EUROPESE
COMMISSIE

Brussel, 12.9.2018
COM(2018) 638 final

Vrije en eerlijke verkiezingen

RICHTSNOEREN

Richtsnoeren van de Commissie voor de toepassing van de EU-gegevensbeschermingswetgeving in het kader van verkiezingen

Een bijdrage van de Europese Commissie aan de bijeenkomst van leiders in Salzburg, 19-20 september 2018

RICHTSNOEREN VAN DE COMMISSIE VOOR DE TOEPASSING VAN DE EU-GEGEVENSBESCHERMINGSWETGEVING IN HET KADER VAN VERKIEZINGEN

Contact met het electoraat is de basis van het democratische proces. Politieke partijen hebben de gewoonte hun verkiezingsboodschappen op het publiek af te stemmen en houden daarbij rekening met de specifieke belangen van dat publiek. Het is dan ook vanzelfsprekend dat de bij verkiezingen betrokken actoren de mogelijkheden verkennen om gebruik te maken van gegevens voor het winnen van stemmen. Met de opkomst van de digitale instrumenten en online platforms zijn er veel nieuwe mogelijkheden ontstaan om politieke debatten te voeren met de burger.

De ontwikkeling waarbij stemmers zeer gericht worden geviseerd ("micro-targeting") met behulp van de onrechtmatige verwerking van persoonsgegevens, zoals in het geval van Cambridge Analytica, is echter van een andere orde. Deze zaak laat de uitdagingen zien waarvoor moderne technologieën ons stellen, maar toont ook aan hoe belangrijk gegevensbescherming in het kader van verkiezingen is. Deze praktijk vormt inmiddels een groot probleem, niet alleen voor individuen, maar ook voor het functioneren van onze democratieën, omdat er sprake is van een ernstige bedreiging voor een eerlijk en democratisch verloop van de verkiezingen en de kans bestaat dat afbreuk wordt gedaan aan het open debat, de eerlijkheid en de transparantie, die in een democratie van wezenlijk belang zijn. De Commissie is van mening dat het uiterst belangrijk is om deze kwestie aan te pakken, zodat het vertrouwen van het publiek in de eerlijkheid van het electorale proces wordt hersteld.

De eerste verslagen van de Britse gegevensbeschermingsautoriteit (Information Commissioner's Office – ICO) over het gebruik van gegevensanalyses bij politieke campagnes[1] en het advies van de Europese Toezichthouder voor gegevensbescherming inzake online manipulatie en persoonsgegevens[2] hebben bevestigd dat micro-targeting, dat oorspronkelijk voor commerciële doeleinden werd ontwikkeld, in het kader van verkiezingen steeds grotere gevolgen heeft.

Diverse gegevensbeschermingsautoriteiten hebben meer in het algemeen aandacht geschonken aan gegevensbescherming in het kader van verkiezingen[3].

[1] Verslagen van de Britse gegevensbeschermingsautoriteiten (Information Commissioner's Office – ICO) van 10 juli 2018: "Investigation into the use of data analytics in political campaigns – Investigation update" en "Democracy Disrupted? Personal information and political influence".

[2] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

[3] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267 "Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale" gepubliceerd in nr. 71 van het officiële blad van de Italiaanse gegevensbeschermingsautoriteit op 26.3.2014 [doc. web n. 3013267]; https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux "Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?", gepubliceerd door de Commission Nationale de l'informatique et des libertés (Franse nationale commissie inzake informatica en vrijheid) op 8.11.2016; https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf Information Commissioner's Office 'Guidance on political campaigning' [20170426].

Verordening (EU) 2016/679 van het Europees Parlement en de Raad (algemene verordening gegevensbescherming)[4], die op 25 mei 2018 in de hele Unie rechtstreeks toepasselijk is geworden, biedt de Unie de instrumenten die nodig zijn om gevallen van onrechtmatig gebruik van persoonsgegevens in het kader van verkiezingen aan te pakken. Alleen een krachtige en consistente toepassing van de regels zal echter de integriteit van het politieke bedrijf in een democratie helpen beschermen. Aangezien deze regels bij de komende verkiezingen voor het Europees Parlement voor de eerste keer in het Europese electorale kader zullen worden toegepast, is het belangrijk duidelijkheid te bieden aan de bij de electorale processen betrokken actoren, zoals nationale verkiezingsautoriteiten, politieke partijen, gegevensmakelaars en -analisten, socialemediaplatforms en online advertentienetwerken. Deze richtsnoeren hebben dus als doel de verplichtingen inzake gegevensbescherming over het voetlicht te brengen die van belang zijn voor verkiezingen. In hun hoedanigheid van handhavers van de algemene verordening gegevensbescherming moeten de nationale gegevensbeschermingsautoriteiten ten volle gebruikmaken van hun versterkte bevoegdheden voor het aanpakken van eventuele inbreuken, met name inbreuken waarbij sprake is van de micro-targeting van kiezers.

1. Het kader voor gegevensbescherming van de Unie

De bescherming van persoonsgegevens is een in het Handvest van de grondrechten van de Europese Unie (artikel 8) en de Verdragen (artikel 16 VWEU) neergelegd grondrecht. De algemene verordening gegevensbescherming versterkt het kader voor gegevensbescherming, waardoor de Unie beter is uitgerust om in de toekomst gevallen van misbruik van gegevensbescherming aan te pakken en alle actoren verantwoordelijker zijn voor de wijze waarop zij met persoonsgegevens omgaan en daarover beter rekenschap moeten afleggen.

