



Wij werken samen met **PRIVACYCOMPANY** 

Informatiebeveiliging binnen digitale stembureauhulpmiddelen

In opdracht van:

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)

Openbaar

Documenteigenschappen

Klant: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)

Datum: 17-12-2025

Versie: 1.0

Classificatie: Openbaar

Offertenummer O-1337

Projectnummer: P-1337

Startdatum: 14-08-2025

Einddatum: 17-12-2025

Auteurs: J. Klerks-Meijboom (Security consultant PuraSec)
J. Christians (Privacy consultant Privacy Company)

Reviewers: A. Roosendaal (Directeur Privacy Company)
P. Knobbe (Operational manager PuraSec)

Versiebeheer

Versiebeheer			
Versie	Datum	Auteur(s)	Beschrijving
0.1	03-12-2025	J. Meijboom en J. Christians	Initiële versie
0.2	04-12-2025	A. Roosendaal	Interne kwaliteitscontrole
0.3	04-12-2025	J. Meijboom en J. Christians	Verwerken feedback
0.4	11-12-2025	J. Meijboom en J. Christians	Conceptversie
0.5	15-12-2025	J. Meijboom en J. Christians	Verwerken feedback BZK
0.9	16-12-2025	J. Meijboom en J. Christians	Oplevering BZK inhoudelijk definitief
0.9	17-12-2025	P. Knobbe	Redigeren
1.0	17-12-2025	J. Meijboom	Definitief

Dit document is geclassificeerd als openbaar. De informatie die in dit document en eventueel bijbehorende bijlagen is gepubliceerd, is bedoeld voor alle geïnteresseerden.

Disclaimer

Het rapport is opgesteld door PuraSec B.V. (m.m.v. Privacy Company B.V.) in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Bij opstellen van deze rapportage is uiterste zorgvuldigheid betracht. Niettemin dient te worden onderkend dat er een risico bestaat dat niet alle mogelijke tekortkomingen of risico's volledig zijn geïdentificeerd. PuraSec B.V. aanvaardt geen aansprakelijkheid voor schade die direct of indirect voortvloeit uit het niet onderkennen van bepaalde risico's of tekortkomingen.

Inhoud

Hoofdstuk 1: Inleiding	5
1.1 Aanleiding.....	5
1.2 Scope	5
1.3 Aanpak	6
1.4 Leeswijzer	6
Hoofdstuk 2: Stemhulpmiddelen	7
2.1 Toelichting stemapps	7
2.2 Overzicht van functionaliteiten en gegevensverwerkingen	7
2.3 Relevante (wettelijke) kaders security en privacy	9
Hoofdstuk 3: Bevindingen en aanbevelingen	10
3.1 Bevindingen en aanbevelingen	10
3.2 Conclusie.....	12

Hoofdstuk 1: Inleiding

1.1 Aanleiding

Gemeenten gebruiken steeds vaker digitale stemhulpmiddelen bij het stemproces. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft PuraSec (m.m.v. Privacy Company) gevraagd om aanbevelingen te beschrijven zodat de stemapps zorgvuldig worden gebruikt en eventuele risico's, die door het papieren proces niet zouden ontstaan, voorkomen worden.

1.2 Scope

De scope is in afstemming met BZK vastgesteld en opgesplitst in een informatiebeveiligingsdeel en privacy deel.

Informatiebeveiliging

Risico's identificeren die voortkomen uit het gebruik van webapplicaties in het stemproces en aanbevelingen opstellen om deze risico's te beheersen.

- Analyse van het bedreigingslandschap rondom stemhulpmiddelen, waaronder toegangsbeveiliging, integriteit van functionaliteit, manipulatie-risico's en ketenafhankelijkheden.
- Toetsen van bevindingen aan bestaande normen en richtlijnen, zoals OWASP ASVS, NCSC ICT-beveiligingsrichtlijnen en vereisten voor verkiezingsprocessen.
- Formuleren van securityaanbevelingen die voorkomen dat digitale hulpmiddelen nieuwe risico's introduceren ten opzichte van het papieren stemproces.

