde Nederlander denkt over Privacy & Cyberweerbaarheid, AI en de rol van Online Platforms. Het onderzoek is ook in deze volgorde ingedeeld.





01
Introductie

02
Datalekken en Cyber-weerbaarheid

01 Meer zorgen over de risico's van datalekken/cyberaanvallen
02 Vertrouwen instanties: Consumenten verwachten transparantie bij datalekken
03 Sterke steun voor een actievere rol van de Europese Unie
04 Weerbaarheid instanties

03
Artificial Intelligence

01 Gebruik van AI in Nederland
02 De "privacy-paradox"
03 Menselijke regie blijft cruciaal
04 Slimme apparaten
05 De "governancegap"

04
Online platforms

01 Platformgebruik verschilt sterk per generatie
02 De "privacy-paradox" - platforms
03 Opleiding beïnvloedt overstapbereidheid
04 Sterke steun voor EU-ingrijpen
05 Breed draagvlak voor actieve aanpak van nepnieuws en contentmoderatie

05
Over KPMG

01 Wat doet KPMG op het gebied van Privacy en Tech-regulering?

06
Uitleg onderzoek

01 Over ons onderzoek

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.



Datalekken en Cyberweerbaarheid

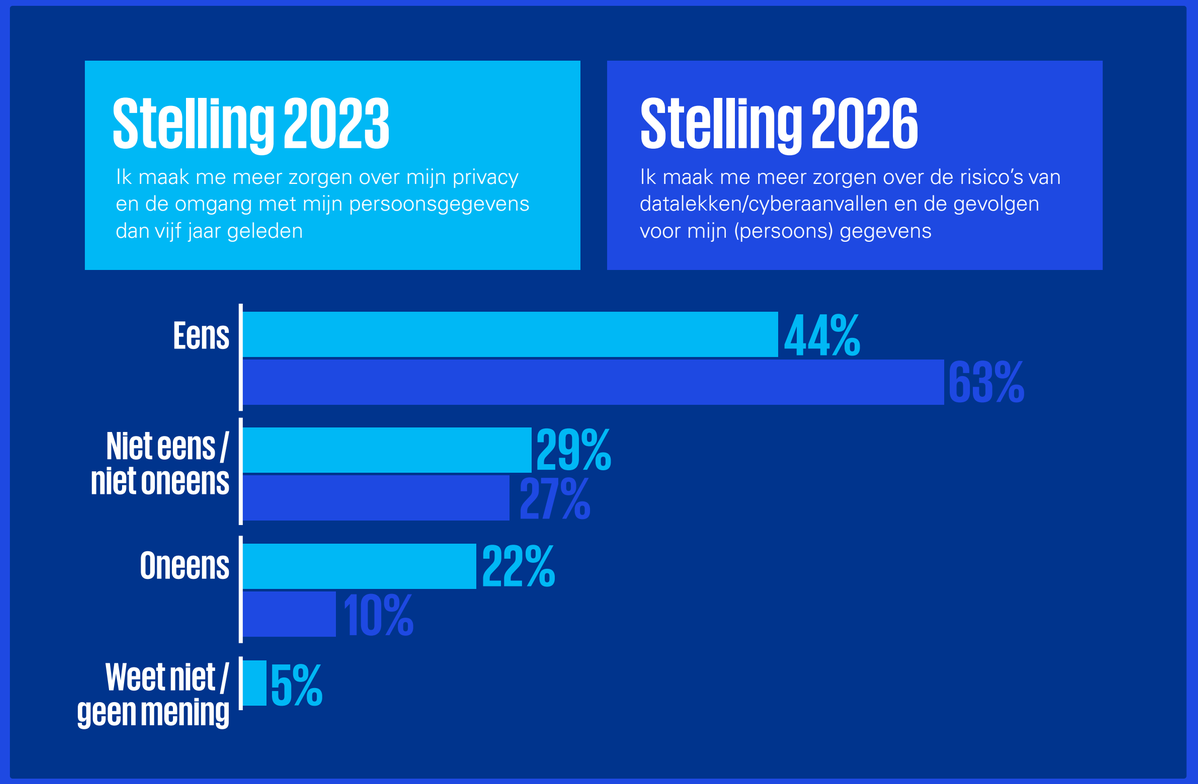
Meer zorgen over de risico's van datalekken/cyberaanvallen

In ons privacy marktonderzoek uit 2023 zagen we al dat Nederlanders zich steeds bewuster werden van het belang van privacy. Respondenten gaven toen aan dat zij het gevoel hadden dat privacy serieuzer werd genomen door organisaties. Tegelijkertijd gaf **44%** aan zich méér zorgen te maken over privacy en de omgang met persoonsgegevens dan vijf jaar daarvoor. Dit toenemende bewustzijn en deze zorgen schreven wij destijds toe aan de groeiende media-aandacht voor privacyschendingen, datalekken en andere digitale incidenten bij zowel publieke als
private organisaties.

Bewustzijn gevolgen en risico's van datalekken aanzienlijk gestegen

In 2026 kan worden geconcludeerd dat deze trend zich niet alleen heeft voortgezet, maar verder is verdiept en verbreed. Met name zorgen over datalekken en cyberaanvallen en de mogelijke gevolgen daarvan voor persoonsgegevens zijn nadrukkelijk aanwezig. Ruim **63%** van de ondervraagden maakt zich, over alle leeftijdsgroepen heen, zorgen over de risico's van datalekken. Waar in 2023 het privacydebat nog sterk werd gevoed door bewustwording en incidenten, lijkt in 2026 sprake van een structureel besef dat digitale risico's een blijvend onderdeel zijn van het dagelijks leven.

Deze ontwikkeling staat niet op zichzelf. In de media zien we de afgelopen jaren een aaneenschakeling van grootschalige datalekken en cyberincidenten, waarbij miljoenen persoonsgegevens tegelijk worden geraakt. Zulke incidenten maken de abstracte risico's van datalekken concreet en persoonlijk, en versterken het gevoel van kwetsbaarheid
onder consumenten.



© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Vertrouwen instanties: Consumenten verwachten transparantie bij datalekken

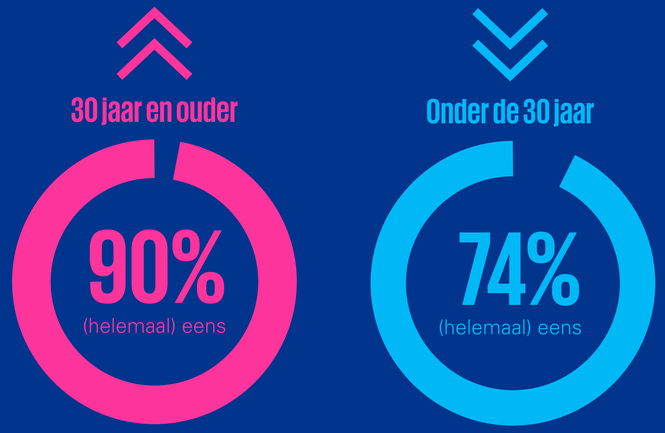
Breed gedragen roep om meer transparantie van bedrijven

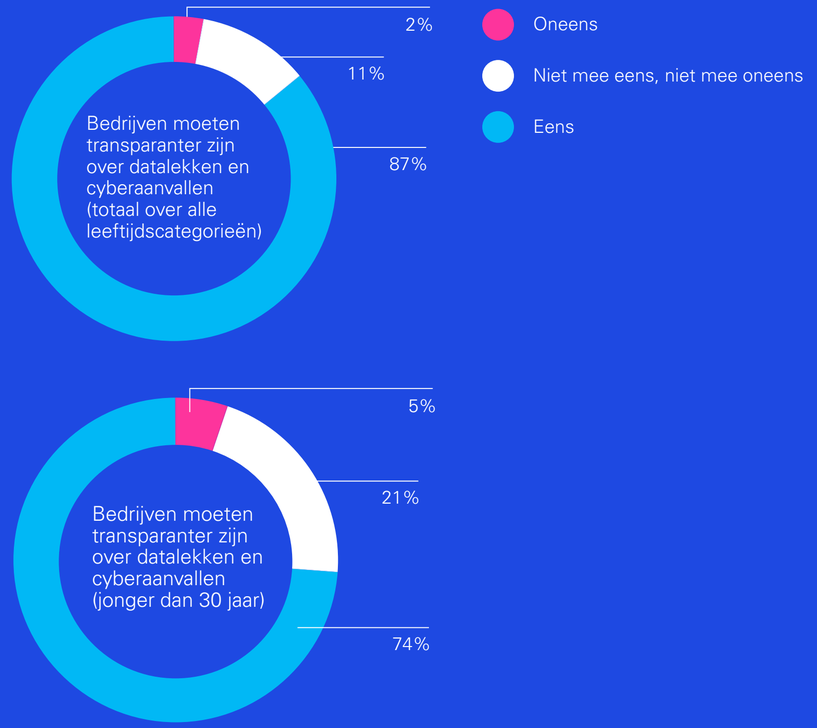
De overgrote meerderheid van de ondervraagden is van mening dat bedrijven transparanter moeten zijn over datalekken en cyberaanvallen. Deze verwachting komt duidelijk tot uiting naar aanleiding van recente datalekken en ransomeware aanvallen, waarbij persoonsgegevens van miljoenen (oud-)klanten zijn buitgemaakt en (deels) openbaar zijn geworden.

