Overzicht Werkprocessen (AVG)

Ter voorbereiding op de inwerkingtreding van de Algemene verordening gegevensbescherming per 25 mei 2018 volgt hieronder een overzicht met alle werkprocessen van de Kiesraad waarbij persoonsgegevens worden verwerkt.

1. Algemeen

- Contactgegevens medewerkers
  Omvat: Telefoonlijst intern, gsm-telefoonlijst (privé-gegevens), Adresgegevens (Privé), Verjaardagkalender, Vakantierooster.
- Contactgegevens leden Kiesraad.
- Relatiebestand Kiesraad (applicatie op G-schijf)
- Verslaglegging (Staf, Vakoverleg, Kiesraadvergadering)
- Distributielijsten in Outlook:
  Omvat o.a.: groep 'Kiesraadleden'.
- Dienstreizen (Persoonsgegevens, Kopie ID enz.)
- Declaraties (Medewerkers & Leden Kiesraad)
- Overzicht medewerkers uitgifte toegangstags.

2. Kerntaken

2.1 Kieswet

- Registratie van aanduidingen
- Kandidaatstelling
- Vaststelling verkiezingsuitslag.

2.2 Wet raadgevend referendum (WRR)

- Inleidend verzoek (Formulier, kopie ID/Paspoort).
- Definitief verzoek (Formulier, kopie ID/Paspoort)
- Uitslag referendum

3. Overige uitvoering

- Noteren contacten met Kiesraad in File Maker Pro (FMP).
- Afdoening: Burgerbrieven, Wob-verzoeken, Klachten e.d.
- Databank verkiezingsuitslagen.
- Register van aanduidingen op websites (met gegevens gemachtigden).
- Beeldbank Kiesraad (foto's van collega's)
- Namen en foto's van collega's en leden Kiesraad op website.

Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

BZK

Directie CIO&I / CZW
BZK

Contactpersoon
5.1.2.e / 5.1.2.e
5.1.2.e

Datum
28 juni 2017

Kenmerk
2017-0000430634

notitie Prioriteren AVG

Afschrift aan

In het proces om alle verwerkingsactiviteiten die plaatsvinden onder verantwoordelijkheid van de Minister van BZK inzichtelijk en AVG-*compliant* te krijgen, is het verstandig om daarin een prioritering aan te brengen, waarbij alle verwerkingsactiviteiten met een hoog risico als eerst beoordeeld en in lijn met de AVG gebracht worden.

Aan de hand van de volgende indicatoren kan prioritering worden aangebracht in de verwerkingsactiviteiten van BZK. De eerste lijst volgt rechtstreeks uit de AVG en is meer bezien vanuit het risico voor betrokkenen. De tweede lijst is meer beredeneerd vanuit de verantwoordelijke.

	Gegevens	***Nee/ weinig***	***Ja/ veel***
a	Verwerking van bijzondere persoonsgegevens *Ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens, gezondheidsgegevens of gegevens m.b.t. seksueel gedrag of seksuele gerichtheid (art. 9 lid 1 AVG).*		
b	Verwerkingen van strafrechtelijke gegevens *Betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (art. 10 AVG).*		
c	Verwerkingen van wettelijk voorgeschreven identificatienummers *Denk hierbij aan:* BSN, Kenteken, BIG-nummer, A-nummer		
d	Verwerkingen van veel verschillende soorten persoonsgegevens *Denk hierbij aan: naam, adres, telefoonnummer, e-mailadres, leeftijd, gewicht, dieetwensen, huwelijkse staat.*		

	Betrokkenen		
E	Verwerkingen waarbij veel betrokkenen zijn *Over hoe meer personen gegevens worden verwerkt, hoe gevoeliger. Dit is een relatieve factor die je moet afzetten tegen alle verwerkingen binnen je domein. Hierbij speelt ook een rol wie betrokkenen zijn: gaat het om medewerkers of om burgers?*		
F	Verwerkingen met kwetsbare betrokkenen *Met kwetsbaar wordt bedoeld dat de negatieve gevolgen van een onrechtmatige gegevensverwerking groter kunnen zijn voor bepaalde betrokkene dan voor andere. Denk hierbij aan: minderjarigen, verstandelijk gehandicapten, mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijshuis verblijven, medewerkers van inlichtingen- en veiligheidsdiensten, klokkenluiders of informanten van politie of justitie.*		
G	Verwerkingen met (mogelijk) grote gevolgen voor betrokkenen *Hoe ingrijpender de (mogelijke) gevolgen voor betrokkenen, hoe risicovoller. Denk hierbij aan juridische gevolgen (in rechten en plichten), financiële/materiële gevolgen, immateriële gevolgen en lichamelijke gevolgen. Mogelijk staat tussen haakjes omdat gevolgen hier niet beperkt zijn tot beoogde gevolgen. Maar ook gevolgen van onbedoelde verwerkingen. Bv. door een datalek komen bepaalde gegevens op straat te liggen. Maar ook niet functioneren van het proces kan dergelijke gevolgen hebben.*		
Partijen			
H	Verwerkingen waarbij veel (externe) partijen betrokken zijn *Hier kan een rol spelen of het gaat om een overheidspartij of om een externe partij. En vervolgens hoe betrouwbaar deze partij is (betrouwbaar in de zin van hoe serieus nemen zij privacy en informatiebeveiliging).*		
I	Verwerkingen buiten de Europese Unie *Hieronder valt ook de opslag van gegevens op een server buiten de EU.*		
Proces			
J	Verwerkingen waarbij koppelingen worden gelegd *Vinden er koppelingen plaats tussen verschillende systemen en datasets?*		
K	Verwerkingen waarbij sprake is van geautomatiseerde besluitvorming *Louter op basis van de persoonsgegevens worden besluiten met rechtsgevolgen (veranderingen in rechten en plichten) genomen dan wel besluiten die betrokkene*		

	anderszins in aanmerkelijke mate treft (art. 22 lid 1 AVG)		
L	Verwerkingen met gebruikmaking van nieuwe technieken		
M	Duur van de verwerkingsactiviteit *Betreft het een tijdelijke of permanente registratie. Hoe lang worden de gegevens bewaard.*		
N	Verwerkingen bestaande uit systematische monitoring *Proces waarbij betrokkene worden geobserveerd, gemonitoord of bedoeld om controle op hem of haar uit te oefenen.*		
O	Verwerkingen met beperkte transparantie *Uitgangspunt van de AVG is transparantie en de plicht van verantwoordelijke om betrokkene te informeren, inzage te verlenen etc. (art. 13-21 AVG). De wet- en regelgeving biedt uitzonderingen hierop (art. 23 AVG). Als betrokkene – hoewel terecht – minder dan wel niet geïnformeerd is, kan dit de privacyrisico's verhogen.*		
	Business		
P	Verwerkingen in het kader van het primaire proces		
Q	Verwerkingen met grote politieke (waaronder imago), bestuurlijke of financiële belangen		
R	Mede-overheden zijn afhankelijk van het proces		
	Totaal		

Notitie

Onderwerp
Voortgang Implementatie AVG; nr. 1

Datum
4 september 2017

Kenmerk
2017-0000429580

Inlichtingen
5.1.2.e
T 070 426 6266
F 070 751 7078

Aan
Staf secretariaat van de Kiesraad

Van
5.1.2.e

1. Inleiding

Op 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG) in werking. De verordening vervangt de Europese Privacyrichtlijn die het Europees Parlement en de Raad van de Europese Unie in 1995 gezamenlijk hebben vastgesteld. Als gevolg daarvan wordt ook de Wet bescherming persoonsgegevens ingetrokken. Anders dan onder de Wet bescherming persoonsgegevens, gelden de bepalingen van de verordening ook voor de verwerking van persoonsgegevens bij de uitvoering van het verkiezingsproces. De AVG blijft daar evenwel niet toe beperkt. De verordening ziet op (bijna) alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen (art. 2 § 1 AVG). Dat betekent dat de AVG niet alleen van invloed kan zijn op de werkprocessen van het secretariaat voor zover het daarin persoonsgegevens van derden verwerkt, maar ook op werkprocessen die geheel intern plaatsvinden. Zoals bijvoorbeeld onkostendeclaraties. Het is belangrijk dat de Kiesraad vóór de inwerkingtreding van de AVG in kaart heeft gebracht welke gevolgen de AVG voor zijn werkprocessen heeft en deze werkprocessen, waar nodig, daarop heeft aangepast. Dit implementatietraject is inmiddels in gang gezet. Het feit dat de Kiesraad formeel geen Informatie Beveiligingsplan heeft en in het verleden de Wet bescherming persoonsgegevens wellicht iets beperkter heeft opgevat dan juridisch wenselijk, zorgen daarbij voor de nodige uitdagingen. Graag informeer ik de staf over de voortgang van dit implementatieproject.

2. Betrokkenheid van BZK bij de implementatie

2.1 Algemeen traject

Vanuit BZK wordt maandelijks een BZK breed AVG-overleg geïnitieerd. De overleggen worden gevoerd door degenen die binnen een cluster c.q. externe organisatie direct betrokken zijn bij de implementatie van de AVG in hun cluster/organisatie. Op verzoek van 5.1.2.e ben ik namens de Kiesraad bij deze

overleggen aanwezig geweest op 20 juni en 23 augustus.[1] Tot op heden hebben de bijeenkomsten vooral een procedureel karakter. Hoewel de inhoud daardoor op dit moment wat verder afstaat van onze behoeften, bieden de bijeenkomsten wel inzicht in de interne werkprocessen van BZK, in de verordening zelf en op de gevolgtrekkingen die onderdelen van BZK uit de verordening maken. In die zin vind ik het nuttig om de bijeenkomsten waar mogelijk te blijven bijwonen.

Op 5 juli 2017 ben ik aanwezig geweest bij een presentatie van het centraal AVG-register van BZK. Op dit moment is dat gelijk aan het Wbp-register van het ministerie van Economische Zaken. Medio oktober wordt een nieuwe release van de web-module verwacht, waarbij deze in lijn met de AVG wordt gebracht. De Kiesraad kan in de toekomst van het centraal AVG-register van BZK gebruikmaken, maar is hier niet toe verplicht. Op een later moment zal ik de staf een notitie voorleggen met daarin een afweging van de voor- en nadelen hiervan en een gemotiveerd voorstel.

Naast het maandelijkse BZK breed AVG-overleg, staan er op dit moment ook twee AVG-leerateliers ingepland. Dit zijn bijeenkomsten waarbij op één of meer inhoudelijke aspecten van de verordening dieper wordt ingegaan. De eerste stond gepland op 6 september. Er is toen onder andere gesproken over het verschil tussen de verwerkingsverantwoordelijke en verwerker en het prioriteren van verwerkingsactiviteiten.

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties vraagt, gelet op de politieke verantwoordelijkheid van de minister om tweemaandelijks verantwoording af te leggen over de actuele voortgang bij de implementatie van de AVG. Dit verzoek wordt telkens gericht aan alle onderdelen van het ministerie, de uitvoeringsorganisaties, maar ook aan de Kiesraad. Het ministerie gebruikt voor deze uitvraag zogenoemde PKI's. PKI's dienen de interne verantwoording van BZK en zijn o.a. bedoeld om te bepalen waar van hoger hand een interventie moet plaatsvinden. Dat past niet bij de zelfstandige positie van de Kiesraad. De PKI's bieden bovendien onvoldoende concrete handvatten om een gewogen oordeel over onze voortgang te rapporteren. Dat maakt ze weinig bruikbaar; een oordeel dat – zo bleek mij tijdens het BZK breed AVG-overleg van 23 augustus – overigens breder leeft. In overleg met 5.1.2.e heb er daarom voor gekozen de PKI's niet in te vullen. De Kiesraad is daar overigens ook niet toe verplicht. In plaats daarvan wordt tweemaandelijks puntsgewijs gemeld waar we staan. BZK is akkoord met die werkwijze.

2.2 Bijzonder traject

De start van het implementatietraject van de AVG viel samen met het moment waarop de Kiesraad gevraagd werd een advies uit te brengen over een concept voor de Aanpassingswet Algemene verordening gegevensbescherming. Met die wet worden verschillende wetten, waaronder de Kieswet, aangepast aan de AVG. Op 25 juli 2017 heb ik met 5.1.2.e (CZW) en 5.1.2.e (Beleid) van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties gesproken over de interpretatie van de verordening. Kennisuitwisseling stond daarbij centraal en heeft mijns inziens ook geleid tot een kwalitatief beter advies. Ik vond het zelf leuk en leerzaam en heb de indruk dat mijn gesprekspartners dat ook vonden, want beiden hebben aangegeven mee te willen blijven denken. Als de gelegenheid zich voordoet zal ik graag van dit aanbod gebruik maken.

---

[1] De bijeenkomst van 18 juli heb ik door verplichtingen elders verstek moeten laten gaan.

3. Stand van zaken

Eén van de aandachtspunten voor een juiste implementatie van de AVG binnen een organisatie, is dat er in de breedte van de organisatie voldoende kennis moet zijn over de verordening en de rechten die derden daaraan kunnen ontlenen. Dat wil niet zeggen dat iedereen AVG-specialist moet worden. Wel is het nodig dat medewerkers van het secretariaat sensitief zijn voor het feit dat zij met persoonsgegevens werken en dat dit zekere verantwoordelijkheden met zich meebrengt. Op 13 juli 2017 heb ik daartoe een lunchlezing over de AVG verzorgd.

BZK heeft een 'Handreiking AVG' gemaakt. Deze handreiking bevat 24 stappen die bij iedere mogelijke verwerking van persoonsgegevens doorlopen moeten worden. Iedere stap moet worden gedocumenteerd. Deze documentatie kan worden gebruikt om op een later moment het AVG-register in te vullen. Hoewel de handreiking zelf een klein en handzaam document is, kan één stap binnen de handreiking uit meerdere onderdelen beslaan en vereist het gebruik van de handreiking soms gedetailleerde kennis van de verordening. Het doorlopen van de handreiking en het vastleggen van de gevraagde documentatie vergt dan ook een forse tijdsinspanning.

Naar aanleiding van de lunchlezing hebben alle medewerkers van het secretariaat geholpen om een inventarisatie te maken van alle werkprocessen van de Kiesraad waarbij (mogelijk) persoonsgegevens worden verwerkt. Aan de hand daarvan zijn 20 verwerkingsprocessen geïdentificeerd. Zie bijlage.

Voor de implementatie van de AVG kunnen sommige van deze verwerkingsprocessen geïntegreerd worden behandeld. Ik stel voor dit waar mogelijk ook te doen.

BZK adviseert bij de implementatie van de AVG voorrang te geven aan de werkprocessen die prioriteit genieten. Om verschillende werkprocessen ten opzichte van elkaar te prioriteren, is door BZK een document opgesteld met aspecten die bij het stellen van prioriteiten betrokken kunnen worden. Zie bijlage 2. Gelet op dit document verdienen de kerntaken van de Kiesraad mijns inziens voorrang bij het implementatietraject. Het gaat dan om de volgende vier werkprocessen:

1. De kandidaatstellingsprocedure.
2. De vaststelling van de verkiezingsuitslag.
3. Inleidende en definitieve verzoeken tot het houden van een referendum.
4. De registratie van aanduidingen van politieke partijen.

De toekomstige Aanpassingswet Algemene verordening gegevensbescherming past de Kieswet aan de verordening aan; met name door enkele uit de verordening voortvloeiende rechten van betrokkenen niet van toepassing te verklaren in het verkiezingsproces. Het heeft minimale invloed op het werk dat verzet moet worden om de verordening te implementeren. Mogelijke wijzigingen in processen zullen eerder voortvloeien uit de verordening zelf dan uit de voormelde Aanpassingswet. Daarbij moet ook bedacht worden dat documentatie, analyses, overeenkomsten, bewijsstukken et cetera een belangrijk onderdeel uitmaken van de implementatie van de verordening en dus minstens zo belangrijk zijn als wat de Kiesraad concreet doet.

Op dit moment ben ik halverwege het in de 'Handreiking AVG' opgenomen stappenplan voor de implementatie van de AVG voor wat betreft de kandidaatstelling. Het streven is er daarbij op gericht om onze huidige werkwijze zoveel mogelijk te behouden.

Beslispunten staf:
1. Ik verzoek de staf om in de stemmen met het voornemen de documentatie van verwerkingsprocessen waarin persoonsgegevens worden verwerkt, zoveel mogelijk met elkaar te integreren.
2. Ik stel voor om, in lijn met BZK, in eerste instantie te streven naar de correcte en tijdige implementatie van de AVG inzake de kerntaken van de Kiesraad en verzoek de staf hiermee in te stemmen.
3. Ik ben er vanuit gegaan dat de staf er de voorkeur aan geeft als onze huidige werkprocessen zoveel mogelijk ongewijzigd blijven. Waar de verordening daar ruimte toe lijkt te bieden, zal ik die nemen. Is deze premisse juist?

4. Komende periode
Ik ben van plan de 'Handreiking AVG' voor één werkproces af te ronden. Het resultaat daarvan zou ik daarna graag ambtelijk met AVG-deskundigen van BZK bespreken. Dat gesprek zou mijns inziens moeten gaan over een eerste concept, waarbij ik vooral twee dingen wil toetsen:
1. Waar ik ruimte heb genomen om de AVG zo te implementeren om een minimale aanpassing op onze huidige werkprocessen te bewerkstellingen, is die interpretatie verdedigbaar?
2. Is de wijze waarop ik nu vormgeef aan de documentatieplicht te omvangrijk, voldoende of te summier?
Nadat eventuele kritiekpunten te hebben verwerkt, zou ik het document daarna graag ter beoordeling aan de staf voorleggen. Deze werkwijze heeft als voordeel dat de staf een uitgewerkt voorstel krijgt dat ook direct op (juridische) houdbaarheid is getoetst en heeft voor mij als bijkomende voordeel dat er lopende het proces al een mogelijkheid tot kennisdeling bestaat.

Beslispunten staf:
4. Kan de staf zich vinden in de voorgestelde werkwijze?

Notitie

Onderwerp
Werkprocedure AVG-rechten

Datum
31 mei 2018

Kenmerk
2018-0000325158

Inlichtingen
5.1.2.e
T 070 426 6266
F 070 751 7078

Blad
1 van 10

Aan
Staf
Van
5.1.2.e

1. Inleiding

De Algemene verordening gegevensbescherming (AVG)[1] heeft de rechten van personen, van wie persoonsgegevens worden verwerkt, versterkt. Zij hebben meer rechten gekregen tegenover personen en organisaties die hun persoonsgegevens verwerken; zoals de Kiesraad. Artikel 12, tweede lid, van de verordening verplicht de Kiesraad om de uitoefening van de in de AVG neergelegde rechten te faciliteren. Daarbij kan een onderscheid gemaakt worden in twee soorten rechten. Er is een recht – het actief informatierecht – dat degene wiens persoonsgegevens worden verwerkt van rechtswege toekomt. Dit recht vergt proactief handelen van de Kiesraad. Daarnaast zijn er rechten waarop natuurlijke personen zich kunnen beroepen en die de Kiesraad verplichten om desgevraagd te reageren c.q. tot actie over te gaan. Deze notitie heeft uitsluitend betrekking op de laatstbedoelde categorie. De notitie geeft antwoord op de vraag hoe de Kiesraad moet handelen als er verzoeken van burgers binnenkomen die gebruik willen maken van een hen krachtens de AVG toekomend recht. Op een later moment volgen nadere voorstellen die betrekking hebben op het actief informatierecht.

Deze notitie is als volgt opgebouwd. Allereerst wordt een concreet voorstel gegeven voor de inrichting van de procedure (§ 2). Dit voorstel wordt themagewijd besproken. Daarna wordt nog uitgebreid ingegaan op de rechten waarop betrokkenen zich jegens de Kiesraad kunnen beroepen (§ 3), omdat kennis van deze rechten noodzakelijk is om het juiste besluit op een aanvraag te kunnen nemen. Het gaat dan vooral om de volgende rechten:

- Art. 15 AVG: Recht op inzage
- Art. 16 AVG: Recht op rectificatie

[1] 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).

– Art. 17 AVG: Recht op vergetelheid
– Art. 18 AVG: Recht op beperking van de verwerking.

2. Voorstel procedure

Hoe om te gaan met verzoeken van burgers die zich beroepen op één van de hen, op grond van de Algemene verordening gegevensbescherming, toekomende rechten? Deze paragraaf geeft themagewijde antwoorden op die vraag. Daarbij wordt er telkens vanuit gegaan dat de Kiesraad de betrokken verwerkingsverantwoordelijke is. Voor sommige verwerkingen is in werkelijkheid de voorzitter van de Kiesraad verwerkingsverantwoordelijke. Daarover meer binnen het thema 'Ondertekening'.

Ontvangst

Een verzoek kan op verschillende manieren bij de Kiesraad worden ingediend:

- Mondeling
  Een telefonisch binnenkomend verzoek moet altijd worden genotuleerd. In deze telefoonnotitie moet minimaal zijn opgenomen:
  a. De naam van de beller: voornaam, voorletters en achternaam.
  b. Het telefoonnummer van de beller.
  c. Het postadres van de beller.
  De informatie wordt namelijk in beginsel schriftelijk verstrekt.[2]
- Schriftelijk
- E-mail
  Als het verzoek elektronisch is ingediend, wordt de informatie – indien mogelijk – elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

Identificeren

Aangenomen dat de Kiesraad geen persoonsgegevens verwerkt van personen die jonger zijn dan zestien jaar, kan iedere betrokkene, die de Kiesraad verzoekt om zijn rechten uit hoofde van de artikelen 15 t/m 22 van de AVG uit te oefenen, dit alleen doen met het oog op persoonsgegevens die de Kiesraad van hem persoonlijk verwerkt. Een verzoek van een natuurlijk persoon mag dus geen betrekking hebben op iemand anders. Dat stelt de Kiesraad voor een dilemma. Enerzijds moet hij faciliteren dat betrokkenen hun in de AVG neergelegde rechten kunnen uitoefenen, anderzijds moet hij ook voorkomen dat er een datalek ontstaat. Een datalek kan bijvoorbeeld ontstaan als de Kiesraad alleen op basis van de naam van een betrokkene persoonsgegevens ter inzage geeft, en de ter inzage verstrekte gegevens van een naamgenoot blijken te zijn. Of als iemand een verkeerde naam opgeeft. De Kiesraad heeft dus de plicht om zich van de identiteit van de verzoeker te vergewissen. Absolute zekerheid is niet vereist. De Kiesraad kan bijvoorbeeld aanvullende persoonsgegevens vragen die het mogelijk maken de identiteit van de betrokkene te bevestigen. Bedrijven doen dit vaak door, naast de naam of het klantnummer, ter controle het huisadres, huisnummer en de geboortedatum te vragen. Is de Kiesraad niet in staat de betrokkene te identificeren, dan kan de Raad weigeren gevolg te geven aan het verzoek van de betrokkene om diens rechten uit hoofde van de artikelen 15 tot en met 22 uit te oefenen. Die situatie zal zich echter niet snel voordoen. Het is echter wel belangrijk dat de Kiesraad altijd meer dan één persoonsgegeven gebruikt alvorens een verzoek inhoudelijk te behandelen.

---

[2] Art. 12 lid 1 AVG.

Beperkingen
De betrokkene kan niet in alle gevallen een beroep doen op een hem, op grond van de Algemene verordening gegevensbescherming, toekomend recht. Vooral bij verwerkingen van persoonsgegevens ter uitvoering van de Kieswet en de Wet raadgevend referendum bestaan er uitzonderingen. Deze beperkingen zijn telkens opgenomen in het hoofdstuk waarin de betreffende verwerking in de wet wordt voorgeschreven. Let wel: bij het schrijven van deze paragraaf ben ik er vanuit gegaan dat het voorstel van wet dat moet leiden tot de Aanpassingswet Algemene verordening gegevensbescherming in werking zal treden zoals het onlangs door de regering bij de Tweede Kamer is ingediend.

Beslissing op verzoek
De Kiesraad moet de betrokkene informeren over het gevolg dat aan het verzoek gegeven is. Welk gevolg gewenst is, hangt af van het recht waarop de betrokkene zich beroept. Meer hierover in paragraaf 3.

Beslistermijn
De Kiesraad moet onverwijld beslissen op een verzoek; doch uiterlijk binnen een maand. Verlenging van de beslistermijn is alleen mogelijk als aan drie voorwaarden wordt voldaan:
- Reden voor verlenging: De zaak is zeer complex óf de Kiesraad heeft erg veel verzoeken ontvangen.
- Moment van verlenging: De betrokkene moet binnen de eerst maand na ontvangst van het verzoek van de verlenging in kennis zijn gesteld.
- Termijn voor verlenging: Maximaal twee maanden.

Kosten
Een besluit op een verzoek dient kosteloos genomen te worden. Overigens is in de verordening wel expliciet voorzien in de mogelijkheid om kosten in rekening te brengen, wanneer verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter.[3] In dezelfde situaties mag de Kiesraad overigens ook weigeren gevolg te geven aan verzoeken.

De lijn
Zolang de Algemene verordening gegevensbescherming nog niet volledig door de Kiesraad is geïmplementeerd, is het praktisch dat ik zelf de primaire conceptbesluiten schrijf. In een later stadium ligt het meer voor de hand aan te sluiten bij de lijn die geldt in het geval de Kiesraad een verzoek op grond van de Wet openbaarheid van bestuur ontvangt.

Ondertekening
De reactie van de Kiesraad op een verzoek van een betrokkene wordt gelijkgesteld aan een appellabel besluit in de zin van artikel 1:3 van de Algemene wet bestuursrecht.[4] Gelet op de aard van het besluit – m.n. verstrekken, wijzigen, verwijderen en vasthouden van persoonsgegevens – en de tijd waarbinnen het besluit genomen moet worden, stel ik voor het Besluit mandaat en machtiging Kiesraad (Stb. 2016, 19763) opnieuw vast te stellen en daarin twee wijzigingen aan te brengen:
- De voorzitter van de Kiesraad wordt gemandateerd om namens de Kiesraad te besluiten en stukken te ondertekenen met betrekking tot

[3] Art. 12 lid 5 AVG.
[4] Art. 34 Uitvoeringswet Algemene verordening gegevensbescherming.

besluiten, waaronder verdagingsberichten, op grond van de Uitvoeringswet algemene verordening gegevensbescherming.
- De secretaris-directeur van de Kiesraad wordt gemandateerd om namens de Kiesraad te besluiten en stukken te ondertekenen met betrekking tot verdagingsberichten als bedoeld in artikel 12, derde lid, van de Algemene verordening gegevensbescherming: verordening (EU) 2016/679.

De voorgestelde bevoegdheidsverdeling voor de ondertekening van besluiten op grond van de Algemene verordening gegevensbescherming wordt daarmee gelijk aan die voor de ondertekening van besluiten op grond van de Wet openbaarheid van bestuur.

Actiepunt:
Het Besluit mandaat en machtiging Kiesraad (Stb. 2016, 19763) opnieuw vaststellen.

De Kiesraad is vaak verwerkingsverantwoordelijke, maar juridisch gezien niet altijd. Soms kent de wet een bevoegdheid expliciet toe aan de voorzitter van de Kiesraad en in die gevallen is de voorzitter zelf verwerkingsverantwoordelijke. Bijvoorbeeld bij de verwerking van persoonsgegevens in het kader van de (tijdelijke) benoeming of het (tijdelijk) ontslag van volksvertegenwoordigers. Als de Kiesraad dit onderscheid belangrijk vindt, dan zou een betrokkene geen informatie krijgen over de verwerking van persoonsgegeven in het kader van deze procedures als hij een algemeen verzoek om informatie tot de Kiesraad richt. Ook niet als de voorzitter zijn persoonsgegevens verwerkt. Een strikt onderscheid betekent ook dat het Besluit mandaat en machtiging voorzitter Kiesraad (Stb. 2016, 19765) na het komen vervallen van de Wet raadgevend referendum niet kan worden ingetrokken, maar nog één bevoegdheid aan de secretaris-directeur moet blijven geven: de bevoegdheid om namens de voorzitter van de Kiesraad te besluiten en stukken te ondertekenen met betrekking tot verdagingsberichten als bedoeld in artikel 12, derde lid, van de Algemene verordening gegevensbescherming: verordening (EU) 2016/679. Ofschoon juridisch helemaal juist: in de dagelijkse praktijk zal een gericht verzoek om informatie aan de Kiesraad over de verwerking van persoonsgegevens in het kader van de (tijdelijke) benoeming of het (tijdelijk) ontslag van volksvertegenwoordigers waarschijnlijk niet door de Kiesraad worden 'doorgestuurd' aan zijn voorzitter. De kans is zelfs aanwezig dat het secretariaat de fout niet ambtshalve hersteld, maar bij de ondertekening de Kiesraad zelf ook als besluitend orgaan vermeldt. Bovendien communiceert het secretariaat in de dagelijkse praktijk ook niet altijd helder naar buiten waar een bevoegdheid ligt: gemeente v. college van burgemeester en wethouders, Kiesraad v. voorzitter van de Kiesraad. Zo schreef het secretariaat op 12 april 2018 nog op de website van de Kiesraad dat de Raad de heer Stoffer heeft benoemd als Tweede Kamerlid;[5] juridisch is dat niet waar. Kan de Raad het een burger dat euvel duiden het onderscheid niet te hebben gemaakt? Mijn voorstel is om besluiten die genomen worden op basis van de in deze notitie beschreven procedure, altijd door de Kiesraad worden genomen. Juridisch is niet helemaal juist, maar het bezwaar wordt grotendeels weggenomen doordat de bevoegdheid om namens de Kiesraad te besluiten aan de voorzitter wordt toegekend.

[5] https://www.kiesraad.nl/actueel/nieuws/2018/04/12/benoeming-c.-stoffer-tot-lid-van-de-tweede-kamer (Laatst bezocht: 2 juni 2016.

Actiepunt:
In een volgende notitie aan de Kiesraad dit onderwerp aan de Raad voorleggen.

Rechtsmiddelenclausule

Op grond van artikel 34 van de Uitvoeringswet Algemene verordening gegevensbescherming geldt de schriftelijke beslissing van een bestuursorgaan op een verzoek als bedoeld in de artikelen 15 tot en met 22 van de verordening als een besluit in de zin van de Algemene wet bestuursrecht.[6] Tegen dit besluit kan een bezwaarschrift worden ingediend.[7] Tegen de beslissing op bezwaar is beroep mogelijk bij de rechtbank binnen het rechtsgebied waarvan de indiener van het beroepschrift zijn woonplaats in Nederland heeft.[8] En tegen de uitspraak van de rechtbank kan de betrokkene nog in hoger beroep bij de Afdeling bestuursrechtspraak van de Raad van State. Tijdens de behandeling van het beroep kunnen de Rechtbank en de Afdeling advies inwinnen bij de Autoriteit Persoonsgegevens.[9]

Naast het starten van een juridische procedure, staat voor de betrokkene evenwel ook een andere weg open.[10] De betrokkene kan zich wenden tot de Autoriteit Persoonsgegevens en een klacht indienen.[11] In de Uitvoeringswet wordt deze mogelijkheid niet expliciet genoemd. In plaats daarvan staat er in de Uitvoeringswet dat de betrokken een 'verzoek te bemiddelen of te adviseren' in een geschil met de Kiesraad kan indienen bij de Autoriteit Persoonsgegevens.[12] Daarmee wordt echter exact hetzelfde bedoeld. Anders dan onder de Wet bescherming persoonsgegevens, is de Autoriteit Persoonsgegevens verplicht alle klachten die bij haar binnenkomen in behandeling te nemen.[13] Zij heeft daarvoor onderzoeks- en sanctiebevoegdheden.[14] Klachtbehandeling bij de Autoriteit Persoonsgegevens is laagdrempelig voor de betrokkene. Mogelijk biedt het de Kiesraad bovendien de gelegenheid om lopende de klachtbehandeling door de Autoriteit Persoonsgegevens meer inzicht te verkrijgen in de wijze waarop deze autoriteit toetst. Geschilbeslechting door de Autoriteit Persoonsgegevens kan dus voor beide partijen meerwaarde hebben en 5.2.1 Al moet de Kiesraad altijd beide mogelijkheden noemen; de mogelijkheid een klacht in te dienen kan uiteraard wel als eerst worden genoemd.

Actiepunt:
Twee nieuwe rechtsmiddelenclausules opstellen: één voor het primaire besluit, één voor een beslissing op bezwaar.

DigiDoc

Binnenkomende verzoeken van betrokkenen, die gebruik willen maken van een hen krachtens de AVG toekomend recht, moeten in DigiDoc opgeslagen worden. Mijns inziens ligt het voor de hand om hiervoor een nieuwe hoofdmap in DigiDoc

[6] Hiermee wordt uitvoering gegeven aan art. 79 AVG.
[7] Art. 34 Uitvoeringswet Algemene wet bestuursrecht jo. art. 8:1 jo. 7:1 Algemene wet bestuursrecht.
[8] Art. 34 Uitvoeringswet Algemene wet bestuursrecht jo. art. 8:1 jo. 8:7 lid 2 Algemene wet bestuursrecht.
[9] Art. 36 lid 2 Uitvoeringswet Algemene verordening gegevensbescherming.
[10] Art. 12 lid 4 AVG.
[11] Art. 77 lid 1 AVG.
[12] Art. 36 lid 1 Uitvoeringswet Algemene verordening gegevensbescherming.
[13] Art. 57 lid 1 onder f AVG.
[14] Art. 58 AVG.

aan te maken, zoals die eerder ook voor Wob-verzoeken - '16. Wob-verzoeken' - is aangemaakt. Hoofdmap '18. Opschonen NAKIJKEN EN VRAGEN' kan worden hernoemd tot '19. Opschonen NAKIJKEN EN VRAGEN', waarna een nieuwe hoofdmap - '18. AVG' - kan worden tussengevoegd.