Zij geeft natuurlijke personen in de Unie aanvullende en sterkere rechten, die met name in het kader van de verkiezingen van belang zijn. Het ging vooral ten koste van de regeling inzake gegevensbescherming die de afgelopen 20 jaar in de Unie van kracht was, dat de regels niet in alle lidstaten op dezelfde wijze werden toegepast, officiële mechanismen voor samenwerking tussen nationale gegevensbeschermingsautoriteiten ontbraken en de handhavingsbevoegdheden van die autoriteiten beperkt waren. De algemene verordening gegevensbescherming verhelpt deze tekortkomingen: zij sluit aan bij de beproefde beginselen inzake gegevensbescherming, harmoniseert belangrijke begrippen als toestemming, versterkt het recht van individuen op informatie over de verwerking van hun gegevens, verduidelijkt de voorwaarden waaronder persoonsgegevens verder mogen worden gedeeld, introduceert regels inzake inbreuken in verband met persoonsgegevens, voert een mechanisme in voor samenwerking tussen de gegevensbeschermingsinstanties in grensoverschrijdende zaken en versterkt de handhavingsbevoegdheden van deze laatste. In geval van inbreuken op de EU-regels inzake gegevensbescherming hebben de gegevensbeschermingsautoriteiten de bevoegdheid tot onderzoek (bijvoorbeeld het geven van een bevel tot het verstrekken van

[4] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

informatie of het uitvoeren van inspecties ter plaatse bij verwerkingsverantwoordelijken en verwerkers) en het corrigeren van gedragingen (bijvoorbeeld het doen uitgaan waarschuwingen en berispingen of het opleggen van een tijdelijke of definitieve schorsing van de verwerking). Zij zijn ook bevoegd boetes op te leggen tot maximaal 20 miljoen EUR of, in geval van ondernemingen, maximaal 4 % van de wereldwijde omzet van de betreffende onderneming[5]. Bij hun beslissing over het opleggen van boetes en de hoogte daarvan zullen de gegevensbeschermingsautoriteiten rekening houden met de individuele omstandigheden van het geval en factoren als de aard, de reikwijdte en het doel van de verwerking, het aantal betrokken personen en de grootte van de schade die zij hebben geleden[6]. In het kader van verkiezingen zullen de ernst van de inbreuk en het aantal betrokken personen waarschijnlijk groot zijn. Dit kan ertoe leiden dat hoge boetes worden opgelegd, met name omdat het vertrouwen van de burger van groot belang is voor het democratisch proces.

Het onlangs opgerichte Europees Comité voor gegevensbescherming, waarin alle nationale gegevensbeschermingsautoriteiten alsook de Europese Toezichthouder voor gegevensbescherming zitting hebben, spelen een cruciale rol bij de toepassing van de algemene verordening gegevensbescherming door richtsnoeren aan te reiken, aanbevelingen te doen en beste praktijken te verspreiden[7]. Als handhavers van de algemene verordening gegevensbescherming en directe aanspreekpunten voor belanghebbenden zijn nationale gegevensbeschermingsautoriteiten bij uitstek in staat om aanvullende rechtszekerheid te bieden over de uitlegging ervan. De Commissie verleent actieve steun aan die werkzaamheden.

De richtlijn betreffende privacy en elektronische communicatie of e-privacyrichtlijn (Richtlijn 2002/58/EC van het Europees Parlement en de Raad[8]) vervolledigt het kader voor gegevensbescherming van de Unie en is relevant in het kader van verkiezingen aangezien zij onder meer regels voor de elektronische verzending van ongevraagde berichten bevat, zoals berichten die met het oog op direct marketing worden verzonden. In de e-privacyrichtlijn zijn ook regels vastgesteld voor de opslag van informatie en het verkrijgen van toegang tot reeds in eindapparatuur (bv. een smartphone of computer) opgeslagen informatie, zoals cookies die kunnen worden gebruikt om het online gedrag van een gebruiker te traceren. Het voorstel van de Commissie voor een verordening betreffende privacy en elektronische communicatie (e-privacyverordening)[9], waarover thans wordt onderhandeld, is op dezelfde beginselen gebaseerd als de e-privacyrichtlijn. De nieuwe verordening zal het toepassingsgebied van de richtlijn verruimen en niet alleen op traditionele telecomexploitanten, maar ook op elektronische communicatiediensten via internet van toepassing zijn.

---

[5] Richtsnoeren van de Commissie inzake de algemene verordening gegevensbescherming, te vinden op: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

[6] Artikel 83 van de algemene verordening gegevensbescherming.

[7] De Europese Toezichthouder voor gegevensbescherming brengt ook adviezen uit.

[8] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

[9] Voorstel voor een verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie), COM (2017) 10 final.