De maatschappelijke impact van dit soort incidenten laat zien hoe groot de behoefte is aan duidelijke, tijdige en volledige communicatie vanuit organisaties bij beveiligingsincidenten. Deze incidenten maken duidelijk dat een gebrek aan openheid het vertrouwen van consumenten onder druk zet en de impact van een datalek voor betrokkenen verder kan vergroten.

Met name onder respondenten van **30 jaar en ouder** is die verwachting sterk: bijna **90%** van hen is het (helemaal) eens met de stelling dat organisaties opener moeten zijn over dergelijke incidenten. Bij jongeren **onder de 30 jaar** ligt dit percentage iets lager, maar nog steeds aanzienlijk met circa **74%**.

Dit laat zien dat transparantie breed wordt gezien als een essentiële voorwaarde voor vertrouwen, omdat openheid consumenten in staat stelt risico's beter te begrijpen, zich tijdig te beschermen en het gevoel te behouden dat organisaties verantwoordelijkheid nemen wanneer er iets misgaat.



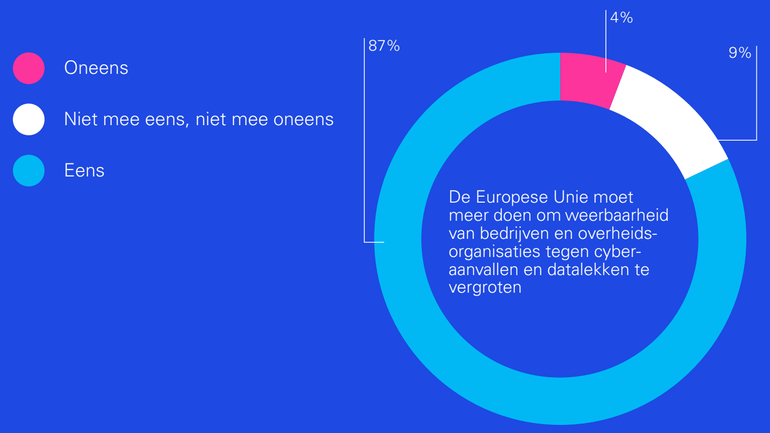


© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Sterke steun voor een actievere rol van de Europese Unie

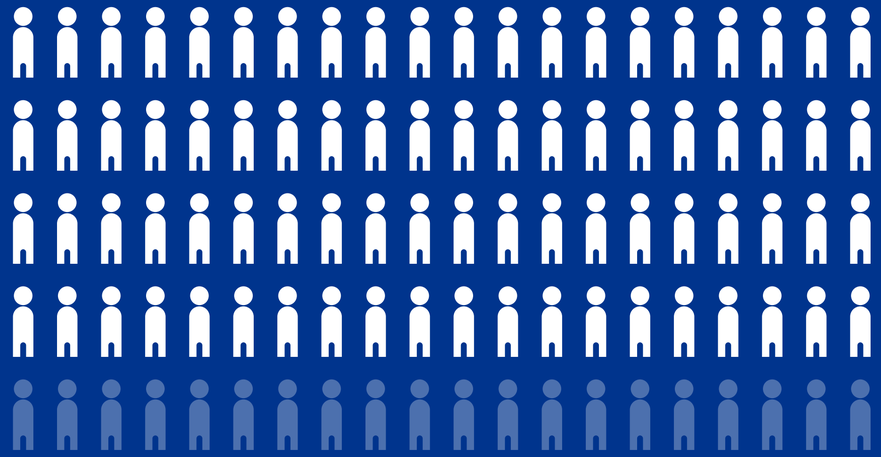
EU wordt gezien als belangrijke speler in cyberweerbaarheid

Uit ons onderzoek blijkt een zeer breed gedragen steun voor een actievere rol van de Europese Unie bij het vergroten van de cyberweerbaarheid van zowel bedrijven als overheidsorganisaties. Maar liefst **87%** van de Nederlanders is het eens met de stelling. Dit onderstreept dat de bescherming van persoonsgegevens door consumenten niet langer wordt gezien als louter nationale of organisatorische verantwoordelijkheid, maar als een grensoverschrijdend vraagstuk dat vraagt om Europese regie en samenwerking.



Draagvlak bij jongeren onder de 30 jaar

Het hoge draagvlak is zichtbaar over vrijwel alle leeftijdsgroepen heen. **Jongeren onder de 30 jaar** zijn met circa **80%** instemming iets terughoudender, maar ook binnen deze groep is de meerderheid duidelijk positief. Dit wijst erop dat consumenten de risico's van datalekken en cyberdreiging erkennen en juist op Europees niveau kansen zien voor versterking van bescherming, handhaving en weerbaarheid.



80% van jongeren onder de 30 steunt een actievere rol van de EU

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Weerbaarheid instanties (1/2)

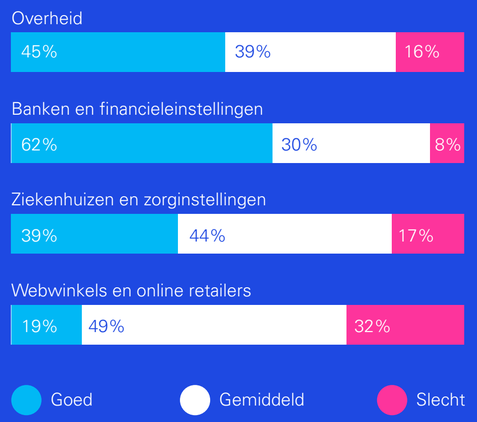
Wie beschermt onze persoonsgegevens écht? Hoe veilig zijn onze data per sector, volgens de consument?

De mate waarin consumenten vertrouwen hebben in de bescherming van hun persoonsgegevens verschilt sterk per sector. Voor de overheid is dat vertrouwen gematigd: **45%** van de Nederlanders vindt dat overheidsinstanties goed beschermd zijn tegen cyberaanvallen en datalekken. Dat staat in contrast met ons eerdere **onderzoek uit 2023**, waarin het vertrouwen in de overheid rond de omgang met persoonsgegevens eens stuk lager lag (**19%**). Wat betreft Cyberweerbaarheid scoort de overheid beduidend beter dan in 2023 en lijkt het vertrouwen van de burger weer enigszins te herstellen.

De financiële sector wordt door consumenten duidelijk gezien als koploper op het gebied van cyberweerbaarheid. In totaal geeft **62%** aan dat banken en financiële instellingen goed beschermd zijn. Dit sterke vertrouwen sluit aan bij het beeld van een sector die zwaar gereguleerd is, onder meer door de invoering van Europese regelgeving zoals de Digital Operational Resilience Act (DORA), en die structureel investeert in digitale weerbaarheid en risicobeheersing.

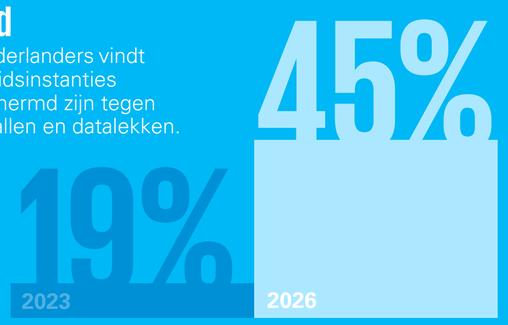
De perceptie van digitale weerbaarheid van digitale handel wordt als relatief laag ervaren. Slechts **19%** denkt dat webwinkels en online retailers goed beschermd zijn tegen cyberaanvallen en datalekken. Hieruit blijkt dat consumenten online retailers zien als een risicovolle schakel in de omgang met persoonsgegevens, ondanks hun centrale rol in het dagelijks leven van mensen. Die perceptie kan samenhangen met de grote hoeveelheid persoonsgegevens die webwinkels verwerken, de afhankelijkheid van complexe digitale ketens en het frequente nieuws over datalekken en fraude in de e-commerce. Hierdoor lijkt het vertrouwen van consumenten in de digitale weerbaarheid van deze sector achter te blijven bij het belang dat zij eraan toekennen in hun dagelijks gedrag.

Hoe goed denk je dat de volgende sectoren beschermd zijn tegen cyberaanvallen en datalekken?



Overheid

Van de Nederlanders vindt dat overheidsinstanties goed beschermd zijn tegen cyberaanvallen en datalekken.