Privacy

Bepalen onder welke voorwaarden de verwerking van persoonsgegevens in digitale stemhulpmiddelen voldoet aan de AVG.

- In kaart brengen van verwerkingsactiviteiten: welke persoonsgegevens worden verwerkt, door wie, voor welk doel en hoe lang.
- Toetsing aan de AVG-beginselen: rechtmatigheid, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid, en transparantie.
- Beoordeling van rollen en verantwoordelijkheden van betrokken partijen (verwerkingsverantwoordelijke, verwerker, onderaannemers).
- Formuleren van concrete privacy maatregelen en organisatorische maatregelen om compliant te blijven.

1.3 Aanpak

In samenwerking met BZK zijn intakegesprekken gevoerd met relevante stakeholders, waaronder functionarissen binnen gemeenten, leveranciers van stembulpmiddelen en beleidsmedewerkers van BZK.

PuraSec en Privacy Company hebben het onderzoek uitgevoerd aan de hand van verschillende onderzoeksmethoden:

- Documentstudie: Onderzoekers hebben verschillende documenten geanalyseerd, waaronder eerdere adviezen, beleidsstukken, overeenkomsten, certificeringen, en (technische) beschrijvingen over verschillende applicaties.
- Interviews: Door middel van interviews met onder meer gemeenten en leveranciers hebben onderzoekers een beeld gevormd van de verschillende aangeboden applicaties en de wijze waarop deze gebruikt worden binnen gemeenten.
- Technisch onderzoek: Aan de hand van technisch onderzoek hebben onderzoekers (beperkt) inzicht gekregen of de applicaties aan belangrijke informatiebeveiligingsvereisten voldoen.

1.4 Leeswijzer

Hoofdstuk 2 biedt een uitgebreide analyse van de beschikbare digitale stembulpmiddelen, waarbij de specifieke functionaliteiten van deze applicaties worden uiteengezet. Tevens worden de potentiële risico's met betrekking tot informatiebeveiliging en privacy geadresseerd. Hoofdstuk 3 presenteert de bevindingen en aanbevelingen aan BZK.

Hoofdstuk 2: Stemhulpmiddelen

2.1 Toelichting stemapps

Een aanzienlijk aantal gemeenten maakt gebruik van applicaties die door stembureauleden in het stemlokaal worden ingezet. Deze applicaties functioneren op mobiele telefoons of iPads, die ofwel persoonlijk eigendom zijn van de gebruiker, ofwel door de gemeente ter beschikking worden gesteld. Dit verschilt per gemeente en is afhankelijk van de lokale keuzes.

De applicatie ondersteunt voor een groot deel de voorzitter van een stembureau bij onder andere de volgende werkzaamheden:

- het controleren of er voldoende stemformulieren aanwezig zijn;
- het registreren van de openings- en sluittijd van het stembureau;
- het bijhouden van aanwezigheid van de stembureauvrijwilligers voor uitbetaling van hun vergoedingen;
- het controleren of er voldoende potloden zijn;
- het beheren van de containers voor de stembureauformulieren;
- het registreren van eventuele allergieën van stembureauleden bij de maaltijdverzorging.

De applicatie beschikt ook over de mogelijkheid om de stempas van de kiezer te scannen. Hierbij wordt de barcode gelezen om een stempasnummer te extraheren, dat vervolgens automatisch wordt vergeleken met een kopie van het Register van Ongeldige Stempassen (ROS). De applicatie geeft vervolgens aan of de kiezer, conform het ROS, kan worden toegelaten tot de stemming. In paragraaf 2.2 worden de meest voorkomende functionaliteiten van dergelijke applicaties gedetailleerd beschreven.

2.2 Overzicht van functionaliteiten en gegevensverwerkingen

Tabel 1 geeft weer wat voor functionaliteiten de digitale stemhulpmiddelen aanbieden. De exact aangeboden functionaliteiten kunnen per applicatie verschillen. Per functionaliteit hebben de onderzoekers beschreven welke typen persoonsgegevens zoal verwerkt worden.