2. Voornaamste verplichtingen van de verschillende actoren

De algemene verordening gegevensbescherming is van toepassing op alle actoren die in het kader van de verkiezingen actief zijn, zoals de Europese en nationale politieke partijen (hierna "politieke partijen" genoemd), Europese en nationale politieke stichtingen (hierna "stichtingen" genoemd), platforms, data-analysebedrijven en voor het electorale proces verantwoordelijke overheidsinstanties. Zij moeten persoonsgegevens (bijvoorbeeld namen en adressen) rechtmatig, eerlijk en op transparante wijze verwerken en mogen dat alleen voor welomschreven doeleinden doen. Zij mogen van die gegevens verder niet gebruikmaken op een wijze die onverenigbaar is met de doeleinden waarvoor de gegevens oorspronkelijk werden verzameld. Verwerking voor journalistieke doeleinden valt in beginsel ook binnen het toepassingsgebied van de algemene verordening gegevensbescherming, zij het dat daarvoor uitzonderingen en afwijkingen krachtens nationaal recht kunnen gelden, gezien het belang van het recht op de vrijheid van meningsuiting en van informatie in een democratische samenleving[10].

Het begrip "persoonsgegevens" is een breed begrip. Persoonsgegevens zijn alle gegevens met betrekking tot een natuurlijk persoon wiens identiteit is of kan worden vastgesteld. Gegevens die in het kader van verkiezingen worden verwerkt, zullen vaak bepaalde speciale categorieën persoonsgegevens omvatten ("gevoelige gegevens"), zoals politieke opvattingen, lidmaatschap van een vakbond, etnische afkomst, seksueel gedrag, etc., waarvoor een meer beschermende regeling geldt[11]. Bovendien kunnen met behulp van gegevensanalyses uit reeksen niet-gevoelige gegevens gevoelige gegevens worden afgeleid (zoals politieke opvattingen, maar ook religieuze overtuigingen of seksuele geaardheid). De verwerking van deze afgeleide gegevens valt ook binnen de werkingssfeer van de algemene verordening gegevensbescherming en moet daarom aan alle voorschriften inzake gegevensbescherming voldoen.

Al met al is op nagenoeg alle gegevensverwerkende handelingen die in het kader van verkiezingen worden verricht, de algemene verordening gegevensbescherming van toepassing.

Omdat de bij het verkiezingsproces betrokken actoren duidelijkheid moet worden geboden en gelet op de eerste bevindingen in de zaak Cambridge Analytica, wordt in de volgende punten aandacht geschonken aan de verplichtingen inzake gegevensbescherming die in het kader van verkiezingen van bijzonder belang blijken te zijn. Zij worden in de bijlage samengevat.

2.1 Verwerkingsverantwoordelijken en verwerkers

Het begrip verantwoordingsplicht van verwerkingsverantwoordelijken en gezamenlijke verwerkingsverantwoordelijken is een centraal kenmerk van de algemene verordening gegevensbescherming. De verwerkingsverantwoordelijke is de organisatie die alleen of samen met anderen beslist waarom en hoe de persoonsgegevens worden verwerkt; de verwerker

[10] Artikel 85, lid 2, van de algemene verordening gegevensbescherming.
[11] Artikel 9, lid 1, van de algemene verordening gegevensbescherming.

verwerkt de persoonsgegevens uitsluitend ten behoeve en in opdracht van de verwerkingsverantwoordelijke (waarbij de relatie tussen beiden in een overeenkomst of andere juridisch bindende handeling is vastgelegd). Verwerkingsverantwoordelijken moeten maatregelen invoeren die passen bij de risico's en van meet af aan zorgen voor gegevensbescherming door ontwerp; zij moeten kunnen aantonen dat zij de algemene verordening gegevensbescherming naleven (verantwoordingsplicht).

De rol van verwerkingsverantwoordelijke of verwerker moet in elk individueel geval worden beoordeeld. In het kader van verkiezingen kan een aantal actoren verwerkingsverantwoordelijke zijn: politieke partijen, individuele kandidaten en politieke stichtingen zijn in de meeste gevallen verwerkingsverantwoordelijken; platforms en data-analysebedrijven kunnen ten aanzien van een bepaalde verwerking (gezamenlijke) verwerkingsverantwoordelijken of verwerkers zijn, al naargelang de mate waarin zij controle over de betrokken verwerking hebben[12]; nationale verkiezingsinstanties zijn verwerkingsverantwoordelijken met betrekking tot de kiesregisters.

Wanneer hun verwerkingsactiviteiten betrekking hebben op het aanbieden van goederen of diensten aan natuurlijke personen in de Unie of op het monitoren van hun gedrag in de Unie, moeten buiten de Unie gevestigde ondernemingen de algemene verordening gegevensbescherming ook naleven. Dit is het geval voor een aantal platforms en data-analysebedrijven.

2.2 Beginselen, rechtmatigheid van verwerking en speciale voorwaarden voor "gevoelige gegevens"

Bij verkiezingen betrokken actoren kunnen persoonsgegevens, met inbegrip van uit openbare bronnen verkregen persoonsgegevens, alleen verwerken in overeenstemming met de beginselen inzake de verwerking van persoonsgegevens en op een beperkt aantal, in de algemene verordening gegevensbescherming duidelijk aangegeven gronden[13]. De meest relevante gronden voor de rechtmatige verwerking in het kader van verkiezingen lijken de toestemming van een individu, de naleving van een wettelijke verplichting uit hoofde van EU- of nationale wetgeving, de uitvoering van een taak in het openbaar belang en het legitiem belang van een van de actoren. Actoren kunnen in het kader van verkiezingen echter alleen de grond van het legitiem belang inroepen wanneer de belangen of grondrechten en fundamentele vrijheden van de betrokken individuen niet prevaleren boven hun eigen belangen.

