Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 61/2024 van 27 juni 2024

Betreft: Ontwerp van ministerieel besluit tot vaststelling van de werkwijze voor de gecentraliseerde elektronische kiezerslijst (CO-A-2024-181)

Kernwoorden: Elektronisch platform - Kiezerslijst - Verwerkingsverantwoordelijke - Gegevensencryptie - Gebruikers- en toegangsbeheer - Maatregelen voor het nemen van vingerafdrukken

Vertaling[1]

Inleiding:

Dit is een ontwerp van ministerieel besluit tot oprichting van een platform (Adele genaamd) om de kiezerslijsten elektronisch en centraal te beheren. Het doel van dit platform is om de voorbereiding en het verloop van lokale verkiezingen te vereenvoudigen en meer zekerheid te bieden wat betreft de kiezerslijsten. In de praktijk beheert Adele het kiesregister, de aan- of afwezigheid van stembureauleden, hun vergoedingsformulieren en de registers van mensen die bij volmacht hebben gestemd.

Bij het onderzoek van dit ontwerp maakt de Autoriteit voornamelijk opmerkingen over :
- verduidelijking van de doeleinden van de verwerking ;
- de identificatie van degenen die verantwoordelijk zijn voor het beheer van het platform ;
- het gebruikers- en toegangsbeheer tot het platform ;
- de registratie van de afgifte van kopieën van kieslijsten door gemeenten aan kandidaten en politieke partijen ;
- het aannemen van maatregelen inzake *fingerprinting.*

De Autoriteit maakt ook enkele algemene opmerkingen en vestigt de aandacht van de auteur van het ontwerp op de technische en organisatorische maatregelen die moeten worden genomen bij het opzetten van dit platform.

Voor een volledige lijst van opmerkingen, zie de conclusies (dispositief, blz. 9 en 10).

[1] Voor de oorspronkelijke versie van de tekst, die collegiaal werd gevalideerd, cf. de Franse versie van de tekst, die beschikbaar is in de FR-versie van de rubriek "adviezen" van de website van de Autoriteit.

De Autorisatie- en Adviesdienst van de Gegevensbescherrmingsautoriteit (hierna 'de Autoriteit'), aanwezig: de dames Cédrine Morlière, Nathalie Ragheno en Griet Verhenneman en de heren Yves-Alexandre de Montjoye, Bart Preneel en Gert Vermeulen;

Gelet op de wet van 3 december *2017 tot oprichting van de Gegevensbeschermingsautoriteit, met* name de artikelen 23 en 26 (hierna "WOG");

Gelet op artikel 43 van het reglement van interne orde van de Autoriteit, volgens hetwelk beslissingen van de Autorisatie- en adviesdienst bij meerderheid van stemmen worden aangenomen ;

Gelet op 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* (hierna "AVG");

Gelet op de wet van 30 *juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op de adviesaanvraag van de heer Bernard Clerfayt, minister van het Brussels Hoofdstedelijk Gewest ((hierna "de minister' of 'de aanvrager'), ontvangen op 16 mei 2024;

Brengt op 27 juni 2024 het volgende advies uit:

I. Onderwerp en context van de adviesaanvraag

1. De minister van het Brussels Hoofdstedelijk Gewest vraagt de Autoriteit om advies over een ontwerp van ministerieel besluit tot vaststelling van de werkwijze voor de gecentraliseerde elektronische kiezerslijst (hierna "**het ontwerp**" of "**het ministerieel besluit**") »).

2. Artikel 14, 3de lid van het nieuw Brussels gemeentelijk kieswetboek (hierna "**het Brussels wetboek**"), bepaalt dat "*de Regering kan beslissen de kiezerslijst elektronisch en gecentraliseerd ter beschikking te stellen van de gemeente".* De Autoriteit heeft in haar advies van 27 april 2023 al advies uitgebracht over de ordonnantie houdende het Nieuw Brussels Gemeentelijk Kieswetboek[2].