Financiële sector

Van de Nederlanders vindt dat banken en financiële instellingen goed beschermd zijn tegen cyberaanvallen en datalekken.



Digitale handel

De perceptie van digitale weerbaarheid van digitale handel wordt als relatief laag ervaren.



© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Weerbaarheid instanties (2/2)

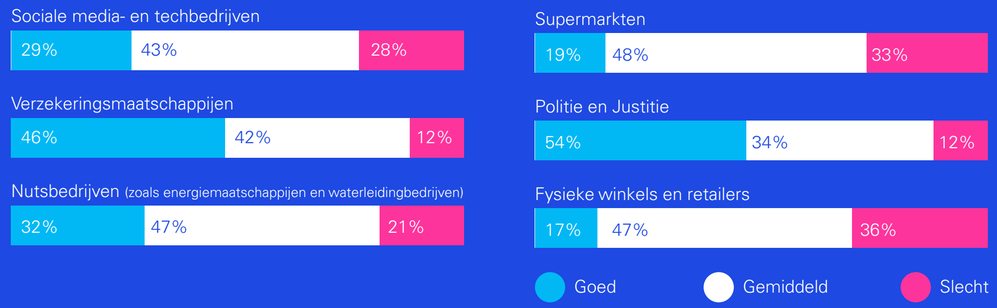
Nederlanders twijfelen in sterke mate aan het vermogen van **sociale media- en techbedrijven** om persoonsgegevens veilig te houden en grootschalige datalekken te voorkomen, ondanks hun technologische expertise en schaalgrootte. Slechts **29%** van de respondenten denkt dat deze bedrijven goed beschermd zijn tegen cyberaanvallen en datalekken. Dit wijst op aanhoudende zorgen over de manier waarop deze bedrijven omgaan met persoonsgegevens, met name rondom dataverzameling, transparantie en controle.

Deze uitkomsten sluiten nauw aan bij ons onderzoek uit 2023, waarin sociale media- en BigTech-bedrijven werden aangemerkt als de minst betrouwbare organisaties als het gaat om de omgang met persoonsgegevens. Destijds gaf **bijna de helft** van de ondervraagden aan deze partijen het minst te vertrouwen. De consistentie tussen beide onderzoeken onderstreept dat het wantrouwen richting grote technologiebedrijven geen tijdelijke perceptie is, maar een structureel en diepgeworteld sentiment onder consumenten.

Slechts **32%** van de respondenten denkt dat nutsbedrijven, zoals energie- en waterleidingbedrijven, goed beschermd zijn tegen cyberaanvallen en datalekken. Dit lage vertrouwen is opvallend gezien het vitale karakter van deze sectoren en wijst op zorgen over maatschappelijke kwetsbaarheid en de mogelijke impact van incidenten op essentiële diensten. Dit onderstreept het belang van een zorgvuldige implementatie van de NIS2-richtlijn, die erop is gericht de digitale weerbaarheid en continuïteit van vitale en essentiële sectoren structureel te versterken.

Het vertrouwen politie- en justitieorganisaties ligt met **54%** hoger dan bij veel andere sectoren. Tegelijkertijd twijfelt bijna helft van de respondenten aan de mate waarin politie en justitie bestand zijn tegen digitale dreigingen. Dat is relevant, gezien de bijzonder gevoelige aard van de persoonsgegevens die binnen deze sector worden verwerkt, zoals strafrechtelijke gegevens. Dit wijst erop dat consumenten enerzijds vertrouwen hebben in de beveiliging binnen deze sector, maar anderzijds beseffen dat ook politie en justitie niet immuun zijn voor steeds geavanceerdere cyberdreigingen.

Hoe goed denk je dat de volgende sectoren beschermd zijn tegen cyberaanvallen en datalekken?



Sociale media- en techbedrijven

Nederlandse consumenten zijn sceptisch over het vermogen van sociale media-en techbedrijven om persoonsgegevens adequaat te beveiligen en grootschalige datalekken te voorkomen

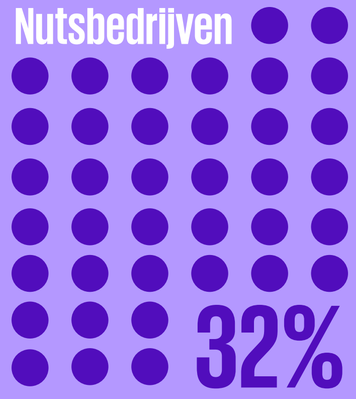


2026 van de Nederlanders heeft vertrouwen in de bescherming van persoonsgegevens door deze bedrijven



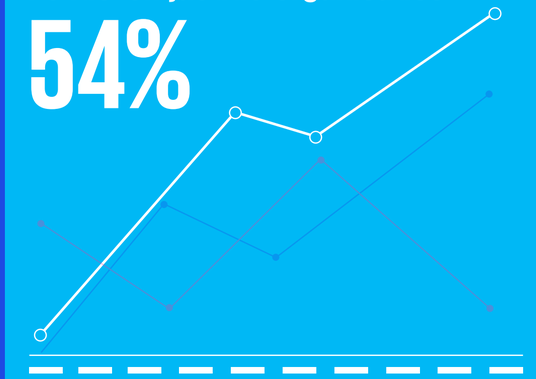
2023 van de Nederlanders gaf aan deze bedrijven het minst te vertrouwen in de omgang met persoonsgegevens

Nutsbedrijven



Denkt dat deze sector goed beschermd is tegen cyberaanvallen en datalekken

Politie- en justitie-organisaties



Vertrouwt op voldoende bescherming tegen cyberaanvallen en datalekken in deze sector

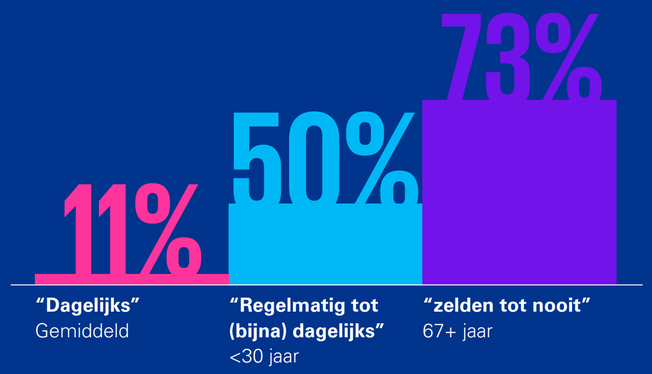
© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.


KPMG
Artificial Intelligence

Gebruik van AI in Nederland

De resultaten van ons onderzoek laten zien dat het gebruik van Artificial Intelligence (AI) in Nederland sterk verschilt tussen bevolkingsgroepen. Met name leeftijd en opleidingsniveau lijken samen te hangen met de mate waarin mensen AI daadwerkelijk gebruiken.

Onder respondenten jonger dan 30 jaar geeft ongeveer de helft aan AI **regelmatig tot (bijna) dagelijks** te gebruiken. In de groep van 67 jaar en ouder komt gebruik **zelden tot nooit (73%)** voor. Wat echter opmerkelijker is dan deze, op zichzelf niet verrassende, generatieverschillen, is dat gemiddeld **slechts 11%** van alle respondenten aangeeft AI-toepassingen **dagelijks** te gebruiken. Dit lage percentage is opvallend, juist omdat AI een groot maatschappelijk onderwerp is en sterk aanwezig lijkt in het publieke debat. De cijfers laten zien dat AI voor de meeste Nederlanders (nog) geen vast onderdeel is van hun dagelijkse digitale routines, ondanks de brede aandacht, groeiende beschikbaarheid van AI-tools en hoge verwachtingen rondom adoptie.



Een vergelijkbaar verschil is zichtbaar op basis van opleidingsniveau. Praktisch opgeleide respondenten geven aanzienlijk vaker aan AI nog nooit te hebben gebruikt **(50,6%)** dan theoretisch opgeleiden **(20,7%)**. Dit kan erop wijzen dat AI-toepassingen momenteel vaker voorkomen in contexten waarin studie, kenniswerk en digitale tools een grotere rol spelen.

Deze verschillen in gebruik zijn relevant voor het bredere maatschappelijke debat over AI en gegevensbescherming. Ze laten zien dat niet alle groepen in dezelfde mate ervaring hebben met AI-toepassingen. Hierdoor kunnen ook de manier waarop mensen de kansen en risico's van AI inschatten, en de perspectieven tussen groepen, uiteenlopen.