In de hoofdmap '18. AVG' moet niet alleen ruimte worden geboden voor de besluiten waar deze notitie op ziet, maar ook voor andere documenten die belangrijk zijn voor de implementatie en/of interpretatie van de AVG. Op dit moment staan die documenten deels verstopt in '14. Internationaal' en deels alleen op mijn deel van de H-schijf. Dat is geen wenselijke situatie. Ik stel daarom voor om voorlopig de volgende structuur in DigiDoc in te richten:

18. AVG
    - AVG-verzoeken
        - AVG-Verzoeken 2018
    - Literatuur
    - Notities
    - Verwerkersovereenkomsten & -afspraken

De getoonde mappen 'AVG-verzoeken', 'AVG-Verzoeken 2018', 'Literatuur', 'Notities' en 'Verwerkersovereenkomsten & -afspraken' zijn daarbij dossiermappen, zodat de portefeuillehouder daaronder zelf de noodzakelijke sub-mappen kan aanmaken. De map 'AVG-verzoeken' staat daarbij bewust anders uitgelijnd, omdat deze zich in de map 'AVG-verzoeken' bevindt. Op een later moment kan deze structuur worden aangevuld.

Actiepunt:
Bovenvermelde structuur in DigiDoc aanmaken

3. AVG-rechten

Een betrokkene heeft op grond van de AVG een aantal rechten. Deze rechten kan de betrokkene inroepen tegenover degene die zijn persoonsgegevens verwerkt. Niet alle rechten zijn in alle omstandigheden inroepbaar. Er zijn uitzonderingen. Soms voorziet de AVG zelf in zo'n uitzondering;[15] in andere gevallen biedt de AVG een grondslag om in nationale wetgeving in een uitzondering te voorzien.[16] De regering beoogd van die laatste mogelijkheid gebruik te maken in de Kieswet en de Wet raadgevend referendum. De daarvoor noodzakelijke wijziging van deze wetten is voorzien in het wetsvoorstel dat moet leiden tot de Aanpassingswet Algemene verordening gegevensbescherming. Dit wetsvoorstel is thans aanhangig bij de Tweede Kamer. Een betrokkene kan zich met een beroep op de AVG jegens de Kiesraad op de navolgende rechten beroepen:

Artikel 15: Recht op inzage

Dit is een passief informatierecht. Het houdt in dat de Kiesraad desgevraagd moet nagaan of hij persoonsgegevens van de betrokkene verwerkt en, zo ja, hem hierover moet informeren. De betrokkene hoeft geen belang te stellen bij zijn verzoek. Het verzoek kan specifiek zijn: heeft u mijn persoonsgegevens verwerkt ten behoeve van verwerkingsactiviteit X? Het verzoek mag ook algemener zijn: verwerkt u mijn

[15] Voorbeeld: de betrokkene kan geen gebruik maken van het recht op vergetelheid als de persoonsgegevensverwerking plaatsvindt op grond van een wettelijke verplichting.
[16] Vgl. art. 23 AVG.

persoonsgegevens? Het is dan aan de Kiesraad om, met behulp van het Register van de verwerkingsactiviteiten, om na te gaan in welke verwerkingsprocessen persoonsgegevens van de betrokkene voor zouden kunnen komen, en in die verwerkingsprocessen naar de persoonsgegevens op zoek te gaan. Denkbaar is bijvoorbeeld dat persoonsgegevens voorkomen in het relatiebestand of in het registratiebestand voor klantcontacten (FMP).

Als de Kiesraad daadwerkelijk persoonsgegevens van de betrokkene verwerkt, dan moet hij inzage geven in deze persoonsgegevens. Dit moet gebeuren op een wijze die de betrokkene in staat stelt om de gegevens te controleren en, zo nodig, om wijziging of verwijdering te vragen. De Kiesraad kan de betrokkene op twee manieren inzage geven in de persoonsgegevens die van hem worden verwerkt:

1. De Kiesraad kan een volledig overzicht opstellen van alle persoonsgegevens die de Raad van de betrokkene verwerkt en hem dit ter beschikking stellen. Gelet op de werkprocessen van de Kiesraad waarin persoonsgegevens worden verwerkt, zal deze manier naar verwachting het vaakst worden gebruikt.
2. De Kiesraad kan de betrokkene ook een kopie of afdruk verstrekken van het originele document waarin de gegevens staan. Deze mogelijkheid kan bijvoorbeeld gebruikt worden als iemand als gemachtigde is aangewezen door een politieke groepering[17], of als iemand een Wob-verzoek heeft ingediend.[18]

Naast dat de Kiesraad de betrokkene moet informeren over de persoonsgegevens die hij van de betrokkene verwerkt, moet de Raad ook de volgende informatie verstrekken:

A) Verwerkingsdoeleinden: waarom verwerkt de Kiesraad deze persoonsgegevens? Wat is het doel?
B) Categorieën van persoonsgegevens: welke persoonsgegevens verwerkt de Kiesraad? Inzage geven. Met de in de verordening gebruikte term ‘categorieën van persoonsgegevens’ worden concrete persoonsgegevens bedoeld. Zie hierover de kennisnotitie ‘Persoonsgegevens, categorieën van persoonsgegevens en bijzondere categorieën van persoonsgegevens.’ (Ons kenmerk: 2018-0000326948).
C) Ontvangers: Aan welke organisatie heeft de Kiesraad deze persoonsgegevens verstrekt, of zal de Kiesraad deze gegevens verstrekken? Het is overigens niet altijd nodig de organisaties bij naam te noemen. Soms kan ook volstaan worden met een categorie van ontvangers, bijvoorbeeld: gemeenten.
D) Bewaartermijn: Hoe lang bewaart de Kiesraad de persoonsgegevens? Als geen bewaartermijn kan worden genoemd, dan moeten de criteria genoemd worden op basis waarvan de bewaartermijn wordt bepaald.
E) Rechten van betrokkene: De betrokkene moet erop worden gewezen dat hij diverse rechten heeft (zoals: rectificeren, wissen, beperken van de verwerking, bezwaar maken tegen de verwerking e.d.).

[17] Origineel document: kopie formulier wijziging gemachtigde.
[18] Origineel document: aanvraag op grond van de Wob.

F) Klachtprocedure: De betrokkene moet erop gewezen worden dat hij het recht heeft een klacht in te dienen bij de Autoriteit Persoonsgegevens.
G) Gegevensbron: Wat is de herkomst van de persoonsgegevens? Als de persoonsgegevens niet bij de betrokkene worden verzameld, moet deze alle beschikbare informatie over de bron van die gegevens krijgen.
H) Geautomatiseerde besluitvorming: N.v.t. op de Kiesraad.

Artikel 16: Recht op rectificatie en aanvulling
Dit is het recht op verbetering van fouten. Een betrokkene kan om drie redenen om rectificatie vragen: 1) zijn persoonsgegevens zijn feitelijk onjuist weergegeven; 2) zijn persoonsgegevens zijn onvolledig of niet ter zake doende voor het doel waarvoor zij zijn verzameld; en 3) zijn persoonsgegevens worden op een andere manier in strijd met de wet door de Kiesraad gebruikt. In alle drie de gevallen kan hij de Kiesraad vragen omverwijld tot rectificatie over te gaan.

Heeft de Kiesraad de te rectificeren persoonsgegevens van de betrokkene ook met derden gedeeld? Dan moet de Kiesraad zo snel mogelijk deze andere organisaties van de wijziging op de hoogte stellen.[19]

Wordt de Kiesraad gevraagd om een professionele indruk, mening of conclusie te rectificeren waar de betrokkene het mee oneens is – bijvoorbeeld in een sollicitatieprocedure –, dan valt dit verzoek buiten de reikwijdte van het recht. De Autoriteit Persoonsgegevens gaat er echter vanuit dat de Kiesraad in een dergelijke situatie de schriftelijke mening van de betrokkene aan het dossier zal toevoegen.

Artikel 17: Recht op vergetelheid
Dit recht wordt ook het recht op gegevenswissing genoemd. De betrokkene heeft het recht de Kiesraad te vragen zijn persoonsgegevens te wissen. Daarnaast bevat de verordening ook een lijst met omstandigheden die, als zij zich voordoen, ertoe moeten leiden dat de Kiesraad uit eigen beweging persoonsgegevens wist. Daarop staan onder andere de volgende omstandigheden:

A) De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt.
   Voorbeeld:
   De Kiesraad verzamelt gegevens van personen die zich aanmelden voor een symposium. Als het symposium heeft plaatsgevonden, heeft de Kiesraad die persoonsgegevens niet langer nodig en moet hij deze wissen.
B) De verwerking berustte op toestemming van de betrokkene en deze trekt zijn toestemming voor de verwerking in.
   Voorbeeld:
   De Kiesraad verzamelt gegevens van personen die zich aanmelden voor een symposium. Als iemand aangeeft bij nader inzien niet te willen komen en zich afmeld, moeten diens persoonsgegevens direct worden gewist.
D) De persoonsgegevens zijn onrechtmatig verwerkt.
   Voorbeeld:
   De Kiesraad komt erachter dat hij persoonsgegevens verwerkt (of heeft verwerkt), terwijl daar geen geldige grondslag voor bestond.

[19] Art. 19 AVG.

E) De persoonsgegevens moeten worden gewist om te voldoen aan een bepaling uit Europese of nationale regelgeving.
Voorbeeld:
De Kieswet schrijft nu voor dat de Kiesraad de bij hem ingeleverde kandidatenlijsten vernietigt, nadat onherroepelijk is beslist over de geldigheid van de kandidatenlijsten (vgl. art. I 19 Kieswet).

Het recht op vergetelheid geldt niet onbeperkt. De Kiesraad heeft bijvoorbeeld niet de plicht om persoonsgegevens te wissen, voor zover de verwerking daarvan plaatsvindt ter uitvoering van een wettelijke plicht.[20] Daarvan is bijvoorbeeld sprake bij de verwerking van persoonsgegevens ter uitvoering van de Kieswet en de Wet raadgevend referendum.

Heeft de Kiesraad de te wissen persoonsgegevens van de betrokkene ook met derden gedeeld? Dan moet de Kiesraad zo snel mogelijk deze andere organisaties van de vernietiging daarvan op de hoogte stellen en dienen deze organisaties hetzelfde te doen.[21]

Mogelijk maakt de Kiesraad gebruik van back-ups. Als persoonsgegevens gewist moeten worden, dan moeten deze persoonsgegevens ook zo snel mogelijk uit de back-ups worden gewist. De Autoriteit Persoonsgegevens adviseert regelmatig back-ups te maken en verouderde gegevens systematisch te verwijderen. Het maken van een back-up leidt tot een aanvullende bewaartermijn. Worden persoonsgegevens in een regulier systeem 1 jaar bewaart, maar hanteert de Kiesraad aanvullend een bewaartermijn van 3 maanden voor back-ups, dan moet dit worden gecommuniceerd. In sommige gevallen is het niet mogelijk om persoonsgegevens uit een back-up te verwijderen. In dat geval moet de Kiesraad goed bijhouden welke persoonsgegevens hij had moeten rectificeren c.q. verwijderen. Is het onverhoopt nodig om een back-up terug te plaatsen? Dan moet de Kiesraad deze gegevens alsnog rectificeren c.q. verwijderen.

Artikel 18: Recht op beperking van de verwerking
Onder bepaalde omstandigheden heeft de betrokkene het recht de Kiesraad minder persoonsgegevens van hem te laten verwerken. Dit is het geval in vier situaties, waaronder de volgende drie:

A) Gegevens zijn mogelijk onjuist.
De betrokkene geeft aan dat de Kiesraad onjuiste persoonsgegevens van hem gebruikt. Totdat de persoonsgegevens zijn gecontroleerd, mogen de persoonsgegevens waarvan de juistheid wordt bestreden, niet worden gebruikt. Totdat de Wet raadgevend referendum op de AVG is aangepast, kan iemand die een verzoek tot het houden van een referendum heeft ingediend, met een beroep op artikel 18 de Kiesraad ertoe bewegen de daarop door hem ingevulde persoonsgegevens te verifiëren en waar nodig te verbeteren.

B) De verwerking is onrechtmatig.

[20] Art. 17 lid 2 onder b AVG.
[21] Art. 19 AVG.

Als de Kiesraad bepaalde persoonsgegevens niet mag verwerken, dan moet hij die wissen. Maar het kan gebeuren dat de betrokkene niet wil dat de Kiesraad deze gegevens wist. Bijvoorbeeld omdat hij de gegevens later wil opvragen. In dat geval moet het wissen van de gegevens worden uitgesteld.

C) De gegevens zijn niet meer nodig.
Als de Kiesraad persoonsgegevens niet meer nodig heeft, dan moet hij deze wissen. Maar het kan gebeuren dat de betrokkene deze gegevens nog wel nodig heeft. Bijvoorbeeld om een juridische procedure tegen de Kiesraad te kunnen voeren.

Beslist de Kiesraad tot beperking van de verwerking van de persoonsgegevens van de betrokkene en heeft de Kiesraad deze persoonsgegevens eerder met derden gedeeld? Dan moet de Kiesraad zo snel mogelijk deze andere organisaties van de beperking op de hoogte stellen. Ook zij moeten dan de verwerking van deze persoonsgegevens staken.[22]

Artikel 20: Recht op overdraagbaarheid van gegevens
Het recht op overdraagbaarheid van gegevens is door de betrokkene alleen inroepbaar als aan twee cumulatieve eisen wordt voldaan:

1. De grondslag voor de verwerking is toestemming van de betrokkene of een met de betrokkene gesloten overeenkomst.
2. De verwerking van persoonsgegevens vindt via geautomatiseerde procedés plaats.

Bij geen van de verwerkingsactiviteiten die de Kiesraad verricht wordt aan beide voorwaarden voldaan.

Artikel 21: Recht van bezwaar
De betrokkene heeft het recht om vanwege een met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van zijn persoonsgegevens: voor de vervulling van een taak van algemeen belang, voor de vervulling van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen óf voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde. In een enkel geval zal de Kiesraad persoonsgegevens verwerken op grond van een taak van algemeen belang.

Artikel 22: Geautomatiseerde individuele besluitvorming
De Kiesraad maakt geen gebruik van geautomatiseerde individuele besluitvorming. Daarom wordt deze bepaling niet nader toegelicht.

[22] Art. 19 AVG.

SvZ: Voortgang implementatieproces AVG

Geldig: 1 juli 2018

Leeswijzer:
Dit document bevat de stand van zaken met betrekking tot de voortgang in de implementatie van de Algemene verordening gegevensbescherming. Het document bevat de status per de bovengenoemde datum. Waar nodig wordt binnen een verwerkingsproces de status van kleinere onderdelen meegegeven. Om een snel beeld te krijgen van de status, kan naar de gebruikte kleuren worden gekeken.

Donker rood = Nog niet gestart.
Rood = Mogelijk wel gestart, maar nog de nodige actie vereist.
Oranje = In een vergevorderd stadium.
Groen = (Zo goed als) gereed.

Werkprocessen in het register van verwerkingen:

1. Registratie van aanduidingen

Status:
Melding in het verwerkingsregister gereed voor publicatie.

2. Kandidaatstellingsprocedure

Status:
Melding in het verwerkingsregister in concept gereed, maar met drie partijen moet mogelijk nog een verwerkerafspraak/-overeenkomst worden overeengekomen, namelijk:

a. KOOP (SDU)):
Vanwege publicatie van de processen-verbaal en kandidatenlijsten in de Staatscourant.
Status:
Ik moet nog uitzoeken of dit echt noodzakelijk is.

b. T&T Vertrouwd verbonden
Vanwege de connectie die zij ons bieden met de Basisregistratie personen.
Status:
Op 27 juni 2018 heeft T&T de Kiesraad per brief geïnformeerd van mening te zijn dat er nog een verwerkerovereenkomst nodig is. Op 28 juni 2018 heeft 5.1.2.e (na overleg) aangegeven dat de Kiesraad deze wens deelt en een concept opgevraagd.

c. RvIG (Rijksdienst voor Identiteitsgegevens)
Vanwege de Basisregistratie personen.
Status:
Ik moet nog uitzoeken of dit echt noodzakelijk is.

3. Vaststelling verkiezingsuitslag

Status:
Melding in het verwerkingsregister is nog in opbouw. Daarnaast moet met één partij mogelijk nog een verwerkersovereenkomst gesloten worden.

1. Xerox OBT
Vanwege het drukken van de kerngegevens
Status:
Ik moet nog uitzoeken of dit echt noodzakelijk is.

4. (Tussentijdse) benoemingen

Status:
Er is nog geen melding in voorbereiding.

5. Verzoeken o.g.v. Wrr

Status:
Melding in het verwerkingsregister in concept gereed, maar met twee partijen moet nog een verwerkersafspraak worden gemaakt.

1. Belastingdienst
   Vanwege het inscannen van alle binnenkomende verzoeken tot het houden van een referendum en ondersteuningsverklaringen.
   Status:

1 februari 2018:	De belastingdienst geeft, bij monde van 5.1.2.e verwerkersafspraken met de Kiesraad te willen maken.
22 mei 2018	Ik heb een voorstel voor verwerkersafspraken aan de Belastingdienst gestuurd. Afgestemd met 5.1.2.e en 5.1.2.e
25 mei 2018	Het concept ligt nu bij 5.1.2.e De belastingdienst dacht dat dit in de DVA was opgenomen, maar dat is niet het geval.

2. DICTU
   Vanwege de referendum applicatie.
   Status:

26 april 2018:	DICTU geeft bij monde van 5.1.2.e aan verwerkersafspraken met de Kiesraad te willen maken, maar hiervoor gegevens nodig te hebben.
23 mei 2018	Ik heb de gevraagde gegevens verstrekt. Dit is afgestemd met: 5.1.2.e 5.1.2.e en 5.1.2.e 5.1.2.e en 5.1.2.e hebben een kopie van de e-mail naar DICTU ontvangen.

Notitie

Onderwerp
Voortgang Implementatie AVG: nr. 2

Datum
2 juli 2018

Kenmerk
2018-0000498271

Inlichtingen
5.1.2.e
T 070 426 6266
F 070 751 7078

Blad
1 van 5

Aan
5.1.2.e
Van
5.1.2.e

1. Inleiding

Op 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG)[1] van toepassing geworden. Deze is nog niet volledig geïmplementeerd door de Kiesraad. Met deze notitie wordt de staf, voor de tweede maal,[2] geïnformeerd over de voortgang van het implementatietraject.

Deze notitie begint met een globaal overzicht van de drie elementen die een rol spelen bij de implementatie van de AVG (§ 2). Inzicht hierin is van belang om de in het implementatietraject gemaakte keuzes te kunnen begrijpen. Daarna wordt kort verantwoording afgelegd over de gemaakte keuzes voor het implementatietraject (§ 3) en een overzicht gegeven van de huidige stand van zaken (§ 4). Tot slot wordt ingegaan op de planning (§ 5).

2. Globaal overzicht

De implementatie van de verordening bevat drie elementen. Namelijk: documentatieplicht (§ 2.1), verantwoordingsplicht (§ 2.2) en informatieplicht (§ 2.3). Deze hangen met elkaar samen. In deze paragraaf wordt dit kort uitgelegd (§ 2.4).

2.1 Verantwoordingsplicht

De verantwoordingsplicht houdt in dat de Kiesraad met documenten moet kunnen aantonen dat de juiste organisatorische en technische maatregelen zijn genomen om aan de AVG te voldoen. Het bijhouden van een register van

---

[1] 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)
[2] Notitie d.d. 4 september 2017, kenmerk: 2017-0000429580.

verwerkingsactiviteiten is hier een onderdeel van. In dit register wordt opgenomen welke gegevens voor welk doel gebruikt worden en met wie deze gegevens worden gedeeld.

Aan iedere verwerking in het register van verwerkingsactiviteiten ligt ten grondslag:

1. Een gedetailleerde beschrijving van het werkproces.
   Deze dient als input voor het register, maar wordt niet zelf in het register opgenomen. Bij de Kiesraad ontbreekt dit type document overigens met grote regelmaat.
2. Informatiebeveiligingsbeleid
   De organisatorische en technische maatregelen die in het informatiebeveiligingsbeleid zijn opgenomen, komen terug in het AVG-register. In het verleden is door 5.1.2.6 wel informatiebeveiligingsbeleid voor de Kiesraad voorbereid, maar dit is (nog) niet afgerond. Er kon geen gebruik van worden gemaakt.
3. Verwerkersafspraken/-overeenkomsten:
   Als de Kiesraad als verwerkingsverantwoordelijke gebruikmaakt van een verwerker, moet hij met deze afspraken maken over de bescherming van persoonsgegevens. Deze afspraken worden vastgelegd in een document dat onderdeel uitmaakt van het AVG-rigister.
   N.b.: een verwerking waarvoor de Kiesraad nog een verwerkersafspraak of -overeenkomst moet afsluiten, mag nog niet gepubliceerd worden.
4. Data protection impact assessment (DPIA)
   Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen, zodat daarna maatregelen genomen kunnen worden om de risico's te verkleinen. Ook DPIA's worden vastgelegd in het register.

Naast het bijhouden van een register van verwerkingsactiviteiten, valt onder de verantwoordingsplicht ook:

a. Het bijhouden van een register van datalekken. Zelfmeldplicht bij iedere beveiligingsinbreuk (dus ook als er een usb-stick met gegevens (tijdelijk) zoekraakt bij de post).
b. Het kunnen aantonen dat een betrokkene daadwerkelijk toestemming heeft gegeven voor een gegevensverwerking wanneer voor deze verwerking toestemming nodig is. Tevens moet aangetoond kunnen worden op basis van welke informatie deze toestemming is gegeven.
c. Het inrichten van een privacyfunctie.
d. Privacy(bewustzijn) als vast onderwerp binnen planning- en controlecyclus en monitoring van het effect van maatregelen.

Eventueel kan het bovenstaande (onverplicht) worden aangevuld met het afleggen van verantwoording over de verwerking van persoonsgegevens in het jaarverslag van de Kiesraad of het voeren van specifiek ICT-beveiligingsbeleid. Hoewel beide mogelijkheden niet verplicht zijn, helpen deze maatregelen volgens de Autoriteit Persoonsgegevens wel om aan de toezichthouder te laten zien dat de Kiesraad

voldoet aan de eisen van de AVG. De staf kan overwegen op een later moment 5.1.2.e /5.1.2.e en 5.1.2.e te vragen hier voorstellen voor te doen.

2.2 Documentatieplicht
Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties maakt een onderscheid tussen de verantwoordingsplicht en de documentatieplicht, maar in de praktijk worden beide begrippen door elkaar heen gebruikt. Dat is logisch, want beide begrippen zijn zeer nauw met elkaar verweven. Bij het invullen van de rapportages richting het ministerie ben ik er vanuit gegaan dat de verantwoordingsplicht meer ziet op het vastleggen hoe met persoonsgegevens wordt omgegaan, terwijl de documentatieplicht de juistheid daarvan onderbouwd. De documentatieplicht gaat in die denkwijze aan de verantwoordingsplicht vooraf.

2.3 Informatieplicht
De informatieplicht vult het transparantiebeginsel in. Het houdt in dat de Kiesraad alle betrokkenen in begrijpelijke taal moet informeren over de wijze waarop hij omgaat met de verwerking van persoonsgegevens. Onder dit kopje vallen het actieve informatierecht[3] en het passief informatierecht.[4] De inhoud van deze communicatie volgt uit de verantwoordingsplicht. Onder de informatieplicht vallen o.a.: het hebben van privacybeschermingsbeleid, privacystatement(s), procedures voor de uitoefening van de rechten van betrokkenen (inzage, correctie, wissing enz.)

2.4 Samenhang
Wat is nu de samenhang tussen de drie genoemde plichten? De documentatieplicht legt verantwoording af over de invulling van de verantwoordingsplicht, terwijl de informatieplicht de verantwoordingsplicht naar buiten toe communiceert. Daaruit volgt ook een volgorde voor de implementatie: eerst kijken wat naar wat moet (documentatieplicht), dan vastleggen wat je doet (verantwoordingsplicht) en vervolgens uitleggen wat er is vastgelegd (informatielicht). Dit wordt voor ieder verwerkingsproces opnieuw gedaan.

3. Verantwoording
In de zomer van 2017 heeft de staf van het secretariaat van de Kiesraad, in lijn met mijn voorstel, besloten dat bij de implementatie van de AVG voorrang wordt gegeven aan de correcte en tijdige implementatie van deze verordening inzake de kerntaken van de Kiesraad. Dat wil zeggen: registratie van aanduidingen, kandidaatstellingsprocedure, vaststelling uitslag, (tijdelijke) benoemingen en verzoeken op grond van de Wet raadgevend referendum. Pas als de AVG voor deze verwerkingen geïmplementeerd is, komen de andere verwerkingen in beeld.

Toen in 2018 duidelijk werd dat de tijdige implementatie van de verordening niet gehaald zou worden, heb ik in mijn werk aan het bovengenoemde uitgangspunt twee uitgangspunten toegevoegd. Het eerste is dat de Kiesraad moet reageren op

---

[3] Zie hierover de kennisnotitie van 26 juni 2018 (documentkenmerk: 2018-0000498825).
[4] Zie hierover de notitie aan de staf d.d. 31 mei 2018 (documentkenmerk: 2018-0000325158).

vragen/verzoeken van externen die de verordening betreffen. Voorbeeld: toen Stb. de Kiesraad vroeg een verwerkerovereenkomst met haar aan te gaan in verband met FMP – een onderdeel dat buiten de kernactiviteiten valt – heb ik met voorrang gekeken of dit nodig is en een conceptreactie opgesteld.[5] Het tweede aanvullende uitgangspunt is dat als de Kiesraad een nieuw verwerkingsproces instelt – zoals gebeurt is bij het symposium van 29 juni 2018 – deze verwerking direct in overeenstemming met de AVG moet plaatsvinden. Op die manier: 1) wordt bredere aandacht binnen de organisatie voor de AVG bewerkstelligt, 2) wordt voorkomen dat de implementatie achter de werkelijkheid aan gaat lopen en 3) wordt ook voor derden duidelijk dat de Kiesraad wel degelijk in overeenstemming met de verordening werkt.

De AVG wordt per verwerkingsproces geïmplementeerd. De volgorde die ik daarin hanteert, is in paragraaf 2 uitgelegd: eerst kijken wat moet, dan vastleggen wat je intern doet en daarna de communicatie daarover naar buiten.

4. Huidige stand van zaken

De huidige stand van zaken is, wat betreft de prioritaire processen, opgenomen in een bijlage bij deze notitie. Verwerkingsprocessen die in augustus 2017 als 'van secondair belang' zijn gekwalificeerd zijn daarin niet opgenomen. Daar moet ik op een later moment nog naar kijken en het is goed mogelijk dat daarbij nog enkele aangedragen processen wegvallen.

Niet in het overzicht opgenomen, maar vermeldenswaardig:

1. Bij brief van 5 juni 2018 (documentkenmerk: 2018-0000327612) heeft de Kiesraad Stb. laten weten vooralsnog geen aanleiding te zien om met dit bedrijf een verwerkerovereenkomst te sluiten, omdat Stb. geen persoonsgegevens voor de Kiesraad verwerkt. De software die wij van Stb afnemen – FMP – draait uitsluitend op ons eigen computernetwerk. De inhoud hiervan is afgestemd met 5.1.2.e en 5.1.2.e Je hebt de brief zelf getekend.
2. 5.1.2.e is bezig met de verlenging van de raamovereenkomst met IVU voor OSV. Samen met 5.1.2.e en 5.1.2.e ben ik nagegaan of de AVG hier consequenties voor heeft. Onze conclusie is ook afgestemd met een AVG-specialist van BZK. Op 28 juni 2018 heb ik 5.1.2.e en 5.1.2.e twee documenten toegestuurd. Een document bevat de standaard Engelstalige verwerkerovereenkomst die IVU met klanten sluit: ik heb daar enkele kanttekeningen bij geplaatst. Het tweede document betreft een concept van de verwerkerovereenkomst zoals de Kiesraad (Lees: Staat der Nederlanden) die met IVU kan sluiten. Daarover verwacht ik in week 27 (2 t/m 6 juli) met 5.1.2.e door te kunnen praten.
3. Er is een notitie d.d. 26 juni 2018 met daarin informatie over de actieve informatieplicht van de Kiesraad (Documentkenmerk: 2018-0000498825). Deze was nodig in verband met de gewenste concretisering van de gevolgen voor onze primaire verwerkingsprocessen.

5. Planning

[5] Zie de brief van 5 juni 2018 (documentkenmerk: 2018-0000327612).

Het heeft weinig zin om hier een compleet overzicht te geven van de planning zoals ik die voor mij zie. Daarom volsta ik met een opsomming van activiteiten die op korte(re) termijn op de planning staan.

- 5.1.2.e heeft in de staf aangegeven te willen weten wat de AVG voor haar betekent. Ik begrijp die wens. Met de notitie 'AVG voor communicatiespecialisten' – die over de publicatie van persoonsgegevens op de website van de Kiesraad gaat – verwacht ik een groot deel van de onzekerheid weg te nemen. De notitie heb ik in mijn planning daarom naar voren geschoven. Een concept is begin deze week gereed.
- Ik ben gestart met een document 'Wijzigingen in werkprocessen' waarin concreet wordt ingegaan op de gevolgen die de AVG (incl. de UAVG en AAVG) heeft voor onze prioritaire werkprocessen. Te weten: registratie van aanduidingen (en aanwijzing gemachtigden), de kandidaatstellingsprocedure enzovoorts. Volgens mij komt dat aan jouw wens tegemoet.
- Er komt een nieuwe privacyverklaring. Mogelijk kan de Kiesraad met één privacyverklaring volstaan, maar de exacte inhoud daarvan is op dit moment nog niet volledig te bepalen (m.n. bewaartermijnen). Onder voorbehoud van wijzigingen, kan ervoor worden gekozen hier een hogere prioriteit aan te geven.
- Het verwerkingsproces waarin FMP wordt gebruikt is een secondair proces, maar daarbinnen natuurlijk erg belangrijk. Ik heb de indruk dat de staf aan dit verwerkingsproces een hoge(re) prioriteit wil toekennen en kom graag aan die wens tegemoet. Een kleine kanttekening van mijn kant is wel dat ook het Informatiepunt Verkiezingen van dit proces gebruikmaakt en dat er dientengevolge overeenstemming met BZK nodig is.
- De vijf prioritaire processen – zes als FMP wordt meegenomen – moeten snel in het register van verwerkingen allemaal ten minste de status 'oranje' hebben. Groen is alleen mogelijk als de verwerkerafspraken/-overeenkomsten ook zijn gemaakt en – gelet op wat er nog gedaan moet worden – is het wellicht productiever om daarop nog niet te rappelleren.
- Op iets langere termijn moet ik één aspect uit de notitie over het 'passief informatierecht' opnieuw bezien: de identificatie van personen. Mogelijk ben ik daarin te soft geweest. Het ministerie van Volksgezondheid Welzijn en Sport stelt veel zwaardere eisen.

Bijlage 1:
Wijzigingen in werkprocessen

De Algemene verordening gegevensbescherming (AVG)[1] maakt het noodzakelijk enkele wijzigingen aan te brengen in bestaande werkprocessen van de Kiesraad. De voorgestelde wijzigingen vloeien deels voort uit de Aanpassingswet Algemene verordening gegevensbescherming[2] – die de Kieswet aan de AVG heeft aangepast – en deels uit de verordening zelf. Soms is er een mogelijkheid om keuzes te maken. Waar dit het geval is, wordt dat in deze notitie telkens expliciet aangegeven. Waar de AVG niet leidt tot aanpassingen, is niets vermeld.

Reikwijdte:
Deze notitie ziet alleen op vijf belangrijkste werkprocessen voor de Kiesraad: de registratie van aanduidingen en de aanwijzing van gemachtigden, de kandidaatstellingsprocedure, de vaststelling van de verkiezingsuitslag, de (tussentijdse) (tijdelijke) benoeming van volksvertegenwoordigers en het raadgevend referendum. Aan de gevolgen van de AVG voor Postbus Kiesraad/Postbus Informatiepunt is een separatie notitie (Kenmerk: 2018-0000626545) gewijd.

1. Registratie aanduidingen & aanwijzing gemachtigden

Voorstel 1.1:
Publiceer de namen van gemachtigden van politieke groeperingen niet langer óók op de website van de Kiesraad.

Grondslag: art. 6 AVG: Rechtmatigheid van de verwerking.
Grondslag: art. 5 lid 1 onder c AVG: minimale gegevensverwerking
Referentie: Zie ook Voorstel 1.2

De publicatie van namen van gemachtigden van politieke groeperingen op de website van de Kiesraad is een verwerking van persoonsgegevens in de zin van de AVG. Deze verwerking is alleen rechtmatig als daarvoor een verwerkingsgrondslag bestaat als bedoeld in artikel 6 van de verordening; die is er niet. De Kiesraad kan overwegen om de gemachtigde expliciet toestemming te vragen voor de publicatie van zijn naam op de website van de Kiesraad. Dit vraagt extra administratieve handelingen.