3. In uitvoering van deze bepaling heeft de Brusselse Hoofdstedelijke Regering het besluit van 25 april 2024[3] aangenomen, dat bepaalt dat de kiezerslijsten elektronisch en centraal ter beschikking van de gemeente worden gesteld via een gewestelijk elektronisch platform. Artikel 5 van dit besluit belast de minister bevoegd voor plaatselijke besturen met de uitvoering van dit besluit en de bepaling van de specifieke kenmerken van dit platform, evenals de werkwijze ervan.

4. Het ontwerp dat ter advies is voorgelegd, zet dit platform genaamd **Adele** op. Het ministerieel besluit beschrijft de **details van het platform en de manier waarop het zal werken**. Het ontwerp specificeert:
    - de gegevens die worden opgenomen in het platform ;
    - de rol en verantwoordelijkheid van de verschillende actoren die betrokken zijn bij de verwerking ;
    - actoren met toegang tot het platform ;
    - bewaartermijnen van gegevens op dit platform ;
    - technische en organisatorische maatregelen om de veiligheid van dit platform te garanderen.

5. Volgens de informatie op het adviesaanvraagformulier heeft het opzetten van dit platform een aantal voordelen. Overschakelen op elektronische lijsten zou de werking van de stembureaus vlotter laten verlopen en tijd besparen voor het personeel van de stembureaus. Het elimineren van de behoefte aan fysieke documenten zou het voorbereidende werk voor lokale autoriteiten aanzienlijk moeten vereenvoudigen, de operationele kosten verlagen en bijdragen aan een beter milieu. Bovendien zou deze elektronische versie van de kiezerslijsten veiliger zijn dan de papieren versies en extra controles mogelijk maken.

II. <u>Onderzoek van de adviesaanvraag</u>

[2] Zie in dit verband advies nr 84/2023 van 27 april 2023.
[3] Besluit van de Brusselse Hoofdstedelijke Regering betreffende de elektronische en gecentraliseerde kiezerslijst, B.S., 7 mei 2024.

1) Evenredigheid en minimale gegevensverwerking

6. Strikt genomen brengt het ontwerp geen nieuwe verwerking van persoonsgegevens met zich mee, aangezien het verkiezingsproces al lang wordt geregeld door de Brusselse kieswet.

7. Bij het lezen van het ontwerp wordt duidelijk dat **het niet alleen artikel 14 van het Brussels kieswetboek implementeert.** Het ministerieel besluit geeft bijvoorbeeld ook uitvoering aan artikel 16 van het Kieswetboek, dat toegang verleent tot de elektronische en gecentraliseerde kiezerslijsten aan de voorzitters van de Franstalige en Nederlandstalige rechtbanken van eerste aanleg in Brussel en aan de vrederechters. Het ontwerp moet worden **gewijzigd om een artikel toe te voegen waarin duidelijk wordt aangegeven welke bepalingen van de het Brussels kieswetboek worden toegepast en waarin de doelstellingen van de oprichting** van dit platform **worden verduidelijkt**.

8. De verwerkte persoonsgegevens geven geen aanleiding tot bijzondere opmerkingen van de Autoriteit. Artikel 2 van het ontwerp bepaalt dat de lijst van kiezers in de centrale gegevensbank de achternaam, de voornamen, het Rijksregisternummer en de hoofdverblijfplaats bevat. Deze gegevens **komen overeen** met de gegevens op de kiezerslijsten overeenkomstig artikel 11 van het Brusselse kieswetboek.

2) Verwerkingsverantwoordelijken

9. Het is **niet de rol van het ontwerp** om de kwalificaties van verwerkingsverantwoordelijken in het Brussels kieswetboek te wijzigen, bijvoorbeeld met betrekking tot het bijhouden van kiezerslijsten. Het is echter wel **aan het ontwerp om duidelijk aan te geven wie verantwoordelijk is voor het beheer** van het platform.