Tabel 1: functionaliteiten digitale stembulpmiddelen

Onderdeel	Functionaliteiten en doelen	Verwerkingen persoonsgegevens
Scannen stempassen	Scannen: Het scannen van stempasnummers door middel van een (mobiele) applicatie om stempassen te controleren tegenover het ROS, herkennen potentieel uitbrengen dubbele stem en tellen van opkomstcijfers.	Stemgerechtigden: Stempasnummers
Webapplicatie stembureaus	Aanmelden stembureauleiden: Registratie aanwezigheid ingeroosterde leden.	Stembureauleiden: Urenregistratie
	Werkproces processtappen: Aanbieden van workflow voor stembureaus tijdens verkiezingen.	n.v.t.
	Bijhouden voorraad stembiljetten: Monitoren van de voorraad zodat deze tijdig kan worden aangevuld.	n.v.t.
	Communicatie met gemeenten: Berichtendienst tussen stembureau en gemeente.	Chatgegevens
	Tellingen: Invoeren van telresultaten en het signaleren van afwijkingen.	n.v.t.
	Facilitair: Monitoren beschikbaarheid voorzieningen (koffie, potloden, etc.).	n.v.t.
	Gegevens stembureauleiden vastleggen: Diverse gegevens over stembureauleiden noodzakelijk voor de werkzaamheden die dag.	Stembureauleiden: NAW-gegevens, bankrekeningnummers, dieetwensen, planning
	Instructie legitimatiebewijs: Digitale handleiding voor uitvoeren identiteitscontrole.	n.v.t.
Gemeentelijke applicatie	Monitoring verloop verkiezingsdag: Overzicht houden op proces en tijdig handelen bij problemen.	n.v.t.
	Onboarding & uitbetaling: Ondersteuning wettelijke verplichtingen gemeenten en uitbetalingen vergoedingen.	Stembureauleiden: NAW-gegevens, bankrekeningnummers, planning

2.3 Relevante (wettelijke) kaders security en privacy

De onderzochte applicaties worden door de leveranciers aangeboden ter ondersteuning van het stemproces. Leveranciers geven ook expliciet aan dat de applicaties niet ingezet mogen worden als vervanging van de bestaande (wettelijke) middelen ter ondersteuning bij het stemproces. Met andere woorden, de applicaties vervullen geen formele rol bij de uitvoering van het huidige stemproces. Daarmee vallen zij buiten de werkingssfeer van de Kieswet.¹

Wel dienen de applicaties te voldoen aan alle overige (algemene) wet- en regelgeving met betrekking tot informatiebeveiliging en privacy. Voor gemeenten betekent dit dat de applicaties dienen te voldoen aan de wettelijke vereisten vastgelegd in de (Uitvoeringswet) Algemene Verordening Gegevensbescherming (UAVG) en de verplichtingen ten aanzien van informatiebeveiliging vastgelegd in de Baseline Informatiebeveiliging Overheid 2 (BIO2). Voor leveranciers van stembureauapps betekent dit dat zij als verwerker de volgende verantwoordelijkheden hebben:

1. **Opvolgen instructies gemeenten:** Leveranciers mogen persoonsgegevens enkel verwerken op instructie van gemeenten. Wanneer de leveranciers buiten deze instructies om zelfstandig handelen, kwalificeren zij voor deze verwerkingen als verwerkingsverantwoordelijke.
2. **Afspraken vastleggen in verwerkersovereenkomst:** De leveranciers en gemeenten zijn verantwoordelijk voor het vastleggen van afspraken over de desbetreffende verwerkingsactiviteiten in een bindende verwerkersovereenkomst.
3. **Toestemming verkrijgen voor het inschakelen van subverwerkers:** Leveranciers mogen vanuit hun rol als verwerker geen andere subverwerkers inschakelen zonder schriftelijke toestemming van gemeenten. De leveranciers zijn verantwoordelijk om te waarborgen dat de subverwerkers een gelijkwaardig beschermingsniveau bieden ten aanzien van de bescherming van deze gegevens.
4. **Veiligheid persoonsgegevens waarborgen:** Leveranciers dienen passende technische en organisatorische maatregelen te treffen om de beveiliging van persoonsgegevens te waarborgen, met inbegrip van bescherming tegen onopzettelijke of onwettige vernietiging of verlies, wijziging, ongeoorloofde openbaarmaking of toegang.
5. **Meldplicht inbreuken persoonsgegevens:** Als leveranciers te maken krijgen met incidenten die de vertrouwelijkheid, integriteit of beschikbaarheid van de betreffende persoonsgegevens raken hebben zij de plicht om dit onverwijld te melden bij de betrokken gemeente(n) en hen op passende wijze te ondersteunen bij de afhandeling daarvan.