Daarnaast kan twijfel rijzen over de vraag hoe de publicatie van deze persoonsgegevens – indien rechtmatig – zich verhoudt tot het in artikel 5 van de verordening neergelegde beginsel van minimale gegevensverwerking. Op grond van dit beginsel moet de verwerking van persoonsgegevens beperkt blijven tot wat noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens zijn verstrekt. Voor die doeleinden reikt de – wel wettelijke geregelde – publicatie van namen van (plaatsvervangend) gemachtigden in de Staatscourant voorafgaand aan decentrale verkiezingen.

Bedacht moet voorts worden dat het hier om de verwerking van bijzondere persoonsgegevens gaat (politieke opvatting en ras of etnische afkomstig, religieuze of levensbeschouwelijke overtuiging). Dat is, zoals de Kiesraad het nu doet, een verboden verwerking. Dat de gemachtigden soms bekende politici zijn, maakt geen verschil.

Voorstel 1.2:
Stuur politieke partijen drie maanden vóór de dag van de kandidaatstelling van elke verkiezing een brief, met daarin de namen van degenen die namens de vereniging zijn aangewezen als gemachtigde en plaatsvervangend gemachtigde ex art. G 1 lid 3 onder d van de Kieswet.

[1] 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).
[2] Wet van 11 juli 2018 tot aanpassing van wetten ter uitvoering van 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) (PbEU 2016, L 119) en de Uitvoeringswet Algemene verordening gegevensbescherming (Aanpassingswet Algemene verordening gegevensbescherming) (Stb. 2018, 247).

Grondslag: n.v.t.
Referentie: Zie ook Voorstel 1.1

Dit voorstel biedt een oplossing voor het probleem dat het secretariaat heeft willen oplossen door de namen van gemachtigden op zijn website te publiceren. Politieke partijen hebben hun administratie niet altijd op orde – wiens probleem moet dat zijn? – en vergeten soms wie zij als gemachtigde hebben aangewezen.

De termijn van drie maanden is voorgesteld, om politieke partijen gelegenheid te bieden hun gemachtigden te wijzigen. De Kiesraad moet op de veertigste (40) dag vóór de dag van de kandidaatstelling voor regionale en lokale verkiezingen de door hem geregistreerde aanduidingen van politieke partijen, voor zover de registratie daarvan onherroepelijk is, alsmede de namen van de gemachtigden en hun plaatsvervangers ter openbare kennis brengen in de Staatscourant. Uiteraard kan over die publicatie een nieuwsbericht worden gemaakt en mag daarin een hyperlink worden geplaatst naar de Staatscourantpublicatie.

Nu het register van aanduidingen niet langer in een Word-bestand staat, maar in een Excel-bestand, is het mogelijk het aanmaken van de brieven (inclusief de adressering) te automatiseren. Dat kan met Microsoft Office, zoals wij dit thans al gebruiken. De extra werkdruk voor het secretariaat zou dus behapbaar kunnen blijven, mits gebruik wordt gemaakt van de mogelijkheden die de software biedt.

Voorstel 1.3:
De Kiesraad moet de stukken die politieke partijen overleggen in het kader van een verzoek tot registratie van een aanduiding c.q. aanwijzing van een (plaatsvervangend) gemachtigde vernietigen zodra deze niet meer relevant zijn.

Grondslag: art. G 1 lid 9 Kieswet

Commented 5.1.2.e: De statuten blijven we nodig hebben om vast te stellen welke functionarissen bevoegd bestuur zijn. De statuten hoeven niet bij een wijzigingsverzoek opnieuw overgelegd te worden 5.2.1

5.2.1

Commented 5.1.2.e: Dat is juist. De statuten kun je blijven bewaren totdat de aanduiding onherroepelijk is geschrapt.

De Aanpassingswet Algemene verordening gegevensbescherming treft een regeling in de Kieswet voor de vernietiging van de stukken die een politieke partij aan het centraal stembureau overlegt bij de registratie van een aanduiding. De regeling is als volgt:

- Als een door een politieke groepering geregistreerde aanduiding onherroepelijk is geschrapt, moet het centraal stembureau alle documenten die op deze registratie zien direct vernietigen. Denk aan:
  a. Registratieverzoek
  b. Notariële akte waarin de statuten van de vereniging zijn vastgelegd
  c. Bewijs van inschrijving in het Handelsregister
  d. Betalingsbewijs van de waarborgsom
  e. Verklaring waarin de politieke groepering een gemachtigde en plaatsvervangend gemachtigde aanwijst.
- Als een politieke groepering een nieuwe verklaring van aanwijzing van een gemachtigde of plaatsvervangend gemachtigde overlegt, moet de voorgaande worden vernietigd.
- Het staat niet expliciet in de wet, maar het volgt er wel uit: bij een verzoek tot wijziging van een reeds geregistreerde aanduiding vernietig het centraal stembureau alleen de documenten die door een nieuw document zijn vervangen. Oftewel:
  a. Registratieverzoek.

Voorstel 1.4:
De kopieën van stukken betreffende de registratie van aanduidingen die aan de Kiesraadstukken worden toegevoegd, dienen op het in artikel G 1, negende lid, bedoelde moment eveneens vernietigd te worden.

Grondslag: Art. 5 lid 1 onder e AVG.

Commented 5.1.2.e: Dit zal in de praktijk lastig uit te voeren zijn aangezien de KR leden erover beschikken. Hier moeten we het nog even over hebben. Heeft mogelijk ook gevolgen voor archief cd-roms die 5.1.2.e 5.1.2.e jaarlijks voor de leden maakt.

Commented 5.1.2.e Idd. goed om het hierover nog te hebben. Is er bestaand beleid voor hoe leden van de Kiesraad met kiesraadstukken mogen omgaan?

Met artikel G 1, negende lid, van de Kieswet wordt uitvoering gegeven aan het in de verordening neergelegde beginsel dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk. Het secretariaat van de Kiesraad bewaart de genoemde documenten in DigiDoc in de map '05. Registratie politieke partijen'. Een kopie van het registratieverzoek en de bijbehorende documenten wordt ook altijd met de Kiesraad gedeeld en staat in de map '01. Kiesraad'. Ook die kopie moet worden vernietigd.

Voorstel 1.5:
De 'notitie van het secretariaat' bij registratieverzoeken kan beter geen persoonsgegevens bevatten.

Grondslag: Art. 5 lid 1 onder c AVG.

Commented 5.1.2e: Dit bespreek ik ook graag nader. Het raakt de vraag of de leden dit niet zelf ook moeten kunnen nagaan of ze vertrouwen wat het secretariaat hierover vaststelt. In dat geval hoef je bepaalde stukken wellicht ook niet meer met de leden te delen (kvK uittreksel bijv.). Maat je ontneemt hen dan wel mogelijkheden. Misschien moeten we de keuze bij de leden neerleggen.

Commented 5.1.2e: Prima. Om misverstanden te voorkomen: mijn voorstel hier is veel beperkter van aard.

De 'notitie van het secretariaat' bevat meestal persoonsgegevens. Een voorbeeld is de notitie die gevoegd is bij het verzoek tot registratie van de aanduiding 'KRUIS 33' dat de Kiesraad op 13 augustus 2018 heeft behandeld. In de Inleiding staat: "Op 4 juli 2018, aangevuld op 3 augustus 2018 met het betalingsbewijs van de waarborgsom, is het verzoek ontvangen van de politieke groepering 'KRUIS 33', ten deze vertegenwoordigd door 5.1.2e voorzitter, 5.1.2e vice-voorzitter en 5.1.2e secretaris-penningmeester, tot opneming van de aanduiding 'KRUIS 33' in het register van aanduidingen ten behoeve van de verkiezing van de leden van de Tweede Kamer der Staten-Generaal." Er kan discussie ontstaan over de vraag of het vermelden van de voorletters en namen van betrokkenen niet in strijd is met het beginsel van minimale gegevensverwerking. Als deze notities op hetzelfde moment worden vernietigd als de stukken bedoeld in artikel G 1, negende lid, van de Kieswet, dan is daar eenvoudiger overheen te stappen dan wanneer deze notities langer bewaard blijven. Als het de bedoeling is om deze notities langer te bewaren, bijvoorbeeld omdat zij historisch relevant worden geacht omdat zij een beeld geven van de wijze waarop de Kiesraad registratieverzoeken toetst, dan is het beter om in deze notities geen persoonsgegevens op te nemen. In het bovenstaande voorbeeld had volstaan kunnen worden met de melding dat de aanvraag door de voorzitter, vice-voorzitter en secretaris-penningmeester is ingediend. Mocht de aanvraag zijn ingediend door personen die hier op grond van de statuten niet toe bevoegd zijn, dan kan dit worden geconstateerd zonder de betrokkenen bij naam te noemen. Voor alle duidelijkheid: namen van verenigingen en aanduidingen van politieke groeperingen zijn geen persoonsgegevens en kunnen dus gewoon in de notitie gebruikt blijven worden.

Mochten de notities langer bewaard worden en zich de zeer onwaarschijnlijke situatie voordoen dat de steller zich genoodzaakt ziet toch persoonsgegevens in de notitie op te nemen, dan kan deze notitie ook worden geanonimiseerd op het moment dat het verzoek om registratie dient te worden vernietigd. Dit is evenwel een arbeidsintensieve oplossing. Vandaar dat het niet gebruiken van persoonsgegevens sterk de voorkeur heeft.

2. Kandidaatstellingsprocedure

Voorstel 2.1:
Geef een ieder die een kandidatenlijst inlevert niet alleen een ontvangstbevestiging, maar ook schriftelijke informatie over de verwerking van zijn persoonsgegevens in het verkiezingsproces. Tenzij de betrokkene hier expliciet geen prijs op stelt.

Grondslag: art. 13 lid 1 AVG: actief informatieplicht
Referentie: Zie ook Voorstel 1.1

Op grond van artikel 13 van de verordening is de Kiesraad verplicht, degene die een kandidatenlijst inlevert informatie te verstrekken over de verwerking van diens persoonsgegevens. Dat moet op het moment dat de kandidatenlijst wordt ingediend, tenzij deze informatie al eerder is verstrekt aan de indiener van de kandidatenlijst. Kan de Kiesraad gebruikmaken van deze uitzondering en de informatie al eerder verstrekken? De Kiesraad verstuurt zijn brief met informatie over de (aanloop naar) de dag van de kandidaatstelling naar de gemachtigde van de politieke groepering. Deze betrokkene hoeft niet noodzakelijkerwijs ook degene te zijn die de kandidatenlijst indient bij het centraal stembureau. Vaak is hij dat niet. In die gevallen zal de Kiesraad alsnog de informatie op de

dag van de kandidaatstelling moeten verstrekken. Hetzelfde geldt voor de situatie dat een kiesgerechtigde een blanco kandidatenlijst indient. Om deze twee redenen wordt voorgesteld degene die een kandidatenlijst indient niet alleen een ontvangstbevestiging te geven, maar ook informatie over de verwerking van zijn persoonsgegevens.

Voorstel 2.2:
Beperk het verstrekken van informatie over de verwerking van persoonsgegevens niet tot de verwerking van de persoonsgegevens van de indiener van de kandidatenlijst.

Grondslag: n.v.t.
Referentie: Zie ook Voorstel 2.1

In zijn advies over de Aanpassingswet Algemene verordening gegevensbescherming heeft de Kiesraad erop gewezen dat het voor derden mogelijk moeilijk te bevatten is dat degene die de kandidatenlijst indient actief geïnformeerd wordt over de verwerking van zijn persoonsgegevens, terwijl anderen, kandidaten bijvoorbeeld, daarover niet hoeven te worden geïnformeerd.[3] De minister heeft dit erkend, maar geen uitzondering willen maken op de actieve informatieplicht.[4] Om aan het bezwaar van de Kiesraad tegemoet te komen, kan besloten worden om onverplicht ook breder informatie te verstrekken rond het thema 'Persoonsgegevensbescherming en het verkiezingsproces'.

Commented [S1]: Kandidaatgegevens vallen niet onder de AVG toch?

Commented [S2]: Jawel. Er geldt echter geen informatieplicht, omdat de verwerking plaatsvindt op basis van een wettelijke verplichting (art. 14 lid 5 onder c AVG).

Voorstel 2.3:
Vernietig alle kandidatenlijsten en bijkomende stukken, met uitzondering van de instemmingsverklaringen, na de vaststelling van de verkiezingsuitslag.

Grondslag: Art. I 19 Kieswet
Grondslag: Art. 17a Kieswet (EP-verkiezing)
Grondslag: Art. S 15 Kieswet (EK-verkiezing)

De Aanpassingswet Algemene verordening gegevensbescherming verduidelijkt en verandert de regeling in de Kieswet voor de vernietiging van stukken. Verduidelijkt wordt dat niet alleen de kandidatenlijst en ondersteuningsverklaringen worden vernietigd, maar ook machtigingen, kopieën van identiteitsbewijzen en betalingsbewijzen. Centraal stembureaus bewaren alleen de instemmingsverklaring van kandidaten. Verandert is het moment waarop deze stukken vernietigd moeten worden. Dat schuift iets verder naar achteren, van "nadat onherroepelijk is beslist over de geldigheid van de ingeleverde lijsten", naar "na de vaststelling van de uitslag". Deze verandering houdt verband met het feit dat het betalingsbewijs van de waarborgsom – waar de naam en het rekeningnummer van de betaler op staan – pas kan worden vernietigd als, indien nodig, de waarborgsom is terugbetaald.

Voorstel 2.4:
Verleng de terinzagelegging van kandidatenlijsten en ondersteuningsverklaringen niet.

Grondslag: Art. I 3 Kieswet

De bij het centraal stembureau ingediende kandidatenlijsten en, indien vereist, ondersteuningsverklaringen worden door het centraal stembureau voor een ieder ter inzage gelegd. In de Kieswet was, en is, niet vastgelegd tot wanneer deze stukken ter inzage liggen. Voorheen werd aangenomen dat de terinzagelegging voortduurde totdat onherroepelijk was beslist over de geldigheid van de ingeleverde kandidatenlijsten, omdat deze stukken daarna vernietigd moesten worden. Het moment waarop de kandidatenlijst en de ondersteuningsverklaringen tegenwoordig vernietigd moeten worden, ligt verderop in de tijd; zie Voorstel 2.3. Men zou kunnen zeggen dat de levensduur van deze documenten daarmee is verlengd, maar er is geen reden om ook de duur van de terinzagelegging te verlengen.

Voorstel 2.5:

[3] Advies Kiesraad d.d. 14 augustus 2017 over Aanpassingswet Algemene verordening gegevensbescherming.
[4] Kamerstukken II 2017/18, 34 939, nr. 3, p. 6 (MvT).

In het draaiboek voor de kandidaatstelling moet gewaarborgd worden dat OSV-bestanden die op de dag van de kandidaatstelling op een digitale gegevensdrager worden ingeleverd, niet alleen veilig bewaard worden maar ook op tijd vernietigd. Vernietiging moet plaatsvinden op hetzelfde moment als de papieren equivalent van de documenten.

Grondslag: Art. 5 lid 1 onder c AVG

De Kieswet gaat uit van een papieren proces. Dat het centraal stembureau in de praktijk software ter beschikking stelt waarmee politieke partijen verkiezingsbescheiden grotendeels digitaal kunnen invullen, doet daar niets aan af. Het papieren proces is leidend en het digitale proces is de Kieswet onbekend. Dit verklaart ook waarom de Kieswet geen regels bevat voor de omgang met digitale bestanden die op de dag van de kandidaatstelling door politieke partijen aan de Kiesraad worden overgedragen. Dat wil echter niet zeggen dat deze gegevens onbeperkt bewaard mogen worden. De Kiesraad heeft op dit moment geen procedure geïmplementeerd die waarborgt dat persoonsgegevens die op een digitale gegevensdrager worden aangeleverd ten behoeve van de kandidaatstellingsprocedure, op enig moment systematisch worden vernietigd. Dat is wel noodzakelijk. Het zou verstandig zijn om dit in het draaiboek voor de kandidaatstelling op te nemen. Indien mogelijk moeten de gegevens tegelijk met de papieren gegevens worden vernietigd. Dat moment sluit het beste aan bij de Kieswet.

Voorstel 2.6:
Wees erop attent dat een reactie op een verzoek van een natuurlijk persoon die een beroep doet op in de AVG neergelegde rechten gelijk is gesteld met een appellabel besluit; ook als deze rechten in de verordening of de Kieswet buiten toepassing zijn verklaard.

Grondslag: Art. Z 11b Kieswet

De algemene verordening gegevensbescherming kent natuurlijke personen van wie persoonsgegevens worden verwerkt een aantal rechten toe. Bij de beantwoording van de vraag of een bepaald recht uit de verordening van toepassing is ten aanzien van een verwerking die plaatsvindt op grond van de Kieswet, moet de Kiesraad kijken naar de uitzonderingen die gelden uit hoofde van de verordening en de beperkingen waar de Kieswet zelf in voorziet. Dit verschilt per verwerking en moet dan ook voor elke verwerking afzonderlijk beoordeeld worden.[5] De soep lijkt in de praktijk echter wat minder heet gegeten te worden. De AVG leidt niet tot grote wijzigingen in het verkiezingsproces. De procedures blijven inhoudelijk grotendeels ongewijzigd. En in de kandidaatstellingsprocedure kan een burger zich nergens op een in de AVG neergelegd recht beroepen. Desondanks moet de Kiesraad zich ervan bewust zijn dat ook de reactie 'u kunt zich niet op recht x beroepen, want buiten toepassing / uitzondering in de verordening / …', in de Kieswet aan een appellabel besluit gelijk is gesteld. Op grond van artikel 2, eerste lid, van het (nog vast te stellen vernieuwde) Besluit mandaat en machtiging Kiesraad worden deze besluiten door de voorzitter van de Kiesraad ondertekend.

3. Vaststelling verkiezingsuitslag

Voorstel 3.1
De Algemene verordening gegevensbescherming heeft geen gevolgen voor de wijze waarop de Kiesraad, in zijn hoedanigheid van centraal stembureau, ingevolge de Kieswet de verkiezingsuitslag vaststelt.

De Kiesraad hoeft geen nadere invulling te geven aan de actieve informatieplicht. Op grond van artikel 14, vijfde lid, onder c, mag het verstrekken van informatie achterwege blijven als het verkrijgen van persoonsgegevens uitdrukkelijk is voorgeschreven in het nationale recht van een lidstaat en de persoonsgegevens niet rechtstreeks van de betrokkene zijn verkregen. Aan beide voorwaarden wordt voldaan.

De in de Algemene verordening gegevensbescherming neergelegde rechten zijn niet van toepassing. Het recht op inzage (art. 15 AVG) is ingevolge artikel P 27 van de Kieswet (nieuw) niet van toepassing. Hetzelfde geldt voor het recht op rectificatie (art. 16 AVG). Het recht op

[5] Kamerstukken II 2017/18, 34 939, nr. 3, p. 4 (MvT).

gegevenswissing is niet van toepassing, omdat de verwerking van persoonsgegevens plaatsvindt in het kader van de door de Kieswet voorgeschreven vaststelling van de verkiezingsuitslag (art. 18 lid 3 onder c AVG). Het recht op beperking van de verwerking (art. 18 AVG) is ingevolge artikel P 27 van de Kieswet (nieuw) niet van toepassing. het recht op overdraagbaarheid van gegevens (art. 20 AVG) is niet van toepassing, omdat de verwerking niet berust op toestemming van de betrokkene en niet op een civielrechtelijke overeenkomst.

Voorstel 3.2
De Kiesraad mag het geslacht van een kandidaat niet zelf opzoeken; ook niet voor statistische doeleinden. Daarvoor ontbreekt de rechtsgrondslag (art. 6 AVG).

Voorstel 3.3
Als de Kiesraad het belangrijk vindt om de man/vrouw-verhouding vast te stellen – daar is vraag naar vanuit de wetenschap, verkiezingswaarnemers en media – dan moet misschien een wijziging in de regelgeving worden overwogen die een toereikende grondslag biedt voor betrouwbare statische informatie.

Commented [ ]: Kandidaatgegevens vallen toch niet onder de AVG? Zie ook hierboven.

Commented [ ]: Jawel. Waarom denk jij van niet?

Als de uitslag van een verkiezing wordt vastgesteld, gaat ook altijd aandacht uit naar de verhouding tussen het aantal gekozen mannen en vrouwen. De Kieswet zelf biedt daarvoor geen grondslag. De vraag is: hoe komt de Kiesraad dan aan dat percentage? Kandidaten kunnen ervoor kiezen om hun geslacht op de kandidatenlijst aan te (laten) geven. Zie artikel H 2, vierde lid, Kiesbesluit. Zij zijn daar echter niet toe verplicht. En het centraal stembureau mag ingevolge de Algemene verordening gegevensbescherming niet extra persoonsgegevens van kandidaten verwerken teneinde een sluitende statistiek te krijgen. Oftewel: het centraal stembureau mag niet het geslacht van een kandidaat achterhalen om zo ook nauwkeurigere berekening te kunnen maken van het aantal gekozen mannen en vrouwen. De consequentie daarvan is dat de berekende statistische informatie (het percentage mannen en vrouwen) bijna altijd een foutmarge heeft; hoe meer gekozenen hun geslacht niet hebben vermeld, des te groter deze foutmarge. Als de Kiesraad nauwkeurige informatie wil delen – en daar is best iets voor te zeggen – dan is een wijziging in de regelgeving zeer wenselijk. Een wijziging in het Kiesbesluit – het vermelden van het geslacht niet langer optioneel, maar verplicht – is voldoende om alle benodigde informatie openbaar te maken. Daarmee komt deze informatie ook beschikbaar voor derden.

Commented [ ]: Volgens mij is dit niet zo, wij krijgen die gegevens. Al is het omdat volgens mij ook uit bijv. de instemmingsverklaring blijkt dat iemand een man of vrouw is.

Commented [ ]: Als het geslacht niet op de kandidatenlijst staat, staat het ook niet op de instemmingsverklaring. Mogelijk bedoel je de identiteitskaart. Het gegeven zelf toevoegen is echter een verwerking waarvoor de rechtsgrondslag ontbreekt en derhalve onrechtmatig.

Voorstel 3.4
Wees erop attent dat een reactie op een verzoek van een natuurlijk persoon die een beroep doet op in de AVG neergelegde rechten gelijk is gesteld met een appellabel besluit; ook als deze rechten in de verordening of de Kieswet buiten toepassing zijn verklaard.

Grondslag: Art. Z 11b Kieswet

Zie de toelichting onder voorstel 2.6.

4. (Tussentijdse) (tijdelijke) benoeming volksvertegenwoordigers

Voorstel 4.1
Vernietig documenten die samenhangen met de (tussentijdse) (tijdelijke) benoeming van leden in de Eerste Kamer, Tweede Kamer en het Europees Parlement nadat de zittingstermijn van het vertegenwoordigend orgaan is afgelopen.

Grondslag: Art. 5 lid 1 onder c AVG

Het in de verordening neergelegde beginsel van minimale gegevensverwerking vereist dat de Kiesraad persoonsgegevens alleen verwerkt – daaronder valt ook: bewaard – voor zover dit ter zake dienend is. Strikt genomen betekent dit dat, zodra in een vacature is voorzien en degene die benoemd is tot het vertegenwoordigend orgaan is toegelaten, alle documenten die op deze benoeming zien vernietigd moeten worden. Alleen W 2-verklaringen, die doorgaans zien op de gehele zittingsperiode van het vertegenwoordigend orgaan, moeten uit hun aard gedurende de hele zittingstermijn bewaard blijven. Om praktische redenen stel ik voor om vooralsnog dezelfde

termijn aan te houden voor de eerstgenoemde categorie documenten. Alle documenten die verband houden met de (tijdelijke) (tussentijdse) benoeming van volksvertegenwoordigers kunnen worden vernietigd, zodra na een daaropvolgende verkiezing meer dan de helft van de geloofsbrieven van de dan benoemde leden is goedgekeurd. Dit betekent dat DigiDoc onder de map '07. Tussentijdse benoemingen' alle dossiermappen vernietigd kunnen worden, met uitzondering van de mappen 'EP Tussentijdse Benoemingen 2014-2019', 'EK Tussentijdse Benoemingen 2015-2019)' en 'TK Tussentijdse Benoemingen 2017-2021'.

5. Raadgevend referendum

Door de inwerkingtreding van de Wet van 10 juli 2018 tot intrekking van de Wet raadgevend referendum (Stb. 2018, 214) op 11 juli – welke terugwerkende kracht heeft tot 10 juli – is dit onderdeel overbodig geworden en niet meer uitgewerkt.

Notitie

Onderwerp
Postbus Kiesraad / Informatiepunt Verkiezingen

Datum
13 juli 2018

Kenmerk
2018-0000626545

Onderdeel
Kiesraad

Blad
1 van 11

Aan
Staf
Van
5.1.2.e

1. Inleiding

Rond elke verkiezing zetten de Kiesraad en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties gezamenlijk het Informatiepunt Verkiezingen op. Bij dit Informatiepunt Verkiezingen kunnen ambtenaren, werkzaam bij decentrale overheden, vertegenwoordigers van politieke groeperingen en burgers terecht met al hun vragen over het Nederlands kiesrecht en het verkiezingsproces. Buiten het verkiezingsproces houdt het Informatiepunt Verkiezingen op te bestaan, maar worden de werkzaamheden ervan voortgezet door de Kiesraad onder de naam: Postbus Kiesraad. Het Informatiepunt Verkiezingen en Postbus Kiesraad zijn telefonisch en per e-mail bereikbaar.

Op 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG)[1] van toepassing geworden. Deze verordening heeft ook gevolgen voor het Informatiepunt Verkiezingen en Postbus Kiesraad. Daarop wordt in deze notitie ingegaan.

2. Verwerkingsverantwoordelijke

Voorstel 1:
Beslis of de Kiesraad en de minister van Binnenlandse Zaken en Koninkrijksrelaties gezamenlijk verwerkingsverantwoordelijk zijn voor het Informatiepunt Verkiezingen, of niet.

Het Informatiepunt Verkiezingen is een gezamenlijk initiatief van de minister van Binnenlandse Zaken en Koninkrijksrelaties en de Kiesraad. Als de minister en de Kiesraad gezamenlijk de doeleinden en middelen van de verwerking bepalen, dan zijn zij beiden gezamenlijk verwerkingsverantwoordelijk. Dat leidt ertoe dat,

[1] 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)

ingevolge artikel 26 van de verordening, de Kiesraad en de minister hun respectievelijke verantwoordelijkheden voor de nakoming van uit de AVG voortvloeiende verplichtingen moeten vastleggen.

> Wat leggen de Kiesraad en BZK dan vast?
> – Wie is verantwoordelijk voor het nakomen van de actieve informatieplicht zoals neergelegd in de artikelen 13 en 14 van de verordening?
> – Uit de gezamenlijke regeling moet blijken welke rol de minister en de Kiesraad vervullen, en wat de respectievelijke verhouding tot de betrokkene is. M.a.w. er moet schriftelijk worden vastgelegd waar die gezamenlijkheid uit bestaat.
> – De wezenlijke inhoud van de regeling moet aan de betrokkene beschikbaar gesteld. Dit kan samen met de informatie die de Kiesraad ingevolge de artikelen 13 en 14 van de verordening

Commented [512e]: Wat houdt dit concreet in?

Commented [512e]: Op grond van de AVG moet informatie worden verstrekt aan degene van wie persoonsgegevens worden verwerkt. Betrokkene moet bijvoorbeeld weten wie, welke gegevens met welke reden verwerkt. Uitgebreider in deze oudere notitie. Als de vraag zich voordoet, is het antwoord m.i. overigens: de Kiesraad.

Als de minister en de Kiesraad niet gezamenlijk de doeleinden en middelen van de verwerking bepalen, roept dit natuurlijk de vraag op waarom het Informatiepunt Verkiezingen een gezamenlijk initiatief wordt genoemd. Maar in dat geval is er geen enkele reden om het Informatiepunt Verkiezingen, naast Postbus Kiesraad, als afzonderlijke verwerkingsactiviteit in het register te vermelden. In dat geval zouden beide verwerkingsactiviteiten in een melding samengevoegd kunnen worden.

3. Verwerkingsgrondslag

Het verwerken van persoonsgegevens is alleen rechtmatig, als er een voldoende verwerkingsgrondslag is. Die is er. De verwerking is noodzakelijk voor de vervulling van een publieke taak, oftewel een taak van algemeen belang, in de zin van artikel 6, eerste lid, onder e, van de verordening. De Kiesraad is een adviesorgaan voor de regering en het parlement waar het de Kieswet en het Nederlandse verkiezingsproces betreft. Met wat fantasie zou men kunnen denken: een kennisinstituut. Vanuit die optiek bestaat ook de plicht voor de Kiesraad om mondeling of schriftelijk binnengekomen berichten te beantwoorden. Weliswaar houdt het in de Grondwet neergelegde petitierecht – art. 5 Grondwet – geen recht op een inhoudelijke reactie in, maar uit de Algemene wet bestuursrecht en de uitspraken van de Nationale Ombudsman~~ombudsprudentie~~ volgt toch dat een bestuursorgaan op z'n minst een ontvangstbevestiging moet sturen. Het primaire doel van de verwerkingsactiviteit laat zich als volgt omschrijven: "Degene die een vraag stelt voorzien van een passende reactie." De keuze voor deze rechtsgrondslag is overigens ambtelijk afgestemd met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.[2]

Commented [512e]: Is dit een bestaand woord?

Commented [512e]: Sorry, vaktaal. Bedoeld is: oordelen van de Nationale Ombudsman.

Bij het Informatiepunt Verkiezingen en Postbus Kiesraad heeft de Kiesraad ook een tweede doel. Dit secondaire doel kan als volgt worden geformuleerd: "De verwerking kan verder gebruikt voor het maken van statistische- en andere overzichten voor interne bedrijfsstatistiek, voor beleids- of wetenschappelijk onderzoek, voor de bedrijfsbeveiliging, het behandelen van geschillen en het doen uitoefenen van accountantscontrole." Voor het Informatiepunt Verkiezingen komt dit doel tot

[2] Zie de e-mail van 512.e van 14 juli 2017 (Kenmerk: 2018-0000626524).

uitdrukking in de rapportages van het Informatiepunt. Voor de Postbus Kiesraad komt dit doel tot uitdrukking in het jaarverslag van de Kiesraad.

4. Minimale gegevensverwerking

Voorstel 2:
Er hoeft geen verandering plaats te vinden in de categorieën van persoonsgegevens die worden verwerkt voor het Informatiepunt Verkiezingen of de Postbus Kiesraad.

Artikel 5, eerste lid, onder c, van de Algemene verordening bevat het beginsel van minimale gegevensverwerking. Dit houdt in dat de Kiesraad alleen persoonsgegevens mag verwerken, voor zolang dit ter zake dienend is en noodzakelijk om het gestelde doel te bereiken. De Kiesraad slaat klantcontacten op in FileMaker Pro 14 (FMP). De categorieën persoonsgegevens die daarbij worden opgeslagen zijn relevant en noodzakelijk voor het doel waarvoor zij worden opgeslagen. Er is dienaangaande geen wijziging nodig van het beleid.

De volgende gegevens worden in FileMaker Pro 14 (FMP) opgeslagen:

FMP-item	Omschrijving	Verwerkingsdoel
Melder als	Keuzemenu, met opties als: burger, politieke partij, gemeente.	Dit keuzemenu is noodzakelijk met het op het maken van statistische overzichten.
Achternaam		Noodzakelijk om de reactie specifiek aan de betrokkene te kunnen versturen.
Voornaam		Idem
Woonplaats		Idem
Website	Dit gegeven komt wel in FMP voor, maar wordt t.b.v. Postbus Kiesraad en/of Informatiepunt Verkiezingen niet gebruikt.	n.v.t.
E-mail	Wordt alleen ingevuld als de vraag per e-mail is binnengekomen of het antwoord per e-mail is gegeven.	Noodzakelijk om de reactie specifiek aan de betrokkene te kunnen versturen.
Telefoon	Wordt alleen ingevuld als de vraag per telefoon is binnengekomen of het antwoord per telefoon is gegeven.	Noodzakelijk om de reactie specifiek aan de betrokkene te kunnen versturen.
Organisatie	Concretisering van het veld 'melder'. Bijv. naam politieke partij, naam gemeente.	Dit keuzemenu is noodzakelijk met het op het maken van statistische overzichten.
Datum melding	Geen persoonsgegeven	
Datum afhandeling	Geen persoonsgegeven	
Behandelaar	Aan de hand van de initialen zijn	Noodzakelijk om de reactie

	medewerkers identificeerbaar. Weten met wie iemand eerder contact heeft gehad helpt een passende reactie te geven.	specifiek aan de betrokkene te kunnen versturen.
Melding via	Keuzemenu: e-mail / telefoon / anders. Geen persoonsgegeven	
Beantwoord:	Keuzemenu: ja/nee Geen persoonsgegeven	
Doorgestuurd	Keuzemenu: ja/nee Geen persoonsgegeven	
Door naar:	Naam van persoon/organisatie naar wie de melding is doorgestuurd.	Noodzakelijk om de reactie specifiek aan de betrokkene te kunnen versturen.
Trefwoord	Keuzemenu Geen persoonsgegeven	
Verkiezing	Keuzemenu Geen persoonsgegeven	
Omschrijving van de melding	Bevat de vraag.	
Aantekening	Bevat interne aantekeningen aangaan de afhandeling van de melding.	
Inhoud van de afhandeling	Bevat het antwoord. Geen persoonsgegevens	

Voorstel 3:
Maak een keuze tussen:
a. Ook bij vragen die per e-mail binnenkomen wordt niet de integrale inhoud van de e-mail in FMP geplaatst, maar formuleert de medewerker met eigen woorden in het kort wat de te beantwoorden vraag is.
b. Het blijft mogelijk om de inhoud van e-mails integraal in FMP op te nemen, maar medewerkers krijgen de aanwijzing mee daarbij het 'onderschrift' niet te kopiëren.