10. Hier herinnert de Autoriteit[4] eraan het in de reglementering vaststellen van de verwerkingsverantwoordelijke bijdraagt tot de **voorspelbaarheid van de norm** en de doeltreffendheid **van de in de AVG vastgelegde rechten** van de betrokkenen. De aanduiding van een verwerkingsverantwoordelijke in de regelgeving dient met andere woorden **te stroken** met de rol die deze actor in **de praktijk opneemt**[5]. Met andere woorden, het is nodig om voor

[4] Zie ook in dit verband advies nr. 06/2024, overweging 48

[5] Het Europees Comité voor gegevensbescherming dringt erop aan dat het concept van verwerkingsverantwoordelijke vanuit een feitelijk perspectief wordt benaderd. Zie : Europees Comité voor gegevensbescherming, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (version 2.0), 7 July 2021, gepubliceerd op https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

elke verwerking van persoonsgegevens na te gaan wie in feite het doel[6] van de verwerking nastreeft en controle heeft over de verwerking. Het tegenovergestelde beweren zou niet alleen ingaan tegen de letter van de AVG maar zou eveneens de doelstelling ervan in gevaar kunnen brengen om een coherent en hoog beveiligingsniveau te verzekeren voor natuurlijke personen.

11. In dit geval lijkt Brussel Plaatselijke Besturen van de Brusselse Gewestelijke Overheidsdienst de bevoegde autoriteit te zijn voor het beheer van het platform. Krachtens artikel 11 van het Brussels Kieswetboek zijn de Federale Overheidsdienst Binnenlandse Zaken en het College van Burgemeester en Schepenen verantwoordelijk voor de inhoud van dit platform. De Autoriteit herinnert eraan dat in het geval er een **gezamenlijke verantwoordelijkheid** bestaat, dit zich nniet noodzakelijkerwijs vertaalt in een gelijkwaardige verantwoordelijkheid [… en] deze operatoren kunnen juist in verschillende stadia en in verschillende mate bij deze verwerking betrokken zijn, zodat het niveau van verantwoordelijkheid van elk van hen moet worden beoordeeld in het licht van alle relevante omstandigheden van het geval[7]. Het is in het kader van zijn verantwoordelijkheden, zijn bevoegdheden en zijn mogelijkheden dat de medeverantwoordelijke zal waken over de conformiteit van zijn activiteit met de regels inzake gegevensbescherming[8].

12. De Autoriteit merkt op dat de auteur van het ontwerp in artikel 20 van het ontwerp de uit het overheidscontract voortvloeiende organisatie heeft aangewezen die verantwoordelijk is voor het technisch beheer van Adele. De Autoriteit adviseert om **in de bepalingen van de tekst de verwerker niet te specificeren**, omdat de verwerker vanzelfsprekend moet kunnen veranderen als de verwerkingsverantwoordelijke van mening is dat er een kwaliteitsprobleem is bij de uitvoering van de taak van de verwerker.

3) Beveiligingsmaatregelen

13. De artikelen 5.1.f), 24.1 en 32 van de AVG verplichten de verwerkingsverantwoordelijke om gepaste technische en organisatorische maatregelen te treffen die nodig zijn voor de bescherming van de persoonsgegevens. Deze maatregelen moeten een passend beveiligingsniveau waarborgen, rekening houdend, enerzijds, met de stand van de techniek ter zake en de kosten voor het toepassen van die maatregelen en, anderzijds, met de aard van de

[6] In overeenstemming met het legaliteitsbeginsel bepaalt de wetgever het doel van gegevensverwerking in de overheidssector. Het identificeren of classificeren van verwerkingsverantwoordelijken in de publieke sector betekent over het algemeen verwijzen naar de organisatie die de publieke taak uitvoert die verband houdt met het doel van de gegevensverwerking in kwestie.
[7] HvJ-EU, (Gr. Kam. , 5 juni 2018 (UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIM v/ WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN GMBH), zaak C-210/16, punt 43. Lees eveneens G29, advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", 16 februari 2010, p. 20.
[8] HvJ-EU, (Grote kamer), Kam.), 13 mei 2014 (Google Spain SL, Google Inc. v/ AEPD), zaak C-132/12, punt 38.