Bovendien moet de wijze waarop informatie in de eindapparatuur (computer, smartphone enz.) wordt opgeslagen of toegang wordt verkregen tot reeds daarin opgeslagen informatie, in overeenstemming zijn met de vereisten van de e-privacyrichtlijn inzake de bescherming van eindapparatuur, wat inhoudt dat de betrokkene zijn toestemming moet geven.

[12] De recente rechtspraak van het Hof van Justitie van de Europese Unie (Getuigen van Jehova, zaak C-25/17, arrest van 10 juli 2018) maakte duidelijk dat een organisatie die invloed uitoefent op het verzamelen en verwerken van persoonsgegevens in bepaalde omstandigheden als verwerkingsverantwoordelijke kan worden beschouwd .
[13] Artikelen 5 en 6 van de algemene verordening gegevensbescherming.

Wanneer toestemming als rechtsgrond wordt ingeroepen, vereist de algemene verordening gegevensbescherming dat deze door middel van een ondubbelzinnige actieve handeling wordt gegeven en vrij en geïnformeerd is[14].

Overheidsinstanties die bij verkiezingen zijn betrokken, verwerken persoonsgegevens om aan een wettelijke verplichting te voldoen of een overheidstaak uit te voeren. Andere actoren die in het kader van de verkiezingen opereren, kunnen gegevens verwerken op grond van toestemming of een gerechtvaardigd belang[15]. Politieke partijen en stichtingen kunnen ook gegevens verwerken op grond van een algemeen belang indien het nationale recht in die mogelijkheid voorziet[16].

Overheidsinstanties mogen bepaalde informatie over individuen die is opgenomen in kies- of bevolkingsregisters alleen aan politieke partijen meedelen wanneer de wetgeving van de lidstaat dat specifiek toestaat en dan alleen met het oog op reclame in verband met verkiezingen en voor zover voor dat doel noodzakelijk (zoals naam en adres).

Bij verwerking in het kader van verkiezingen zal het vaak om "gevoelige gegevens" gaan. De verwerking van dergelijke gegevens, met inbegrip van afgeleide "gevoelige gegevens", is in het algemeen verboden, tenzij een van de specifieke rechtvaardigingen van toepassing is die in de algemene verordening gegevensbescherming worden vermeld[17]. De verwerking van "gevoelige gegevens" vereist dat aan specifieke, strengere voorwaarden wordt voldaan: de betrokkene moet uitdrukkelijke toestemming hebben gegeven[18] of de betreffende gegevens openbaar hebben gemaakt[19]. Politieke partijen en stichtingen kunnen "gevoelige gegevens" ook verwerken wanneer er sprake is van een zwaarwegend algemeen belang op grond van het recht van de Unie of lidstatelijk recht, en er passende waarborgen worden geboden[20]. De algemene verordening gegevensbescherming bepaalt dat zij "gevoelige gegevens" ook mogen verwerken voor zover de verwerking uitsluitend betrekking heeft op hun leden of voormalige leden of op personen die regelmatig contact met hen onderhouden, doch uitsluitend met het oog op bekendmaking binnen de politieke partij of stichting[21]. Een politieke partij mag zich echter niet op deze specifieke bepaling beroepen voor de verwerking van gegevens van toekomstige leden of kiezers.

Het doel van de gegevensverwerking moet op het moment van de gegevensverzameling welbepaald zijn ("doelbinding")[22]. Gegevens die voor een bepaald doel zijn verzameld,

[14] Artikelen 7 en 4, punt 11, van de algemene verordening gegevensbescherming.
[15] Dit mag dan echter geen ernstige gevolgen voor de rechten en vrijheden van de betrokken individuen hebben.
[16] Zie overweging 56 van de algemene verordening gegevensbescherming, waarin wordt gesteld dat "[a]ls het bij verkiezingsactiviteiten voor de goede werking van de democratie in een lidstaat vereist is dat politieke partijen persoonsgegevens over de politieke opvattingen van personen verzamelen, [...] de verwerking van zulke gegevens op grond van een algemeen belang [kan] worden toegestaan, mits er passende waarborgen worden vastgesteld".
[17] Artikel 9 van de algemene verordening gegevensbescherming.
[18] Artikel 9, lid 2, onder a), van de algemene verordening gegevensbescherming.
[19] Artikel 9, lid 2, onder e), van de algemene verordening gegevensbescherming.
[20] Artikel 9, lid 2, onder g), van de algemene verordening gegevensbescherming.
[21] Artikel 9, lid 2, onder d), van de algemene verordening gegevensbescherming. Zonder de toestemming van de betrokkene mogen politieke partijen of stichtingen gegevens over hun leden of voormalige leden of over personen die regelmatig contact met hen onderhouden, niet met een derde delen.
[22] Artikel 5, lid 1, van de algemene verordening gegevensbescherming.

mogen uitsluitend voor een met dat doel verenigbaar doel verder worden verwerkt; anders dient voor de verwerking voor het nieuwe doel een andere in de algemene verordening gegevensbescherming vermelde rechtsgrond te worden gevonden, zoals toestemming. Met name mogen gegevens die gegevensmakelaars of platforms voor commerciële doeleinden verzamelen, niet in het kader van verkiezingen verder worden verwerkt.