In de bovenstaande tabel is de FMP-item 'Omschrijving van de melding' oranje gekleurd. Dit veld hoeft geen persoonsgegevens te bevatten, maar doet dit soms wel. Als een vraag telefonisch wordt gesteld, bevatten deze velden meestal respectievelijk slechts een korte vraag en een kort antwoord. De melding in FMP bevat in dat geval geen extra persoonsgegevens. Komt de vraag evenwel per e-mail binnen, dan gebruiken medewerkers meestal gemakshalve de integrale inhoud van de binnenkomende e-mail als 'Omschrijving van de melding' en de integrale inhoud van de uitgaande e-mail als 'Inhoud van de afhandeling'.

Soms bevat een binnengekomen e-mail meer persoonsgegevens dan noodzakelijk is voor de verwerking. Die persoonsgegevens zijn in dat geval niet ter zake dienend en niet noodzakelijk en mogen dus niet verwerkt worden.[3] Binnengekomen e-mails worden bewaard. Het is onmogelijk om daar informatie uit te verwijderen. De Kiesraad kan zich echter wel inspannen om te voorkomen

[3] Art. 5 lid 1 onder c AVG.

dat deze persoonsgegevens nog verder worden verwerkt. Dat kan op twee manieren. De meest effectieve manier, is de werkwijze waarbij medewerkers vragen die per e-mail binnenkomen op dezelfde wijze in FMP noteren als telefonisch binnengekomen vragen. Oftewel: medewerkers nemen de inhoud van een ontvangen e-mail niet langer integraal in FMP op, maar formuleren de daarin opgenomen vraag in eigen woorden en noteren die in FMP. De antwoorden kunnen wel integraal in FMP opgenomen blijven worden. Vanuit privacyoogpunt is dit de beste keuze. Deze werkwijze heeft als nadeel dat het (her)formuleren van de in een e-mail gestelde vraag extra tijd kost, terwijl slechts een klein deel van de e-mails overbodige persoonsgegevens bevat.

Commented [5.1.2e]: Overnemen vraag zonder ondertekening volstaat toch meestal? Naam vraagsteller wordt toch ook in FMP opgenomen en dient ook een doel.

Commented [5.1.2e]: Dat is het voorstel onder B. Zie ook de alinea na het voorbeeld van een onderschrift.

Als een e-mail meer persoonsgegevens bevat dan ter zake dienend en noodzakelijk voor de verwerking, bevinden deze persoonsgegevens zich veelal in het onderschrift van de e-mail.

Voorbeeld van een onderschrift:

5.1.2e
Secretaris-directeur

KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag

T 5.1.2e / 5.1.2e
E 5.1.2e @kiesraad.nl
W www.kiesraad.nl

FOLLOW US ON twitter

100 JAAR KIESRECHT

Als medewerkers de onderschriften van e-mails niet meer in FMP plaatsen, wordt daarmee (grotendeels) voorkomen dat FMP meer persoonsgegevens bevat dan op grond van de Algemene verordening gegevensbescherming is toegestaan. Dit is een (bijna) sluitende oplossing die geen meerwerk oplevert. Daarbij moet wel een kanttekening worden geplaatst. Deze oplossing werkt niet in situaties waarin de extra (onnodige) persoonsgegevens deel uitmaken van de daadwerkelijke tekst in de e-mail. Dat komt evenwel nagenoeg niet voor.

Voorstel 4:
Medewerkers krijgen als aandachtspunt mee in het veld 'aantekening' in FMP geen persoonsgegevens te vermelden.

Soms kan het nodig zijn een aantekening bij een klantcontact op te nemen. Bijvoorbeeld omdat een klant twee vragen heeft gesteld, waarvan er één direct beantwoord is en de ander op een later moment beantwoord zal worden. Het aantekeningenveld kan ook gebruikt worden voor een sfeerimpressie van het klantcontact. Bijvoorbeeld als de medewerker het telefoongesprek vroegtijdig heeft beëindigd vanwege agressief taalgebruik en/of bedreigingen. Ik heb geen aanwijzing dat medewerkers in FMP-item 'Aantekening' persoonsgegevens van

betrokkenen noteren, maar het kan geen kwaad medewerkers erop attent te maken dat dit (inderdaad) niet de bedoeling is.

5. Informatieplicht

Voorstel 5:
De auto-responder op e-mails aan aan kiesraad@kiesraad.nl en informatiepunt@kiesraad.nl wordt aangepast.

De persoonsgegevens die de Kiesraad verwerkt bij de registratie van vragen, krijgt hij rechtstreeks van de betrokkene. Op grond van artikel 13 van de Algemene verordening gegevensbescherming berust op de Kiesraad een actieve informatieplicht. Over de actieve informatieplicht is een separate notitie opgesteld (kenmerk: 2018-0000498825). De enige uitzondering op deze actieve informatieverplichting doet zich voor als de betrokkene al over de informatie beschikt.

Postbus Kiesraad ontvangt vragen van overheden, politieke partijen en burgers via twee kanalen: e-mail en telefoon. Aan de actieve informatieplicht is bij e-mails het eenvoudigst te voldoen. Iedereen die een e-mail naar Postbus Kiesraad stuurt, krijgt nu standaard al automatisch een ontvangstbevestiging teruggestuurd. De tekst daarvan luidt als volgt:

> Geachte heer/mevrouw,
>
> Hiermee bevestigen wij de ontvangst van uw e-mail.
> Wij streven ernaar om uw e-mail binnen drie werkdagen in behandeling te nemen.
>
> Met vriendelijke groet,
>
> Secretariaat Kiesraad

Deze tekst zou aangevuld kunnen worden, met een melding over de verwerking van persoonsgegevens. Bijvoorbeeld:

> Geachte heer/mevrouw,
>
> Hiermee bevestigen wij de ontvangst van uw e-mail. Wij streven ernaar om uw e-mail binnen drie werkdagen in behandeling te nemen.
>
> Informatie over ons privacybeleid vindt u op onze website – www.kiesraad.nl – onder het kopje 'Privacy'. Mocht u, vanwege een met uw specifieke situatie verband houdende reden, bezwaar hebt tegen de registratie van deze e-mail, dan verzoeken wij u dit te melden.
>
> Met vriendelijke groet,
>
> Secretariaat Kiesraad

Het is waar dat met deze oplossing de te verstrekken informatie strikt genomen niet rechtstreeks aan de betrokkene wordt verstrekt. Veeleer wordt de betrokkene erop attent gemaakt dat zijn persoonsgegevens worden verwerkt en wordt hij

geïnformeerd over de plek waar hij zelf informatie over deze gegevensverwerking kan vinden. Het is evenwel een makkelijke manier om de AVG te implementeren. Mocht deze methode in de toekomst onvoldoende blijken, dan kan dit worden aangepast.

Voorstel 6:
Het Informatiepunt Verkiezingen wordt permanent beschikbaar. Onderzocht moet worden op welke wijze dit technisch te realiseren is.

Commented [5.1.2.d]: Ik zie zelf wel degelijk voldoende belang bij het onderscheid, maar ben met 5.1.2.e eens dat de vraagsteller hier geen last van moet hebben. Dat is volgens mij ook niet het geval, nu de nummers doorgeschakeld zijn en de mails doorgestuurd worden.

Commented [5.1.2.e]: De vraag is dan hoe je Voorstel 7 in de huidige situatie inpast. Wil de Kiesraad dat iedereen die het secretariaat van de Kiesraad belt voortaan ook eerst een bandje krijgt?

Ambtenaren werkzaam bij gemeenten, politieke partijen, burgers en andere geïnteresseerden kunnen met hun vragen over de Nederlandse Kieswet op één plek terecht: de Kiesraad. Maar de Kiesraad heeft twee gezichten: binnen reguliere verkiezingsperioden lijkt het wel of mensen contact hebben met een andere organisatie dan daarbuiten.

Rond reguliere verkiezingsperioden:	**Buiten reguliere verkiezingsperioden:**
Informatiepunt Verkiezingen E-mail: informatiepunt@kiesraad.nl Tel.: 070-4267329	Postbus Kiesraad E-mail: kiesraad@kiesraad.nl Tel.: 070 426 6266

Niet alleen de werknaam van de Kiesraad verschilt, maar ook het e-mailadres en het telefoonnummer. De vraag is: waarom? Wat is het feitelijke (naar buiten toe relevante) verschil tussen Informatiepunt Verkiezingen en Postbus Kiesraad? Beiden beantwoorden vragen over de Nederlandse Kieswet en het verkiezingsproces. Het verschil tussen Informatiepunt Verkiezingen en Postbus Kiesraad zit aan de achterkant. Voor de bemensing van Informatiepunt Verkiezingen worden externen aangetrokken. En er wordt intern gecommuniceerd dat het Informatiepunt Verkiezingen een gemeenschappelijk initiatief is van de Kiesraad en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, al is onduidelijk wat daarmee wordt bedoeld: zie Voorstel 1 van deze notitie. Bellers ervaren het verschil niet. Voor hen zijn de nieuwsbrieven die vanuit het ministerie van Binnenlandse Zaken en Koninkrijksrelaties worden verstuurd gewoon nieuwsbrieven van de Kiesraad. Bovendien: is het echt voorstelbaar dat vanuit Postbus Kiesraad inhoudelijk andere antwoorden worden gegeven dan vanuit Informatiepunt Verkiezingen? Neen. In het zeldzame geval dat de Kiesraad en het ministerie over een onderwerp niet op één lijn liggen, en geen compromis kunnen bereiken, wordt tot op heden altijd gestreefd naar een tekst die recht doet aan het standpunt van beide partijen. Of de onenigheid bestaat in een tijd dat de Kiesraad zich presenteert als Postbus Kiesraad of in een tijd dat hij zich presenteert als Informatiepunt Verkiezingen maakt daarbij geen verschil. En als nieuwe medewerkers starten bij Informatiepunt Verkiezingen, gebruiken zij de e-mails die vanuit de Postbus Kiesraad zijn verstuurd ook gewoon ter inspiratie.

Op het eerste gezicht lijkt dit voorstel zich veeleer te richten op heldere communicatie naar buiten dan op de implementatie van nieuwe regelgeving. Instemmen met dit voorstel, vergemakkelijkt echter de implementatie van de Algemene verordening gegevensbescherming, zie Voorstel 7.

Voorstel 7:
De tekst op het meldingsbandje van Informatiepunt Verkiezingen wordt gewijzigd.

Personen die telefonisch contact opnemen met het Informatiepunt Verkiezingen krijgen altijd eerst een bandje met een korte ingesproken tekst. Deze luidt nu: "Welkom bij het Informatiepunt Verkiezingen." Pas daarna gaan de telefoons op het Informatiepunt over en kan één van de medewerkers het telefoongesprek aannemen.

Consumenten die een bedrijf of instelling opbellen, krijgen ook vaak eerst een bandje te horen voordat zij iemand aan de lijn krijgen. De ingesproken tekst is dan vaak iets in de trant van: "U bent verbonden met x. Dit gesprek kan worden opgenomen ten behoeve van trainingsdoeleinden en kwaliteitscontrole." De Kiesraad zou de tekst op het bandje ook kunnen aanpassen. Bijvoorbeeld: "U bent verbonden met Informatiepunt Verkiezingen. Dit telefoongesprek kan geregistreerd worden. Informatie over ons privacybeleid vindt u op onze website – www.kiesraad.nl – onder het kopje 'Privacy'. Mocht u, vanwege een met uw specifieke situatie verband houdende reden, bezwaar hebt tegen de registratie van dit telefoongesprek, dan verzoeken wij u dit te melden." Voor een toelichting op de laatste zin, zie paragraaf 6 (Rechten van betrokkenen), art. 21 AVG.

Commented [5.1.2.1]: 5.2.1
Wellicht zou volstaan kunnen worden met een zin met een verwijzing naar het privacybeleid

Commented [5.1.2.2]: De keuze voor de laatste zin hangt samen met artikel 21 lid 4 van de AVG. Daarin staat dat deze informatie "duidelijk en gescheiden van enige andere informatie" moet worden weergegeven.
5.2.1

6. Rechten van betrokkenen

De Kiesraad slaat klantcontacten op in FileMaker Pro 14 (FMP). De klanten kunnen zich op de volgende, in de verordening neergelegde rechten beroepen:

Art. 15 AVG: Recht op inzage
De betrokkene heeft er recht op te weten of de Kiesraad van hem verwerkt en, wanneer dit het geval is, inzage te krijgen van deze persoonsgegevens. Daarnaast moet de Kiesraad aanvullende informatie verstrekken.

Art. 16 AVG: Recht op rectificatie
De betrokkene heeft het recht om rectificatie te vragen van onjuiste persoonsgegevens – bijvoorbeeld een verkeerd gespelde naam – en het recht om nog ontbrekende persoonsgegevens aan te vullen.

Art. 17 AVG: Recht op vergetelheid
De betrokkene heeft het recht te vragen om de hem betreffende gegevens te wissen, maar alleen als één van de in de verordening genoemde situaties zich voordoet.

Art. 18 AVG: Recht op beperking van de verwerking
In bepaalde gevallen heeft de betrokkene recht op beperking van de verwerking van de hem betreffende persoonsgegevens. Op dit recht zal in dit werkproces evenwel niet snel een (succesvol) beroep gedaan kunnen worden.

Art. 21 AVG: Recht van bezwaar
Gelet op de verwerkingsgrondslag – art. 6, eerste lid, onder e – heeft de betrokkene het recht om, vanwege met zijn specifieke situatie verband houdende redenen, bezwaar te maken tegen de opname van zijn persoonsgegevens in FMP. In dit geval mag de Kiesraad de gegevens van de betrokkene niet verwerken, tenzij er "dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene". Op grond van artikel 22, vierde lid, moet dit recht uiterlijk op het eerste contact met de betrokkene uitdrukkelijk onder de aandacht van de betrokkene worden gebracht. Bovendien moet deze informatie duidelijk van andere informatie gescheiden worden weergegeven. Om deze reden is bij het voorstel voor de tekst

op het bandje van Informatiepunt Verkiezingen de laatste zin over het recht op bezwaar toegevoegd. Overigens kan de behandelend ambtenaar, ook als de betrokkene zich op artikel 22 van de verordening beroept, nog wel de gegevens vastleggen die geen persoonsgegevens zijn. Bijvoorbeeld dat een burger heeft gebeld met vraag x, waarop antwoord Y is gegeven. Onder de naam kan dan 'Anoniem' worden genoteerd.

7. Bewaartermijn

Voorstel 8:
Gegevens die in FMP worden ingevoerd worden vijf kalenderjaren bewaard.

Op grond van artikel 5, eerste lid, onder c, van de verordening mag de Kiesraad persoonsgegevens alleen verwerken als deze gegevens ter zake dienend zijn en de verwerking beperkt blijft tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. De vraag is: hoe lang mag de Kiesraad namen en contactgegevens bewaren? Het bewaren van namen en contactgegevens is praktisch om terug te kunnen vallen op eerdere communicatie met de betrokkene. Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties hanteert de lijn van 5 jaar. Die termijn kan worden overgenomen. De vernietigingstermijn van 5 jaren gaat lopen na het verstrijken van het kalenderjaar waarin het proces is afgerond. Concreet: alle vragen (en persoonsgegevens) die in 2018 en 2019 over de Europees Parlementsverkiezing worden gesteld, behoren tot hetzelfde proces. De vernietigingstermijn van deze stukken gaat lopen na het verstrijken van het kalenderjaar waarin het proces is afgerond. Oftewel: de vernietigingstermijn van archiefbescheiden die betrekking hebben op de Europees Parlementverkiezing van 2019 vangt aan op 1 januari 2020. Vijf jaar later – 1 januari 2025 – worden de stukken vernietigd. Op deze manier wordt gegarandeerd dat bij de beantwoording van vragen over een verkiezing altijd teruggegrepen kan worden op de antwoorden die bij de laatstgehouden verkiezing voor hetzelfde vertegenwoordigende orgaan zijn gegeven op soortgelijke vragen.

Voorstel 9:
Voor in- en uitgaande e-mail geldt dezelfde bewaartermijn als voor FMP.

De bewaarcyclus is niet alleen relevant voor FMP, maar ook voor de e-mails. Daarvoor kan dezelfde bewaartermijn worden gehanteerd. Het gaat per slot van rekening om dezelfde gegevens.

Voorstel 10:
Introduceer een nieuw systeem om e-mails te archiveren. Streef naar een 'clean and mean'-structuur. Op pagina 11 van deze notitie staat een suggestie.

Op dit moment wordt bij het bewaren van e-mails al een onderscheid gemaakt tussen e-mails die binnenkomen in de periode dat er een Informatiepunt Verkiezingen is en e-mails die binnenkomen als er geen Informatiepunt Verkiezingen is. Deze structuur zag er op 6 augustus 2018 als volgt uit:

Postbus Informatiepunt:	**Postbus Kiesraad:**

- Behandelde e-mails
  - 11. Gemeenteraadsverkiezingen en EP-verkiezing
  - 12. Tussenperiode vanaf juni 2014
  - 13. PS, AB, ER, EK
  - 15. Raadgevend referendum 2016
  - 17. Tweede Kamerverkiezing
  - 19. GR en RR 2018
  - Handige e-mails
  - 2010 Herindelingsverkiezingen
  - 2011 Eerste Kamerverkiezing
  - 2011 Provinciale Statenverkiezingen
  - Mails HSB's deelnemende partijen
  - TK 2017
- Hertellingen GR/NF 2018
- Nieuwsbrieven BZK
  - 1. Nieuwsbrieven
  - 1. Gemeenteraadsverkiezingen 2010
  - 2. Tweede Kamerverkiezing 2010
  - 3. Herindelingsverkiezingen 2010
  - 4. Provinciale Statenverkiezingen 2011
  - 2014
  - 2015
  - 2016
  - 2017
- OSV
- OSV 2018
- Standaard e-mails op veelgestelde vragen.
  - 2010 Gemeenteraadsverkiezingen
  - 2010 Herindelingsverkiezingen
  - 2010 Tweede Kamerverkiezing
  - 2011 Eerste Kamerverkiezing
  - 2011 Provinciale Statenverkiezingen
- Verkiezingsbestanden/OSV
	- a. Aanmeldingen symposium 29-6-2018
	- a. Essaywedstrijd
	- Aanmeldingen symposium 18 juni 2015
	- Aanmeldingen vrijwilligers 24 mrt 2018
	- Behandelde e-mails
	  - 05. Tussenperiode 2009
	  - 11. Tussenperiode 2011
	  - 12. Tussenperiode 2012
	  - Diversen najaar 2012
	  - Diversen zomer 2012
	  - 13. Tussenperiode 2013
	  - Standaardantwoorden
	  - 14. Tussenperiode 2014
	  - 15. Tussenperiode 2015
	  - 16. Tussenperiode 2016
	  - 17. Tussenperiode 2017
	  - Hoofdstembureau
	  - Verslag
	  - 18. Tussenperiode 2018
	- Controle uitslag

Wat opvalt, is het gebrek aan structuur in de mappen; met name bij het Informatiepunt Verkiezingen. Binnen het Informatiepunt Verkiezingen zijn maarliefst drie mappen waarin e-mails staan die betrekking hebben op de in 2010 gehouden reguliere gemeenteraadsverkiezingen. Ook e-mails over OSV staan verspreid. Diverse nieuwsbrieven van BZK zijn in Outlook bewaard, maar de nieuwsbrieven over de laatstgehouden gemeenteraadsverkiezingen staan uitsluitend nog in DigiDoc. Kortom: er ontbreekt structuur.

In lijn met het voorstel onder Voorstel 6, stel ik de volgende structuur voor:

Informatiepunt Verkiezingen	**Postbus Kiesraad**
- Behandelde e-mails	- Behandelde e-mails

- Binnen verkiezingsperiode:
  - 2014: GR & EP
  - 2015: AB, PS, ER & EK
  - 2016: RR
  - 2017: TK
  - 2018: GR en RR
  - 2019: AB, PS, ER, KK, EK, & EP
- Buiten verkiezingsperiode
  - Tussenperiode 2013
  - Tussenperiode 2014
  - Tussenperiode 2015
  - Tussenperiode 2016
  - Tussenperiode 2017
  - Tussenperiode 2018
	- 2013
	- 2014
	- 2015
	- 2016
	- 2017
	- 2018

Toelichting:
Vragen aan de Kiesraad over de Kieswet of het Nederlandse verkiezingsproces komen in de nieuw voorgestelde opzet alleen binnen bij Informatiepunt Verkiezingen. Uiteraard kan een e-mail daar (zo nodig) naartoe worden gesleept. Het onderscheid tussen verkiezingsperiodes en niet-verkiezingsperiodes blijft behouden. Dit vergemakkelijkt het maken van rapportages door het Informatiepunt Verkiezingen tijdens verkiezingsperiodes. De namen van de organen waarvoor een verkiezing wordt gehouden, worden consequent afgekort:

AB = algemeen bestuur van het waterschap
EK = Eerste Kamer der Staten-Generaal
EP = Europees Parlement
ER = eilandsraad
GR = gemeenteraad
KK = kiescollege
PS = provinciale staten
RR = raadgevend referendum
TK = Tweede Kamer der Staten-Generaal

Onder de eigen map van een groep verkiezingen kunnen desgewenst submappen worden aangemaakt voor nieuwsbrieven en e-mails over OSV. De voorgestelde structuur geeft meer duidelijkheid en maakt het eenvoudig om e-mails op tijd te vernietigen. Op 1 januari 2019 wordt de map 'Tussenperiode 2019' aangemaakt bij Informatiepunt Verkiezingen en wordt de map 'Tussenperiode 2013' (met inhoud) gedelete.

8. Andere verwerker(s)

Voor deze verwerkingsactiviteit wordt geen gebruik gemaakt van de diensten van andere verwerkers. Zie hierover ook de brief van de Kiesraad d.d. 5 juni 2018 aan Stb Automatisering & Advies B.V. (kenmerk: 2018-0000327612).

Notitie

Onderwerp
AVG voor communicatiespecialisten

Datum
5 juli 2018

Kenmerk
2018-0000594824

Inlichtingen
5.1.2.e
T 070 426 6266
F 070 751 7078

Blad
1 van 6

Aan
Staf
Van
5.1.2.e

1. Inleiding

Op 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing geworden. Wat zijn de gevolgen van deze verordening voor communicatiespecialisten? Die vraag is niet alomvattend te beantwoorden. Wel biedt deze notitie een handreiking voor publicaties op de website.

De notitie begint met een paragraaf over het begrip 'open normen' (§ 2). Kennis van dit begrip is belangrijk voor een goed begrip van de status van deze notitie. De AVG bevat namelijk veel open normen die in deze notitie nader worden ingekleurd. Daarna volgen enkele rubrieken, waarin telkens enkele concrete handvatten worden gegeven. Sommige handvatten zal de lezer als vanzelfsprekend ervaren. Dat komt omdat er al veel goed gaat. Iedere rubriek begint met een opsomming van concrete normen, gevolgd door uitleg en concrete tips om AVG-proof te handelen. De in deze notitie opgenomen rubrieken zijn: medewerkers (§ 3), foto's en video's (§ 4) en nieuwsberichten (§ 5).

2. Open normen

De AVG bevat heel veel zogenoemde 'open normen'. Simpel gezegd zijn dit verplichtingen waarvan de inhoud niet vast staat; afhankelijk van de omstandigheden van het geval moet de norm nader worden geconcretiseerd. Een voorbeeld van een open norm is de in de AVG neergelegde verplichting om bij de verwerking van persoonsgegevens zorg te dragen voor "passende beveiliging".[1] Wat de Kiesraad concreet moet doen om te kunnen zeggen dat de beveiliging

[1] Art. 5 lid 1 onder f AVG.

passend is, hangt af van verschillende factoren waaronder: het soort persoonsgegevens dat verwerkt wordt, de gevoeligheid van de verwerking en de technische mogelijkheden tot bescherming. Een kenmerk van open normen is dus dat zij in de praktijk nader moeten worden ingevuld. Of dit op de juiste wijze wordt gedaan, is uiteindelijk aan de Autoriteit Persoonsgegevens.

Open normen hebben nog een ander kenmerk: ze zijn fluïde. Dat wil zeggen: wat de norm precies inhoud voor een bepaalde situatie, kan in de loop der tijd veranderen. Voorbeeld: nieuwe technieken in de informatietechnologie kunnen noodzaken andere concrete maatregelen te nemen in informatiebeveiliging. Een tweede kenmerk is dus dat de invulling van een open norm nooit helemaal vast staat. Het is mogelijk dat veranderingen in de regelgeving, jurisprudentie, uitspraken van de Autoriteit Persoonsgegevens en gewijzigde maatschappelijke opvattingen op enig moment tot bijstelling nopen van de concrete handvatten die in deze notitie worden gegeven.

Open normen zijn door hun flexibiliteit toekomstbestendig, maar vereisten wel maatwerk. Voor deze notitie is voor dit maatwerk aangesloten bij algemeen geaccepteerde opvattingen inzake de bescherming van persoonsgegevens. De notitie is afgestemd met een gespecialiseerd jurist van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

3. Medewerkers

3.1	Contactgegevens van medewerkers, privé en zakelijk, worden nooit aan personen verstrekt die niet werkzaam zijn bij het secretariaat van de Kiesraad.
3.2	Namen en foto's van medewerkers mogen niet zonder toestemming van medewerkers op de website of in een jaarverslag worden gepubliceerd. De Kiesraad moet kunnen aantonen dat er toestemming is verleend en op basis van welke informatie deze toestemming is verleend.

Commented [[redacted]]: Hoe zit dat met persoonsgegevens medewerkers op adviezen en onder mailtjes (Informatiepunt)? Of is hier bedoeld: (verstrekt) door anderen dan henzelf?

De Kiesraad verwerkt niet alleen persoonsgegevens van derden, maar ook van zijn eigen medewerkers. Ook daarop is de Algemene verordening gegevensbescherming van toepassing.

Handreiking 3.1:
Deze handreiking houdt verband met het beginsel van integriteit en vertrouwelijkheid, zoals neergelegd in artikel 5, eerste lid, onderdeel e, van de AVG. Het is een passende organisatorische maatregel om te voorkomen dat

persoonsgegevens van medewerkers niet ongeoorloofd of onrechtmatig worden verwerkt. Deze handreiking ziet niet alleen op het de privégegevens van medewerkers. Dat komt omdat het grondrecht op bescherming van persoonsgegevens volgens de Autoriteit Persoonsgegevens ook op de werkvloer geldt. Het zakelijke e-mailadres en telefoonnummer vallen er dus ook onder.

Hoe dan wel?
Noteer de contactgegevens van de derde. Speel zijn/haar vraag samen met de contactgegevens door aan de collega die de vraag kan beantwoorden.

Handreiking 3.2
Deze handreiking houdt verband met twee beginselen: dat van minimale gegevensverwerking zoals neergelegd in artikel 5, eerste lid, onder c, van de verordening en het beginsel van behoorlijkheid, zoals neergelegd in artikel 5, eerste lid, onder a.

De Kiesraad mag persoonsgegevens van medewerkers alleen verwerken, voor zover dit noodzakelijk is voor de doeleinden waarvoor zij zijn verkregen.[2] Het is niet noodzakelijk om namen, functies en foto's van medewerkers van de Kiesraad op de website te publiceren of in een jaarverslag. Deze handreiking is gebaseerd op een informatiebrochure van 28 januari 2014 van het College bescherming persoonsgegevens waar door de Autoriteit Persoonsgegevens naar wordt verwezen. Daarin staat letterlijk: "Plaats niet zomaar gegevens van uw werknemers, zoals naam, functie en foto, op uw (bedrijfs)website."

Commented [ ]: Dit klinkt overigens naar mijn idee niet heel categorisch (verbiedend)...

Hoe dan wel? jaarverslag
In het jaarverslag kan worden volstaan met het noemen van het totaal aantal fte's en het totaal aantal medewerkers.

Hoe dan wel? (groeps)foto van medewerker(s)
De naam, functie en de foto van een medewerker mag alleen op de website van de Kiesraad worden gezet, als de betreffende medewerker daar ondubbelzinnig toestemming voor heeft gegeven. Om geldige toestemming aan te tonen, moet de Kiesraad kunnen laten zien op basis van welke informatie de betrokken personen de toestemming hebben gegeven. het is dus onvoldoende om alleen de toestemming zelf vast te leggen.[3]

---

[2] Zie ook overweging 39 bij de verordening.
[3] Art. 7 lid 1 AVG.De bepaling benadrukt dat de verwerkingsverantwoordelijke de toestemming moet kunnen aantonen en noemt zowel schriftelijke als mondelinge toestemming. Overweging 42 van de verordening is daarmee in lijn.

Daaraan voorafgaand moet de medewerker dan wel de in artikel 13 van de verordening bedoelde informatie hebben ontvangen. Zie hierover uitgebreid de notitie van 26 juni 2018 (kenmerk: 2018-0000498825).

> **Informatie aan medewerkers over persoonsgegevensverwerkingen:**
> Over deze onderwerpen moet een medewerker informatie hebben ontvangen alvorens hij toestemming geeft voor de verwerking van zijn persoonsgegevens in het jaarverslag en/of de website:
> - Identiteit en contactgegevens van de verwerkingsverantwoordelijke (= Kiesraad).
> - De persoonsgegevens die verwerkt worden.
> - Het doel waarmee deze persoonsgegevens verwerkt worden.
> - De juridische grondslag van de verwerking.
> - Informatie over wie deze persoonsgegevens ontvangt.
> - De bewaartermijn van de persoonsgegevens.
> - De rechten van de medewerker. Te weten: recht op inzage, recht op rectificatie, recht op wissing en recht op beperking van de verwerking.
> - Dat het de medewerker volkomen vrij staat geen toestemming te verlenen, en dat deze te allen tijde de mogelijkheid heeft de gegeven toestemming weer in te trekken.
> - Contactgegevens functionaris voor gegevensbescherming.
> - De mogelijkheid een klacht in te dienen over de verwerking van persoonsgegevens bij de Autoriteit Persoonsgegevens.

Deze informatie kan meegezonden worden met de uitnodiging voor de fotoshoot. Punt van aandacht is ook dat de toestemming vrijelijk moet zijn verkregen. Medewerkers mogen op geen enkele manier onder druk worden gezet, of zich onder druk gezet voelen, om de benodigde toestemming te verlenen. Het moet duidelijk zijn dat iedereen vrij is te weigeren en dat dit geen enkele (negatieve) consequentie zal hebben. Bovendien hebben medewerkers ingevolge artikel 7, derde lid, van de verordening altijd het recht om hun toestemming in te trekken. Hoewel het intrekken van de toestemming de eerdere publicatie van hun foto niet onrechtmatig maakt, maakt de intrekking verder gebruik van die foto dat wel. Voor groepsfoto's, al dan niet met medewerkers getarget (zoals nu op de website van de Kiesraad), geldt hetzelfde regime. De groepsfoto die thans op de website staat voldoet niet aan deze eisen.

4. Nieuwsberichten

4.1	Nieuwsberichten over benoemdverklaringen van nieuwe leden van vertegenwoordigende organen mogen de namen van de benoemden bevatten.

4.2	Nieuwsberichten naar aanleiding van een openbare zitting van de Kiesraad of een symposium kunnen inclusief foto's worden gepubliceerd.
4.3	Nieuwsberichten kunnen desgewenst ongelimiteerd vindbaar blijven op de website van de Kiesraad.

In artikel 43 van de Uitvoeringswet Algemene verordening gegevensbescherming is geregeld, dat de AVG voor een groot deel niet van toepassing is als persoonsgegevens uitsluitend voor journalistieke doeleinden worden verwerkt. Deze uitzondering heeft bijvoorbeeld tot gevolg dat als persoonsgegevens worden verwerkt met het oog op een journalistiek doel, de personen op wie deze persoonsgegevens betrekking hebben geen beroep kunnen doen op in de verordening neergelegde rechten zoals het recht op inzage, het recht op rectificatie en het recht op gegevenswissing.[4] Om persoonsgegevens voor journalistieke doeleinden te verwerken hoeft men geen journalist te zijn. Ook het publiceren van een nieuwsbericht op de website van de Kiesraad valt waarschijnlijk onder de uitzondering. Alle andere onderdelen van de website, doen dit niet.