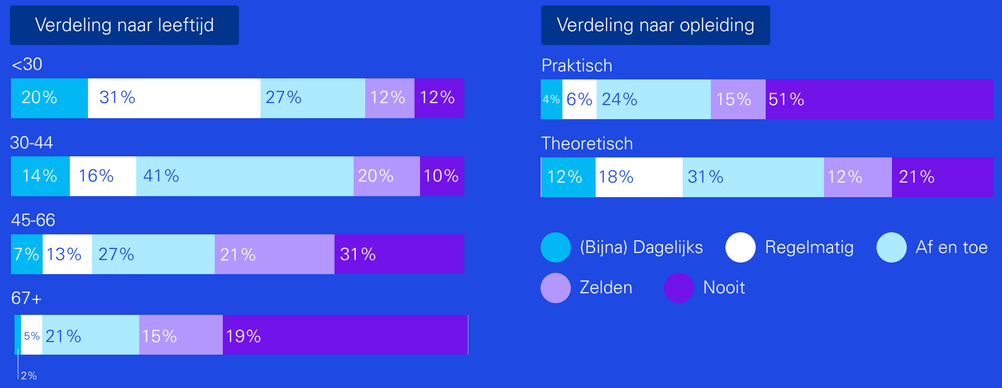
Praktisch opgeleide respondenten geven aanzienlijk vaker aan AI nog nooit te hebben gebruikt



Praktisch opgeleide respondenten **50,6%**

Theoretisch opgeleide respondenten **20,7%**

In hoeverre maak je zelf in je dagelijkse leven en/of werk gebruik van AI?



Duidelijke adoptiekloof tussen generaties en opleidings-niveaus

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

De “Privacy-paradox”

De enquête laat daarnaast zien dat de houding ten opzichte van privacy verschilt tussen leeftijdsgroepen. In de literatuur wordt deze houding soms beschreven als een privacy-paradox*: mensen geven aan privacy belangrijk te vinden, maar delen tegelijkertijd persoonlijke gegevens wanneer daar gebruiksgemak of voordelen tegenover staan.

In dit onderzoek valt op dat jongere respondenten redelijk vaak aangeven zich zorgen te maken over hun privacy **(46%)**, maar tegelijkertijd ook vaker bereid zijn persoonsgegevens te delen wanneer daar bijvoorbeeld gemak of innovatie tegenover staat **(35%)** ten opzichte van hogere leeftijdscategorieën.



46% >> 35%

In dit onderzoek valt op dat bijna de helft van de jongere respondenten **(46%)** aangeeft zich zorgen te maken over hun privacy. Tegelijkertijd is deze groep, vergeleken met hogere leeftijdscategorieën, ook vaker bereid persoonsgegevens te delen wanneer daar gemak of innovatie tegenover staat **(35%)**.

46% **35%**

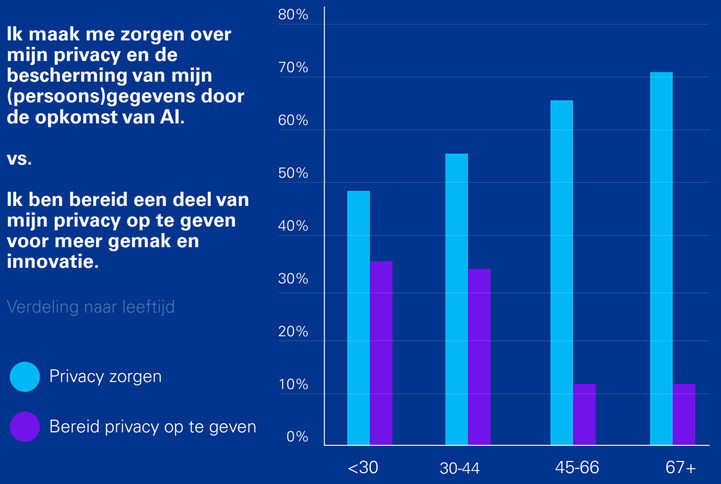
Deze combinatie wijst op een duidelijke privacy-paradox: jongeren maken zich zorgen over hun privacy, maar kiezen desondanks vaker voor situaties waarin zij persoonsgegevens delen. Mogelijk speelt daarbij mee dat jongeren veel intensiever gebruikmaken van technologie, sociale media en digitale diensten. Daardoor zouden zij meer gewend kunnen zijn aan het idee dat hun data voortdurend wordt verwerkt, en dat het delen van gegevens soms een vanzelfsprekende voorwaarde is om toegang te krijgen tot bepaalde platforms of functionaliteiten. Dit zou kunnen verklaren waarom zij relatief vaker bereid lijken om persoonsgegevens te delen, zonder dat dit hun zorgen volledig wegneemt.

Ik maak me zorgen over mijn privacy en de bescherming van mijn (persoons)gegevens door de opkomst van AI.

vs.

Ik ben bereid een deel van mijn privacy op te geven voor meer gemak en innovatie.

Verdeling naar leeftijd



Voor organisaties die AI toepassen is dit een relevant aandachtspunt. Wanneer de bereidheid om privacy af te wegen tegen voordelen beperkt is, kan het belang van duidelijke waarborgen rond gegevensbescherming en keuzevrijheid, bijvoorbeeld in de vorm van transparantie en opt-out mogelijkheden, zwaarder wegen voor het vertrouwen van gebruikers. En zoals blijkt uit de enquête, geldt dit voor oudere gebruikers in grotere mate dan voor jongere gebruikers.

**een theorie die stelt dat mensen rationeel de risico’s (zoals datamisbruik) afwegen tegen de voordelen (zoals gepersonaliseerde diensten of gemak) voordat ze persoonlijke informatie delen. Het is een continue kosten-batenanalyse die bepaalt of het delen van gegevens de verwachte “beloning” waard is.*

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Menselijke regie blijft cruciaal

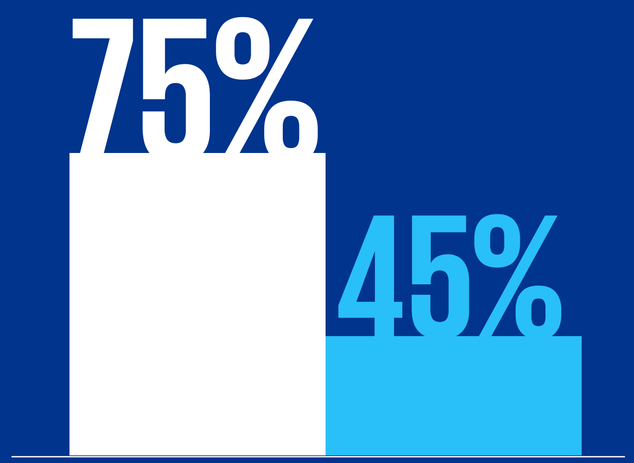
Afwijzing van AI bij het nemen van belangrijke beslissingen

Een ander belangrijk inzicht uit het onderzoek betreft de rol die mensen AI toedichten bij belangrijke beslissingen. De stelling dat men AI meer vertrouwt dan mensen bij het nemen van belangrijke beslissingen wordt door een **meerderheid** van de respondenten afgewezen **(gemiddeld 63%)**.

Gemiddeld

63%

Hoewel ook onder jongere respondenten een aanzienlijk deel het met deze stelling oneens is **(45%)**, neemt het aandeel dat AI minder vertrouwt dan mensen duidelijk toe bij oudere leeftijdsgroepen. Onder respondenten van 45 jaar en ouder is ongeveer **driekwart** het (helemaal) oneens met de stelling.

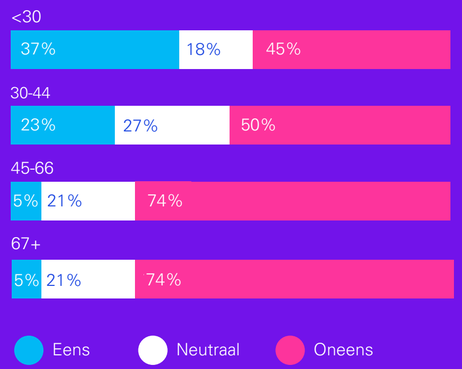


De resultaten suggereren dat AI door veel respondenten eerder wordt gezien als ondersteunend hulpmiddel dan als vervanging van menselijke besluitvorming. Met name bij beslissingen die gevolgen kunnen hebben voor rechten, kansen of persoonlijke omstandigheden lijken respondenten het belangrijker te vinden dat er menselijke betrokkenheid is.

In de context van gegevensbescherming en algoritmische besluitvorming raakt dit direct aan onderwerpen zoals uitlegbaarheid, menselijke controle en mogelijkheden tot bezwaar of herbeoordeling. De uitkomsten laten zien dat vertrouwen in AI-toepassingen niet alleen samenhangt met de technologie zelf, maar ook met de manier waarop het gebruik ervan wordt georganiseerd en gecontroleerd.

Ik vertrouw AI meer dan mensen bij het nemen van belangrijke beslissingen.

