

Wettelijke regels voor politieke reclame

Informatie van de Autoriteit Persoonsgegevens (AP)

Inleiding

Voor het verspreiden van politieke reclame geldt (Europese) wetgeving. Een deel daarvan is nieuw. Daarom informeert de Autoriteit Persoonsgegevens (AP) u hierbij over enkele regels die belangrijk zijn voor uw campagne in aanloop naar de Gemeenteraadsverkiezingen.

Wij geven beknopte uitleg over de Verordening betreffende transparantie en gerichte politieke reclame (VPR), de Algemene verordening gegevensbescherming (AVG) en de AI-verordening. Ons advies is dat u zich vervolgens zelf verder in de wetgeving verdiept, zodat u goed op de hoogte bent van uw wettelijke verplichtingen.

VPR: nieuwe regels voor gerichte online politieke reclame

Op 10 oktober 2025 is de Verordening betreffende transparantie en gerichte politieke reclame (VPR) in werking getreden. In de VPR staan specifieke regels voor gerichte online politieke reclame.¹

De AP zal toezicht houden op de artikelen 18 en 19 van de VPR. De AP verwacht ook toezicht te houden op artikel 20 van de VPR. De AP heeft die bevoegdheid nog niet, maar zal later in de Uitvoeringswet worden aangewezen. Kort gezegd staan in deze artikelen de eisen waaraan verwerkingsverantwoordelijken moeten voldoen om mensen te mogen benaderen met gerichte online politieke reclame. Als u besluit – al dan niet samen met anderen – om uw politieke reclame te richten op specifieke groepen mensen, dan kunt u als verwerkingsverantwoordelijke worden aangemerkt. Daarnaast stelt de VPR eisen aan de manier waarop deze verwerkingsverantwoordelijken informatie moeten geven over hun gerichte online politieke reclame. Daarnaast bevat de VPR normen waar andere toezichthouders op toezien.

Samengevat zijn dit de regels voor (gezamenlijk) verwerkingsverantwoordelijken:

Regels voor gericht adverteren

U mag alleen gericht adverteren onder deze voorwaarden:

1. U, of de partijen waar u mee samenwerkt, heeft de benodigde persoonsgegevens van diegene zelf gekregen.
2. U gebruikt bij de targeting géén zogeheten bijzondere persoonsgegevens, zoals gegevens over iemands politieke opvattingen.

¹ <https://eur-lex.europa.eu/NL/legal-content/summary/transparency-and-targeting-of-political-advertising.html>

3. De persoon aan wie politieke reclame wordt gericht heeft uitdrukkelijke toestemming gegeven voor de verwerking van persoonsgegevens voor het ontvangen van de gerichte online politieke reclame. Bij communicatie door een politieke partij aan (ex-)leden gelden deze regels niet. Zij kunnen dus nieuwsbrieven en dergelijke blijven ontvangen.
4. De persoon is 17 jaar of ouder. Kunt u redelijkerwijs weten dat iemand jonger is dan 17 jaar? Dan mag gerichte online politieke reclame aan deze persoon niet.

Regels voor informeren over gerichte online politieke reclame

- Wilt u gerichte online politieke reclame gaan inzetten, dan moet u daarvoor een beleid opstellen. Dit beleid moet u zeven jaar bewaren.
- U moet een register bijhouden voor uw gerichte online politieke reclame. Dat register moet de gebruikte mechanismen en parameters voor de online politieke reclame bevatten.
- U moet mensen goed informeren over de gerichte online politieke reclame, zodat zij kunnen begrijpen hoe en waarom u hen benaderd heeft.
- U moet een jaarlijkse interne risicobeoordeling doen voor het gebruik van targetingtechnieken. Hierbij brengt u de risico's in kaart voor de grondrechten en fundamentele vrijheden van mensen, zoals hun recht op bescherming van persoonsgegevens. U moet de resultaten van deze risicobeoordeling openbaar maken.

Advies:

- Bekijk de regels in de VPR. Bepaal wat uw rol is bij gerichte online politieke reclame en welke verantwoordelijkheden daarbij horen.
- Wees kritisch naar organisaties die diensten aanbieden waarbij u kunt adverteren gericht op bepaalde voorkeuren of doelgroepen of op persoonlijke kenmerken. Ga alleen in zee met organisaties die aan de VPR en AVG voldoen. Controleer dit door bijvoorbeeld te vragen hoe zij het gericht adverteren precies uitvoeren, wat hun privacybeleid is en hoe zij omgaan met de privacyrechten van mensen. Vraag ook naar de databronnen die zij gebruiken en een data protection impact assesment.²
- We wijzen u op De leidraad gerichte online politieke reclame die u kan vinden via [Gerichte online politieke reclame | Autoriteit Persoonsgegevens](#)

AVG: regels voor gegevens over politieke opvattingen, voor beveiliging en voor cookies

Naast de regels uit de VPR staan er in de AVG algemene regels voor het verwerken van persoonsgegevens. Hiermee heeft u ook te maken bij uw campagnes. We gaan hier op drie punten in: gegevens over politieke opvattingen, beveiliging en cookies.