te beveiligen gegevens en de potentiële risico's. Deze en andere maatregelen dienen bovendien van in de ontwerpfase, alsook via standaardinstellingen, geïmplementeerd te worden

14. De platformbeheerder heeft veel aandacht besteed aan de technische en organisatorische maatregelen die het platform moeten omkaderen. De opmerkingen van de Autoriteit over deze maatregelen zijn dan ook voornamelijk van algemene aard.

a) Encryptie van gegevens en gegevensdragers

15. Uit de aanvullende informatie blijkt dat de gegevens op het Adele-platform veilig worden opgeslagen ; de **gegevens en gegevensdragers zijn versleuteld**. De Autoriteit herhaalt[9] dat wanneer encryptie wordt gebruikt, er in ieder geval **duidelijke garanties moeten zijn voor een passend codebeheer**, aangezien de veiligheid van gegevens uiteindelijk afhangt van de vertrouwelijkheid van de encryptiesleutels.

b) Toegangsbeheer platform

16. Artikel 12 van het ontwerp bepaalt dat toegang tot Adele alleen is toegestaan voor :
"- Het bedrijf Civadis (onderdeel van NRB) om de correcte functionering van het systeem Adele te verzekeren;
- De personen aangeduid door Brussel Plaatselijke Besturen (onderdeel van de Gewestelijke Overheidsdienst Brussel) om de correcte functionering van het systeem Adele en het goede verloop van de gemeenteraadsverkiezingen te verzekeren;
- De gemeenten voor de gegevens betreffende de inwoners van hun gemeente, en de door de gemeente aangestelde afgevaardigden;
- De voorzitters van de hoofdbureaus voor de gegevens betreffende de inwoners van hun gemeente, en de door de voorzitters van de hoofdbureaus aangestelde afgevaardigden;
- De voorzitters van de stembureaus voor de gegevens betreffende de kiezers van hun gemeente;
- De bijzitter in een stembureau verantwoordelijk voor de aanstipping van de kiezers op de kiezerslijst, onder dezelfde voorwaarden als de voorzitter van het stembureau;
- Het college van deskundigen aangeduid overeenkomstig art. 4, § 1 van het Nieuw Brussels Gemeentelijk Kieswetboek".

17. De Autoriteit herhaalt[10] dat het essentieel is **dat alleen bevoegde personen of organisaties toegang hebben tot het platform** en dat zij alleen de informatie kunnen raadplegen waartoe zij gemachtigd zijn. Een **gebruikers- en toegangsbeheersysteem** zorgt ervoor dat alleen

[9] Zie ook in dit verband advies nr. 10/2016 van 24 februari 2016, overweging 90.
[10] Zie ook in dit verband advies nr. 160/2023 van 11 december 2023, overwegingen 21 tot 24.

de categorieën betrokkenen die positief zijn geïdentificeerd en van wie de **identiteit** is geverifieerd **door middel van een authenticatieproces**, toegang hebben tot de delen van het platform waartoe zij op grond van hun functie gerechtigd zijn.

18. Uit aanvullende informatie blijkt dat medewerkers van de bureaus zich op de verkiezingsdag kunnen authenticeren en toegang krijgen tot het platform met behulp van een gebruikersnaam en wachtwoord. De gebruikersnaam is specifiek voor een bepaald bureau en het wachtwoord is een lange tekst, inclusief alfanumerieke tekens en symbolen volgens de best practice voor wachtwoorden (voldoet aan de NIST-wachtwoordvereisten[11]).