Verdeling naar leeftijd



Vertrouwen in AI zakt sterk vanaf 45 jaar

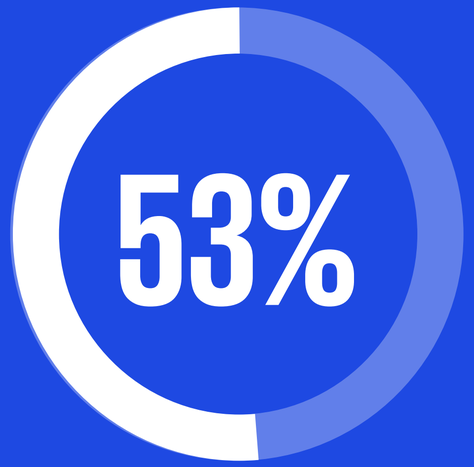
73%↘

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Slimme apparaten (1/2)

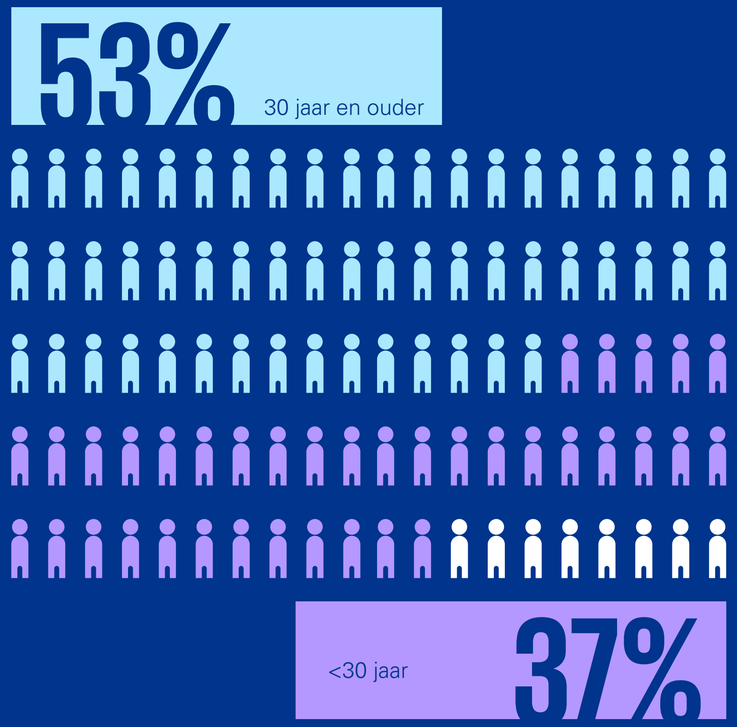
Privacy risico's van slimme apparaten

Wanneer privacyrisico's concreter worden gemaakt, bijvoorbeeld door te kijken naar slimme apparaten in huis, blijkt een **aanzienlijk deel** van de respondenten deze technologie als een mogelijk privacyrisico te zien.



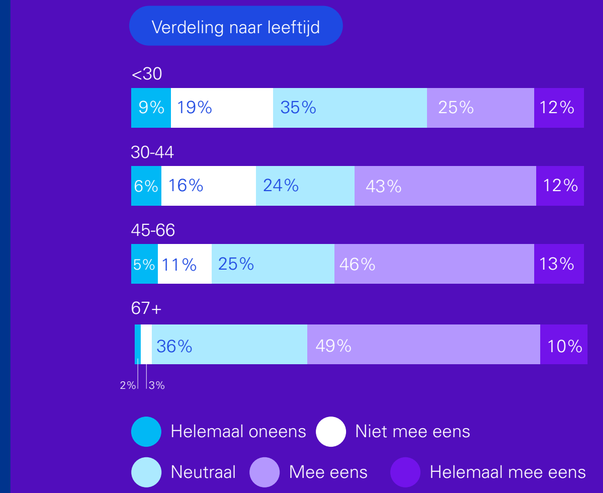
van de respondenten geeft aan dat apparaten zoals smartphones, smart speakers en beveiligingscamera's een risico kunnen vormen voor de persoonlijke levenssfeer.

Opvallend is dat respondenten van 30 jaar en ouder dit vaker onderschrijven **(55%)** dan de jongste groep **(37%)**.



Deze uitkomst kan erop wijzen dat de perceptie van privacyrisico's sterker wordt wanneer technologie zichtbaar aanwezig is in de dagelijkse leefomgeving en potentieel continu data verzamelt, bijvoorbeeld via microfoons, camera's of sensoren.

Ik heb het gevoel dat slimme apparaten, zoals smart phones, smart speakers en beveiligingscamera's, een risico vormen voor mijn privacy doordat ze meeluisteren of meekijken zonder dat ik het doorheb.



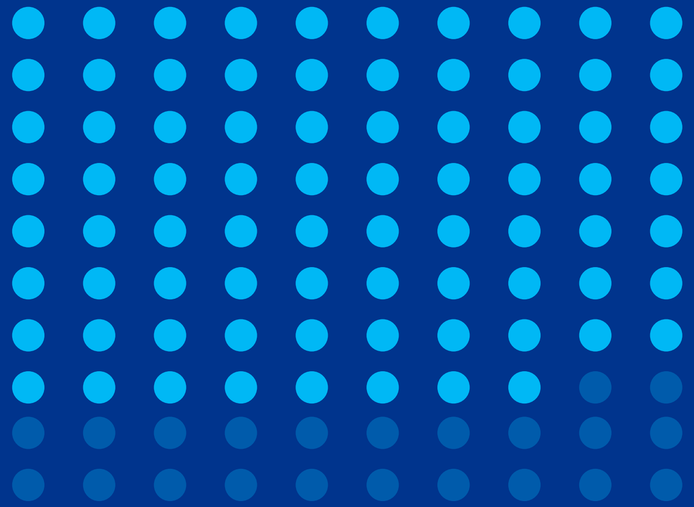
Slimme apparaten worden massaal als privacyrisico gezien

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Slimme apparaten (2/2)

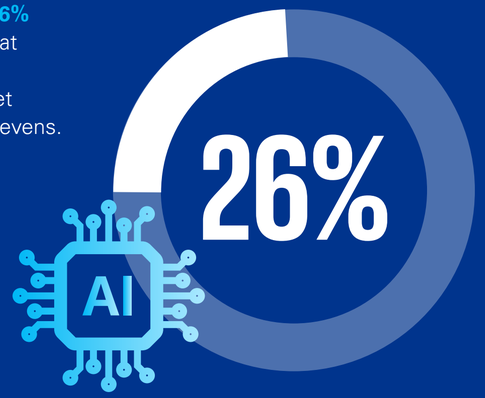
Tot slot laat het onderzoek een opvallend verschil zien tussen wat respondenten wenselijk vinden en hoe zij het huidige handelen van organisaties ervaren.

Een **grote meerderheid** van de respondenten **(gemiddeld 78%)** geeft aan dat strenge regels voor het gebruik van AI en algoritmes door bedrijven en overheden belangrijk zijn.



gemiddeld 78%

Tegelijkertijd geeft slechts **26%** aan vertrouwen te hebben dat organisaties transparant zijn over hoe zij AI inzetten bij het verwerken van persoonsgegevens.



Dit verschil tussen de wens voor duidelijke regelgeving en het ervaren gebrek aan transparantie kan worden gezien als een vorm van een governance-gap. De resultaten suggereren dat respondenten AI niet per definitie afwijzen, maar dat acceptatie sterk samenhangt met de mate waarin er duidelijke waarborgen bestaan rondom het gebruik van data en algoritmes.

Voor organisaties betekent dit dat vertrouwen niet uitsluitend ontstaat door te communiceren dat zorgvuldig met data wordt omgegaan. Respondenten lijken vooral behoefte te hebben aan inzicht in hoe AI daadwerkelijk wordt toegepast, welke gegevens worden gebruikt en welke verantwoordelijkheden daarbij horen. Transparantie, controleerbaarheid en duidelijke verantwoordelijkheidsstructuren spelen daarbij een belangrijke rol.

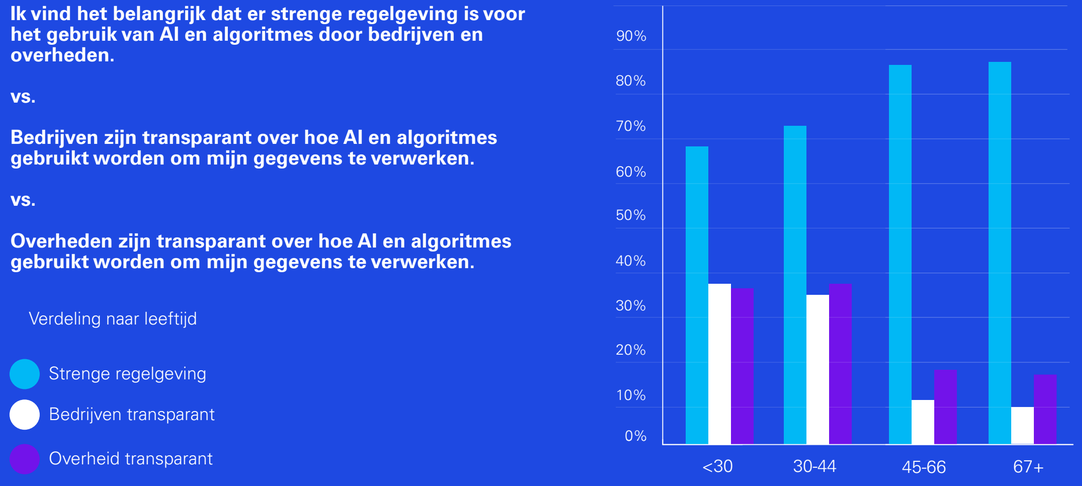
Ik vind het belangrijk dat er strenge regelgeving is voor het gebruik van AI en algoritmes door bedrijven en overheden.

vs.