Tenzij politieke partijen en stichtingen due diligence betrachten en controleren of de gegevens rechtmatig zijn verkregen, kunnen zij van een derde verkregen gegevens niet gebruiken.

2.3 Transparantievereisten

De zaak Cambridge Analytica heeft laten zien hoe belangrijk het is om onduidelijkheid tegen te gaan en de betrokken personen naar behoren te informeren. Betrokkenen weten vaak niet wie hun persoonsgegevens verwerkt en voor welke doeleinden dat gebeurt. Overeenkomstig de beginselen van behoorlijke en transparante verwerking moeten betrokkenen op de hoogte worden gesteld van het feit dat er verwerking plaatsvindt en van de doeleinden daarvan[23]. De algemene verordening gegevensbescherming verduidelijkt de verplichtingen van verwerkingsverantwoordelijken in dit opzicht. Zij moeten betrokkenen informeren over de belangrijkste aspecten in verband met de verwerking van hun persoonsgegevens zoals:

- de identiteit van de verwerkingsverantwoordelijke,
- de verwerkingsdoeleinden,
- de ontvangers van de persoonsgegevens,
- de bron van de gegevens, indien deze niet rechtstreeks bij de betrokkene werden verzameld,
- het bestaan van geautomatiseerde besluitvorming en
- alle aanvullende informatie om een behoorlijke en transparante verwerking te waarborgen[24].

De algemene verordening gegevensbescherming vereist bovendien dat informatie wordt verstrekt in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal[25]. Een korte, onduidelijke mededeling over gegevensbescherming die alleen in kleine letters op verkiezingsmateriaal is afgedrukt, zou bijvoorbeeld niet aan de transparantievereisten voldoen.

Volgens de voorlopige bevindingen was onvolledige informatie over het doel waarvoor de gegevens werden verzameld een belangrijke tekortkoming in de zaak Cambridge Analytica, die ook vragen opriep over de geldigheid van de toestemming van de betrokken personen. Alle organisaties die in het kader van verkiezingen gegevens verwerken, moeten ervoor zorgen dat voordat betrokkenen hun toestemming geven of de verwerkingsverantwoordelijke overgaat tot verwerking op een andere grond voor de verwerking, zij volledig begrijpen hoe en met welk doel hun persoonsgegevens zullen worden gebruikt.

[23] Artikel 5, lid 1, onder a), van de algemene verordening gegevensbescherming.
[24] Artikelen 13 en 14 van de algemene verordening gegevensbescherming.
[25] Richtsnoeren van Europees Comité voor gegevensbescherming.

Betrokkenen dient in elke stadium van de verwerking informatie te worden verstrekt en niet alleen bij het verzamelen van gegevens.

Met name wanneer politieke partijen gegevens verwerken die zij uit bronnen van derden hebben verkregen (zoals uit kiesregisters, van gegevensmakelaars, van gegevensanalisten of uit andere bronnen) moeten zij als regel de betrokkenen informeren en uitleggen hoe zij deze gegevens combineren en gebruiken, wil er van eerlijke verwerking sprake zijn[26].

2.4 Profilering, geautomatiseerde besluitvorming en micro-targeting

Profilering is een vorm van geautomatiseerde verwerking die wordt toegepast om bepaalde aspecten, zoals persoonlijke voorkeuren, interesses, economische situatie enz. te analyseren of te voorspellen[27]. Profilering kan worden gebruikt voor micro-targeting van natuurlijke personen, door persoonsgegevens (zoals bijvoorbeeld de zoekgeschiedenis op internet) te analyseren, teneinde vast te stellen wat de bijzondere interesses van een specifiek publiek of individu zijn, zodat zijn handelingen kunnen worden beïnvloed. Micro-targeting kan worden gebruikt om een individu of publiek een gepersonaliseerd bericht te doen toekomen via een online dienst, zoals sociale media.

De zaak Cambridge Analytica heeft de bijzondere problemen laten zien die micro-targetingmethoden op sociale media met zich meebrengen. Organisaties kunnen de via gebruikers van sociale media verzamelde gegevens door middel van datamining gebruiken om kiezersprofielen op te stellen. Hierdoor kunnen dergelijke organisaties wellicht kans zien, vast te stellen welke kiezers gemakkelijker kunnen worden beïnvloed, hetgeen deze organisaties in staat kan stellen invloed op de uitkomst van de verkiezingen uit te oefenen.

Alle algemene beginselen en regels van de algemene verordening gegevensbescherming zijn op een dergelijke gegevensverwerking van toepassing, zoals het rechtmatigheids-, billijkheids- en transparantiebeginsel en het beginsel van doelbinding. Individuen zijn zich er vaak niet van bewust dat er een profiel van hen wordt opgesteld: zij begrijpen niet waarom zij bepaalde reclame ontvangen die zo duidelijk verband houdt met hun laatste zoekopdrachten of waarom zij van verschillende organisaties gepersonaliseerde boodschappen ontvangen. De algemene verordening gegevensbescherming verplicht alle verwerkingsverantwoordelijken, zoals politieke partijen of gegevensanalisten, om wanneer zij dergelijke technieken gebruiken, individuen daarover en over de gevolgen ervan, te informeren[28].