Gegevens over politieke opvattingen

Voor het gebruik van gegevens over iemands politieke opvattingen gelden speciale regels. Die staan in de AVG. Deze regels gelden in aanvulling op de regels uit de VPR voor gerichte online politieke reclame, maar gelden ook als er geen sprake is van gerichte online politieke reclame.

² <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia>

Gegevens over iemands politieke opvattingen zijn extra beschermd in de AVG. Het verwerken van deze zogeheten bijzondere persoonsgegevens is verboden (art. 9 AVG). Hierop zijn een paar uitzonderingen (art. 9 lid 2 AVG). Voor u is van belang:

- U mag persoonsgegevens verwerken als die noodzakelijk zijn voor de registratie van en communicatie met de leden van uw partij. Dit geldt ook als dit bijzondere persoonsgegevens zijn.
- U mag gegevens over politieke opvattingen van mensen verwerken als zij hiervoor vooraf uitdrukkelijke toestemming hebben gegeven. U moet kunnen aantonen dat u aan de eisen voor uitdrukkelijke toestemming heeft voldaan.³

Advies:

- Houd er in uw campagne rekening mee dat gegevens over politieke opvattingen extra gevoelig zijn en dat het meestal verboden is om deze gegevens te verwerken.
- Ga ook zeer zorgvuldig om met de persoonsgegevens die u van uw leden heeft.
- Wees transparant over de verwerkingen van persoonsgegevens die u tijdens uw campagne uitvoert.

Let op:

- Krijgt u van derde partijen bestanden aangeboden met persoonsgegevens over (vermeende) politieke opvattingen van mensen? Hoogstwaarschijnlijk voldoen die bestanden niet aan de wet, omdat het dus meestal verboden is om deze persoonsgegevens te verwerken. U mag die bestanden dan dus niet gebruiken.
- U kunt medeverantwoordelijk (en aansprakelijk) zijn voor gegevensverwerkingen waarbij u met derde partijen 'doel en middelen' heeft bepaald.⁴

Beveiliging van persoonsgegevens

In artikel 32 van de AVG staat dat u passende technische en organisatorische maatregelen moet nemen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking (dat betekent: tegen de regels uit de wet). Dus in uw geval ook tegen onrechtmatig gebruik van persoonsgegevens door uw medewerkers, partijleden, campagneleden of kandidaten van uw partij. Wat 'passend' is, hangt af van de risico's van uw verwerking en hoe gevoelig de gegevens zijn die u verwerkt. Verder speelt mee wat er technisch gezien mogelijk is en wat de kosten zijn voor u.

³ Zie: <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslag-toestemming#uitdrukkelijke-toestemming>

⁴ Samenvattend betekent het bepalen van doel en middelen bij de verwerking van persoonsgegevens: wie, waarom, met welk doel, met welk budget en hoe je mensen benadert. Voor meer informatie over 'gezamenlijke verwerkingsverantwoordelijkheid', zie: <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verantwoordelijke-en-verwerker>

Online tracking en cookies

Met cookies en vergelijkbare technologieën (zoals javascripts, webbeacons en HTML5 Local Storage) kunnen organisaties informatie verzamelen en opslaan over het websitebezoek of over het apparaat van gebruikers.

Met tracking cookies kunnen organisaties het gedrag van een websitebezoeker over verschillende websites volgen, met als doel diegene anders te behandelen. Bijvoorbeeld door gepersonaliseerde advertenties of aanbiedingen te tonen.

Tracking cookies maken het mogelijk om profielen van mensen op te stellen (profilering) en hen anders te behandelen. Met tracking cookies en vergelijkbare trackingtechnologieën worden persoonsgegevens verwerkt. Hierop is de AVG van toepassing.⁵

In de AVG staat dat voor deze verwerkingen toestemming van websitebezoekers vereist is. In de AVG staat ook wanneer sprake is van rechtsgeldige toestemming en hoe een organisatie die moet krijgen. Volgens de AVG is toestemming “elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt”.⁶

Leidt de vormgeving of inhoud van uw cookiebanner ertoe dat niet is voldaan aan alle elementen van deze definitie? Dan is er geen sprake van geldige toestemming. De verwerking van persoonsgegevens is dan in strijd met de AVG.⁷

Op de website van de AP vindt u vuistregels voor het ontwerpen van een goede cookiebanner.⁸ Als u de vuistregels volgt en juist implementeert, vraagt u uw websitebezoekers op de goede manier om toestemming. U heeft dan dus een cookiebanner die voldoet aan de AVG.