Bedrijven zijn transparant over hoe AI en algoritmes gebruikt worden om mijn gegevens te verwerken.

vs.

Overheden zijn transparant over hoe AI en algoritmes gebruikt worden om mijn gegevens te verwerken.



Grote behoefte aan regels, beperkt vertrouwen in transparantie

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.



Online platforms

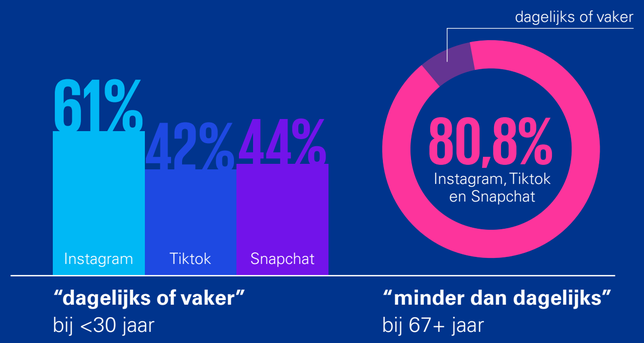
Platformgebruik verschilt sterk per generatie

Voor de interpretatie van het onderzoek zijn de percentages omtrent platformgebruik relevant. Beleidsvragen, privacy-afwegingen en moderatiediscussies landen per generatie op andere platforms, met verschillende gebruikscontexten en verwachtingen. Dat betekent dat “het platformdebat” in de praktijk meerdere parallelle debatten omvat, afhankelijk van doelgroep en kanaal.

Tabel 1 —Dagelijks of vaker gebruik (% per leeftijdsgroep)

Platform	<30	30-44	45-66	67+
Facebook	24,6%	54,3%	44%	52,3%
Instagram	61,3%	50%	25,8%	14%
Youtube	47,3%	39,1%	19%	13,7%
Tiktok	41,7%	22,3%	11,3%	3,4%
Snapchat	43,7%	13,6%	2,6%	1,8%
Linkedin	17%	14,4%	9,6%	3,5%
X (voorheen Twitter)	14,4%	15,3%	7,6%	6,4%

De grafiek laat zien dat platformgebruik sterk verschilt per generatie en dat sociale media geen homogeen landschap vormen. Jongere respondenten bewegen zich vooral op visuele en entertainment-gerichte platforms zoals Instagram, YouTube, TikTok en Snapchat, terwijl Facebook voor hen een veel beperktere rol speelt. Naarmate de leeftijd toeneemt, verschuift het gebruik duidelijk richting Facebook, terwijl jongerenplatforms bij oudere groepen grotendeels ontbreken of zelfs bijna helemaal niet worden gebruikt.



Tabel 2 —Interesses (% per leeftijdsgroep)

Interesse	<30	30-44	45-66	67+
Influencers	42,9%	23,9%	4,9%	0,8%
Nieuwskanalen	44,2%	38,8%	25,6%	31,1%
Vrienden/ familie/bekenden	73,5%	73,8%	68,1%	77,5%

De vraag naar interesses op sociale media laat zien dat communicatie met vrienden, familie en bekenden in alle leeftijdsgroepen het belangrijkste motief blijft. Andere interesses, zoals het volgen van influencers, blijken sterk leeftijdsafhankelijk.

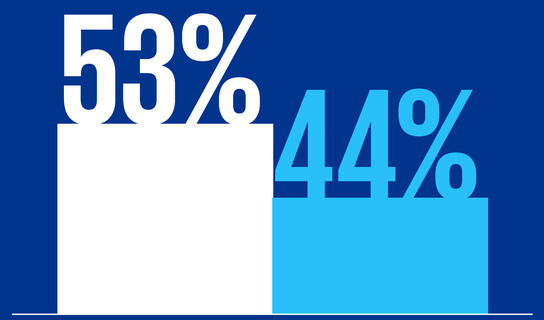
De interesse in nieuwsaccounts is zichtbaar in alle leeftijdsgroepen, maar is relatief het sterkst onder personen jonger dan 30 jaar (44%).

personen jonger dan **30** jaar ≫ **44%**

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

De “privacy-paradox” - platforms

De resultaten laten een uitgesproken **privacy-paradox** zien bij de jongste doelgroep. Jongeren onder de 30 jaar geven in meerderheid **(53%)** aan dat zij de voorkeur geven aan socialmediaplatforms die hun privacy beter waarborgen, zelfs wanneer dit ten koste gaat van functies of netwerkvoordelen. Tegelijkertijd is deze groep relatief positief over gepersonaliseerde advertenties: **44%** van de jongeren onder de 30 ervaart dat gepersonaliseerde ads hun online ervaring verbeteren. Dit is opvallend, omdat personalisatie in de praktijk vaak samenhangt met tracking en uitgebreide dataverzameling – precies de praktijken die doorgaans als privacy-gevoelig worden gezien.



Deze combinatie suggereert dat privacy voor jongeren minder draait om het volledig vermijden van datagebruik, en meer om **controle, transparantie en keuzevrijheid.** Jongeren lijken vaker bereid tot een expliciete ruil (“data-voor-gemak”), mits de voordelen concreet zijn, zoals relevantere content of advertenties, en zolang zij het gevoel hebben de regie te behouden over hun gegevens.



Bij oudere leeftijdsgroepen verschuift dit beeld duidelijk. In de groep van 30–44 jaar loopt de voorkeur voor privacy-waarborging op tot **58%**, terwijl de waardering voor gepersonaliseerde advertenties daalt naar **27%**. Deze trend zet zich sterker door bij 45–66-jarigen: **63%** geeft prioriteit aan privacy, terwijl nog slechts **12%** aangeeft dat gepersonaliseerde advertenties de ervaring verbeteren. Bij 67-plussers bereikt dit contrast een hoogtepunt: **65%** verkiest privacy boven functionaliteit en slechts **5%** ziet personalisatie als een verbetering.

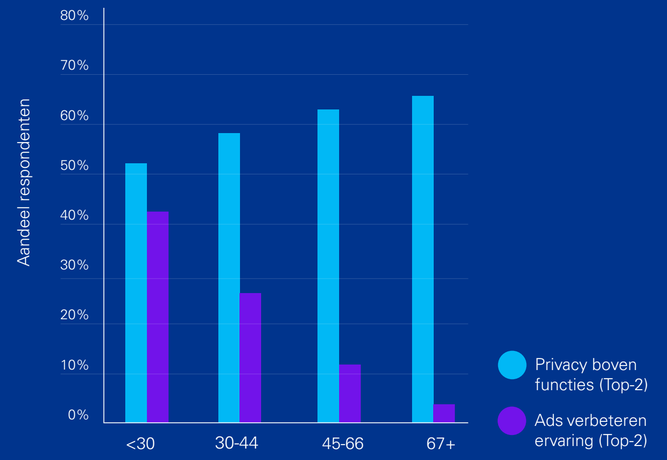
Dit patroon laat zien dat met toenemende leeftijd niet alleen het belang dat aan privacy wordt gehecht toeneemt, maar ook het comfort met datagedreven personalisatie sterk afneemt. Leeftijd lijkt daarmee een bepalende factor voor hoe mensen de balans ervaren tussen gebruiksgemak, personalisatie en privacybescherming.

Jongeren willen privacy... maar waarderen gepersonaliseerde advertenties juist het meest

Ik geef de voorkeur aan een social media-platform dat mijn privacy waarborgt, zelfs als dat minder functies of connecties biedt.

vs.

Gepersonaliseerde online advertenties maken mijn internetervaring beter.



© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Opleiding beïnvloedt overstapbereidheid

Een tweede opvallend resultaat is de duidelijke kloof tussen respondenten met een praktische opleiding en respondenten met een theoretische opleiding als het gaat om de bereidheid om daadwerkelijk van platform te wisselen voor betere privacy. Respondenten met een theoretische opleiding geven bijna twee keer zo vaak aan dat zij overwegen over te stappen naar privacyvriendelijke alternatieven zoals Signal of Telegram **(31%)** dan respondenten met een praktische opleiding **(16%)**. Bij deze laatste groep overheerst juist terughoudendheid: een relatief groot deel geeft expliciet aan het (helemaal) oneens te zijn met een overstap.