De algemene verordening gegevensbescherming onderkent dat geautomatiseerde besluitvorming, met inbegrip van profilering, ernstige gevolgen kan hebben. De algemene verordening gegevensbescherming bepaalt dat een betrokkene het recht heeft niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft, tenzij deze verwerking onder strikte voorwaarden wordt uitgevoerd, namelijk wanneer de

[26] Artikel 14 van de algemene verordening gegevensbescherming.
[27] Zoals gedefinieerd in artikel 4, lid 4, van de algemene verordening gegevensbescherming.
[28] Artikel 13, lid 2, van de algemene verordening gegevensbescherming.

betrokkene uitdrukkelijk toestemming heeft gegeven of wanneer een Unierechtelijke of lidstaatrechtelijke bepaling die in passende bescherming voorziet, dat toestaat[29].

Micro-targetingpraktijken in het kader van verkiezingen vallen binnen deze categorie wanneer zij betrokken in aanmerkelijke mate treffen. Het Europees Comité voor gegevensbescherming heeft verklaard dat dat het geval is wanneer het besluit het potentieel heeft om de omstandigheden, het gedrag of de keuzen van de betrokken personen in aanmerkelijke mate te treffen of om een langdurig of blijvend effect op de betrokkene te hebben[30]. Het comité was van mening dat gerichte online reclame in bepaalde omstandigheden het potentieel heeft om de betrokkenen in aanmerkelijke mate te treffen, bijvoorbeeld wanneer de reclame een indringend karakter heeft of gebruikmaakt van kennis over de kwetsbaarheden van de betrokkenen. Gelet op het belang van de uitoefening van het democratische stemrecht kunnen gepersonaliseerde boodschappen die bijvoorbeeld als mogelijk gevolg hebben dat personen ervan worden weerhouden om te stemmen of op een bepaalde wijze gaan stemmen, in principe voldoen aan het criterium inzake het in aanmerkelijke mate treffen.

In het kader van verkiezingen moeten verwerkingsverantwoordelijken er daarom voor zorgen dat elke verwerking waarbij van dergelijke technieken gebruik wordt gemaakt, rechtmatig is, d.w.z. strookt met de hierboven vermelde beginselen en strikte voorwaarden van de algemene verordening gegevensbescherming.

2.5 Beveiliging en nauwkeurigheid van persoonsgegevens

Beveiliging is in het kader van verkiezingen van bijzonder belang, gelet op de omvang van de betrokken gegevensbestanden en het feit dat dergelijke bestanden vaak “gevoelige gegevens” bevatten. De algemene verordening gegevensbescherming verplicht zowel verwerkingsverantwoordelijken als verwerkers ertoe passende technische en organisatorische maatregelen te nemen die een beveiligingsniveau waarborgen dat is afgestemd op de risico’s van de verwerking voor de rechten en vrijheden van natuurlijke personen[31].

De algemene verordening gegevensbescherming schrijft voor dat verwerkingsverantwoordelijken een inbreuk in verband met persoonsgegevens zonder onredelijke vertraging en uiterlijk binnen 72 uur moeten melden aan de bevoegde toezichthoudende autoriteit. Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, moet de verwerkingsverantwoordelijke ook de getroffen natuurlijke personen die inbreuk onverwijld meedelen[32].

Politieke partijen en andere bij het verkiezingsproces betrokken actoren moeten er met name op toezien dat de juistheid van persoonsgegevens is gewaarborgd wanneer het om

[29] Artikel 22 van de algemene verordening gegevensbescherming.
[30] Richtsnoeren van het Europees Comité voor gegevensbescherming inzake geautomatiseerde besluitvorming, WP251rev.01, zoals laatstelijk gewijzigd en vastgesteld op 6 februari 2018.
[31] Artikel 32 van de algemene verordening gegevensbescherming.
[32] Artikelen 33 en 34 van de algemene verordening gegevensbescherming en de Richtsnoeren van het Europees Comité voor gegevensbescherming voor de melding van inbreuken in verband met persoonsgegevens.

omvangrijke gegevensreeksen gaat en wanneer gegevens uit verschillende, heterogene bronnen bijeen worden gebracht. Onjuiste gegevens moeten onmiddellijk worden gewist of gerectificeerd en, indien nodig, worden geactualiseerd.

2.6 Gegevensbeschermingseffectbeoordeling

De algemene verordening gegevensbescherming introduceert een nieuw instrument voor de beoordeling van het risico voor aanvang van de verwerking: de gegevensbeschermingseffectbeoordeling. Deze dient steeds plaats te vinden wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen[33]. In het kader van verkiezingen is daarvan sprake wanneer een verwerkingsverantwoordelijke persoonlijke aspecten van een natuurlijk persoon systematisch en uitgebreid beoordeelt (met inbegrip van profilering) en die persoon daardoor wezenlijk wordt getroffen, en wanneer de verwerkingsverantwoordelijke "gevoelige gegevens" grootschalig verwerkt. Nationale verkiezingsautoriteiten die handelen in het kader van de uitoefening van hun openbare taken, hoeven wellicht geen gegevensbeschermingseffectbeoordeling uit te voeren wanneer deze reeds heeft plaatsgevonden in het kader van de vaststelling van de wetgeving.