Sommige onderdelen van de AVG zijn wel van toepassing op nieuwsberichten die de Kiesraad publiceert. Dit zijn de belangrijkste:

- De beginselen die in de verordening zijn vastgelegd, gelden ook voor de publicatie van nieuwsberichten. Voorbeelden:
  - Beginsel van minimale gegevensverwerking.
    Dit beginsel houdt in dat de verwerking toereikend moet zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt. Dat het vermelden van een persoonsgegeven *leuk* of *interessant* kan zijn, is onvoldoende reden om daartoe over te gaan.
  - Beginsel van juistheid
    Dit beginsel houdt in dat er moet nauwkeurig worden gewerkt. De Kiesraad moet redelijke maatregelen nemen om de persoonsgegevens die onjuist zijn, onverwijld te wissen of te rectificeren. Aan dit beginsel wordt nu al invulling gegeven door elk nieuwsbericht vóór publicatie door een jurist te laten lezen.
- De verwerking is alleen rechtmatig als daar een geldige verwerkingsgrondslag voor bestaat.
  Bij een nieuwsbericht over de benoemdverklaring van een kandidaat kan men zeggen dat de verwerking noodzakelijk is voor de behartiging van een taak van algemeen belang: artikel 6, eerste lid, onder e, van de verordening. Dit algemeen belang zit hem erin dat de uitslag van een verkiezing in een

[4] Art. 43 lid 2 UAVG.

openbare zitting is vastgesteld, er een vacature is ontstaan en het voor kiezers belangrijk is om zich te kunnen informeren over de wijze waarop de voorzitter van het centraal stembureau tot de benoeming van een andere kandidaat is gekomen.
Ook een nieuwsbericht over het verloop van een openbare zitting van de kiesraad vindt zijn grondslag in de publicatie ter behartiging van een taak van algemeen belang. De zitting is openbaar en door publicatie van een nieuwsbericht kan een groter deel van het electoraat daar kennis van nemen.

- Als iemand materiële of immateriële schade heeft geleden als gevolg van een inbreuk op de AVG in een nieuwsbericht, kan hij op grond van artikel 82 van de verordening schadevergoeding eisen.
- In een nieuwsbericht op de website van de Kiesraad mogen ook zogenoemde bijzondere categorieën van persoonsgegevens – zoals iemand politieke voorkeur – worden verwerkt, maar alleen als dit noodzakelijk is voor het journalistieke doel. Bij een nieuwsbericht over de benoeming van kandidaat X van de lijst van Politieke Groepering Y is dit relevant. De politieke partij die nieuwe leden van de Kiesraad aanhangen is niet relevant en mag derhalve niet worden gepubliceerd.

Tot slot nog een enkele opmerking over het gebruik van foto's bij nieuwsberichten. Een foto is een persoonsgegeven als iemand herkenbaar in beeld wordt gebracht. Hiervan is bijvoorbeeld sprake als tijdens een openbare zitting foto's worden gemaakt van de leden van de Kiesraad. Foto's van het publiek zijn geen persoonsgegeven omdat het publiek doorgaans met behulp van de foto nog niet eenvoudig te identificeren is. Dat geldt in ieder geval voor algemene overzichtfoto's van het publiek (van achter genomen). De vooruitgang in de informatietechnologie gaat echter snel en computers zijn al in staat om personen van foto's te herkennen. Gelet daarop is enige terughoudendheid met foto's, waarop personen uit het publiek in beeld zijn, wenselijk.

Notitie

Onderwerp
Grotere vraagstukken rond de AVG

Datum
16 augustus 2018

Kenmerk
2018-0000719019

Inlichtingen
5.1.2.e
T 070 426 6266
F 070 751 7078

Blad
1 van 5

Aan
Staf
Van
5.1.2.e

1. Inleiding

Bij de implementatie van de Algemene verordening gegevensbescherming doen zich een aantal vraagstukken voor die zich op een ander niveau afspelen. Mogelijk is het wenselijk enkele daarvan ook aan de Kiesraad zelf voor te leggen.

waarover op een hoger niveau besloten moet worden. Deze zijn in deze notitie gebundeld.

Voorstel 1:
Kiest de Kiesraad ervoor dezelfde persoon als Functionaris voor Gegevensbescherming aan te wijzen als het ministerie van Binnenlandse Zaken en Koninkrijksrelaties?

Op grond van artikel 37, eerste lid, onder a, van de Algemene verordening gegevensbescherming zijn overheidsinstanties en overheidsorganen verplicht om een Functionaris voor Gegevensbescherming (FG) aan te wijzen. De Kiesraad is een zelfstandig bestuursorgaan dat onderdeel uitmaakt van de Staat der Nederlanden en valt derhalve onder deze verplichting.

Wat doet een FG?
De taken die een Functionaris voor Gegevensbescherming minimaal verricht staan opgesomd in artikel 39 van de verordening. De Functionaris heeft vijf taken. Hij:

a. Informeert en adviseert de Kiesraad over zijn verplichtingen aangaande de bescherming van persoonsgegevens.
b. Ziet toe op de naleving van de verordening door de Kiesraad en het door hem vastgestelde beleid aangaande gegevensbescherming. Daaronder valt onder andere dat hij toeziet op de verantwoordelijkheden, de bewustwording en de opleiding van medewerkers waar het gegevensbescherming betreft.
c. Brengt advies uit over gegevensbeschermingseffect-beoordelingen (PIA's) en ziet toe op de uitvoering daarvan.

d	Werkt, indien nodig, samen met de Autoriteit Persoonsgegevens.
e.	Is contactpunt met de Autoriteit Persoonsgegevens.

Hoewel de verordening er niet aan in de weg staat om een FG binnen de eigen organisatie te benoemen (art. 37 lid 6 AVG), is dit gelet op de noodzakelijke kennis, de taken die aan de FG worden toegekend en zijn positie, niet aantrekkelijk in een kleine organisatie. Ik raad daarom aan om een externe Functionaris voor Gegevensbescherming aan te wijzen. Vooralsnog is er, ook door het ministerie, vanuit gegaan dat de Kiesraad dezelfde Functionaris voor Gegegevensbescherming heeft als het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Dat is echter niet noodzakelijk en dient in dat geval nog wel met de betrokkene te worden overeengekomen. Dat is nog niet gedaan.

Commented [5175]: Op welke manier?

Commented [5176]: Een overeenkomst. We zouden kunnen beginnen met een brief om te vragen of hij onze FG wil zijn.

Het gebruikmaken van een externe Functionaris voor Gegevensbescherming zal kosten met zich meebrengen, omdat de betrokkene immers ook werkzaamheden zal uitvoeren ten behoeve van de Kiesraad.

Het aanwijzen van dezelfde persoon als Functionaris voor Gegegevensbescherming als het ministerie van Binnenlandse Zaken en koninkrijksrelaties – betrokkene is ook al FG voor het ministerie van Justitie en Veiligheid – is een praktische keuze waarbij de bestaande situatie nagenoeg hetzelfde blijft. Mocht in de praktijk blijken dat deze FG te weinig aandacht heeft voor de bijzondere noden van een kleine organisatie, dan kan uiteraard op een later moment een andere FG worden gezocht.

Voorstel 2:
Maak een e-mailadres aan voor de Functionaris voor Gegevensbescherming: fg@kiesraad.nl en stuur alle e-mail die daarop binnenkomt automatisch door naar het e-mailadres van de Functionaris.

In de algemene privacyverklaring die nu op de website van de Kiesraad staat, wordt er vanuit gegaan dat de Functionaris voor Gegevensbescherming van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties ook de Functionaris voor de Kiesraad is. Ook zijn BZK e-mailadres staat op onze website. Los van het feit dat deze e-mail in de praktijk automatisch wordt doorgestuurd naar zijn primaire e-mailadres van het ministerie van Justitie en Veiligheid, is het mijns inziens, gelet op de onafhankelijke positie van de Kiesraad, beter om zelf een afzonderlijk e-mailadres aan te maken voor onze Functionaris en de daarop binnenkomende e-mails door te sturen. De betrokkene zou bijvoorbeeld bereikbaar kunnen zijn op 'fg@kiesraad.nl'. Mocht de Kiesraad in de toekomst iemand anders als Functionaris voor Gegevensbescherming aanwijzen, dan hoeft alleen de forwarder te worden aangepast.

Voorstel 3:
Ga na of de FG het heel belangrijk vindt dat de Kiesraad gebruikmaakt van het register van verwerkingen zoals dit hem door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties ter beschikking is gesteld.

Op grond van artikel 30 van de verordening is de Kiesraad verplicht om een register van verwerkingen bij te houden. Een dergelijk register wordt ook wel een verwerkingenregister of een AVG-register genoemd. Het register moet in schriftelijke vorm, waaronder mede wordt verstaan elektronisch, bestaan (art. 30 lid 3 AVG). Het register is een hulpmiddel voor de Functionaris voor Gegevensbescherming en moet desgewenst ter beschikking gesteld kunnen worden aan de Autoriteit

Persoonsgegevens. Op het moment van schrijven van deze notitie wordt vooralsnog gebruikgemaakt van een elektronisch register dat door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties ter beschikking wordt gesteld. Maar aan dat gebruik ligt nog geen beslissing van de staf of de Kiesraad ten grondslag. Inmiddels staan voor drie verwerkingsprocessen van de Kiesraad in concept meldingen in het hier bedoelde register. Het betreft de registratie van aanduidingen en (plaatsvervangend) gemachtigden, de kandidaatstellingsprocedure, en de vaststelling van de uitslag inclusief de benoeming van kandidaten in (tussentijdse) (tijdelijke) vacatures in vertegenwoordigende organen. Een voordeel van het huidige register is dat het voor de Kiesraad mogelijk is om inspiratie op te doen aan de hand van de verwerkingsactiviteiten die het ministerie in het register heeft opgenomen. Omgekeerd, zo is mij verzekerd, kunnen bij het ministerie werkzame ambtenaren niet kijken in de verwerkingsprocessen van de Kiesraad. Een tweede voordeel is dat de Kiesraad, door het register te gebruiken, zeker weet dat de wijze waarop zijn register is ingericht overeenstemt met de eisen die de Autoriteit Persoonsgegevens daaraan stelt. En het gebruik van het digitale register stelt de huidige Functionaris voor Gegevensbescherming in staat om altijd te kunnen kijken naar het actuele register van verwerkingen van de Kiesraad. Nadelen zijn er echter ook. Een nadeel is dat het invoeren van een verwerkingsproces erg arbeidsintensief is. Een ander nadeel is dat in situaties waarin de Kiesraad gebruikmaakt van verwerkers, in het register niet kan worden vastgelegd welke werkzaamheden zo'n verwerker ten behoeve van de Kiesraad verricht. En tot slot heeft het gebruikmaken van een digitaal register voor een organisatie als de Kiesraad zelf eigenlijk weinig toegevoegde waarde.

Welke gegevens moeten er minimaal in een register van verwerkingen zijn opgenomen betreffende een verwerkingsproces?

a. De naam en contactgegevens van de verwerkingsverantwoordelijke(n).
b. De naam en contactgegevens van de vertegenwoordiger van de verwerkingsverantwoordelijke (i.c. ben ik dat) en van de FG.
c. De verwerkingsdoeleinden.
d. Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens die worden verwerkt.
e. Categorieën van ontvangers aan wie de persoonsgegevens zijn, of zullen worden, verstrekt. Onder meer ontvangers in derde landen of internationale organisaties.
f. Indien van toepassing: doorgifte van persoonsgegevens aan derde-landen of internationale organisaties.
g. Indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van persoonsgegevens moeten worden gewist. (Anders: de criteria daarvoor)
h Indien mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen als bedoeld in artikel 32 lid 1 AVG.

Voorstel 4:
Als de Kiesraad gebruikmaakt van een digitaal register van verwerkingen, voorkom dan dat uittreksel daarvan op Rijksoverheid.nl worden geplaatst.

Het register van verwerkingen is niet openbaar. Wel zijn er plannen om een deel van de informatie die in dit register is opgenomen ten aanzien van ministeries openbaar te maken op Rijksoverheid.nl. In het beste geval staat de Kiesraad dan tussen de ministeries en hun uitvoeringsorganisaties op Rijksoverheid.nl. In het slechtste geval

als onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

5.2.1

5.2.1 Als besloten wordt (al dan niet tijdelijk) gebruik te blijven maken van het door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties aangeboden digitale register, dan lijkt het mij goed om op een iets hoger niveau – bijvoorbeeld het niveau van secretaris-directeur – aan te geven dat wij er wel op vertrouwen dat onze input in het register niet (gedeeltelijk) openbaar wordt gemaakt. Overigens zijn de voorgenomen specifieke privacyverklaringen van de Kiesraad zodanig, dat aan de openbaarmaking van (een deel van) de in het register opgenomen informatie hoogstwaarschijnlijk ook geen behoefte meer zal bestaan.

Commented [5124]: Tast dit echt de onafhankelijkheid aan?

Commented [5125]: M.n. beeldvorming. Overigens geldt voor de Kiesraad dat hij specifieke privacyverklaringen op zijn website kan plaatsen. Die zijn leesbaarder en beter vindbaar.

Voorstel 5:
De Kiesraad en de voorzitter van de Kiesraad zijn elk een bestursorgaan en zijn elk verwerkingsverantwoordelijke in de zin van de AVG. In het door BZK aangeboden register is het evenwel alleen mogelijk om de voorzitter als verwerkingsverantwoordelijke aan te wijzen.

In de algemene privacyverklaring staat netjes dat zowel de Kiesraad zelf, als zijn voorzitter, verwerkingsverantwoordelijke zijn. Als jurist hecht ik daaraan. Anderzijds ben ik voornemens om in de specifieke privacyverklaringen steeds alleen het woord Kiesraad te gebruiken, omdat dit het meest gebruiksvriendelijk is. Voor het door het ministerie ter beschikking gestelde register geldt dat hierin alleen de voorzitter van de Kiesraad als verwerkingsverantwoordelijke kan worden aangewezen. Mijn voorstel is om die onvolkomenheid maar ongemoeid te laten. Daarbij ga ik er vanuit dat het register zelf alleen intern beschikbaar zal zijn (en dan nog alleen voor de FG en ondergetekende).

Voorstel 6:
De secretaris-directeur is bevoegdom de opname van een verwerkingsproces in het register te accorderen.

Eerder in deze notitie (p. 3) is gemeld dat voor drie verwerkingsprocessen van de Kiesraad in concept een melding gereed is in het digitale register. Bij het aanmaken van een verwerkingsactiviteit in het register van verwerkingsactiviteiten heeft deze de status 'In bewerking'. Als de verwerkingsactiviteit volledig is ingevuld, kan de status worden gewijzigd in 'vastgesteld'. Dit roept de vraag op of de verwerkingsverantwoordelijke zelf de wijze waarop de verwerkingsactiviteit in het AVG-register is opgenomen moet accorderen. Ik ga er vanuit dat dit niet het geval is. De term 'vastgesteld' wil in casu alleen zeggen dat de registermelding volledig en 'officieel' is, in de zin dat de Autoriteit Persoonsgegevens en de FG uit mogen gaan van de daarin opgenomen informatie. Instemming van de secretaris-directeur is daarvoor voldoende. Overigens kan deze instemming in voorkomende gevallen niet gegeven worden dan nadat de noodzakelijke verwerkersafspraken of verwerkersovereenkomsten gesloten zijn.

Bijlage 4:
SvZ: Voortgang implementatieproces AVG

Geldig: 16 augustus 2018

Leeswijzer:
Dit document bevat de stand van zaken met betrekking tot de voortgang in de implementatie van de Algemene verordening gegevensbescherming. Het document bevat de status per de bovengenoemde datum. Waar nodig wordt binnen een verwerkingsproces de status van kleinere onderdelen meegegeven. Om een snel beeld te krijgen van de status, kan naar de gebruikte kleuren worden gekeken.

Donker rood = Nog niet gestart.
Rood = Mogelijk wel gestart, maar nog de nodige actie vereist.
Oranje = In een vergevorderd stadium.
Groen = (Zo goed als) gereed.

Werkprocessen in het register van verwerkingen:

1. Registratie van aanduidingen

Status:
Melding in het verwerkingsregister gereed voor publicatie. Met één partij moeten nog verwerkersafspraken worden gemaakt.

a. KOOP (SDU)):
Vanwege publicatie van de processen-verbaal en kandidatenlijsten in de Staatscourant.
Status:
Afstemming met BZK (7 en 8 augustus) bevestigt dat verwerkersafspraken met deze partij noodzakelijk zijn. Ik heb een conceptovereenkomst opgesteld (13 augustus). Als 5.1.2.e terug is van vakantie wordt dit verder opgepakt.

2. Kandidaatstellingsprocedure

Status:
Melding in het verwerkingsregister in concept gereed. Met één partij moeten nog verwerkersafspraken worden gemaakt. Met één andere partij moet nog een verwerkingsovereenkomst worden gesloten. Namelijk:

a. KOOP (SDU)):
Vanwege publicatie van de processen-verbaal en kandidatenlijsten in de Staatscourant.
Status:
Afstemming met BZK (7 en 8 augustus) bevestigt dat verwerkersafspraken met deze partij noodzakelijk zijn. Ik heb een conceptovereenkomst opgesteld (13 augustus). Als 5.1.2.e terug is van vakantie wordt dit verder opgepakt.

b. T&T Vertrouwd verbonden:
Vanwege de connectie die zij ons bieden met de Basisregistratie personen.
Status:
Op 27 juni 2018 heeft T&T de Kiesraad per brief geïnformeerd van mening te zijn dat er nog een verwerkerovereenkomst nodig is.
Op 28 juni 2018 heeft 5.1.2.e (na overleg) aangegeven dat de Kiesraad deze wens deelt en een concept opgevraagd.
Op 7 augustus 2018 is T&T telefonisch gevraagd de conceptovereenkomst opnieuw toe te sturen (reden: niet eerder ontvangen).

c. RvIG (Rijksdienst voor Identiteitsgegevens)
Vanwege de Basisregistratie personen.
Status:
Er hoeven geen verwerkersafspraken gemaakt te worden met de RvIG, omdat de toegang tot de Basisregistratie personen via T&T Compt&t verloopt. Voor de zekerheid is deze conclusie met de RvIG gedeeld. (Kenmerk: 2018-0000686229).

3. Vaststelling verkiezingsuitslag & tussentijdse benoemingen

Status:
In eerste instantie voorzag ik dat voor de vaststelling van de verkiezingsuitslag en de tussentijdse benoemingen elk een afzonderlijke melding zou worden aangemaakt in het verwerkingenregister. Daar ben ik van teruggekomen. De melding in het verwerkingsregister is in concept gereed. Daarnaast moet met één partij een verwerkersovereenkomst gesloten worden. Met een andere partij moeten nog verwerkersafspraken worden gemaakt.

1. Xerox OBT
   Vanwege het drukken van de kerngegevens
   Status:
   Afstemming met BZK (7 en 8 augustus) bevestigt dat een verwerkersovereenkomst noodzakelijk is. Ik heb een conceptovereenkomst opgesteld (9 augustus 2018). Als 5.1.2.e terug is van vakantie wordt dit verder opgepakt.

a. KOOP (SDU))
   Vanwege publicatie van de processen-verbaal en kandidatenlijsten in de Staatscourant.
   Status:
   Afstemming met BZK (7 en 8 augustus) bevestigt dat verwerkersafspraken met deze partij noodzakelijk zijn. Ik heb een conceptovereenkomst opgesteld (13 augustus). Als 5.1.2.e terug is van vakantie wordt dit verder opgepakt.

Notitie

Onderwerp
Voortgang Implementatie AVG: nr. 4

Datum
6 augustus 2018

Kenmerk
2018-0000684934

Inlichtingen
5.1.2.e
T 070 426 6266
F 070 751 7078

Blad
1 van 3

Aan
Staf
Van
5.1.2.e

1. Inleiding

Voor u ligt de vierde rapportage over de voortgang van de implementatie van de Algemene verordening gegevensbescherming[1] door de Kiesraad.

Overzicht van eerdere voortgangsrapportages:
1. Rapportage van 4 september 2017 (kenmerk: 2017-0000429580).
2. Voorstel werkprocedure AVG-rechten (kenmerk: 2018-0000325158).
3. Rapportage van 2 juli 2018 (kenmerk: 2018-0000498271).

2. Gevolgen van de AVG in kaart gebracht

In het stafoverleg van 26 juni 2018 (Kenmerk: 2018-0000643017) is gevraagd prioriteit te geven aan het maken van een overzicht van de gevolgen die de Algemene verordening gegevensbescherming heeft voor de primaire werkprocessen van de Kiesraad. In 'Bijlage 1' en 'Bijlage 2' zijn deze gevolgen als 'voorstellen' geformuleerd. In 'Bijlage 3' wordt over handreikingen gesproken. Inhoudelijk wordt evenwel hetzelfde bedoeld.

Bijlage 1 bevat de gevolgen van de verordening voor de volgende processen:
- Registratie van aanduidingen en de aanwijzing van gemachtigden
- Kandidaatstellingsprocedure
- Vaststelling van de verkiezingsuitslag
- (Tussentijdse) (Tijdelijke) Benoeming van volksvertegenwoordigers
- Raadgevend referendum

Bijlage 2 bevat de gevolgen van de verordening voor:
- Postbus Kiesraad / Informatiepunt Verkiezingen

[1] 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)

Bijlage 3 bevat de notitie 'AVG voor communicatiespecialisten'. In die notitie wordt ingegaan op de gevolgen van de verordening voor werkzaamheden op het gebied van communicatie. De volgende thema's komen hierin aan de orde:
- Medewerkers
- Foto's en video's
- Nieuwsberichten

De notitie is niet uitputtend bedoeld. Over de publicatie van namen van gemachtigden van politieke groeperingen, bijvoorbeeld, is ook een voorstel opgenomen in 'Bijlage 1'. Aan de registratie van perscontacten in FMP is vooralsnog in geen enkele notitie (of bijlage) aandacht besteed, hoewel het wel activiteiten zijn waarbij persoonsgegevens worden verwerkt. Hetgeen in 'Bijlage 2' is voorgesteld ten aanzien van 'Postbus Kiesraad / Informatiepunt Verkiezingen' kan mutatis mutandis ook op persvragen worden toegepast. Een afzonderlijke notitie over dat onderwerp staat daarom vooralsnog niet op de planning.

Naast notities over specifieke verwerkingen, bevat deze rapportage ook een bijlage over grote vraagstukken rondom de implementatie van de AVG waarover nog enkele beslissingen genomen moeten worden. Zie Bijlage 4.

3. Huidige stand van zaken

Evenals bij de voortgangsrapportage van 2 juli 2018 is de huidige stand van zaken, wat betreft de prioritaire processen, opgenomen in een bijlage bij deze notitie: Bijlage 5.

Niet in het overzicht opgenomen, maar vermeldenswaardig:
- Het Besluit mandaat en machtiging Kiesraad moet opnieuw worden vastgesteld. Daarvoor bestaan drie redenen, waaronder de van toepassingwording van de Algemene verordening gegevensbescherming. Een notitie (kenmerk: 2018-0000521329) en een conceptbesluit (kenmerk: 2018-0000516462) zijn voorbereid. Het Besluit mandaat en machtiging voorzitter Kiesraad kan worden ingetrokken, vgl. het conceptbesluit (kenmerk: 2018-0000519535). Nu de Wet raadgevend referendum is ingetrokken, heeft handhaving van dit besluit geen nut.
- Er is een nieuwe algemene privacyverklaring opgesteld (kenmerk: 2018-0000695916). Deze is met [redacted] afgestemd. De nieuwe verklaring staat inmiddels op de website. Op een later moment komen er specifieke verklaringen bij voor bepaalde verwerkingsactiviteiten. Zie planning.
- De Kiesraad is verplicht een register van verwerkingen bij te houden. Ik heb drie meldingen in concept gereed. Het betreft:
  1. Registratie aanduidingen van politieke partijen & (plaatsvervangend) gemachtigden
  2. Kandidaatstellingsprocedure
  3. Vaststelling verkiezingsuitslag & tussentijdse benoemingen

4. Planning

De werkzaamheden zoals die waren opgenomen op de planning die in de rapportage van 2 juli 2018 was opgenomen, zijn grotendeels voltooid en als concreet resultaat in deze notitie terug te vinden. De huidige planning is als volgt:
- Het maken van specifieke privacyverklaringen, in aanvulling op de algemene privacyverklaringen, met per thema meer informatie over de verwerking van persoonsgegevens door de Kiesraad.

- Gevolgen van de AVG voor de secondaire verwerkingsprocessen in kaart brengen.
- Het register van verwerkingen verder aanvullen.
- Een lijstje maken voor alle medewerkers van het secretariaat waarin de wijzigingen, zonder nadere uitleg, zijn opgenomen.

- Op iets langere termijn moet ik de notitie over het 'passief informatierecht' aanpassen, omdat ik daar te soft ben geweest v.w.b. de plicht tot identificatie van de aanvrager.

Overzicht:
Wijzigingen in werkprocessen ter implementatie van de AVG

Registratie aanduidingen & aanwijzing gemachtigden:

1. De namen van (plv.) gemachtigden worden niet langer op de website van de Kiesraad gepubliceerd.
   Reden: Ontbrekende verwerkingsgrondslag. Mogelijk ook in strijd met beginsel van minimale gegevensverwerking.
2. Stuur politieke partijen drie maanden vóór de dag van de kandidaatstelling van elke verkiezing een brief, met daarin de namen van degenen die namens de vereniging zijn aangewezen als (plv.) gemachtigden.
   Reden: Compensatie voor het voorgaande.
3. Vernietig de stukken die politieke partijen overleggen in het kader van een verzoek tot registratie van een aanduiding c.q. aanwijzing van een (plv.) gemachtigde zodra deze niet meer relevant zijn. Zowel op papier als in DigiDoc. Ook de kopieën die als Kiesraadstuk worden bewaard.
   Reden: art. G 1 lid 9 Kieswet
4. In de 'notitie van het secretariaat' bij een registratieverzoek worden functienamen i.p.v. persoonsgegevens gebruikt.
   Reden: Beginsel van minimale gegevensverwerking.

Kandidaatstellingsprocedure

1. De ontvangstbevestiging wordt uitgebreid. Voortaan wordt ook informatie over de verwerking van persoonsgegevens medegedeeld.
   Reden: Art. 13 lid 1 AVG & advies Kiesraad.
2. Na vaststelling verkiezingsuitslag: vernietiging kandidatenlijsten en bijbehorende stukken (m.u.v. instemmingsverklaringen).
   Reden: Art. I 19 / Art. S 15 / Art. Y 17a Kieswet.
3. Terinzagelegging blijft eindigen als onherroepelijk is beslist over de geldigheid van de ingediende kandidatenlijsten.
4. Digitale en papieren gegevens mogen even lang worden bewaard. Het draaiboek moet waarborgen dat ook OSV-bestanden betreffende de kandidaatstelling op tijd worden vernietigd.
   Reden: Art. 5 lid 1 onder c AVG

Vaststelling verkiezingsuitslag

1. Er wordt nooit meer informatie van kandidaten gebruikt, dan zij geven. Ontbreekt bijv. het geslacht, dan wordt dit niet (t.b.v. de statistiek) nagetrokken.

(Tussentijdse) (Tijdelijke) benoeming volksvertegenwoordigers

1. Na afloop zittingstermijn vertegenwoordigend orgaan alle documenten die samenhangen met (tussentijdse) (tijdelijke) benoemingen vernietigen.
   Reden: Art. 5 lid 1 onder c AVG

Postbus Kiesraad / Informatiepunt verkiezingen

1. Van ontvangen e-mails die in FMP worden opgeslagen, wordt het zogenoemde 'onderschrift' - de ondertekening - niet gekopieerd; alleen de inhoud.
   Reden: Art. 5 lid 1 onder c AVG
   Uitzondering: als de inhoud van een e-mail veel persoonsgegevens van derden bevat, wordt de inhoud niet gekopieerd, maar wordt de vraag door de medewerker geherformuleerd (zoals ook bij telefonische vragen gebruikelijk is).
2. In het veld 'Aantekening' in FMP worden geen persoonsgegevens genoteerd.
3. Gegevens die in FMP worden ingevoerd, worden vijf kalenderjaren bewaard. Hetzelfde geldt voor e-mails in Outlook.

Notitie

Onderwerp
Werkprocedure AVG-rechten

Datum
31 mei 2018
Geactualiseerd (§ 2) op:
11 december 2018

Kenmerk
2018-0000947707

Inlichtingen
5.1.2.e
T 070 426 6266
F 070 751 7078

Blad
1 van 10

Aan
Staf
Van
5.1.2.e

1. Inleiding

De Algemene verordening gegevensbescherming (AVG)[1] heeft de rechten van personen, van wie persoonsgegevens worden verwerkt, versterkt. Zij hebben meer rechten gekregen tegenover personen en organisaties die hun persoonsgegevens verwerken; zoals de Kiesraad. Artikel 12, tweede lid, van de verordening verplicht de Kiesraad om de uitoefening van de in de AVG neergelegde rechten te faciliteren. Daarbij kan een onderscheid gemaakt worden in twee soorten rechten. Er is een recht – het actief informatierecht – dat degene wiens persoonsgegevens worden verwerkt van rechtswege toekomt. Dit recht vergt proactief handelen van de Kiesraad. Daarnaast zijn er rechten waarop natuurlijke personen zich kunnen beroepen en die de Kiesraad verplichten om desgevraagd te reageren c.q. tot actie over te gaan. Deze notitie heeft uitsluitend betrekking op de laatstbedoelde categorie. De notitie geeft antwoord op de vraag hoe de Kiesraad moet handelen als er verzoeken van burgers binnenkomen die gebruik willen maken van een hen krachtens de AVG toekomend recht. Op een later moment volgen nadere voorstellen die betrekking hebben op het actief informatierecht.

Deze notitie is als volgt opgebouwd. Allereerst wordt een concreet voorstel gegeven voor de inrichting van de procedure (§ 2). Dit voorstel wordt themagewijd besproken. Daarna wordt nog uitgebreid ingegaan op de rechten waarop betrokkenen zich jegens de Kiesraad kunnen beroepen (§ 3), omdat kennis van deze rechten noodzakelijk is om het juiste besluit op een aanvraag te kunnen nemen. Het gaat dan vooral om de volgende rechten:

– Art. 15 AVG: Recht op inzage
– Art. 16 AVG: Recht op rectificatie

[1] 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).

– Art. 17 AVG: Recht op vergetelheid
– Art. 18 AVG: Recht op beperking van de verwerking.

2. Voorstel procedure

Hoe om te gaan met verzoeken van burgers die zich beroepen op één van de hen, op grond van de Algemene verordening gegevensbescherming, toekomende rechten? Deze paragraaf geeft themagewijde antwoorden op die vraag. Daarbij wordt er telkens vanuit gegaan dat de Kiesraad de betrokken verwerkingsverantwoordelijke is. Voor sommige verwerkingen is in werkelijkheid de voorzitter van de Kiesraad verwerkingsverantwoordelijke. Daarover meer binnen het thema 'Ondertekening'.

Ontvangst

Een verzoek kan op twee manieren bij de Kiesraad worden ingediend: per e-mail en schriftelijk. Het mondeling indienen van een verzoek is niet mogelijk. Als het verzoek elektronisch is ingediend, wordt de informatie – indien mogelijk – elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt (vgl. art. 22 lid 3 AVG).

Identificeren

Aangenomen dat de Kiesraad geen persoonsgegevens verwerkt van personen die jonger zijn dan zestien jaar, kan iedere betrokkene, die de Kiesraad verzoekt om zijn rechten uit hoofde van de artikelen 15 t/m 22 van de AVG uit te oefenen, dit alleen doen met het oog op persoonsgegevens die de Kiesraad van hem persoonlijk verwerkt. Een verzoek van een natuurlijk persoon mag dus geen betrekking hebben op iemand anders. Dat stelt de Kiesraad voor een dilemma. Enerzijds moet hij faciliteren dat betrokkenen hun in de AVG neergelegde rechten kunnen uitoefenen, anderzijds moet hij ook voorkomen dat er een datalek ontstaat. Een datalek kan bijvoorbeeld ontstaan als de Kiesraad alleen op basis van de naam van een betrokkene persoonsgegevens ter inzage geeft, en de ter inzage verstrekte gegevens van een naamgenoot blijken te zijn. Of als iemand een verkeerde naam opgeeft. De Kiesraad heeft dus de plicht om zich van de identiteit van de verzoeker te vergewissen. Is de Kiesraad niet in staat de betrokkene te identificeren, dan kan de Raad weigeren gevolg te geven aan het verzoek van de betrokkene om diens rechten uit hoofde van de artikelen 15 tot en met 22 uit te oefenen. Identificatie kan plaatsvinden aan de hand van een (geldig) identiteitsdocument, zoals een paspoort, identiteitskaart of rijbewijs.

Beperkingen

De betrokkene kan niet in alle gevallen een beroep doen op een hem, op grond van de Algemene verordening gegevensbescherming, toekomend recht. Vooral bij verwerkingen van persoonsgegevens ter uitvoering van de Kieswet en de Wet raadgevend referendum bestaan er uitzonderingen. Deze beperkingen zijn telkens opgenomen in het hoofdstuk waarin de betreffende verwerking in de wet wordt voorgeschreven. Let wel: bij het schrijven van deze paragraaf ben ik er vanuit gegaan dat het voorstel van wet dat moet leiden tot de Aanpassingswet Algemene verordening gegevensbescherming in werking zal treden zoals het onlangs door de regering bij de Tweede Kamer is ingediend.