Theoretisch opgeleiden respondenten die bereid zijn om over te stappen

31%

Praktische opgeleiden respondenten die bereid zijn om over te stappen

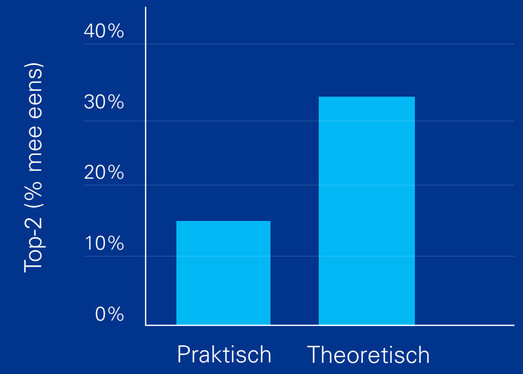
16%

Dit verschil is relevant omdat het laat zien waar privacy vooral een **principieel standpunt** blijft en waar privacy zich daadwerkelijk vertaalt naar **gedragsintentie.** Respondenten met een theoretische opleiding lijken privacyzorgen vaker te koppelen aan concreet handelen. Zij zijn relatief bereid om de nadelen van een overstap, zoals minder bereik, verlies van actieve contacten of gewenning aan een nieuw platform, te accepteren in ruil voor verbeterde privacybescherming.

Respondenten met een praktische opleiding lijken daarentegen sterker te hechten aan het bestaande netwerk en het gebruiksgemak van de huidige platforms. Voor deze groep vormt overstappen een hogere drempel, ook wanneer privacy-alternatieven beschikbaar zijn. Voor de interpretatie van de resultaten is dit belangrijk, omdat het aangeeft dat de adoptie van privacy-vriendelijke platforms waarschijnlijk ongelijk verdeeld zal zijn binnen de populatie. Privacy-first proposities zullen naar verwachting in eerste instantie meer tractie vinden onder theoretisch opgeleiden, terwijl bij praktisch opgeleiden eerder winst te behalen is met privacyverbeteringen binnen bestaande platforms, zoals sterkere standaardinstellingen, eenvoudiger privacy-opties en concrete, laagdrempelige communicatie over datagebruik.

Respondenten met een theoretische opleiding zijn veel eerder bereid hun platform te verlaten voor privacy.

Ik overweeg om over te stappen naar alternatieve social media platforms (Signal, Telegram) die mijn privacy beter waarborgen, ook al zijn daar minder mensen actief.



© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Sterke steun voor EU-ingrijpen

Op het niveau van systeemoplossingen is het beeld uitzonderlijk eenduidig: er bestaat brede steun voor een actievere rol van de Europese Unie in het reguleren van online platforms en het inperken van de macht van BigTech. Over alle leeftijdsgroepen heen spreekt een ruime meerderheid zich uit vóór strengere EU-regels om de veiligheid op platforms te verbeteren, het beperken van de macht van grote technologiebedrijven en investeringen in Europese technologie om de afhankelijkheid van Amerikaanse en Chinese spelers te verminderen.

Ook onder jongeren is deze steun substantieel. In de leeftijdsgroep onder de 30 jaar steunt **68,3%** strengere regels voor platformveiligheid, wil **66,7%** dat de EU de macht van BigTech verder begrenst en is **70,6%** positief over investeringen in Europese technologie. Daarmee ligt de steun al dicht bij de **70%**, met relatief beperkte afwijzing. In de groep van 30–44 jaar blijft het patroon vergelijkbaar: **74,1%** steunt strengere veiligheidsregels, **65,7%** het inperken van BigTech en **76,2%** investeringen in Europese tech.

Vanaf middelbare leeftijd neemt de steun verder toe. Bij respondenten van 45–66 jaar lopen de percentages op tot **84,5%** voor strengere regels rond platformveiligheid, **88,2%** voor het beperken van de macht van BigTech en **88,1%** voor investeringen in Europese technologie. Onder 67-plussers is de steun het hoogst: respectievelijk **91,4%**, **87,5%** en **92,0%** onderschrijft deze drie vormen van EU-ingrijpen.

Wat deze uitkomst extra interessant maakt, is dat de steun voor EU-ingrijpen weliswaar toeneemt met de leeftijd, maar ook **onder jongeren duidelijk aanwezig** is. Daarmee onderscheidt dit thema zich van onderwerpen zoals gepersonaliseerde advertenties of overstappen naar alternatieve platforms, waar de meningen sterker uiteenlopen. In het consumentenonderzoek kan dit worden geduid als een breed gedragen gevoel dat problemen rond platforms (zoals veiligheid, machtsconcentratie en geopolitieke afhankelijkheid) **niet uitsluitend via individuele keuzes of “slimme instellingen” kunnen worden opgelost.** De Europese Unie wordt kennelijk gezien als een legitieme en noodzakelijke actor om normerend en corrigerend op te treden.



© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Breed draagvlak voor contentmoderatie

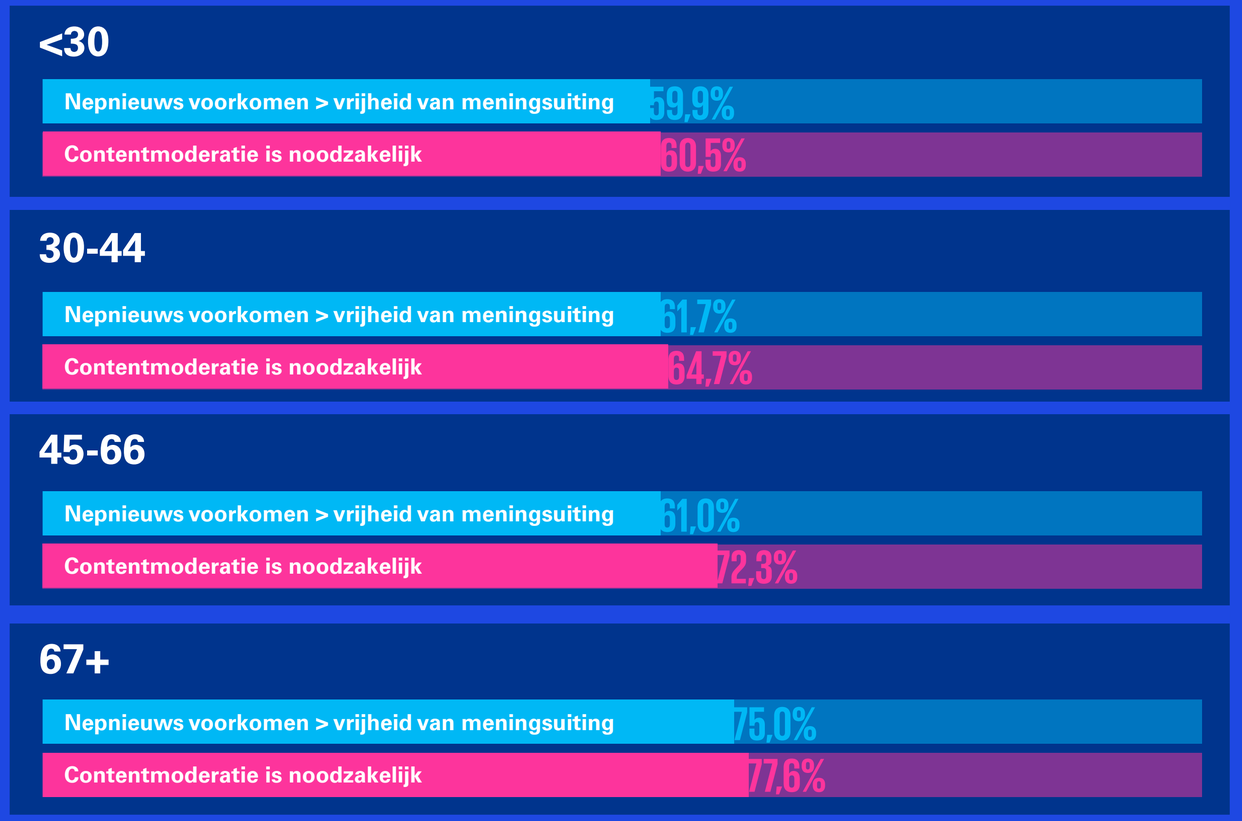
De uitkomsten rond nepnieuws en contentmoderatie laten een duidelijke normatieve richting zien: respondenten kiezen in meerderheid voor een actieve aanpak van desinformatie, zelfs wanneer dit kan botsen met een onbeperkte invulling van vrijheid van meningsuiting. Over alle leeftijdsgroepen heen onderschrijft een ruime meerderheid dat het voorkomen van nepnieuws zwaarder weegt dan het volledig handhaven van vrijheid van meningsuiting, en dat contentmoderatie noodzakelijk is om de verspreiding van nepnieuws te beperken.