De door de diverse actoren in het kader van verkiezingen uit te voeren effectbeoordelingen dienen de nodige elementen te bevatten op grond waarvan de risico's kunnen worden aangepakt waarmee een dergelijke verwerking gepaard gaat, met name de rechtmatigheid van de verwerking, onder andere met betrekking tot van derden verkregen gegevensreeksen, en de transparantievereisten.

3. Rechten van natuurlijke personen

De algemene verordening gegevensbescherming geeft natuurlijke personen aanvullende en sterkere rechten die met name in het kader van verkiezingen van belang zijn:

- het recht op toegang tot hun persoonsgegevens;
- het recht om te verzoeken om het wissen van hun persoonsgegevens wanneer de verwerking op toestemming is gebaseerd en die toestemming wordt ingetrokken, wanneer de gegevens niet langer noodzakelijk zijn of wanneer de verwerking onrechtmatig is, alsmede
- het recht op rectificatie van onjuiste of onvolledige persoonsgegevens.

Natuurlijke personen hebben ook het recht bezwaar te maken tegen verwerking (bijvoorbeeld van gegevens die zijn opgenomen in aan politieke partijen doorgegeven kiesregisters) wanneer de verwerking van hun gegevens is gebaseerd op een "gerechtvaardigd belang" of "algemeen belang".

[33] Artikelen 35 en 36 van de algemene verordening gegevensbescherming en de Richtsnoeren van het Europees Comité voor gegevensbescherming inzake gegevensbeschermingseffectbeoordelingen.

Natuurlijke personen hebben het recht niet te worden onderworpen aan uitsluitend op geautomatiseerde verwerking gebaseerde besluiten. In dergelijke gevallen kan de betreffende persoon om de tussenkomst van een natuurlijk persoon verzoeken en heeft hij het recht om zijn standpunt kenbaar te maken en het besluit aan te vechten.

Teneinde natuurlijke personen in staat te stellen deze rechten uit te oefenen, dienen alle betrokken actoren de nodige instrumenten en kaders te bieden. De algemene verordening gegevensbescherming voorziet in de mogelijkheid een gedragscode op te stellen die wordt goedgekeurd door een gegevensbeschermingsautoriteit en beschrijft hoe de verordening op specifieke terreinen, zoals bij verkiezingen, dient te worden toegepast.

De algemene verordening gegevensbescherming verleent natuurlijke personen ook het recht om een klacht in te dienen bij een toezichthoudende autoriteit en het recht op een voorziening in rechte. Zij geeft natuurlijke personen ook het recht om een niet-gouvernementele organisatie de opdracht te geven om namens hen een klacht in te dienen[34]. In bepaalde lidstaten staat nationale wetgeving het toe dat een niet-gouvernementele organisatie een klacht indient zonder daartoe een opdracht van een natuurlijke persoon te hebben gekregen. Dit is met name van belang in het kader van verkiezingen, gezien het grote aantal personen dat dit mogelijk aangaat.

[34] Artikel 80, lid 1, van de algemene verordening gegevensbescherming.

Belangrijke kwesties op het gebied van gegevensbescherming die in het kader van het verkiezingsproces relevant zijn[35]

Politieke partijen en politieke stichtingen	Politieke partijen en stichtingen zijn verwerkingsverantwoordelijken
	• Voldoen aan het beginsel van doelbinding, en verwerken gegevens alleen voor verenigbare doeleinden (bijvoorbeeld wanneer gegevens met platforms worden gedeeld) • Kiezen de passende rechtsgrondslag voor verwerking (ook bij afgeleide gegevens): toestemming, gerechtvaardigd belang, taak van algemeen belang (indien bij wet voorzien), specifieke voorwaarden voor "gevoelige gegevens" (bijvoorbeeld: politieke opvatting) • Voeren een gegevensbeschermingseffectbeoordeling uit • Informeren betrokkenen over elk doeleinde van de verwerking (transparantievereisten), hetzij bij het rechtstreeks verzamelen van gegevens, hetzij bij het verkrijgen van gegevens van derden • Zorgen voor de juistheid van gegevens, met name in geval van uit verschillende bronnen afkomstige gegevens en van afgeleide gegevens • Controleren of gegevens die van derden zijn ontvangen, rechtmatig zijn verkregen en voor welke doeleinden zij zijn verkregen (bijvoorbeeld: of de betrokken personen geïnformeerd toestemming voor een bepaald doel hebben gegeven) • Houden rekening met de specifieke risico's van profilering en stellen passende waarborgen vast • Voldoen aan specifieke voorwaarden bij het gebruik van geautomatiseerde besluitvorming (verkrijgen bijvoorbeeld expliciete toestemming en zorgen voor passende waarborgen) • Stellen duidelijk vast wie toegang tot de gegevens heeft • Zorgen voor de beveiliging van verwerking door middel van technische en organisatorische maatregelen; melden inbreuken in verband met persoonsgegevens • Verduidelijken verplichtingen in overeenkomsten die zijn gesloten met gegevensverwerkers, zoals data-analysebedrijven, of in andere juridisch bindende handelingen die met die partijen zijn overeengekomen