¹ Zie vooral de bepalingen in *Hoofdstuk Ea. Digitale ondersteuning in het verkiezingsproces* van de Kieswet.

Hoofdstuk 3: Bevindingen en aanbevelingen

3.1 Bevindingen en aanbevelingen

Op basis van het uitgevoerde onderzoek hebben PuraSec en Privacy Company een aantal bevindingen en aanbevelingen geformuleerd die door BZK opgevolgd kunnen worden. In algemene zin merken onderzoekers op dat het gebruik van stembureauapps momenteel niet onder de werkingssfeer (en toezicht) van de Kieswet vallen. Alle onderzochte aanbieders van de verschillende applicaties geven aan dat het gebruik van dergelijke scanners enkel ondersteunend is bij het stemproces, en niet leidend of ter vervanging van het ‘papieren’ proces mag zijn. De vraag of dit in praktijk ook daadwerkelijk het geval is, kunnen de onderzoekers niet volledig beantwoorden. Dit hangt immers niet alleen af van de leveranciers van de applicaties, maar ook van de wijze waarop gemeenten en stembureauleden daarmee in de praktijk werken.

In onderstaande tabel hebben PuraSec en Privacy Company gezamenlijk een aantal bevindingen en aanbevelingen opgesteld. Deze dragen bij aan het uitgangspunt dat het papieren stemproces leidend is en dat het gebruik van ondersteunende systemen voldoende beschermd is zodat er geen risico's kleven aan het gebruik van deze digitale middelen die bij een volledig analoog stemproces niet zouden bestaan.

Tabel 2: bevindingen en aanbevelingen

Bevinding	Aanbeveling
Telfunctionaliteiten kunnen leiden tot een risico dat ondanks dat de systemen hier niet geschikt voor zijn, gegevens toch invloed hebben bij het handmatig tellen van stemmen.	Vergroot het bewustzijn bij gemeenten en stembureauleden dat gegevens die worden vastgelegd in deze diensten niet gebruikt mogen worden voor het uitvoeren van formele tellingen. Geef gemeenten concrete adviezen op welke wijze zij kunnen voorkomen dat de inzet van stempasscanners tot een verhoogd risico leidt.
Het is belangrijk dat gemeenten voldoende maatregelen treffen in situaties waarin de beschikbaarheid, integriteit of veiligheid van de applicaties niet langer gewaarborgd is.	Adviseer gemeenten een Business Impact Analyse (BIA) uit te laten voeren ten aanzien van het stemproces om in kaart te brengen wat de gevolgen zijn als de door gemeente gebruikte applicatie onverwachts niet meer beschikbaar is. Bied waar mogelijk handvatten aan om hen hierbij te ondersteunen. Bijvoorbeeld door een document op stellen met belangrijke vragen die gemeenten zichzelf kunnen stellen bij het uitvoeren van een BIA. De resultaten van de BIA kunnen bijvoorbeeld leiden tot nadere afspraken in een Service Level Agreement (SLA).
Het stemproces is in grote mate afhankelijk van de medewerking van vrijwilligers en betrokken burgers. Zij zijn in veel gevallen niet gebonden aan een gemeentelijk informatiebeveiligingsbeleid en hebben daardoor mogelijk onvoldoende training gehad om te begrijpen op welke wijze de systemen veilig gebruikt kunnen worden.	Vergroot het bewustzijn bij gemeenten dat zij bij het gebruik van deze applicaties zorgen dat eindgebruikers voldoende training hebben gehad. Meer specifiek zou deze boodschap gericht moeten zijn aan functies als de (Chief) Information Security Officer, Privacy Officer, of Functionaris Gegevensbescherming binnen gemeenten. Zij