Ook bij jongeren is deze steun duidelijk aanwezig. In de leeftijdsgroep onder de 30 jaar vindt **59,9%** dat het tegengaan van nepnieuws belangrijker is dan onbeperkte vrijheid van meningsuiting, terwijl **60,5%** contentmoderatie noodzakelijk acht. In de groep van 30–44 jaar loopt dit verder op: **61,7%** geeft prioriteit aan het voorkomen van nepnieuws en **64,7%** steunt actieve moderatie. Deze trend zet zich sterker door bij oudere respondenten. Bij 45–66-jarigen stijgt de steun naar respectievelijk **61,0%** en **72,3%**, en onder 67-plussers is het draagvlak het grootst: **75,0%** vindt het tegengaan van nepnieuws doorslaggevend en **77,6%** beschouwt contentmoderatie als noodzakelijk.

Tegelijkertijd laat de grafiek zien dat de afwijzing relatief beperkt blijft, maar dat er wel een omvangrijke neutrale middengroep bestaat. Ongeveer een kwart van de respondenten positioneert zich niet expliciet vóór of tegen deze stellingen. Deze neutraliteit is belangrijk om te duiden, omdat zij erop wijst dat steun voor contentmoderatie geen “blanco cheque” inhoudt. Een neutrale houding ontstaat vaak wanneer respondenten voorwaarden willen stellen aan moderatie: wie bepaalt wat als nepnieuws geldt, hoe transparant dat proces is, welke mogelijkheden tot bezwaar bestaan en hoe willekeur of politieke beïnvloeding wordt voorkomen.

In de praktijk betekent dit dat er brede bereidheid is om in te grijpen tegen desinformatie, maar dat het maatschappelijk draagvlak sterk afhankelijk is van de **legitimiteit van de moderatiepraktijk.** Zorgvuldigheid, transparantie en verantwoording zijn daarmee cruciaal: niet om steun te creëren, maar om bestaande steun te behouden en te verstevigen.

Breed draagvlak voor actieve aanpak van nepnieuws en contentmoderatie.



© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.



Over KPMG

Wat doet KPMG op het gebied van Privacy en Tech-regulering?

KPMG Cyber & TechLaw ondersteunt organisaties bij:
- het versterken van hun digitale weerbaarheid;
- het vergroten van vertrouwen bij klanten en stakeholders;
- en het realiseren van effectieve en toekomstbestendige compliance.

Met een unieke combinatie van juridische expertise, technologische kennis en pragmatische professionals helpen wij organisaties complexe regelgeving beheersbaar te maken en vertrouwen duurzaam te verankeren in de organisatie.

Samen kunnen we een betrouwbare digitale wereld creëren waarmee je de grenzen van het mogelijke kunt oprekken. Met KPMG kun je vol vertrouwen de uitdagingen op het gebied van cybersecurity & tech regulering tegemoet treden en voorop blijven lopen.

Wereldwijd meer dan 500 tech lawyers en privacy professionals (CIPP/E, CIPM en CIPT) zijn getraind en gekwalificeerd op het gebied privacy, tech-reguleringen en het verantwoordelijk omgaan met AI. Met diepgaande kennis en ervaring op zowel juridisch, organisatorisch als technisch gebied, zijn wij zijn hands-on in het implementeren van pragmatische, effectieve en op maat gemaakte compliance programma's en strategische advisering rondom tech regulering.

Een greep uit onze dienstverlening:

- **Tech Regulatory Horizon Scanning**
- **Strategisch advies en impact-analyse Tech regulering**
- **Implementatie ondersteuning compliance met Tech-regulering**
  (AVG, AI Act, Digital Services Act, Data Act, DORA, NIS2, etc.)
- **Privacy diensten**
  (DPIA's, Privacy Tooling, Interim DPO, AVG processen en implementaties)
- **Soevereiniteits-vraagstukken Cloud, IT en Data**

Contact



Stephan Idema
Director
Cyber & TechLaw
+31 (0)20 656 40 48
idema.stephan@kpmg.nl



Stanny van der Louw
Senior Consultant
Cyber & TechLaw
+31 (0)20 656 86 52
vanderlouw.stanny@kpmg.nl



Milan Smit
Senior Consultant
Cyber & TechLaw
+31 20 65 67 833
smit.milan@kpmg.nl

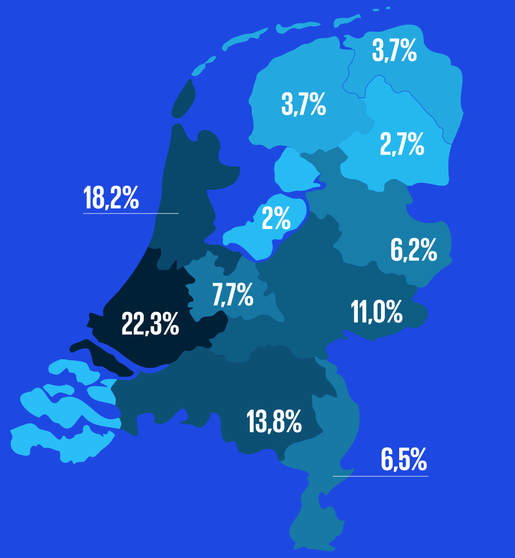
© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.



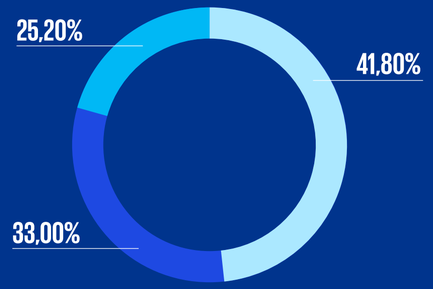
Uitleg onderzoek

Over ons onderzoek

In opdracht van KPMG ondervroeg Blauw Research in het begin van 2026 501 Nederlanders vanaf 18 jaar met de volgende kenmerken over verschillende thema's op het gebied van privacy en AI. De resultaten zijn gewogen en representatief voor de Nederlandse bevolking op leeftijd, opleiding, geslacht en regio.



Opleiding

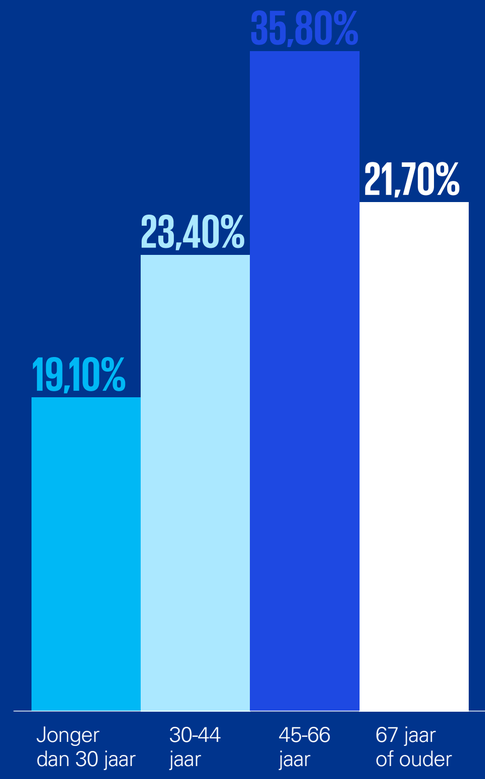


Beroepsonderwijs
- geen of basisonderwijs
- LBO /VMBO / (kader of beroepsgericht) / MBO 1 /VBO
- MAVO / HAVO of VWO (overgegaan naar 4e klas) /VMBO / (M)ULO
- MBO 2, 3, 4, of MBO vóór 1998

Hoger beroepsonderwijs
- HAVO of VWO (met diploma afgerond) / HBS / MMS

Propedeuse (HBO of universitair)
- Wetenschappelijk onderwijs
- Bachelor/kandidaats (HBO of universitair)
- Master/doctoraal/postdoctoraal (HBO of universitair)

Leeftijd



Geslacht



© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

kpmg.com/socialmedia

De in dit document vervatte informatie is van algemene aard en is niet toegespitst op de specifieke omstandigheden van een bepaalde persoon of entiteit. Wij streven ernaar juiste en tijdige informatie te verstrekken. Wij kunnen echter geen garantie geven dat dergelijke informatie op de datum waarop zij wordt ontvangen nog juist is of in de toekomst blijft. Daarom adviseren wij u op grond van deze informatie geen beslissingen te nemen behoudens op grond van advies van deskundigen na een grondig onderzoek van de desbetreffende situatie.

De naam KPMG en het logo zijn geregistreerde merken die onder licentie worden gebruikt door de zelfstandige ondernemingen die lid zijn van de wereldwijde KPMG organisatie.

© 2026 KPMG Advisory N.V., een naamloze vennootschap en lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Limited, een Engelse entiteit. Alle rechten voorbehouden.

Document Classification: KPMG Public


KPMG