19. Hoewel het wachtwoord aan bepaalde eisen voldoet, is de Autoriteit van mening dat het gebruik van een identificatiecode en een wachtwoord **onvoldoende bescherming biedt**[12]. De Autoriteit beveelt de auteur van het ontwerp aan om expliciet in het ontwerp op te nemen dat de verbinding met het platform afhankelijk is van elektronische identificatieschema's die de betrouwbaarheid garanderen van de identiteit waarop de gebruiker[13] aanspraak maakt of beweert te maken, met een hoog garantieniveau in de zin van artikel 8.2 c) van de eIDAS-verordening[14]. In de overheidssector beveelt de Autoriteit het gebruik van een **sterke authenticatiemethode aan, zoals de authenticatiemodule van de identiteitskaart of een gelijkwaardig systeem**[15].

20. Voor het overige, verwijst de Autoriteit naar haar aanbeveling met betrekking tot het toegangs- en gebruikersbeheer in de overheidssector[16].

c) Logging en fingerprinting

21. Artikel 21 bepaalt "elke toevoeging*, verwijdering of andere wijziging van persoonsgegevens is traceerbaar in Adele".* De Autoriteit staat positief tegenover deze bepaling. Met een dergelijke logging kan worden nagegaan wie wat, waarom en wanneer op het platform heeft

[11] Voor meer informatie over dit onderwerp, zie de NIST-richtlijnen en best practices over wachtwoorden, beschikbaar op https://pages.nist.gov/800-63-3/sp800-63b.html

[12] Zie ook in dit verband advies nr. 186/2019 van 29 december 2019, overweging 24.

[13] Kandidaten moeten er goed op letten dat ze de medewerkers van de verschillende stembureaus er in de uitnodiging op wijzen dat ze hun identiteitskaart en pincode moeten meenemen.

[14] Verordening (EU) nr. 910/2014 van 23 juli 2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.

[15] Het gebruik van eID of Itsme kan worden beschouwd als een authenticatiemiddel. De Autoriteit wijst erop dat België de eID en Itsme heeft aangemeld als elektronische identificatiesystemen die een hoog garantieniveau bieden in de zin van artikel 8,2, c), van de eIDAS-verordening.

[16] Zie Aanbeveling nr. 01/2008 van 24 september 2008 met betrekking tot het gebruikers- en toegangsbeheer in de overheidssector, beschikbaar op https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-01-2008.pdf

geraadpleegd, zodat elke raadpleging van de gegevens voor een niet-intern doel of op persoonlijke basis kan worden opgespoord of bestraft[17].

22. Artikel 17 van het ontwerp bepaalt *"de gemeente kan een afschrift van de kiezerslijst voor haar gemeente uit Adele geven aan de lijstindieners en kandidaten overeenkomstig artikel 13 van het Nieuw Brussels Gemeentelijk Kieswetboek"*. Om veiligheidsredenen is het essentieel dat elke levering van electorale kopieën ook wordt gelogd. Als het ontwerp niet voorziet in rechtstreekse toegang tot het platform voor politieke partijen en kandidaten (toegang die dus zou worden geregistreerd), moet het een **duidelijke verplichting voor gemeenten bevatten om de afgifte van kopieën van de kiezerslijst aan politieke partijen of kandidaten te registreren**.

23. In een eerder advies[18] heeft de Autoriteit aanbevolen aanvullende garanties in te voeren voor de afgifte van kiezerslijsten aan politieke partijen en kandidaten. De Autoriteit herhaalt deze aanbeveling ; het ontwerp moet **voorzien in de vaststelling van maatregelen voor *fingerprinting* bij de meegedeelde bestanden**. Met een geautomatiseerd systeem zoals het huidige is dit type maatregel uit de aard der zaak vereist als **basisveiligheidsmaatregel voor de mededeling** van kiezerslijsten. *Ter herinnering, fingerprinting* is een identificatietechnologie gebaseerd op het invoegen van een digitaal watermerk, afhankelijk van de naam van de ontvanger in een afbeelding, bestand of video, om hun herkomst of oorsprong te traceren en om de bron van eventuele kopieën te kunnen opsporen. Op deze manier kan gebruik dat niet in overeenstemming is met het wettelijke kader gemakkelijk worden opgespoord en bestraft.