Beslissing op verzoek
De Kiesraad moet de betrokkene informeren over het gevolg dat aan het verzoek gegeven is. Welk gevolg gewenst is, hangt af van het recht waarop de betrokkene zich beroept. Meer hierover in paragraaf 3.

Beslistermijn
De Kiesraad moet onverwijld beslissen op een verzoek; doch uiterlijk binnen een maand. Verlenging van de beslistermijn is alleen mogelijk als aan drie voorwaarden wordt voldaan:
- Reden voor verlenging: De zaak is zeer complex óf de Kiesraad heeft erg veel verzoeken ontvangen.
- Moment van verlenging: De betrokkene moet binnen de eerst maand na ontvangst van het verzoek van de verlenging in kennis zijn gesteld.
- Termijn voor verlenging: Maximaal twee maanden.

Kosten
Een besluit op een verzoek dient kosteloos genomen te worden. Overigens is in de verordening wel expliciet voorzien in de mogelijkheid om kosten in rekening te brengen, wanneer verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter.[2] In dezelfde situaties mag de Kiesraad overigens ook weigeren gevolg te geven aan verzoeken.

De lijn
Zolang de Algemene verordening gegevensbescherming nog niet volledig door de Kiesraad is geïmplementeerd, is het praktisch dat ik zelf de primaire conceptbesluiten schrijf. In een later stadium ligt het meer voor de hand aan te sluiten bij de lijn die geldt in het geval de Kiesraad een verzoek op grond van de Wet openbaarheid van bestuur ontvangt.

Ondertekening
De reactie van de Kiesraad op een verzoek van een betrokkene wordt gelijkgesteld aan een appellabel besluit in de zin van artikel 1:3 van de Algemene wet bestuursrecht.[3] Gelet op de aard van het besluit – m.n. verstrekken, wijzigen, verwijderen en vasthouden van persoonsgegevens – en de tijd waarbinnen het besluit genomen moet worden, stel ik voor het Besluit mandaat en machtiging Kiesraad (Stb. 2016, 19763) opnieuw vast te stellen en daarin twee wijzigingen aan te brengen:
- De voorzitter van de Kiesraad wordt gemandateerd om namens de Kiesraad te besluiten en stukken te ondertekenen met betrekking tot besluiten, waaronder verdagingsberichten, op grond van de Uitvoeringswet algemene verordening gegevensbescherming.
- De secretaris-directeur van de Kiesraad wordt gemandateerd om namens de Kiesraad te besluiten en stukken te ondertekenen met betrekking tot verdagingsberichten als bedoeld in artikel 12, derde lid, van de Algemene verordening gegevensbescherming: verordening (EU) 2016/679.

De voorgestelde bevoegdheidsverdeling voor de ondertekening van besluiten op grond van de Algemene verordening gegevensbescherming wordt daarmee gelijk aan die voor de ondertekening van besluiten op grond van de Wet openbaarheid van bestuur.

---

[2] Art. 12 lid 5 AVG.
[3] Art. 34 Uitvoeringswet Algemene verordening gegevensbescherming.

Actiepunt:
Het Besluit mandaat en machtiging Kiesraad (Stb. 2016, 19763) opnieuw vaststellen.

De Kiesraad is vaak verwerkingsverantwoordelijke, maar juridisch gezien niet altijd. Soms kent de wet een bevoegdheid expliciet toe aan de voorzitter van de Kiesraad en in die gevallen is de voorzitter zelf verwerkingsverantwoordelijke. Bijvoorbeeld bij de verwerking van persoonsgegevens in het kader van de (tijdelijke) benoeming of het (tijdelijk) ontslag van volksvertegenwoordigers. Als de Kiesraad dit onderscheid belangrijk vindt, dan zou een betrokkene geen informatie krijgen over de verwerking van persoonsgegeven in het kader van deze procedures als hij een algemeen verzoek om informatie tot de Kiesraad richt. Ook niet als de voorzitter zijn persoonsgegevens verwerkt. Een strikt onderscheid betekent ook dat het Besluit mandaat en machtiging voorzitter Kiesraad (Stb. 2016, 19765) na het komen vervallen van de Wet raadgevend referendum niet kan worden ingetrokken, maar nog één bevoegdheid aan de secretaris-directeur moet blijven geven: de bevoegdheid om namens de voorzitter van de Kiesraad te besluiten en stukken te ondertekenen met betrekking tot verdagingsberichten als bedoeld in artikel 12, derde lid, van de Algemene verordening gegevensbescherming: verordening (EU) 2016/679. Ofschoon juridisch helemaal juist: in de dagelijkse praktijk zal een gericht verzoek om informatie aan de Kiesraad over de verwerking van persoonsgegevens in het kader van de (tijdelijke) benoeming of het (tijdelijk) ontslag van volksvertegenwoordigers waarschijnlijk niet door de Kiesraad worden 'doorgestuurd' aan zijn voorzitter. De kans is zelfs aanwezig dat het secretariaat de fout niet ambtshalve hersteld, maar bij de ondertekening de Kiesraad zelf ook als besluitend orgaan vermeldt. Bovendien communiceert het secretariaat in de dagelijkse praktijk ook niet altijd helder naar buiten waar een bevoegdheid ligt: gemeente v. college van burgemeester en wethouders, Kiesraad v. voorzitter van de Kiesraad. Zo schreef het secretariaat op 12 april 2018 nog op de website van de Kiesraad dat de Raad de heer Stoffer heeft benoemd als Tweede Kamerlid;[4] juridisch is dat niet waar. Kan de Raad het een burger dat euvel duiden het onderscheid niet te hebben gemaakt? Mijn voorstel is om besluiten die genomen worden op basis van de in deze notitie beschreven procedure, altijd door de Kiesraad worden genomen. Juridisch is niet helemaal juist, maar het bezwaar wordt grotendeels weggenomen doordat de bevoegdheid om namens de Kiesraad te besluiten aan de voorzitter wordt toegekend.

[4] https://www.kiesraad.nl/actueel/nieuws/2018/04/12/benoeming-c.-stoffer-tot-lid-van-de-tweede-kamer (Laatst bezocht: 2 juni 2016.

> **Actiepunt:**
> In een volgende notitie aan de Kiesraad dit onderwerp aan de Raad voorleggen.

Rechtsmiddelenclausule

Op grond van artikel 34 van de Uitvoeringswet Algemene verordening gegevensbescherming geldt de schriftelijke beslissing van een bestuursorgaan op een verzoek als bedoeld in de artikelen 15 tot en met 22 van de verordening als een besluit in de zin van de Algemene wet bestuursrecht.[5] Tegen dit besluit kan een bezwaarschrift worden ingediend.[6] Tegen de beslissing op bezwaar is beroep mogelijk bij de rechtbank binnen het rechtsgebied waarvan de indiener van het beroepschrift zijn woonplaats in Nederland heeft.[7] En tegen de uitspraak van de rechtbank kan de betrokkene nog in hoger beroep bij de Afdeling bestuursrechtspraak van de Raad van State. Tijdens de behandeling van het beroep kunnen de Rechtbank en de Afdeling advies inwinnen bij de Autoriteit Persoonsgegevens.[8]

Naast het starten van een juridische procedure, staat voor de betrokkene evenwel ook een andere weg open.[9] De betrokkene kan zich wenden tot de Autoriteit Persoonsgegevens en een klacht indienen.[10] In de Uitvoeringswet wordt deze mogelijkheid niet expliciet genoemd. In plaats daarvan staat er in de Uitvoeringswet dat de betrokken een 'verzoek te bemiddelen of te adviseren' in een geschil met de Kiesraad kan indienen bij de Autoriteit Persoonsgegevens.[11] Daarmee wordt echter exact hetzelfde bedoeld. Anders dan onder de Wet bescherming persoonsgegevens, is de Autoriteit Persoonsgegevens verplicht alle klachten die bij haar binnenkomen in behandeling te nemen.[12] Zij heeft daarvoor onderzoeks- en sanctiebevoegdheden.[13] Klachtbehandeling bij de Autoriteit Persoonsgegevens is laagdrempelig voor de betrokkene. Mogelijk biedt het de Kiesraad bovendien de gelegenheid om lopende de klachtbehandeling door de Autoriteit Persoonsgegevens meer inzicht te verkrijgen in de wijze waarop deze autoriteit toetst. Geschilbeslechting door de Autoriteit Persoonsgegevens kan dus voor beide partijen meerwaarde hebben en 5.2.1 Al moet de Kiesraad altijd beide mogelijkheden noemen; de mogelijkheid een klacht in te dienen kan uiteraard wel als eerst worden genoemd.

> **Actiepunt:**
> Twee nieuwe rechtsmiddelenclausules opstellen: één voor het primaire besluit, één voor een beslissing op bezwaar.

DigiDoc

Binnenkomende verzoeken van betrokkenen, die gebruik willen maken van een hen krachtens de AVG toekomend recht, moeten in DigiDoc opgeslagen worden. Mijns inziens ligt het voor de hand om hiervoor een nieuwe hoofdmap in DigiDoc

---

[5] Hiermee wordt uitvoering gegeven aan art. 79 AVG.
[6] Art. 34 Uitvoeringswet Algemene wet bestuursrecht jo. art. 8:1 jo. 7:1 Algemene wet bestuursrecht.
[7] Art. 34 Uitvoeringswet Algemene wet bestuursrecht jo. art. 8:1 jo. 8:7 lid 2 Algemene wet bestuursrecht.
[8] Art. 36 lid 2 Uitvoeringswet Algemene verordening gegevensbescherming.
[9] Art. 12 lid 4 AVG.
[10] Art. 77 lid 1 AVG.
[11] Art. 36 lid 1 Uitvoeringswet Algemene verordening gegevensbescherming.
[12] Art. 57 lid 1 onder f AVG.
[13] Art. 58 AVG.

aan te maken, zoals die eerder ook voor Wob-verzoeken - '16. Wob-verzoeken' - is aangemaakt. Hoofdmap '18. Opschonen NAKIJKEN EN VRAGEN' kan worden hernoemd tot '19. Opschonen NAKIJKEN EN VRAGEN', waarna een nieuwe hoofdmap - '18. AVG' - kan worden tussengevoegd.

In de hoofdmap '18. AVG' moet niet alleen ruimte worden geboden voor de besluiten waar deze notitie op ziet, maar ook voor andere documenten die belangrijk zijn voor de implementatie en/of interpretatie van de AVG. Op dit moment staan die documenten deels verstopt in '14. Internationaal' en deels alleen op mijn deel van de H-schijf. Dat is geen wenselijke situatie. Ik stel daarom voor om voorlopig de volgende structuur in DigiDoc in te richten:

18. AVG
    AVG-verzoeken
        AVG-Verzoeken 2018
    Literatuur
    Notities
    Verwerkersovereenkomsten & -afspraken

De getoonde mappen 'AVG-verzoeken', 'AVG-Verzoeken 2018', 'Literatuur', 'Notities' en 'Verwerkersovereenkomsten & -afspraken' zijn daarbij dossiermappen, zodat de portefeuillehouder daaronder zelf de noodzakelijke sub-mappen kan aanmaken. De map 'AVG-verzoeken' staat daarbij bewust anders uitgelijnd, omdat deze zich in de map 'AVG-verzoeken' bevindt. Op een later moment kan deze structuur worden aangevuld.

Actiepunt:
Bovenvermelde structuur in DigiDoc aanmaken

3. AVG-rechten

Een betrokkene heeft op grond van de AVG een aantal rechten. Deze rechten kan de betrokkene inroepen tegenover degene die zijn persoonsgegevens verwerkt. Niet alle rechten zijn in alle omstandigheden inroepbaar. Er zijn uitzonderingen. Soms voorziet de AVG zelf in zo'n uitzondering;[14] in andere gevallen biedt de AVG een grondslag om in nationale wetgeving in een uitzondering te voorzien.[15] De regering beoogd van die laatste mogelijkheid gebruik te maken in de Kieswet en de Wet raadgevend referendum. De daarvoor noodzakelijke wijziging van deze wetten is voorzien in het wetsvoorstel dat moet leiden tot de Aanpassingswet Algemene verordening gegevensbescherming. Dit wetsvoorstel is thans aanhangig bij de Tweede Kamer. Een betrokkene kan zich met een beroep op de AVG jegens de Kiesraad op de navolgende rechten beroepen:

Artikel 15: Recht op inzage
Dit is een passief informatierecht. Het houdt in dat de Kiesraad desgevraagd moet nagaan of hij persoonsgegevens van de betrokkene verwerkt en, zo ja, hem hierover moet informeren. De betrokkene hoeft geen belang te stellen bij zijn verzoek. Het verzoek kan specifiek zijn: heeft u mijn persoonsgegevens verwerkt ten behoeve van verwerkingsactiviteit X? Het verzoek mag ook algemener zijn: verwerkt u mijn

[14] Voorbeeld: de betrokkene kan geen gebruik maken van het recht op vergetelheid als de persoonsgegevensverwerking plaatsvindt op grond van een wettelijke verplichting.
[15] Vgl. art. 23 AVG.

persoonsgegevens? Het is dan aan de Kiesraad om, met behulp van het Register van de verwerkingsactiviteiten, om na te gaan in welke verwerkingsprocessen persoonsgegevens van de betrokkene voor zouden kunnen komen, en in die verwerkingsprocessen naar de persoonsgegevens op zoek te gaan. Denkbaar is bijvoorbeeld dat persoonsgegevens voorkomen in het relatiebestand of in het registratiebestand voor klantcontacten (FMP).

Als de Kiesraad daadwerkelijk persoonsgegevens van de betrokkene verwerkt, dan moet hij inzage geven in deze persoonsgegevens. Dit moet gebeuren op een wijze die de betrokkene in staat stelt om de gegevens te controleren en, zo nodig, om wijziging of verwijdering te vragen. De Kiesraad kan de betrokkene op twee manieren inzage geven in de persoonsgegevens die van hem worden verwerkt:

1. De Kiesraad kan een volledig overzicht opstellen van alle persoonsgegevens die de Raad van de betrokkene verwerkt en hem dit ter beschikking stellen. Gelet op de werkprocessen van de Kiesraad waarin persoonsgegevens worden verwerkt, zal deze manier naar verwachting het vaakst worden gebruikt.
2. De Kiesraad kan de betrokkene ook een kopie of afdruk verstrekken van het originele document waarin de gegevens staan. Deze mogelijkheid kan bijvoorbeeld gebruikt worden als iemand als gemachtigde is aangewezen door een politieke groepering[16], of als iemand een Wob-verzoek heeft ingediend.[17]

Naast dat de Kiesraad de betrokkene moet informeren over de persoonsgegevens die hij van de betrokkene verwerkt, moet de Raad ook de volgende informatie verstrekken:

A) Verwerkingsdoeleinden: waarom verwerkt de Kiesraad deze persoonsgegevens? Wat is het doel?
B) Categorieën van persoonsgegevens: welke persoonsgegevens verwerkt de Kiesraad? Inzage geven. Met de in de verordening gebruikte term ‘categorieën van persoonsgegevens’ worden concrete persoonsgegevens bedoeld. Zie hierover de kennisnotitie ‘Persoonsgegevens, categorieën van persoonsgegevens en bijzondere categorieën van persoonsgegevens.’ (Ons kenmerk: 2018-0000326948).
C) Ontvangers: Aan welke organisatie heeft de Kiesraad deze persoonsgegevens verstrekt, of zal de Kiesraad deze gegevens verstrekken? Het is overigens niet altijd nodig de organisaties bij naam te noemen. Soms kan ook volstaan worden met een categorie van ontvangers, bijvoorbeeld: gemeenten.
D) Bewaartermijn: Hoe lang bewaart de Kiesraad de persoonsgegevens? Als geen bewaartermijn kan worden genoemd, dan moeten de criteria genoemd worden op basis waarvan de bewaartermijn wordt bepaald.
E) Rechten van betrokkene: De betrokkene moet erop worden gewezen dat hij diverse rechten heeft (zoals: rectificeren, wissen, beperken van de verwerking, bezwaar maken tegen de verwerking e.d.).

[16] Origineel document: kopie formulier wijziging gemachtigde.
[17] Origineel document: aanvraag op grond van de Wob.

F) Klachtprocedure: De betrokkene moet erop gewezen worden dat hij het recht heeft een klacht in te dienen bij de Autoriteit Persoonsgegevens.
G) Gegevensbron: Wat is de herkomst van de persoonsgegevens? Als de persoonsgegevens niet bij de betrokkene worden verzameld, moet deze alle beschikbare informatie over de bron van die gegevens krijgen.
H) Geautomatiseerde besluitvorming: N.v.t. op de Kiesraad.

Artikel 16: Recht op rectificatie en aanvulling
Dit is het recht op verbetering van fouten. Een betrokkene kan om drie redenen om rectificatie vragen: 1) zijn persoonsgegevens zijn feitelijk onjuist weergegeven; 2) zijn persoonsgegevens zijn onvolledig of niet ter zake doende voor het doel waarvoor zij zijn verzameld; en 3) zijn persoonsgegevens worden op een andere manier in strijd met de wet door de Kiesraad gebruikt. In alle drie de gevallen kan hij de Kiesraad vragen omverwijld tot rectificatie over te gaan.

Heeft de Kiesraad de te rectificeren persoonsgegevens van de betrokkene ook met derden gedeeld? Dan moet de Kiesraad zo snel mogelijk deze andere organisaties van de wijziging op de hoogte stellen.[18]

Wordt de Kiesraad gevraagd om een professionele indruk, mening of conclusie te rectificeren waar de betrokkene het mee oneens is – bijvoorbeeld in een sollicitatieprocedure –, dan valt dit verzoek buiten de reikwijdte van het recht. De Autoriteit Persoonsgegevens gaat er echter vanuit dat de Kiesraad in een dergelijke situatie de schriftelijke mening van de betrokkene aan het dossier zal toevoegen.

Artikel 17: Recht op vergetelheid
Dit recht wordt ook het recht op gegevenswissing genoemd. De betrokkene heeft het recht de Kiesraad te vragen zijn persoonsgegevens te wissen. Daarnaast bevat de verordening ook een lijst met omstandigheden die, als zij zich voordoen, ertoe moeten leiden dat de Kiesraad uit eigen beweging persoonsgegevens wist. Daarop staan onder andere de volgende omstandigheden:

A) De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt.
   Voorbeeld:
   De Kiesraad verzamelt gegevens van personen die zich aanmelden voor een symposium. Als het symposium heeft plaatsgevonden, heeft de Kiesraad die persoonsgegevens niet langer nodig en moet hij deze wissen.
B) De verwerking berustte op toestemming van de betrokkene en deze trekt zijn toestemming voor de verwerking in.
   Voorbeeld:
   De Kiesraad verzamelt gegevens van personen die zich aanmelden voor een symposium. Als iemand aangeeft bij nader inzien niet te willen komen en zich afmeld, moeten diens persoonsgegevens direct worden gewist.
D) De persoonsgegevens zijn onrechtmatig verwerkt.
   Voorbeeld:
   De Kiesraad komt erachter dat hij persoonsgegevens verwerkt (of heeft verwerkt), terwijl daar geen geldige grondslag voor bestond.

[18] Art. 19 AVG.

E) De persoonsgegevens moeten worden gewist om te voldoen aan een bepaling uit Europese of nationale regelgeving.
Voorbeeld:
De Kieswet schrijft nu voor dat de Kiesraad de bij hem ingeleverde kandidatenlijsten vernietigt, nadat onherroepelijk is beslist over de geldigheid van de kandidatenlijsten (vgl. art. I 19 Kieswet).

Het recht op vergetelheid geldt niet onbeperkt. De Kiesraad heeft bijvoorbeeld niet de plicht om persoonsgegevens te wissen, voor zover de verwerking daarvan plaatsvindt ter uitvoering van een wettelijke plicht.[19] Daarvan is bijvoorbeeld sprake bij de verwerking van persoonsgegevens ter uitvoering van de Kieswet en de Wet raadgevend referendum.

Heeft de Kiesraad de te wissen persoonsgegevens van de betrokkene ook met derden gedeeld? Dan moet de Kiesraad zo snel mogelijk deze andere organisaties van de vernietiging daarvan op de hoogte stellen en dienen deze organisaties hetzelfde te doen.[20]

Mogelijk maakt de Kiesraad gebruik van back-ups. Als persoonsgegevens gewist moeten worden, dan moeten deze persoonsgegevens ook zo snel mogelijk uit de back-ups worden gewist. De Autoriteit Persoonsgegevens adviseert regelmatig back-ups te maken en verouderde gegevens systematisch te verwijderen. Het maken van een back-up leidt tot een aanvullende bewaartermijn. Worden persoonsgegevens in een regulier systeem 1 jaar bewaart, maar hanteert de Kiesraad aanvullend een bewaartermijn van 3 maanden voor back-ups, dan moet dit worden gecommuniceerd. In sommige gevallen is het niet mogelijk om persoonsgegevens uit een back-up te verwijderen. In dat geval moet de Kiesraad goed bijhouden welke persoonsgegevens hij had moeten rectificeren c.q. verwijderen. Is het onverhoopt nodig om een back-up terug te plaatsen? Dan moet de Kiesraad deze gegevens alsnog rectificeren c.q. verwijderen.

Artikel 18: Recht op beperking van de verwerking
Onder bepaalde omstandigheden heeft de betrokkene het recht de Kiesraad minder persoonsgegevens van hem te laten verwerken. Dit is het geval in vier situaties, waaronder de volgende drie:

A) Gegevens zijn mogelijk onjuist.
De betrokkene geeft aan dat de Kiesraad onjuiste persoonsgegevens van hem gebruikt. Totdat de persoonsgegevens zijn gecontroleerd, mogen de persoonsgegevens waarvan de juistheid wordt bestreden, niet worden gebruikt. Totdat de Wet raadgevend referendum op de AVG is aangepast, kan iemand die een verzoek tot het houden van een referendum heeft ingediend, met een beroep op artikel 18 de Kiesraad ertoe bewegen de daarop door hem ingevulde persoonsgegevens te verifiëren en waar nodig te verbeteren.

B) De verwerking is onrechtmatig.

[19] Art. 17 lid 2 onder b AVG.
[20] Art. 19 AVG.

Als de Kiesraad bepaalde persoonsgegevens niet mag verwerken, dan moet hij die wissen. Maar het kan gebeuren dat de betrokkene niet wil dat de Kiesraad deze gegevens wist. Bijvoorbeeld omdat hij de gegevens later wil opvragen. In dat geval moet het wissen van de gegevens worden uitgesteld.

C) De gegevens zijn niet meer nodig.
Als de Kiesraad persoonsgegevens niet meer nodig heeft, dan moet hij deze wissen. Maar het kan gebeuren dat de betrokkene deze gegevens nog wel nodig heeft. Bijvoorbeeld om een juridische procedure tegen de Kiesraad te kunnen voeren.

Beslist de Kiesraad tot beperking van de verwerking van de persoonsgegevens van de betrokkene en heeft de Kiesraad deze persoonsgegevens eerder met derden gedeeld? Dan moet de Kiesraad zo snel mogelijk deze andere organisaties van de beperking op de hoogte stellen. Ook zij moeten dan de verwerking van deze persoonsgegevens staken.[21]

Artikel 20: Recht op overdraagbaarheid van gegevens
Het recht op overdraagbaarheid van gegevens is door de betrokkene alleen inroepbaar als aan twee cumulatieve eisen wordt voldaan:

1. De grondslag voor de verwerking is toestemming van de betrokkene of een met de betrokkene gesloten overeenkomst.
2. De verwerking van persoonsgegevens vindt via geautomatiseerde procedés plaats.

Bij geen van de verwerkingsactiviteiten die de Kiesraad verricht wordt aan beide voorwaarden voldaan.

Artikel 21: Recht van bezwaar
De betrokkene heeft het recht om vanwege een met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van zijn persoonsgegevens: voor de vervulling van een taak van algemeen belang, voor de vervulling van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen óf voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde. In een enkel geval zal de Kiesraad persoonsgegevens verwerken op grond van een taak van algemeen belang.

Artikel 22: Geautomatiseerde individuele besluitvorming
De Kiesraad maakt geen gebruik van geautomatiseerde individuele besluitvorming. Daarom wordt deze bepaling niet nader toegelicht.

[21] Art. 19 AVG.

Notitie

Onderwerp
Voortgang implementatie AVG: nr. 5

Datum
10 december 2018

Kenmerk
2018-0000942792

Inlichtingen
5.1.2.e
T 070 426 6266
F 070 751 7078

Blad
1 van 4

Aan
Staf

Van
5.1.2.e

1. Inleiding

Voor u ligt de vijfde rapportage over de voortgang van de implementatie van de Algemene verordening gegevensbescherming door de Kiesraad.

2. Stand van zaken

2.1 In aanvulling op de 'algemene privacyverklaring' van de Kiesraad zijn er drie specifieke privacyverklaringen opgesteld en gepubliceerd. Namelijk:
- a. Privacyverklaring voor de registratie van aanduidingen.
- b. Privacyverklaring voor de kandidaatstelling.
- c. Privacyverklaring voor de vaststelling van de uitslag.

2.2 Begin augustus is er een conceptbrief opgesteld om tot verwerkersafspraken met KOOP(SDU) te komen (Ons kenmerk: 2018-0000696425) ten behoeve van de publicaties die de Kiesraad in de Staatscourant doet. Deze is nog niet verstuurd, omdat de verwerkersafspraken nog niet volledig zijn. Bovendien is het wellicht goed de verwerkersafspraken eerst ambtelijk af te stemmen. Op dit moment ben ik nog in afwachting van informatie van 5.1.2.e iets vergelijkbaars speelt bij een concept van de verwerkersovereenkomst met Xerox OBT. Eventueel kan er – bij wijze van alternatief – ook voor worden gekozen om de genoemde organisaties aan te schrijven met het verzoek om ons te informeren over: a) of er rijksbrede afspraken zijn gemaakt en)b wat deze inhouden.

2.3 Op 28 september jl. heeft de secretaris-directeur een brief aan de beoogd Functionaris voor Gegevensbescherming (5.1.2.e) gestuurd (Ons kenmerk: 2018-0000794826). Omdat een reactie uitbleef, is op 30 oktober dezelfde brief per e-mail gestuurd. Deze is vooralsnog onbeantwoord gebleven.

2.4 Op verzoek van de secretaris-directeur heeft er op 4 december 2018 een gesprek plaatsgevonden met 5.1.2.e (CISO BZK) over datalekken. Een conceptverslag staat in DigiDoc, inclusief de daarbij gemaakte afspraken.

2.5 De concept verwerkersovereenkomst van T&T is inmiddels ontvangen. 5.1.2.e 5.1.2.e en ondergetekende hebben deze bekeken. Ik heb op basis van onze beide reacties begin november een conceptreactie (Ons kenmerk: 2018-5.1.2.e) opgesteld en ben in afwachting van de reactie van 5.1.2.e en 5.1.2.e daarop.

2.7 Er is een bijeenkomst voor alle medewerkers van het secretariaat georganiseerd over de implementatie van de AVG. Maandag 10 december 2018.

3. Aantekeningen t.b.v. staf

Naar aanleiding van de vorige notitie over de implementatie van de Algemene verordening gegevensbescherming door de Kiesraad, heeft de staf een groot aantal beslissingen genomen. In twee gevallen lijkt het goed om, vanuit juridisch oogpunt, een aantekening bij de reactie van de staf te maken.

– Bijlage 2, voorstel 5: Aanpassing auto-responder
De staf heeft beslist dat in de auto-responder wordt verwezen naar het privacybeleid. Omdat de mogelijkheid om bezwaar te maken staat vermeld in de algemene privacyverklaring, wordt het niet nodig gevonden die mogelijkheid (ook) expliciet in de auto-responder te noemen.
Aantekening: Omdat de verwerking van persoonsgegevens plaatsvindt op grond van een algemeen belang – art. 6 lid 1 onder e AVG – is de Kiesraad verplicht om betrokkene in het eerste contact op het recht van bezwaar attent te maken. Dit moet duidelijk en gescheiden van andere informatie gebeuren (vgl. art. 21 lid 4 AVG). Ik denk dat de beslissing van de staf daarom niet helemaal conform de AVG is.

– Bijlage 2, voorstel 6: Postbus Kiesraad & Informatiepunt Verkiezingen samenvoegen
De staf meent dat het voorstel om het Informatiepunt Verkiezingen permanent te maken niet met de implementatie van de AVG van doen heeft: het wordt te zijner tijd herbezien.
Aantekening: Het voorstel heeft in zoverre met de implementatie van de AVG te maken, dat – nu het voorstel niet is gevolgd – er ook voor het algemeen nummer van de Kiesraad een bandje ingesproken zal moeten worden, met daarop ingesproken informatie over de wijze waarop de Kiesraad persoonsgegevens verwerkt. Dat beoogde mijn eerdere voorstel te voorkomen.

4. Andere verwerkingen

Voor de meest in het oog springende verwerkingen van persoonsgegevens door de Kiesraad, zijn de nodige stappen gezet. Er zijn ook verwerkingen die tot op heden onderbelicht zijn gebleven. Denk bijvoorbeeld aan de registratie van contactgegevens van medewerkers en leden van de Kiesraad, het relatiebestand en declaraties. Maar het is de vraag of de AVG voor deze verwerkingen wel expliciet

door de Kiesraad geïmplementeerd moet worden. Voor sommige processen, zoals declaraties, worden uitgevoerd door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Medewerkers van de Kiesraad zijn ook bij dit ministerie in dienst, dus voor die AVG-comptabiliteit is de minister verantwoordelijk. Voor relatiebestanden van de Kiesraad geldt mogelijk dat de op centraal departementaal niveau vastgestelde registraties ook van toepassing zijn op de Kiesraad, of minimaal ter inspiratie gebruikt kunnen worden.

5. Correctie

Eerder heb ik een notitie opgesteld met daarin een suggestie voor een werkprocedure voor de afhandelingen van verzoeken van burgers die gebruik willen maken van een hen krachtens de AVG toekomend recht. De verwerkingsverantwoordelijke moet de verzoeker identificeren. De ministerie van Binnenlandse Zaken en Koninkrijksrelaties en Volksgezondheid, Welzijn en Sport en ook grote marktpartijen als NS, hebben zwaardere waarborgen ingebouwd om zich van de identiteit van de verzoeker te vergewissen – deze moet een kopie van zijn legitimatiebewijs met zijn verzoek meesturen – dan in mijn oorspronkelijke voorstel was voorzien. De consequentie hiervan is ook dat een verzoek op grond van de AVG alleen schriftelijk of per e-mail, en niet langer ook mondeling, kan worden ingediend. Ik heb de notitie op dit onderdeel aangepast. Zie bijlage 2, paragraaf 2.

6. Toekomst

Er zijn een aantal grote stappen gezet. Er zijn ook een paar losse eindjes.

6.1 In de vorige rapportage over de implementatie van de AVG is al melding gemaakt van de noodzaak het 'Besluit mandaat en machtiging Kiesraad' te wijzigen en het 'Besluit mandaat en machtiging voorzitter Kiesraad' in te trekken. De conceptbesluiten en begeleidende notitie zijn gereed (hier, hier en hier), maar nog niet aan de Kiesraad voorgelegd. Dit kan op korte termijn gerealiseerd worden.

6.2 In aanvulling op de 'algemene privacyverklaring' van de Kiesraad ontbreken er nog een aantal specifieke privacyverklaringen. De volgende twee onderwerpen verdienen in elk geval nog aandacht:

a. (Tijdelijke) benoeming van volksvertegenwoordigers.
b. Omgang met persoonsgegevens bij het beantwoorden van burgerbrieven, Wob-verzoeken, Informatiepunt Verkiezingen / Postbus Kiesraad.

6.3 De Autoriteit Persoonsgegevens is een toezichthoudende autoriteit als bedoeld in artikel 51 van de AVG. Als duidelijk is wie de 'Functionaris voor gegevensbescherming' (FG) van de Kiesraad is, moet deze bij de Autoriteit Persoonsgegevens worden gemeld. Dit kan hier: https://autoriteitpersoonsgegevens.nl/nl/aanmeldenfg

6.4 In paragraaf 2 ('Stand van Zaken') van deze notitie is benoemd dat de Kiesraad nog bezig is met het maken van verwerkersovereenkomsten met T&T, IVU en Xerox OBT en het maken van verwerkersafspraken met KOOP (SDU). Deze processen moeten nog worden afgerond.

6.5 De nieuwe tekst voor de auto-responders van de Kiesraad (kiesraad@kiesraad.nl / informatiepunt@kiesraad.nl) is opnieuw vastgesteld (vgl. Voortgang Implementatie AVG nr. 4, bijlage 2, voorstel 5, nadat de door de staf gewenste wijzigingen zijn aangebracht), maar moet nog geïmplementeerd worden.

6.6 De tekst op het informatiebandje van het Informatiepunt Verkiezingen moet nog worden aangevuld. Vgl. Voortgang Implementatie AVG nr. 4, bijlage 2, voorstel 7.