Bevinding	Aanbeveling
	zijn verantwoordelijk voor het inrichten en toezicht houden op dergelijke maatregelen.
Er zijn op dit moment geen duidelijke technische vereisten vastgesteld waaraan de systemen moeten voldoen. Verschillende leveranciers hebben uitgesproken deze behoefte wel te hebben.	Laat het verantwoordelijke orgaan duidelijke technische vereisten vaststellen waaraan de systemen zouden moeten voldoen. Overweeg daarbij om (deels) aan te sluiten bij bestaande vereisten die voortvloeien uit de Kieswet en geldende wet- en regelgeving. Leg onder meer concrete eisen vast ten aanzien van: - eisen met betrekking tot het bewaken van de integriteit van het ROS en de afhankelijkheid van menselijke procedures daarbij te minimaliseren; - secure development lifecycle processes (SDLC); - het gebruik van encryptie en wachtwoordbeleid; - de inzet van devices buiten het beheer van gemeenten; - afhankelijkheid van cloudproviders; - het gebruik van software die publiekelijk controleerbaar is; - implementatie van centrale logging, monitoring en alerting; - beveiligingsmechanismes en configuratiebeleid; - toegangsbeheer; - uitvoeren van updatebeleid; en - aantonen van certificeringen en onafhankelijk laten toetsen van de veiligheid van systemen door middel van audits en pentests).
De scope van de verwerkersovereenkomsten is niet altijd actueel en dekt daardoor niet volledig de verwerkingen die binnen applicaties plaatsvinden. Het is belangrijk voor gemeenten om Bijlage 1 van de verwerkersovereenkomst volledig en accuraat bij te houden omdat dit een belangrijk middel kan zijn bij het waarborgen van het juiste informatiebeveiligingsniveau.	Informeer gemeenten over het belang om deze overeenkomsten periodiek te controleren en te actualiseren. Eventueel kunnen gemeenten in de verwerkersovereenkomsten de door BZK vastgestelde technische maatregelen (zie vorige aanbeveling) opnemen.
Enkele leveranciers bieden een uitgebreid pakket met functionaliteiten die gezamenlijk leiden tot het verwerken van veel (gevoelige) persoonsgegevens. Bijvoorbeeld wanneer in de applicaties naast algemene contactgegevens ook financiële gegevens worden vastgelegd, dieetgegevens (allergieën) en/of authenticatiegegevens van gebruikers.	Adviseer gemeenten om te controleren of de inzet van de applicatie aan de criteria voor de verplichting tot het uitvoeren van een DPIA voldoet en, indien noodzakelijk, deze alsnog uit te voeren.

3.2 Conclusie

Tijdens het onderzoek is naar voren gekomen dat met de introductie van stembureauapps de scheiding tussen het papieren stemproces en een digitaal stemproces minder duidelijk wordt. Hoewel de applicaties weliswaar formeel geen onderdeel zijn van de middelen bij het stemproces, en daardoor buiten de werkingssfeer van de Kieswet vallen, kunnen de toepassingen toch (indirect) van invloed worden op de uitkomsten. Hoewel de resultaten van het onderzoek niet hebben geleid tot een beeld dat het gebruik van deze applicaties op dit moment invloed heeft, zien de onderzoekers wel mogelijkheden voor gemeenten en het ministerie van BZK om de aanpak hiervoor te verbeteren.

De belangrijkste verbeteringen hiervoor bestaan uit het vergroten van het bewustzijn van gemeenten over de rol die zij zelf vervullen en het vaststellen van heldere (technische) eisen ten aanzien van systemen. Daarbij is het van belang om met name rekening te houden met elementen als (I) de unieke aard van het verkiezingsproces, (II) de unieke eigenschappen van de omgeving en stakeholders daarbinnen, waaronder de inzet van grote groepen vrijwilligers en (III) de wensen van aanbieders om duidelijke (eenduidige) eisen te ontvangen waaraan systemen dienen te voldoen.