24. De Autoriteit benadrukt dat de toegepaste fingerprinting afhankelijk moet zijn van de persoonlijke account van elke ontvanger (natuurlijke persoon), en dat het doorgegeven bestand ook moet worden voorzien van een tijdstempel (zowel wat betreft de datum als het tijdstip van beschikbaarheid van het bestand met de kiezerslijst). De fingerprintingmethode moet ook voldoen aan de huidige stand van de techniek en dus aan de eisen van **robuustheid** (niet gemakkelijk te verwijderen), **onzichtbaarheid** en **geheimhouding** (de gebruikte fingerprintingtechniek moet geheim blijven).

4) Bewaartermijn

[17] Zie in dit verband de aanbeveling uit eigen beweging van de Autoriteit 06/2012 van 2 mei 2012, *m.b.t. het verkrijgen van informatie uit de bevolkingsregisters in toepassing van het koninklijk besluit van 16 juli 1992 betreffende het verkrijgen van informatie uit de bevolkingsregisters en uit het vreemdelingenregister,* beschikbaar op https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-06-2012.pdf

[18] Zie ook in dit verband advies nr. 160/2023, overweging 26.

25. Artikel 22 van het ontwerp bepaalt dat de gegevens in de gecentraliseerde elektronische kiezerslijst en de gegevens op usb-datadragers worden gewist zodra de gemeenteraadsverkiezingen definitief zijn gevalideerd. Gegevens die naar de rechtbanken en het openbaar ministerie zijn gestuurd, worden ook verwijderd wanneer ze niet langer nodig zijn voor de doeleinden waarvoor ze beschikbaar zijn gesteld.

26. Deze bewaarperiode, beschreven in functionele termen, is **passend**. Voor alle praktische doeleinden verwijst de Autoriteit naar haar aanbeveling over technieken voor het opschonen van gegevens en de vernietiging van gegevensdragers[19].

OM DIE REDENEN,

is de Autoriteit van oordeel dat de gegevensverwerkingen reeds vrij goed worden omkaderd in het ontwerp. Desondanks vindt ze dat het gepast is om :

- het ontwerp te wijzigen met de toevoeging van een artikel waarin duidelijk wordt aangegeven welke bepalingen van het Brussels kieswetwetboek worden toegepast en waarin de doelstellingen van de oprichting van dit platform worden verduidelijkt (overw. 7) ;
- duidelijk aan te geven wie verantwoordelijk is voor het beheer van het platform (overw. 9 tot 11) ;
- te voorzien in een gebruikers- en toegangsbeheer voor het platform met behulp van een sterk authenticatiemiddel (overw. 17 en 18);
- bij gebrek aan rechtstreekse toegang tot het platform voor politieke partijen en kandidaten, te voorzien in een duidelijke verplichting voor gemeenten om de uitgifte van verkiezingskopieën aan politieke partijen en kandidaten te registreren (overw. 22) ;

[19] Zie voor meer informatie de aanbeveling van 11 december 2020 inzake technieken gegevens op te schonen en gegevensdragers te vernietigen, beschikbaar op https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-03-2020-van-11-december-2020.pdf

- te voorzien in de vaststelling van maatregelen voor fingerprinting, die moeten voldoen aan de vereisten van robuustheid, onzichtbaarheid en geheimhouding (overw. 23 en 24).

De Autoriteit vestigt de aandacht van de aanvrager op de volgende elementen:

- Naleving van artikel 32 van de AVG en de verplichting van de verwerkingsverantwoordelijke om de passende technische en organisatorische maatregelen te treffen die nodig zijn om persoonsgegevens te beschermen (overw. 13 t/m 23).

Voor de Autorisatie- en Adviesdienst

(get.) Cédrine Morlière, directeur