[35] De informatie hierboven is geenszins volledig. Zij strekt ertoe een aantal belangrijke verplichtingen in het kader van de algemene verordening gegevensbescherming onder de aandacht te brengen die in het kader van het verkiezingsproces van belang zijn. Zij passen bij een scenario waarin politieke partijen zelf gegevens verzamelen (uit openbare bronnen, op sociale media, rechtstreeks van kiezers, enz.) en gebruikmaken van de diensten van gegevensmakelaars of data-analysebedrijven met het doel zich via de sociale media op kiezers te richten. Ook platforms kunnen voor de hierboven genoemde actoren een bron van gegevens zijn. Andere wetgeving kan eveneens relevant zijn, zoals de regels inzake de verzending van ongewenste communicatie en de bescherming van eindapparatuur in de e-privacyrichtlijn.

<table>
<tr><td></td><td colspan="2">• Wissen gegevens wanneer die niet langer nodig zijn voor het oorspronkelijke doel waarvoor zij werden verzameld</td></tr>
<tr><td rowspan="3">Gegevensmakelaars en data-analysebedrijven</td><td colspan="2">Gegevensmakelaars en data-analysebedrijven zijn (gezamenlijke) verwerkingsverantwoordelijken of verwerkers, afhankelijk van de mate waarin zij controle hebben over de verwerking.</td></tr>
<tr><td>Als verwerkingsverantwoordelijke</td><td>Als verwerker</td></tr>
<tr><td>• Voldoen aan het beginsel van doelbinding en verwerken gegevens alleen verder voor verenigbare doeleinden (met name wanneer gegevens met derden worden gedeeld)
• Kiezen de passende rechtsgrondslag voor verwerking: toestemming, gerechtvaardigd belang. Bij “gevoelige gegevens” is verwerking alleen mogelijk in geval van uitdrukkelijke toestemming of als het gaat om persoonsgegevens die kennelijk openbaar zijn gemaakt
• Voeren een gegevensbeschermings-effectbeoordeling uit
• Informeren natuurlijke personen over elk doeleinde van de verwerking (transparantievereisten) – met name wanneer om toestemming wordt gevraagd omdat de gegevens doorgaans aan een derde zullen worden verkocht
• Voldoen aan specifieke voorwaarden bij het gebruik van geautomatiseerde besluitvorming (verkrijgen bijvoorbeeld expliciete toestemming en zorgen voor passende waarborgen)
• Besteden bijzondere aandacht aan de rechtmatigheid van de verwerking en aan de</td><td>• Voldoen aan verplichtingen uit hoofde van de met de verwerker gesloten overeenkomst of de met de verwerker overeengekomen andere juridisch bindende handeling
• Zorgen voor de beveiliging van verwerking door middel van technische en organisatorische maatregelen
• Ondersteunen de ververwerkingsverantwoordelijke bij de gegevensbeschermings-effectbeoordeling of bij de uitoefening van de rechten van de betrokkene of bij het onverwijld meedelen aan de verwerkingsverantwoordelijke van een inbreuk in verband met persoonsgegevens zodra zij daarvan kennis krijgen.</td></tr>
</table>

	juistheid wanneer verschillende reeksen gegevens worden gecombineerd • Zorgen voor de beveiliging van verwerking door middel van technische en organisatorische maatregelen; melden inbreuken in verband met persoonsgegevens	
	Platforms zijn gewoonlijk verwerkingsverantwoordelijke met betrekking tot de verwerking die op het platform plaatsvindt en eventueel mede-verwerkingsverantwoordelijke met andere organisaties	
Socialemediaplatforms en online advertentienetwerken	• Kiezen de passende rechtsgrondslag voor verwerking: overeenkomst met natuurlijke personen, toestemming, gerechtvaardigd belang. Bij "gevoelige gegevens" is verwerking alleen mogelijk in geval van uitdrukkelijke toestemming of als het gaat om persoonsgegevens die kennelijk openbaar zijn gemaakt • Gebruiken alleen gegevens die noodzakelijk zijn voor het vastgestelde doel • Voeren een gegevensbeschermingseffectbeoordeling uit • Waarborgen rechtmatigheid wanneer zij gegevens van leden met derden delen • Voldoen aan transparantievereisten, met name met betrekking tot de voorwaarden, wanneer gegevens vervolgens met een derde worden gedeeld, enz. • Voldoen aan specifieke voorwaarden bij het gebruik van geautomatiseerde besluitvorming (verkrijgen bijvoorbeeld uitdrukkelijke toestemming en zorgen voor passende waarborgen) • Zorgen voor de beveiliging van verwerking door middel van technische en organisatorische maatregelen; melden inbreuken in verband met persoonsgegevens • Zorgen voor controles en kaders zodat natuurlijke personen hun rechten daadwerkelijk kunnen uitoefenen, met inbegrip van het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit	
	Nationale verkiezingsautoriteiten zijn verwerkingsverantwoordelijken	
Nationale verkiezingsautoriteiten	• Rechtsgrondslag voor verwerking: wettelijke verplichting of op recht gebaseerde taak van algemeen belang • Voeren een gegevensbeschermingseffectbeoordeling uit als het effect niet reeds beoordeeld is in het kader van de wetgeving	