6.7 De Kiesraad voldoet nog niet aan de in artikel 30 van de verordening neergelegde registratieplicht.

Aanvankelijk is aangesloten bij het AVG-register dat ook door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties wordt gebruikt. Hier zijn al concepten in opgenomen voor de registratie van aanduidingen, de kandidaatstelling en de benoeming. Een voordeel is dat de FG het register kan zien. Het register kan ook (deels) ontsloten worden op Rijksoverheid.nl Nadelen zijn er ook. Het invoeren ervan neemt veel tijd in beslag. Het twee ogen principe kan bij het invoeren niet worden gevolgd. En het kost de Privacy Officer van de Kiesraad veel tijd, zonder dat duidelijk wordt wat de meerwaarde voor de organisatie is.

Een alternatief is het gebruik van een eigen register. Dat register kan ook uit één of meer Word-bestanden bestaan, die in DigiDoc worden opgeslagen. Als de AVG gevolgd wordt, kan worden volstaan met een vrij beperkt (papieren) register dat voor medewerkers raadpleegbaar is. De algemene en specifieke privacyverklaringen van de Kiesraad zorgen voor ruim voldoende transparantie.

Omdat de FG van de Kiesraad één van de weinige personen is die het AVG-register van de Kiesraad zal inzien, is op dit moment nog geen definitieve keuze gemaakt.

6.8 De Kiesraad moet passende technische en organisatorische maatregelen nemen, om te waarborgen – en te kunnen aantonen – dat de verwerking van persoonsgegevens door de Kiesraad in overeenstemming met de AVG plaatsvindt. Dit zogenoemde gegevensbeschermingsbeleid (Vgl. art. 24 lid 2 AVG) kan een onderdeel worden van het Informatiebeveiligingsbeleid van de Kiesraad, dat in 2019 verder uitgewerkt zal worden. Daaronder valt ook het beleid inzake de omgang met datalekken.

6.9 Privacy is een onderwerp dat nooit 'af' is. Het onderwerp heeft blijvende aandacht nodig. In het bijzonder wanneer beleid of activiteiten ontwikkeld of gewijzigd worden. Hoe kan dit het best geborgd worden? Het is goed om in 2019 bij die vraag stil te staan. Vgl. ook art. 25 lid AVG.

6.10 In aanvulling op de DigiDoc opruimochtenden, zou het secretariaat van de Kiesraad op één dag in het jaar even extra aandacht kunnen besteden aan privacy. Bijvoorbeeld jaarlijks op 28 januari: de Dag van de Privacy! Over vorm en inhoud kan nog worden nagedacht.

Notitie

Onderwerp
Voortgang implementatie AVG: nr. 6

Datum
24 juli 2019

Kenmerk
2019-0000396678

Inlichtingen
5.1.2.e
T 070 426 8566

Aan
Staf

Van
5.1.2.e

1. Inleiding

Sinds de laatste notitie over de voortgang op het AVG-dossier is er weer veel gebeurd. Het leek mij daarom verstandig de staf hierover te informeren. Met het oog op de vakantieperiode en de wens om enkele zaken de komende weken uit te (laten) voeren, vraag ik op een enkel punt om instemming of actie van de zijde van de staf. Deze notitie is besproken in de stafvergadering van 6 augustus 2019 en overeenkomstig bijgewerkt.

2. Stand van zaken

In de eerste helft van dit jaar is begonnen met de concrete uitwerking van de laatste openstaande punten. Het gaat om:

Functionaris voor Gegevensbescherming
Eerder dit jaar hebben we eindelijk bevestigd gekregen dat 5.1.2.e als onze Functionaris Gegevensbescherming wil optreden. In de praktijk gingen we daar al langer van uit, we hebben hem ingeschakeld bij diverse dossiers, maar een meer formele bevestiging heeft lang op zich laten wachten. De FG ziet toe op een correcte naleving van de AVG. Sommige organisaties hebben deze functie intern aangesteld of juist extern aangewezen. Wij hebben voor een tussenvorm gekozen; de FG is niet bij ons werkzaam, maar ook niet geheel extern. 5.1.2.e vervult deze functie namelijk ook voor het ministerie van BZK, het ministerie van V&J, de huurcommissie en het COA. Aangezien ons privacybeleid voor een groot deel overeenkomt met het beleid van BZK, is het eerder als voordeel gezien om dezelfde FG te hebben als BZK.

De FG kan klachten ontvangen over een bepaalde gegevensverwerking en houdt verder toezicht op de maatregelen die wij nemen om een gerechtvaardigde gegevensverwerking te waarborgen. Zijn werkwijze is dat klachten worden ontvangen op het mailadres fg@kiesraad.nl en dat hij deze vervolgens ter behandeling doorstuurt naar mij, als privacy officer. Wij worden vervolgens in de gelegenheid gesteld de klacht zelfstandig af te handelen waarbij 5.1.2.e eventueel

beschikbaar is voor afstemming. Het genoemde mailadres is nieuw (technisch in beheer bij 5.1.2e) en is in onze privacyverklaring opgenomen. Voor het houden van toezicht kunnen wij 5.1.2e op enig moment uitnodigen voor een 'review'. Samen met enkele deskundigen komt hij dan kijken hoe wij de gegevensbescherming hebben ingericht. Wij kunnen hem hiervoor uitnodigen als wij naar onze opvatting klaar zijn met de AVG-implementatie. Dat lijkt mij op dit moment nog niet opportuun.

De functionaris gegevensbescherming valt voor zover het de Kiesraad betreft onder de hoogste ambtenaar van de Kiesraad (de secretaris-directeur). In de praktijk zal hij in eerste instantie vooral met mij contact hebben (en andersom). Desgewenst kunnen jullie ook rechtstreeks contact met hem opnemen. 5.1.2e is te bereiken via 5.1.2e en fg@kiesraad.nl.

Maatschappelijke correspondentie

Er was enige achterstand in de archivering van maatschappelijke correspondentie. De mailboxen Postbus Kiesraad en Postbus Informatiepunt bevatten veel mails die ouder waren dan de bewaartermijn (5 jaar). Deze achterstand is weggewerkt. Ook is geregeld dat voortaan onderhoud gepleegd wordt zodat correspondentie tijdig wordt vernietigd (5.1.2e is actiehouder). Het is niet werkbaar dat dagelijks te doen. Er is daarom gekozen om voortaan aan het begin van elk jaar de correspondentie ouder dan 5 jaar te verwijderen.

Dat geldt niet voor alle correspondentie. Zo kan 'incidentele correspondentie' veelal eerder verwijderd worden (denk aan aanmeldingen symposia, reacties op verzoek om uitslagen of contactgegevens). Er is namelijk geen reden om aanmeldingen te bewaren als het evenement heeft plaatsgevonden, tenzij er vooraf ook nog andere doelen waren geformuleerd (zoals het versturen van een mailing achteraf). Het lijkt mij verstandig dat als dit soort incidentele correspondentie voorzien wordt, er goed nagedacht en zo nodig met mij overlegd wordt hoe met de vernietiging hiervan om te gaan. Ook ben ik zelf alert op het bewaren van dit soort incidentele correspondentie.

Er is ook correspondentie die juist langer bewaard moet worden. In de selectielijst (die bepaalt wanneer wat vernietigd mag worden), staat dat 'correspondentie over uitslagen' bewaard moet blijven. Het is een wat ongelukkige omschrijving, die met een ruime interpretatie onwenselijke gevolgen zou hebben. Enige inperking is mogelijk door dit strikt te zien in het licht van onze taak als centraal stembureau. Om op een werkbare manier deze mails te onderscheiden van gewone correspondentie, kunnen we het criterium hanteren dat het moet gaan om mails waar (1) de Kiesraad als centraal stembureau heeft gereageerd op verzoeken om (2) uitslagen te corrigeren. Bij het jaarlijks opruimmoment kunnen deze mails gezocht worden door op inhoud te zoeken op 'hertel' en die vervolgens in Digidoc te plaatsen (5.1.2e is actiehouder).

Correspondentie is ook opgenomen in FileMaker Pro (FMP). Dit programma ondersteunt het eenvoudig verwijderen van jaargangen nog niet. Dit vergt functionele aanpassing van het programma. 5.1.2e heeft de financiële mogelijkheden hiervoor onderzocht. Het gewenste onderhoud valt niet onder de 16-uur die wij jaarlijks aan onderhoud kunnen besteden. Indien wij deze aanpassing toch dit jaar door wensen te voeren, kost ons dat 5.1.2f (ex. BTW) + 5.1.2f reiskosten. Als hier geen budgettaire ruimte voor is, kunnen we de onbenutte onderhoudsuren van dit jaar begin volgend jaar inzetten voor deze vorm van onderhoud. Vanzelfsprekend lopen we tegen die tijd ruim achter bij het vernietigen van correspondentie.

Vraag: hoe kijkt de staf aan tegen het moment van uitvoeren van onderhoud aan FMP met het oog op de vernietiging overeenkomstig de bewaartermijn?

Beslissing staf: in 2019 uit te voeren. Eerst mogelijkheden onderzoeken bestaande uren in te zetten, anders akkoord met uitvoeren onderhoud volgens offerte.

De automatische berichten die vanuit de beide postbussen verstuurd worden, zijn zoals afgesproken aangepast. Ook het bandje dat een beller hoort wanneer deze in verkiezingstijd naar het Informatiepunt belt, is aangepast. Eenzelfde bandje moet nog op het algemene nummer gezet worden. Hiervoor is bij SSC-ICT een melding aangemaakt. Dit wordt verder afgewacht.

Register van verwerkingen
Alle verwerkingen die wij als Kiesraad hebben, moeten worden geregistreerd. BZK-breed wordt hiervoor een tool ingezet waarmee registraties aangemaakt kunnen worden en gepubliceerd. Publicatie is overigens strikt genomen niet geëist. Wel wordt BZK-breed de opvatting gedeeld dat het goed is transparant te zijn over de verwerkingen die er zijn. Dit register staat inmiddels online. Bij een eerdere notitie aan de staf was nog onduidelijk hoe dit online register eruit zou komen te zien. Er bestond toen enige vrees voor de beeldvorming omtrent de onafhankelijke positie van de Kiesraad. Nu beter zicht is op de wijze waarop het register online gepubliceerd wordt, bestaat er wat mij betreft geen beletsel meer om onze verwerkingen daarin te publiceren. De blijvende afwezigheid van de Kiesraad in dat overzicht kan namelijk ook weer voor vragen zorgen die, naar ik meen, niet goed te pareren zijn met genoemde argumenten.

Voorstel: eerder is door de staf besloten dat het verwerkingsregister niet online in te zien zou moeten zijn. Ik raad aan dit besluit te herzien.

Beslissing staf: akkoord

Naast een aantal BZK-brede meldingen die ook betrekking hebben op de Kiesraad, zijn er een paar Kiesraadspecifieke verwerkingen. Binnen deze verwerkingen vallen een paar handelingen die de Kiesraad met inzet van een verwerker verricht. Met deze verwerkers moeten verwerkersovereenkomsten gesloten worden om te waarborgen dat deze verwerkers de bescherming van persoonsgegevens volgens onze normen en aanwijzingen uitvoeren. Deze verwerkersovereenkomsten zijn nog niet allemaal afgesloten, waarmee ook de Kiesraadspecifieke verwerkingen nog niet konden worden afgerond. De Kiesraad voldoet daarmee nog niet helemaal aan de in artikel 30 van de AVG neergelegde registratieplicht.

De status van de verwerkingen is als volgt:

1. **Registratie van aanduidingen**. Deze verwerking is in afwachting van de verwerkersovereenkomst met KOOP (publicatie lijst met gemachtigden in de Staatscourant). Hiervoor zijn de eerste contacten gelegd. In het verleden is gewacht op afronding van deze verwerkersovereenkomsten alvorens de verwerking af te ronden. Voorlopig is de verwerking niet aan de orde, de eerste publicatie met de namen van de gemachtigden is pas voorzien in 2020 (er zijn dit jaar geen herindelingen). Ik zie er daarom geen kwaad in om de verwerking wel al af te ronden en daarbij te vermelden dat KOOP verwerker is. Parallel gaan we dan aan de slag met het afronden van de verwerkersovereenkomst. Wat mij betreft kan de registratie (die inhoudelijk akkoord is), worden afgerond.

2. **Kandidaatstelling**. Deze verwerking is in afwachting van de verwerkersovereenkomst met KOOP (publicatie Staatscourant) en T&T (raadplegen BRP). Voor beide overeenkomsten zijn contacten gelegd. Ook voor deze verwerking geldt dat deze voorlopig niet aan de orde is, de eerste verkiezing is pas in 2020 gepland. Ik zie er daarom eveneens geen kwaad in om de verwerking al af te ronden en daarbij te vermelden dat KOOP en T&T verwerker zijn. Parallel gaan we dan aan de slag met het afronden van de verwerkersovereenkomsten. Wat mij betreft kan de registratie (die inhoudelijk akkoord is), worden afgerond.
3. **Vaststellen uitslag**. Deze verwerking is eveneens in afwachting van de verwerkersovereenkomst met KOOP (publicatie Staatscourant). Net als hiervoor is dat wat mij betreft geen beletsel de melding af te ronden. Eerder is de aandacht gevestigd op de mogelijke situatie dat de Kiesraad bij een onverhoopt probleem met OSV, uitslagen met IVU zou moeten delen. Voor die situatie is een aparte verwerkersovereenkomst nodig. Sindsdien hebben 5.1.2.e en 5.1.2.e overwogen of het opportuun is een dergelijke overeenkomst nu af te sluiten. Hierbij speelt mee dat deze verwerking geen standaardprocedure is in het vaststellen van een uitslag en dat het betrekkelijk eenvoudig is 'ad hoc' een verwerkersovereenkomst af te sluiten als een dergelijke verwerking daadwerkelijk plaats moet vinden (een concept staat in Digidoc). Wat mij betreft kan de registratie (die inhoudelijk akkoord is), worden afgerond.
4. **Maatschappelijke correspondentie**. Deze is nieuw in de opsomming. Dat komt doordat de staf op 16 oktober 2018 heeft besloten dat de Kiesraad als verwerkingsverantwoordelijke gezien moet worden voor het Informatiepunt Verkiezingen, en niet BZK. Daarmee voldoet de BZK-brede verwerkingsregistratie niet meer. Om dit te verhelpen is een eigen verwerkingsregistratie ontworpen, die overigens inhoudelijk zoveel mogelijk bij de BZK-brede registratie aansluit. Hieronder zou alle maatschappelijke correspondentie van de Kiesraad komen te vallen. Wat mij betreft kan de registratie (die inhoudelijk akkoord is), worden afgerond.

In de komende maanden moet worden bezien hoe om te gaan met een enkele andere verwerking:

- Net als bij de rol van de Kiesraad ten aanzien van maatschappelijke correspondentie zou overwogen kunnen worden om de verwerkingen omtrent Awb-zaken in een eigen melding onder te brengen. Dit omdat de verwerkersverantwoordelijkheid dichter bij de Kiesraad ligt, dan bij de directeur CZW (die als verantwoordelijke is aangewezen voor de BZK-brede verwerking).

<u>Verwerking van persoonsgegevens van medewerkers</u>
Een onderwerp dat in het verleden wel is aangestipt maar nog niet was uitgewerkt, betreft de verwerking van persoonsgegevens van medewerkers. In het oog springende verwerkingen zijn de foto's op de website en het verspreiden van de verjaardagskalender. Veel medewerkergerelateerde verwerkingen die in de organisatie plaatsvinden, zijn essentieel voor een normale bedrijfsvoering. Er is dan een gerechtvaardigd belang om deze verwerkingen te doen. Het gaat dan om:

A. Verwerkingen nodig voor logische toegang tot de systemen
B. Verwerkingen nodig voor fysieke toegang tot het gebouw
C. Verwerkingen nodig voor het beheer, beveiliging en controle op de digitale werkomgeving

D. Verwerkingen nodig voor het beheer, beveiliging en controle op de fysieke toegang tot het gebouw.
E. Verwerkingen nodig voor een interne adressengids en zakelijke documenten (uitsluitend met zakelijke relevante gegevens) en voor zakelijke communicatie (zowel in- als extern).

De BZK-brede registratiemelding (M2499) is hiervoor afdoende. Aan die normen wordt reeds voldaan, mede omdat FMH en SSC-ICT als verwerker betrokken zijn bij de verwerkingen A t/m D.

De BZK-brede registratiemelding voorziet ook verwerkingen van persoonsgegevens van medewerkers die niet essentieel zijn voor de normale bedrijfsvoering. Verwerking kan dan alleen als daarmee wordt ingestemd. Het structureel bijhouden van deze instemming is momenteel nog niet in onze organisatie geïmplementeerd. Een speciaal toestemmingsformulier is ontworpen om hierin te kunnen voorzien. De verwerkingen die hierop zijn opgenomen zijn:

1) het vermelden van mijn voor- en achternaam in het overzicht van secretariaatsmedewerkers op de website;
2) het vermelden van mijn voor- en achternaam in het overzicht van secretariaatsmedewerkers in het jaarverslag;
3) het opnemen van een door mij goedgekeurde foto bij het overzicht van secretariaatsmedewerkers op de website;
4) het opnemen van mijn geboortedatum op de verjaardagskalender die intern verspreid wordt en medewerkers desgewenst kunnen ophangen.

Voorstel: geef nieuwe medewerkers in de inwerkmap een formulier waarop zij hun toestemming kunnen aangeven. De toestemmingen en eventuele latere wijzigingen worden door de ‘privacy officer’ bijgehouden. Voor de huidige medewerkers wordt dit formulier ook verspreid en ingezameld.

Beslissing staf: akkoord

Van secretariaatsuitjes en bijeenkomsten kunnen foto’s gemaakt worden die voor de aardigheid bewaard blijven op de gemeenschappelijk schijf. Hiervoor is geen toestemming vereist. Het lijkt mij zinvol de medewerkers hierop te wijzen en aan te geven dat als zij een foto tegen komen waar ze minder gelukkig mee zijn, zij dan de ‘privacy officer’ kunnen vragen deze te verwijderen. Ik heb dit in het toestemmingsformulier opgenomen.

De consequenties van het niet instemmen met één van de vier verwerkingen lijken duidelijk. Ten aanzien van de laatste (de verjaardagskalender), lijkt het me goed om iets meer uit te werken wat het gevolg is als iemand geen toestemming geeft. Mijns inziens is het vanuit de organisatie een gerechtvaardigd belang dat de secretaris-directeur een collega feliciteert en een attentie (zoals een bloemetje) overhandigt. Voor het (laten) bijhouden van de verjaardagen voor de secretaris-directeur is daarom geen toestemming nodig; dit kan altijd plaatsvinden. Het weigeren van de toestemming heeft hoogstens tot gevolg dat andere collega’s niet op de hoogte zijn van de verjaardag. Een collegiale attentie (zoals het versieren van de kamer) blijft daarmee vermoedelijk achterwege.

Voorstel: beleg in de organisatie het bijhouden van twee verjaardagskalenders, één (geheime) voor de secretaris-directeur en één die intern verspreid kan worden.

Beslissing staf: de verjaardagen worden als geheim item in de agenda's van de staf gezet (geen aparte kalender). Iedereen die daarvoor toestemming geeft wordt vermeld op de interne verjaardagskalender.

Voorstel: beleg in de organisatie dat binnen 180 dagen na het beëindigen van een dienstverband verzamelde gegevens worden verwijderd uit de verjaardagskalender, de website en de map met daarvoor gemaakte portretfoto's.

Beslissing staf: opschonen kalender in checklist beëindigen dienstverband. Opschonen website en map met daarvoor gemaakte portretfoto's actie 5.1.2.e

Overige uitwerkingen

Er is de afgelopen maanden ook een en ander uitvoerend werk verricht:

1) De namen van de gemachtigden en hun plaatsvervangers staan niet meer op onze website.
2) Inleveraars van een kandidatenlijst krijgen schriftelijk informatie over de verwerking van persoonsgegevens in het verkiezingsproces.
3) Het streven naar een FMP met geminimaliseerde data is vertaald naar een instructie in de FMP-handleiding.
4) Onze FG is formeel als FG van de Kiesraad aangemeld bij de Autoriteit Persoonsgegevens.

Nog uit te werken

Een aantal onderwerpen moet nog in de reguliere werkzaamheden worden belegd:

- Stuur politieke partijen drie maanden vóór de dag van kandidaatstelling van elke verkiezing een brief met daarin de namen van degenen die namens de vereniging zijn aangewezen als gemachtigde en plaatsvervangend gemachtigde.
- De Kiesraad moet de stukken die politieke partijen overleggen in het kader van een verzoek tot registratie van een aanduiding c.q. aanwijzing van een (plv.) gemachtigde vernietigen zodra deze niet meer relevant zijn.

Voorstel: beleg deze twee uitwerkingen in de organisatie.

Beslissing staf: eerste onderwerp wordt door 5.1.2.e opgenomen in oude draaiboeken, als uitgangspunt voor toekomstige verkiezingen. Tweede onderwerp laat 5.1.2.e door 5.1.2.e oppakken.

Een aantal andere onderwerpen vraagt nog nadere overdenking:

- De Kiesraad moet kunnen aantonen dat passende technische en organisatorische maatregelen genomen zijn om te waarborgen dat de verwerking van persoonsgegevens door de Kiesraad in overeenstemming met de AVG plaatsvindt. Het is de bedoeling dat dit een onderdeel is van het Informatiebeveiligingsbeleid van de Kiesraad, dat in 2019 o.m. door 5.1.2.e verder uitgewerkt wordt.
- Het beleid inzake de omgang met datalekken.
- Nadenken over een jaarlijks moment van interne bewustwording over privacybescherming, gecombineerd met enkele praktische taken (vergelijkbaar met een Digidocopruimdag).

Incidenten melden

Deze pagina bevat de volgende onderwerpen:

Terug naar homepagina Informatiebeveiliging

In geval van **aanwezigheid** CISO

Melden

Alle vragen en meldingen van (mogelijke) incidenten kun je doen via het mailadres 5.1.2.i @kiesraad.nl wanneer de CISO aan het werk is. Wacht hierna op instructies. Incidenten worden zo anoniem mogelijk geregistreerd en behandeld.

Dus wees een held; meldt!

Voor algemene vragen over de werkplek of ICT kan je de **SSC ICT servicedesk** bellen op: 070-4267447

In geval van **afwezigheid** CISO/Privacy Officer

Er is (mogelijk) sprake van een datalek/incident *binnen* de Kiesraad

Let op: betreft het een incident die een leverancier komt melden? Scroll dan verder naar beneden op deze pagina.

1. **Is de CISO (langer dan 24 uur) niet bereikbaar?**
   a. De CISO is langer dan 24 uur niet bereikbaar; *ga naar stap 2.*
   b. De CISO is korter dan 24 niet bereikbaar/is gewoon aan het werk; stuur een email naar 5.1.2.i @kiesraad.nl en wacht op verder contact.
2. **Wat is er aan de hand?**
   a. Er is sprake van een **storing/ICT probleem/ander soort beveiligingsprobleem** wat kan wachten tot de CISO terug is; stuur een email met uitleg over het incident naar 5.1.2.i @kiesraad.nl en bewaar alle relevante informatie en correspondentie (dus ook Signal/WhatsApp communicatie). Hou bij met wie, wanneer, waarover overleg is geweest en zet dat ook in de email. Als het inmiddels is opgelost, zet er dan ook bij wat de oplossing is geweest en wanneer het precies opgelost is.
   b. Er is sprake van een incident met een **fysieke component** (toegangspas verloren, toegangsdeur wil niet goed sluiten etc); meldt het incident bij de BVC en volg verder de instructies zoals bij 2a hierboven.
   c. Er is (mogelijk) sprake van een **datalek**; *ga naar stap 3.*
3. **Betreft het een datalek met persoonsgegevens?**
   a. **Persoonsgegevens** zijn alle gegevens die (in theorie) in de gelekte context door iemand (wie dan ook) te herleiden zijn naar de identiteit van een levend, natuurlijk persoon. Bijvoorbeeld: telefoonnummer, naam, adres, email adres, IP adres, ID nummer, schoenmaat, etc. Dat het voor een gemiddelde burger niet te herleiden is, is daarvoor niet relevant. Een IP adres kan een burger niet herleiden, maar een internetprovider bijvoorbeeld wel. Dat het IP adres gelekt is naar het internet, maakt daarvoor niet uit. Het is in theorie door iemand te herleiden en daarmee een persoonsgegeven. Neem maatregelen om het datalek te stoppen. Bij verkeerd verzonden emails; vraag de ontvanger de email te verwijderen en dit schriftelijk aan jou te bevestigen. Leg alle interne en externe communicatie vast als een soort logboek. Ook WhatsApp berichten.; *ga naar stap 4.*
   b. **Geen persoonsgegevens**; bepaal of er actie ondernomen moet worden om de impact te verkleinen/het lek te stoppen. Vraag bij verkeerd verzonden emails de ontvanger te bevestigen de mail te hebben verwijderd bijvoorbeeld. Bepaal of er impact te verwachten is voor de betrokkenen wiens informatie is gelekt (ook als het niet om persoonsgegevens, maar bijvoorbeeld zakelijke informatie gaat). Overleg in dat geval met het dienstdoende directielid wat je moet doen. Leg alles vast (communicatie intern, genomen stappen, mails etc) en stuur deze naar 5.1.2.i @kiesraad.nl. Zet erbij wanneer je met wie iets hebt besproken etc. Als een soort logboek.
4. **Neem contact op met de Privacy Officer (** 5.1.2.e **)**
   a. **De Privacy Officer is bereikbaar: volg diens instructies op. Hier eindigen de stappen.**
   b. **De Privacy Officer is NIET bereikbaar:** ***ga naar stap 5.***
5. **Maak een afweging omtrent de rechten en vrijheden van de betrokkene(n)**
   a. **Ik voorzie wel dat de betrokkene(n) in rechten en vrijheden beperkt kan worden**, dan wel last van ondervinden van dit datalek.; iemand kan bijvoorbeeld in de problemen komen omdat diens politieke voorkeur, BSN, mening, geloofsovertuiging, woonadres of andere informatie is gelekt. *ga naar stap 5.*
   b. **Ik voorzie dat de betrokkene(n) geen noemenswaardige inperking van rechten of vrijheden kan verwachten**, dan wel noemenswaardige hinder zal ondervinden van dit datalek. Overleg in dit geval met het dienstdoende directielid. Leg de afweging vast (waarom denk je dit?) en mail alles naar 5.1.2.e @kiesraad.nl.

6. **Indien de betrokkene(n) in rechten en vrijheden beperkt kan worden**:
    a. Overleg met het dienstdoende directielid en vertel dat mogelijk melden bij de Autoriteit Persoonsgegevens en/of betrokkenen zal moeten plaatsvinden.
    b. Neem contact op met de Functionaris Gegevensbescherming [redacted]. Vraag hem om advies.
    c. Leg alle overwegingen en besluiten vast. Bovenstaande moet binnen 72 uur na ontdekking van het datalek zijn voltooid ivm meldplicht.
    d. Indien wordt besloten melding te doen bij de AP; *ga naar stap 6*.
7. **Volg de instructies op de website van de AP en doe een voorinvulling.** Laat het betrokken directielid en de FG de voorinvulling goedkeuren voor verzending. Verzend de melding na goedkeuring. Stuur alle relevante informatie, communicatie (mail/weergave van telefonische of persoonlijke overleggen/WhatsApp gesprekken etc) naar [redacted]@kiesraad.nl. Probeer hierbij een zo volledig mogelijke weergave te geven van het incident en hoe er is gehandeld in de tijd.
8. **Meld het datalek bij betrokkene(n)**
    a. **Er is 1 of meerdere bekende betrokkenen wiens contactgegevens bekend zijn bij ons**: informeer hen en geef aan welke activiteiten de betrokkene kan ondernemen om de impact te verkleinen.
    b. **Er zijn meerdere betrokkenen van wie wij geen contactgegevens hebben**; in dit geval dient er een bericht op een eenvoudig zichtbare plaats op onze website te worden geplaatst om eventuele betrokkenen te informeren.

Een leverancier wil een incident melden/ik kom er niet uit

Verwijs hen naar Office Management. Zij hebben mijn privé telefoonnummer en mogen deze met jou delen in dit geval.

Wees een Held; Meld!

In mei 2023 is de nieuwe procedure incidentmelden vastgesteld. Om deze bekend te maken is een kleine bewustwordingscampagne georganiseerd. Hieronder vind je daarvan de getoonde presentatie en het proces zelf.

Melden

Melden

Alle vragen en meldingen van (mogelijke) incidenten kun je doen via het mailadres 5.1.2.i @kiesraad.nl . Wacht hierna op instructies. Incidenten worden zo anoniem mogelijk geregistreerd en behandeld.

Dus wees een held; meldt!

Contact

Voor overige Informatiebeveiligingsvragen:

5.1.2.e

5.1.2.e @kiesraad.nl

Telefoon: 5.1.2.e

Functie: Chief Information Security Officer

Afdeling: Informatiebeveiliging

Tips

Op de hoogte blijven?

- Elke week op maandagochtend tussen 10:00 en 11:00 heeft de CISO, 5.1.2.e een spreekuur waarin ze vragen kan beantwoorden of jou meer vertellen over informatiebeveiliging. Vind haar in de bieb!
- Elke maand komt de Nieuwsbrief informatiebeveiliging uit op Confluence. Deze is binnen de Afdeling Informatiebeveiliging te vinden en voor iedereen te lezen: Nieuwsbrief Informatiebeveiliging
- Elke maand komt er een Rapportage informatiebeveiliging uit op Confluence. Deze zijn binnen de Afdeling Informatiebeveiliging te vinden en voor iedereen te lezen: Rapportages Informatiebeveiliging

KIESRAAD

TOESTEMMINGSFORMULIER

Gebruik persoonlijke gegevens

Kenmerk
2019-0000395571

Onderdeel
Kiesraad

Inlichtingen
5.1.2.e
T 5.1.2.e

Beste medewerker,

Bij de reguliere werkzaamheden van de Kiesraad kunnen er persoonsgegevens verwerkt worden. De meeste verwerkingen zijn noodzakelijk voor een goede bedrijfsvoering. In aanvulling hierop kunnen medewerkers afzonderlijk toestemming geven voor de volgende (verdere) verwerkingen:

☐ Ik geef toestemming voor het opnemen van mijn **geboortedatum** op de **verjaardagskalender** die intern verspreid wordt en medewerkers desgewenst kunnen raadplegen en ophangen.

☐ Ik geef toestemming voor het vermelden van mijn **voor- en achternaam** in het overzicht van secretariaatsmedewerkers **in het jaarverslag**.

☐ Ik geef toestemming voor het vermelden van mijn **voor- en achternaam** in het overzicht van secretariaatsmedewerkers **op de website**.

☐ Ik geef toestemming voor het **op de website** publiceren van een advies of notitie met daarin de persoonsgegevens die ik zelf als steller heb vermeld (zoals **voor- en achternaam en initialen)**.

☐ Ik geef toestemming voor het opnemen van een door mij goedgekeurde **foto** bij het overzicht van secretariaatsmedewerkers **op de website**.

Een verleende toestemming kan altijd worden ingetrokken. Dit doe je door een aangepast toestemmingsformulier te ondertekenen en bij de privacy officer in te leveren.

Van secretariaatsuitjes en bijeenkomsten kunnen foto's gemaakt worden die voor de aardigheid gedeeld worden en worden opgeslagen op de gemeenschappelijk schijf om ze later bij interne aangelegenheden te gebruiken. Hiervoor is geen toestemming vereist. Mocht er een foto tussen zitten waar je desondanks minder gelukkig mee bent, dan kan je de privacy officer vragen deze te verwijderen.

Datum: _____

Naam: _____

Dit formulier inleveren bij de privacy officer van de Kiesraad 5.1.2.e kamer 14.22).

Wat is de juridische grondslag?
De wijze waarop gegevens van u als medewerker verwerkt worden, is opgenomen in de BZK-brede beschrijving van verwerkingen ten behoeve van de interne bedrijfsvoering (M2499). Voor een aantal verwerkingen is apart instemming vereist. De Kiesraad vraagt als verwerkingsverantwoordelijke toestemming voor de verwerking van uw persoonsgegevens voor genoemde doeleinden (art. 6 lid 1 onder a AVG).

Wie ontvangt de persoonsgegevens?
De website van de Kiesraad is voor een ieder raadpleegbaar. De persoonsgegevens die daar met uw toestemming geplaatst worden, zijn daardoor door derden raadpleegbaar. Uw geboortedatum wordt, als u daarvoor toestemming geeft, alleen raadpleegbaar voor uw collega's.

Wanneer worden mijn gegevens verwijderd?
De door u verstrekte gegevens worden binnen 180 dagen na uw vertrek als medewerker van het secretariaat verwijderd.

Ben ik verplicht om toestemming te verlenen?
Nee. Het verlenen van toestemming geschiedt op basis van vrijwilligheid. Weigert u, dan heeft dit geen nadelige gevolgen voor uw beoordeling of carrièrekansen.

Kan ik mijn toestemming op een later moment intrekken?
Ja, dat is mogelijk. Het intrekken van uw toestemming maakt eerdere verwerking overigens niet onrechtmatig en heeft enkel betrekking op toekomstig gebruik.