Tot slot: let op dat u geen tracking cookies mag plaatsen vóór de websitebezoeker toestemming heeft gegeven of nadat de websitebezoeker toestemming heeft geweigerd.

AI-verordening: gebruik van AI-gegenereerde content

De mogelijkheid om met AI (artificiële intelligentie) content te maken, is tijdens de komende verkiezingen voor het eerst op grote schaal voor iedereen toegankelijk. Gaat u bij uw campagne AI-gegenereerde content publiceren, zoals foto's of video's? Het is dan verstandig te vermelden dat het om AI-content gaat. Publiceert u door AI gemaakte of bewerkte teksten? Vermeld dit dan ook óf laat de tekst door een mens controleren.

De verplichting om duidelijk te maken dat u AI heeft gebruikt, staat in de Europese AI-verordening. Deze verplichting treedt pas in werking op 2 augustus 2026. Wij raden u wel aan om al bij de komende

⁵ Als deze persoonsgegevens vervolgens worden gebruikt voor gerichte online politieke reclame, is daarop de VPR van toepassing.

⁶ Vergelijk artikel 4, aanhef en onder 11, van de AVG.

⁷ Vergelijk artikel 5, eerste lid, aanhef en onder a, gelezen in samenhang met artikel 6, eerste lid, aanhef en onder a, van de AVG.

⁸ Zie <https://www.autoriteitpersoonsgegevens.nl/cookiebanners>.

verkiezingen het gebruik van AI-gegenereerde content duidelijk te vermelden. Zo informeert u kiezers goed. Zij weten dan dat zij met AI te maken hebben en worden dus niet misleid.

Misleiding door AI-genereerde content kan schadelijke gevolgen met zich meebrengen.⁹ Dit geldt in het bijzonder tijdens verkiezingen, waarbij betrouwbare informatie essentieel is.¹⁰ Weten kiezers niet of informatie betrouwbaar is? Dan kunnen zij hun stemrecht niet goed uitoefenen.

Wat staat er precies in de AI-verordening?

In de AI-verordening staat dat organisaties bij het publiceren van bepaalde AI-gegenereerde content duidelijk moeten maken dat er sprake is van AI (art. 50 lid 4). Bijvoorbeeld met een duidelijke en onderscheidende disclaimer dat het om AI-gegenereerde content gaat. Deze verplichting geldt ook voor politieke partijen die bijvoorbeeld AI-gegenereerde content willen gebruiken voor hun campagne (art. 3 lid 4).

Deze verplichting geldt bij “AI gegenereerd beeld-, audio- of videomateriaal dat een gelijkenis vertoont met bestaande personen, voorwerpen, plaatsen, entiteiten of gebeurtenissen en door een (gemiddeld) persoon ten onrechte voor authentiek of waarheidsgetrouw zou worden aangezien” (artikel 3 aanhef en onder 60). Kortom: iedere door AI-gegenereerde afbeelding, audio of video die voor echt kan doorgaan.

De verplichting geldt ook voor AI-gegenereerde of bewerkte teksten die organisaties publiceren om het publiek te informeren over zaken van algemeen belang. Dit geldt in de praktijk vrijwel altijd voor politieke partijen. De verplichting geldt echter niet als de tekst door een mens is gecontroleerd. Als politieke partij kunt u dus aan de verplichting voldoen door het gebruik van AI duidelijk te vermelden of de tekst door een mens te laten controleren.

Advies:

- Zorg dat u weet wat de risico's zijn van (generatieve) AI voordat u dit gebruikt.¹¹
- Vermeld duidelijk het gebruik van AI-gegenereerde content, ook al is het nu nog niet verplicht. Zo informeert u kiezers goed.

Vragen?

Heeft u vragen over het verwerken van persoonsgegevens bij uw campagnes? Dan kunt u terecht bij uw functionaris gegevensbescherming (FG). Vraag de FG in ieder geval om advies vóór u besluit een bepaald middel te gebruiken of een bepaalde organisatie in te huren.

Heeft u nog geen FG? Dan adviseren wij u om alsnog een FG aan te stellen. Uiteraard kunt u ook bij anderen (juridisch) advies inwinnen.

⁹ *How AI deepfakes polluted elections in 2024*, NPR, 21 december 2024. [OPM. IHU: EEN LINK IN DEZE VORM HEEFT GEEN ZIN IN EEN PAPIEREN BRIEF] <https://www.npr.org/2024/12/21/nx-s1-5220301/deepfakes-memes-artificial-intelligence-elections>

¹⁰ B. van der Sloot, Y. Wagenveld, B. Koops (WODC) 2021, *Deepfakes: De juri dische uitdagingen van een synthetische samenleving*, Hoofdstuk 2.

¹¹ <https://www.autoriteitpersoonsgegevens.nl/documenten/rapportage-algoritmerisicos-nederland>