Welke rechten heb ik?
Op grond van de Algemene verordening gegevensbescherming heeft u recht op inzage, recht op rectificatie, recht op vergetelheid en recht van bezwaar. Zie voor een uitleg van deze rechten: www.kiesraad.nl/privacy.

Waar kan ik, zo nodig, een klacht indienen?
Een klacht over de verwerking van persoonsgegevens door de Kiesraad kan worden ingediend bij de Functionaris voor de Gegevensbescherming van de Kiesraad; 5.1.2.e (fg@kiesraad.nl). Als u het niet eens bent met de reactie op uw klacht, dan kunt u zich wenden tot de Autoriteit Persoonsgegevens. Zie: www.autoriteitpersoonsgegevens.nl.

KIESRAAD

Notitie

Onderwerp
Samenvatting privacy- en informatiebeveiligingsbeleid en plan

Datum
2 maart 2020

Ons kenmerk
2020-0000111035

Onderdeel
Kiesraad

Inlichtingen
5.1.2.e
T 5.1.2.e

Blad
1 van 5

Aan
De leden van de Kiesraad

Van
5.1.2.e

Op 25 februari jongstleden is het Privacy- en informatiebeveilgingsbeleid Kiesraad 2019-2022 (hierna: het beleid) en het Privacy- en informatiebeveilgingsplan Kiesraad 2020 (hierna: het plan) akkoord bevonden in het stafoverleg. Deze notitie bevat een managementsamenvatting van het 16 pagina's tellende beleid en het 49 pagina's tellende plan, zodat u zich binnen korte tijd van de inhoud op de hoogte kunt stellen.

Beleid

Opzet
Het beleid bevat uitgangspunten op het gebied van privacy en informatiebeveiliging in de periode tot en met 2022. Het sluit in belangrijke mate aan bij het beleid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK). Hiervoor is gekozen omdat de Kiesraad in een aantal opzichten verbonden is met BZK. Zo neemt de Kiesraad verschillende vormen van dienstverlening af bij BZK en zijn de medewerkers, die aan de Kiesraad verantwoording afleggen, in dienst bij BZK.

Hoewel privacy- en informatiebeveiliging niet identiek zijn, hebben ze wel veel gemeen. Daarom is ervoor gekozen om deze onderwerpen samen te betrekken in het op te stellen beleid en plan. De overlap tussen de twee gebieden zit met name in te treffen maatregelen, waarbij de regels over privacybescherming vaak aanvullende eisen stellen ten aanzien van de verwerking van persoonsgegevens.

Organisatie
Het beleid bevat een beschrijving van de relevante actoren voor privacy- en informatiebeveiliging bij de Kiesraad. Het gaat om achtereenvolgens de secretaris-directeur, het hoofd informatiebeveiliging, de proceseigenaren, de privacy en security officer, de functionaris gegevensbescherming en experts bij BZK. Vanwege de raakvlakken met BZK nemen de privacy en security officer deel aan de periodieke overleggen die BZK over privacy- en informatiebeveiliging organiseert.

De taakverdeling is kortgezegd als volgt. De secretaris-directeur gaat, in overleg met de andere stafleden, over de goedkeuring van het beleid en plan. Het hoofd

informatiebeveiliging ziet toe op de realisatie daarvan. De proceseigenaren van gegevensverwerkingen en informatiesystemen zijn verantwoordelijk voor de specifieke risicoafwegingen. De privacy- en security officer dragen zorg voor de uitvoering van het van privacy- en informatiebeveiligingsbeleid en -plan in de dagelijkse praktijk. Ze kunnen advies inwinnen of ondersteuning vragen bij de functionaris gegevensbescherming en andere experts bij BZK.

Doelen
Het beleid bevat een aantal doelen die continue aandacht verdienen, te weten het:
- opstellen en actualiseren van het beleid en plan;
- bijhouden van relevante wet- en regelgeving;
- zorgdragen voor bewustwording onder medewerkers;
- zorgdragen voor voldoende mensen en middelen voor dit onderwerp;
- aandacht hierop vestigen bij het ontwikkelen en beheren van systemen.

Doelen die in bepaalde perioden aandacht verdienen zijn het:
- inrichten van een incidentenproces;
- uitvoeren van integrale risicoanalyses;
- inrichten van een zogeheten Plan Do Check Act cyclus (PDCA);
- vaststellen van de volwassenheidsniveaus van beheersprocessen.

Uitgangspunten
Het beleid bevat de uitgangspunten die bij de Kiesraad voor privacy- en informatiebeveiliging gelden, verdeeld over de volgende onderwerpen:
- Bescherming van persoonsgegevens en andere informatie: conform de gelende wet- en regelgeving zoals bijvoorbeeld de Algemene Verordening; Gegevensbescherming en Baseline Informatiebeveiliging Overheid (BIO);
- Risicomanagement: onder meer door het uitvoeren van risico- en impactanalyses en het stellen van betrouwbaarheidseisen;
- Organisatie privacy- en informatiebeveiliging: over de onderlinge verdeling van taken en het hebben zelfstandige rollen;
- Risicomanagement en de relatie met toezicht en verantwoording: over de manier van verantwoorden zoals het opstellen van in control verklaringen;
- Inkoop, ontwikkeling en beheer: bij onder meer de inkoop en ingebruikname van ICT-diensten, waaronder eventuele clouddiensten;
- Incident- en crisisbeheer: in het geval van bijvoorbeeld een datalek;
- Standaarden, baselines en websites: zoals het gebruik van veilige internetstandaarden;
- Verzoeken en rechten van betrokkenen: zoals een verzoek om correctie van of inzage in persoonsgegevens.

Met een bewustwordingsprogramma zullen medewerkers over bovenstaande doelen en uitgangspunten geïnformeerd worden.

Plan

Opzet
Activiteiten die binnen het tijdsbestek van een jaar nodig zijn om invulling te geven aan het beleid zijn opgenomen in het plan. Het plan wordt jaarlijks opnieuw ter goedkeuring voorgelegd aan de staf en is gerubriceerd als departementaal vertrouwelijk. Het plan bevat in het eerste hoofdstuk een beschrijving van de toepasselijke wet- en regelgeving en een beschrijving van relevante terminologie.

De Baseline Informatiebeveiliging Overheid, oftewel de BIO, geeft ruimte om op basis van een risicoafweging te werken. Het is mogelijk om prioriteiten te stellen in wat bij de Kiesraad nu gedaan moet worden en wat tot een later moment kan

wachten. Het vertrekpunt van het plan is een inventarisatie van de context en de processen bij de Kiesraad, om vast te stellen wat de essentiële processen en informatiesystemen zijn. In onderstaande tabel staan de processen en systemen, de eigenaren en een eerste prioritering. Het is mogelijk dat een later in 2020 uit te voeren uitgebreide risicoanalyse tot de conclusie leidt dat bepaalde processen- en systemen anders geprioriteerd dienen te worden, bijvoorbeeld die van financiën.

Proces	**Eigenaar**	**Prio**	**Informatiesystemen**	**Eigenaar**
Registratie politieke partijen	CC JZ	+		
Uitvoeren kandidaatstelling	CC JZ	++	OSV (++), T&T (+)	CC IB
Uitvoeren uitslagvaststelling	CC JZ	++	OSV (++)	CC IB
Tussentijdse benoemingen	CC JZ	+		
Opstellen adviezen	CC JZ			
Wob-verzoeken behandelen	CC JZ			
Bezwaar, beroep en inlichtingen	CC JZ			
Opstellen beleidsregels en regelingen	CC JZ			
Uitvoeren onderzoek	CC CO			
Verzorgen communicatie	CC CO		Website	CC CO
Informatieverstrekking en -verwerking	CC CO		FMP	CC CO
Ontwikkeling en beheer OSV	CC IB	+	OSV (++)	CC IB
Ontwikkeling en beheer Databank	CC CO		Databank	CC CO
Personeel	SD		P-Direkt, Job2	SD
Financiën	SD	?	3F, Webfocus (?)	SD
Huisvesting	SD			
Automatisering	SD	+	iBabs, Office, Digidoc (+), IT-netwerk (+)	SD
Informatiebeleid	SD			SD

Legenda	
Eigenaar	SD = Secretaris-Directeur, CC = Cluster Coördinator
Thema	JZ = Juridische Zaken, COO: Communicatie en Onderzoek, IB = Informatiebeleid
Prioriteit	+ = Zeer belangrijk, ++ = Kritiek

In het plan zijn bovenstaande kritieke en zeer belangrijke informatiesystemen met behulp van de Handreiking Quickscan Information Security (v 1.0) uitvoeriger tegen het licht gehouden en geclassificeerd als nuttig, belangrijk of vitaal. Vervolgens is een inschatting gemaakt van te stellen eisen aan de beschikbaarheid, integriteit en vertrouwelijkheid van die systemen. De voornaamste kwetsbaarheden zijn benoemd en de invloed is bepaald die de Kiesraad, ketenpartners en dienstenleveranciers hebben op het treffen van mitigerende maatregelen.

Op basis van voormelde analyse zijn de maatregelen die in de BIO zijn opgenomen in het plan geprioriteerd. In het plan is een onderverdeling aangebracht tussen maatregelen die in 2020 ten uitvoer moeten worden gebracht en maatregelen die na dit jaar kunnen worden opgepakt. Dat overzicht, met de hoofdstukken uit de BIO en de bijbehorende activiteiten in 2020 of daarna, treft u aan in onderstaande tabellen.

Prioriteit	BIO-hoofdstuk
1	**5. Informatiebeveiligingsbeleid**
	Beveiligingsbeleid en plan vaststellen
	Beveiligingsbeleid communiceren
	Beveiligingsbeleid beoordelen
	Beveiligingsplan 2021 opstellen
	Beleid en plan voor 2021 vaststellen
2	**6. Organiseren van informatiebeveiliging**
	Beoordelen rollenstructuur
	Vaststellen gewijzigde rollenstructuur
	Beschrijving taken en controleurs verkiezingen
	Overzicht contactgegevens opstellen
	Beoordelen rollenstructuur
3	**14. Acquisitie, ontwikkeling en onderhoud**
	Voorwaarden opnemen in testplan
	Meegeven voor aanbesteding
4	**15. Leveranciersrelaties**
	Leidraad IB en leveranciers opstellen
5	**18. Naleving**
	Opstellen PDCA-cyclus
	Opstellen ISMS
	Audit- en testplan opstellen
	ICV doorontwikkelde OSV opstellen
6	**7. Veilig personeel**
	Informatie indiensttreding beoordelen
	Bewustwordingsprogramma maken
	Bewustwordingsdag organiseren
7	**16. Beheer beveiligingsincidenten**
	IB incidentenproces opstellen
	IB incidentenproces vaststellen

Het uitgangspunt is dat zaken waar de Kiesraad veel invloed op kan uitoefenen en die veel impact hebben op het verkleinen van de belangrijkste risico's, prioriteit hebben. Dit om 'quick wins' zo snel mogelijk op te pakken. In onderstaande tabel staan activiteiten die, gelet op deze analyse, na 2020 kunnen worden opgepakt.

Rest	BIO-hoofdstuk
	8. Verantwoordelijkheid bedrijfsmiddelen
	Beoordelen inventarisatie bedrijfsmiddelen
	Eigenaren inventarisatie bedrijfsmiddelen
	Gedragsregels contracten externen
	Procedure teruggave bedrijfsmiddelen
	Classificatie informatie OSV en verkiezingen
	Classificatieschema ontwerpen
	Informatie: labelen en procedures
	Beleid en eisen verwijderen en transporteren media
	9. Toegangsbeveiliging
	Beleid toegangsbeveiliging beoordelen
	Beschrijving rolverdeling OSV bij verkiezingen
	Na classificatie inlogprocedure beoordelen
	Na analyse wachtwoordbeleid beoordelen
	10. Cryptografie
	11. Fysieke beveiliging en van de omgeving

	Expliciteren interne maatregelen
	12. Beveiliging bedrijfsvoering
	Beoordelen doorontwikkeling
	Meegeven voor aanbesteding
	13. Communicatiebeveiliging
	Beoordelen doorontwikkeling
	Meegeven voor aanbesteding
	17. Communicatiebeveiliging
	Inventariseren continuïteitsplannen

In het plan staat voor ieder van de beheersmaatregelen uit de BIO beschreven welke activiteiten daar voor de Kiesraad uit voortvloeien. Het betreft de activiteiten die in bovenstaande tabellen met steekwoorden zijn opgeschreven.

KIESRAAD

Privacy- en informatiebeveiligingsbeleid Kiesraad

2019 - 2022

Versie 1.0

Dit document wordt beheerd door de privacy en security officer, in naam van het hoofd informatiebeveiliging.

Versie	Omschrijving	Toelichting	Steller	Datum
0.1	Concept 1	Voorstel	5 1 2 e	20-09-2019
0.2	Concept 2	Aangepast nav eerste review en cl.oördinator toegevoegd	5 1 2 e	27-09-2019
1.0	Goedkeuring	Voorstel voor stafoverleg	5 1 2 e	07-02-2019

Afkortingen

AVG	Algemene Verordening Gegevensbescherming
BIO	Baseline Informatiebeveiliging Overheid
BIR	Baseline Informatiebeveiliging Rijksdienst
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CIO	Chief Information Officer, oftewel het hoofd informatiebeleid
CIO&IM	Directie CIO en Informatiemanagement binnen BZK
CISO	Chief Information Security Officer
FG	Functionaris voor de Gegevensbescherming
ICV	In Control Verklaring
NDN	Nationaal Detectie Netwerk
NCSC	Nationaal Cyber Security Centrum
PDCA-cyclus	Plan Do Check Act cyclus.
PIA	Privacy Impact Assessment
VIR	Voorschrift Informatiebeveiliging Rijksdienst
VIR-BI	Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie

Voorwoord

Voor u ligt het Privacy- en informatiebeveiligingsbeleid Kiesraad 2019 (hierna: het Beveiligingsbeleid). De omvang en ernst van de digitale dreiging in Nederland zijn aanzienlijk en blijven zich ontwikkelen. Digitale dreiging rond verkiezingen kreeg de afgelopen jaren in binnen- en buitenland veel aandacht. De Kiesraad, waar in dit document zowel de Raad als diens secretariaat onder verstaan wordt, vervult als centraal stembureau, adviesorgaan en informatiecentrum een belangrijke rol op gebied van verkiezingen en het kiesrecht. Reden te meer om voldoende aandacht te besteden aan de beveiliging van informatie bij de Kiesraad.

Het Beveiligingsbeleid bevat strategische uitgangspunten van de Kiesraad op het gebied van privacy en informatiebeveiliging, in termen van te realiseren doelen in de periode tot en met 2022. De Kiesraad gebruikt deze strategische uitgangspunten als richtsnoer in de dagelijkse praktijk en bij het uitwerken van toekomstige plannen. Activiteiten die binnen het tijdsbestek van een jaar nodig zijn om invulling te geven aan het Beveiligingsbeleid worden opgenomen in het Privacy- en informatiebeveiligingsplan Kiesraad (hierna: het Beveiligingsplan).

In het Beveiligingsbeleid is uitgewerkt op welke wijze de omgang met privacy- en informatiebeveiliging inzichtelijk gemaakt wordt, hoe hierop gestuurd wordt en hoe er verantwoording over wordt afgelegd. Kern van het Beveiligingsbeleid is dat de invulling ervan gebaseerd is op risicobeheersing, waarbij verschillende aspecten en belangen worden gewogen. De proceseigenaar van de verwerking of het informatiesysteem maakt uiteindelijk de integrale risicoafweging.

Het Beveiligingsbeleid is in belangrijke mate ontleend aan het beleidskader Privacy- en Informatiebescherming 2019 van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Hiervoor is gekozen omdat de Kiesraad in een aantal opzichten verbonden is met BZK. Zo neemt de Kiesraad verschillende vormen van dienstverlening af bij dat ministerie en zijn de ambtenaren, die bij de Kiesraad werkzaam zijn en aan de Kiesraad verantwoording afleggen, in dienst bij BZK.

Inhoudsopgave

1. Inleiding

De Rijksoverheid, en daarmee de Kiesraad, is gehouden aan allerhande wet- en regelgeving, waaronder de regels over de bescherming van persoonsgegevens en informatiebeveiliging. Zowel de Algemene Verordening Gegevensbescherming (AVG) als het kader rondom informatiebeveiliging biedt de ruimte om beslissingen te nemen gebaseerd op een risico-inschatting. De Kiesraad zal risico-inschattingen maken en daarbij ook kijken naar de impact die privacy- en informatiebeveiliging heeft op de kwaliteit en effectiviteit van de taken die de Kiesraad uitvoert.

Privacy- en informatiebeveiliging
Privacybescherming en informatiebeveiliging zijn niet identiek, maar hebben veel met elkaar gemeen. Dat is de reden waarom één beleidskader is opgesteld, dat zowel de uitgangspunten van de Kiesraad op het gebied van privacybescherming als informatiebeveiliging bevat. De overlap tussen de twee gebieden zit met name in te treffen maatregelen, waarbij de regels over privacybescherming vaak aanvullende eisen stellen ten aanzien van de verwerking van persoonsgegevens.

Medewerkers
Voor medewerkers is algemene kennis op het gebied van privacy- en informatiebeveiliging essentieel. Met behulp van een bewustwordingsprogramma wordt die kennis aangeboden, toegespitst op de werkzaamheden binnen de Kiesraad. Daarbij zal aandacht worden besteed aan de algemene gedragsregels. Naleving van die gedragsregels, zoals ook vastgesteld in de rijksbrede gedragscode integriteit en de gedragsreling voor de digitale werkomgeving, is vereist.

Informatiebeleid
De secretaris-directeur is primair verantwoordelijk voor het vaststellen van het Beveiligingsbeleid en het Beveiligingsplan, bijgestaan door de andere stafleden. Als hoofd informatiebeveiliging is de secretaris-directeur ook verantwoordelijk voor het realiseren van privacy- en informatiebeveiliging.

Er kan wrijving ontstaan tussen het belang dat gediend is bij minimalisatie van de risico's op het gebied van privacy- en informatiebeveiliging en de belangen die spelen bij het uitvoeren van Kiesraadtaken. De proceseigenaar van een verwerking of informatiesysteem maakt op basis van risicobeheersing de uiteindelijke afweging en neemt beslissingen, waar nodig met assistentie van de privacy en security officer. De wijze waarop dit gebeurt is uitgewerkt in dit Beveiligingsbeleid. De secretaris-directeur en de privacy en security officer kunnen bij BZK desgewenst advies inwinnen of om ondersteuning vragen.

Opbouw
Het Beveiligingsbeleid, dit document, is als volgt opgebouwd. Allereerst wordt beknopte beschrijving gegeven van de voor privacy- en informatiebeveiliging relevante actoren binnen de Kiesraad (hoofdstuk 1). Daarna worden de strategische doelen van de Kiesraad benoemd en onderbouwd (hoofdstuk 2). En vervolgens worden op basis van die doelen de uitgangspunten geformuleerd die de Kiesraad hanteert (hoofdstuk 3).

2. Organisatie

Rollen en verantwoordelijkheden

Binnen de Kiesraad zijn de volgende taken en verantwoordelijkheden relevant met betrekking tot privacy- en informatiebeveiliging:

Hoofd informatiebeveiliging (secretaris directeur, in toekomst mogelijk de cluster coördinator IT en Informatiebeleid)
- stelt het Beveiligingsbeleid en het Beveiligingsplan vast, in samenspraak met de andere stafleden;
- rapporteert aan de Kiesraad over de vaststelling van het Beveiligingsbeleid en -plan;
- is verantwoordelijk ervoor te zorgen dat voldoende kennis en kunde op het gebied van privacy- en informatiebeveiliging binnen de Kiesraad aanwezig is;
- rapporteert aan de Kiesraad over de uitvoering van het Beveiligingsbeleid en -plan;
- draagt zorg voor de naleving van het Beveiligingsbeleid en -plan en de uitvoering ervan, onder meer met betrekking tot bij de Kiesraad aanwezige informatiesystemen en verwerkingen;
- wijst vanuit zijn/haar verantwoordelijkheid een privacy en security officer aan, met een onafhankelijke rol (zie uitgangspunten nrs. 15 en 16), voor de ondersteuning van privacy- en informatiebeveiliging;
- geeft de privacy en security officer aandachtspunten mee bij de toetsing van de uitvoering van het Beveiligingsbeleid en -plan;
- zorgt voor de totstandkoming van de jaarlijkse verantwoording over de privacy- en informatiebeveiliging;

Proceseigenaar (secretaris-directeur en clustercoördinatoren)
- is proceseigenaar van de onder hem of haar verantwoordelijkheid vallende verwerkingen, informatiesystemen en diensten;
- legt bij de beheersing van ICT-projecten nadruk op het tijdig opleveren van essentiële producten, zoals risicoanalyses en privacy impact analyses;
- stelt, overeenkomstig de planning in het Beveiligingsbeleid- en plan en met assistentie van de privacy en security officer, de betrouwbaarheidseisen vast voor de systemen, verwerkingen en werkprocessen op basis van een integrale risicoanalyse;
- draagt, met assistentie van de privacy en security officer, zorg voor een adequaat stelsel van gedocumenteerde en verifieerbare beheersmaatregelen naar aanleiding van gehouden risicoanalyses;
- evalueert en actualiseert, met assistentie van de privacy en security officer, aanwezige integrale risicoanalyses minimaal iedere twee jaar, of eerder indien wijzigingen in proces of beheersomgeving dit vereisen.
- stimuleert dat medewerkers tot deelname aan het bewustwordingsprogramma van de Kiesraad rondom privacy- en informatiebeveiliging;

Privacy officer
- aanspreekpunt op het gebied van privacybescherming;
- adviseren over privacybescherming;
- uitvoeren van taken die voortvloeien uit het Beveiligingsbeleid- en plan;
- bewaken naleving van de geldende wet- en regelgeving;
- agenderen onderwerpen op het gebied van privacybescherming bij het hoofd informatiebeveiliging en de staf;
- verzorgen communicatie over privacybescherming;
- zorgt dat medewerkers zorgvuldig met (persoons)gegevens, informatiesystemen en overige hulpmiddelen omgaan en de daarvoor vastgestelde reglementen naleven;
- vertegenwoordigen van de Kiesraad op het gebied van privacybescherming in het CISO-overleg bij BZK;
- inventariseert jaarlijks actuele risico's waarbij de te beschermen belangen een bepaald niveau overschrijden (zie uitgangspunt nr. 14);

- richt een planning en control cyclus in voor de verantwoording over privacybescherming;
- richt een incidentenprocedure in voor privacybescherming;
- toezien op naleving van de incidentenprocedure binnen de Kiesraad;
- afhandelen incidenten en hierover rapporteren aan het hoofd informatiebeveiliging.

Security officer
- aanspreekpunt op het gebied van informatiebeveiliging;
- adviseren over informatiebeveiliging;
- uitvoeren van taken die voortvloeien uit het Beveiligingsbeleid- en plan;
- bewaken naleving van de geldende wet- en regelgeving;
- agenderen onderwerpen op het gebied van informatiebeveiliging bij het hoofd informatiebeveiliging en de staf;
- verzorgen communicatie over informatiebeveiliging;
- zorgt dat medewerkers zorgvuldig met (persoons)gegevens, informatiesystemen en overige hulpmiddelen omgaan en de daarvoor vastgestelde reglementen naleven;
- vertegenwoordigen van de Kiesraad op het gebied van informatiebeveiliging in het CISO-overleg bij BZK;
- inventariseert jaarlijks actuele risico's waarbij de te beschermen belangen een bepaald niveau overschrijden (zie uitgangspunt nr. 14);
- richt een planning en control cyclus in voor de verantwoording over informatiebeveiliging;
- richt een incidentenprocedure in voor informatiebeveiliging;
- toezien op naleving van de incidentenprocedure binnen de Kiesraad;
- afhandelen incidenten en hierover rapporteren aan het hoofd informatiebeveiliging.

Buiten de Kiesraad zijn de volgende taken en verantwoordelijkheden relevant met betrekking tot privacy- en informatiebeveiliging:

CIO bij BZK
- stelt namens de SG de kaders voor privacy- en informatiebeveiliging van BZK op en evalueert deze periodiek;
- adviseert en ondersteunt de Kiesraad desgewenst over risicomanagement;
- zorgt voor de totstandkoming van de jaarlijkse verantwoording over de privacy- en informatiebeveiliging voor de verwerkingen en systemen die onderdeel zijn van de risicokaart BZK.

CISO bij BZK (Chief Information Security Officer)
- voert taken uit voor de bescherming van privacy en informatie, onder de verantwoordelijkheid van de CIO-BZK.
- onderhoudt contact met de CISO's en privacy-officers van de diverse BZK-onderdelen en met de privacy en security officer van de Kiesraad;
- zit het CISO-overleg voor.

Functionaris gegevensbescherming (FG)
- ziet toe op de juiste toepassing van de AVG binnen de Kiesraad;
- ondersteunt hiermee de secretaris-directeur bij zijn ambtelijke verantwoordelijkheid ten aanzien van de beveiliging van persoonsgegevens;
- kan de Kiesraad adviseren bij het vaststellen van eisen die uit de AVG volgen.

3. Strategische doelen

Nieuwe technologieën volgen elkaar tegenwoordig in hoog tempo op. Toegenomen digitalisering en complexere dienstverlening leiden tot kwetsbaardere systemen en infrastructuren. Er bestaat ook een verhoogde dreiging van statelijke actoren, criminele organisaties en hackers.

Dit hoofdstuk uit het Beveiligingsbeleid bevat strategische doelen om uitdagingen op het gebied van privacy- en informatiebeveiliging het hoofd te bieden. De doelen zijn hieronder verdeeld over drie vragen: de vraag wat continue aandacht verdient (continuïteit), wat er begin 2020 gedaan moet zijn (kortetermijndoelen) en wat er in de periode 2020-2022 en daarna bereikt zou moeten worden (langetermijndoelen).

Continuiteit

Beveiligingsplan
De strategische doelen worden op basis van een interne analyse in het Beveiligingsplan vertaald naar een concrete planning.

> **Actie**: activiteiten die binnen het tijdsbestek van een jaar nodig zijn om invulling te geven aan het Beveiligingsbeleid worden door het hoofd informatiebeveiliging opgenomen in het Beveiligingsplan. Het plan voor 2020 wordt eind 2019 door het hoofd informatiebeveiliging vastgesteld.

Regelgeving
De Kiesraad dient geldende regels op het gebied van informatiebeveiliging na te leven, waaronder het Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007). Voor de bescherming van privacy geldt de AVG, uitgewerkt in de Uitvoeringswet AVG en de Aanpassingswet AVG, waarmee ook de Kieswet gewijzigd is.

> **Actie**: de privacy en security officer bewaken de naleving van de geldende wet- en regelgeving en houden voor de Kiesraad relevante wijzigingen bij. Zo nodig brengen de privacy en security officer hierover advies uit aan de staf.

Bewustzijn
Informatiebeveiligingsincidenten kunnen niet alleen ontstaan door hackers met kwade bedoelingen, maar ook door onzorgvuldigheid van medewerkers. Het is belangrijk dat medewerkers veilig en bewust werken met informatie, zowel offline als online. De verantwoordelijkheid om te zorgen dat informatie voldoende beschermd is tegen dreigingen, moet leven in het bewustzijn van de volledige organisatie.

> **Actie**: de privacy en security officer zullen aandacht besteden aan bewustzijn op het gebied van privacy- en informatiebeveiliging. Deels generiek en deels specifiek, toegespitst op de werkzaamheden binnen de Kiesraad.

Organisatorisch
Om te zorgen dat privacy- en informatiebeveiliging zowel binnen projecten als de dagelijkse werkzaamheden van de Kiesraad geborgd is, dient van de privacy- en informatiebeveiligingsfunctie voldoende kracht uit te gaan. Dit betekent voldoende stevig uitgedrukt in mensen, middelen, capaciteit en de positie binnen de Kiesraad als organisatie.

> **Actie**: het hoofd informatiebeveiliging bekijkt of, en zo ja waar, de privacy- en informatiebeveiligingsfunctie verstrekt moet worden, zowel binnen projecten als bij dagelijkse werkzaamheden. Waar nodig bespreekt het hoofd informatiebeveiliging dit in de staf.

Ontwikkeling en beheer
Aandacht voor privacy- en informatiebeveiliging in het stadium van ontwikkeling, inrichting en beheer van diensten heeft een positief effect op het tegengaan van dreigingen. Juist bij de ontwikkeling van diensten is het van belang privacy- en informatiebeveiliging vanaf het begin mee te nemen. In een later stadium toevoegen van vergeten eisen is kostbaar en soms onmogelijk.

Actie: bij het ontwikkelen van beleid, systemen en diensten wordt privacy- en informatiebeveiliging meegenomen. Bij de beheersing van ICT-projecten zal de proceseigenaar nadruk leggen op het tijdig opleveren van essentiële producten, zoals risicoanalyses en privacy impact analyses.

Korte termijn

Risicokaart
Risico's ten aanzien van informatiebeveiliging zijn niet tegen te gaan door het treffen van alleen preventieve maatregelen. Het wordt van steeds groter belang om eventueel geslaagde indringpogingen te detecteren. Werkplekken die vanuit SSC-ICT worden geleverd zijn aangesloten op het Nationaal Detectie Netwerk (NDN). Organisaties die deelnemen aan het NDN leveren (anoniem) informatie. Wanneer acute of relevante dreiging ontstaat, stuurt het Nationaal Cyber Security Centrum (NCSC) een melding naar alle aangesloten organisaties.

Eind 2019 zullen alle diensten op de risicokaart van BZK aangesloten zijn op de dienstverlening van het NCSC. Dit houdt in dat de dienst bij het NCSC bekend is en dat meldingen ten aanzien van kwetsbaarheden worden ontvangen en opgevolgd. Diensten op de risicokaart waar de Kiesraad gebruik van maakt zijn DigiD, Haagse Ring, Officiële elektronische bekendmakingen, Digidoc, P-direkt en generieke ICT dienstverlening van SSC-ICT.

Actie: de risicokaart van BZK bestaat uit diensten/voorzieningen met een I(CT)-component waar BZK voor verantwoordelijk is en waarvan de risico's zodanig groot zijn dat het wenselijk is dat op bestuurlijk niveau inzicht wordt gegeven in de risico's. Als de Kiesraad een I(CT)-dienst afneemt die ontbreekt op de risicokaart, maar waaraan wel dat gewicht toegekend dient te worden, dan stelt het hoofd informatiebeveiliging het ministerie van BZK hiervan op de hoogte.

Verwerkingen
Persoonsgegevens zijn een bijzondere categorie van informatie. Artikel 30 van de AVG bepaalt dat de verwerkingsverantwoordelijke in een register informatie moet bijhouden over de verwerkingen van persoonsgegevens die hij verricht. De verwerkingsverantwoordelijke moet op grond van artikel 12 van de AVG passende maatregelen nemen om de betrokkene te informeren over de gegevensverwerking.

Actie: de privacy officer neemt alle (risicovolle) verwerkingen van persoonsgegevens op in het AVG register rijksoverheid[1], stelt een privacyverklaring over de verwerking van persoonsgegevens op en publiceert deze.[2] Verder vraagt de privacy officer aan medewerkers toestemming voor de verwerking van persoonsgegevens op de website, in het jaarverslag en als steller in documenten.

Incidentenproces
Eind 2019 zal een BZK-breed incidentenproces ingericht zijn en functioneren, zodat incidenten bij het departement of uitvoeringsorganisaties, die een mogelijk bestuurlijke of politieke impact hebben, worden gemeld bij de CIO-BZK.

Actie: de privacy en security officer stellen een incidentenproces vast waarin staat hoe binnen de Kiesraad met privacy- en informatiebeveiligingsincidenten wordt omgegaan en aan wie die worden gemeld.

Internetstandaarden
Alle websites die bij private partijen zijn ondergebracht dienen aan de veilige Internetstandaarden te voldoen, zoals gedefinieerd door het Forum Standaardisatie[3].

1 https://www.avgregisterrijksoverheid.nl/Ministerie_van_Binnenlandse_Zaken_en_Koninkrijksrelaties/index.html
2 https://www.kiesraad.nl/privacy
3 Zie notitie Forum Standaardisatie: FS 181010.4B en de controle die wordt uitgevoerd via www.internet.nl

Actie: de privacy en security officer stellen vast of websites van de Kiesraad die bij private partijen zijn ondergebracht aan de veilige Internetstandaarden voldoen en, zo nee, hoe en binnen welk tijdsbestek die websites aan deze eisen zullen voldoen.

Lange termijn

Integrale risicoanalyses
Persoonsgegevens zijn een bijzondere categorie van informatie. Artikel 32 van de AVG stelt dat passende technische en organisatorische maatregelen moeten worden getroffen ter bescherming van de verwerking van de persoonsgegevens. Op dit vlak komen privacybescherming en informatiebeveiliging bij elkaar. Het is van belang om impactanalyses over de verwerking van persoonsgegevens niet los te zien van de impactanalyses die betrekking hebben op de 'overige' informatieverwerking.

Voor alle (risicovolle) verwerkingen van persoonsgegevens worden bij BZK en diens uitvoeringsorganisaties actuele, integrale risicoanalyses opgesteld, inhoudend dat zowel de privacyrisico's als de informatiebeveiligingsrisico's worden beschouwd.

Actie: het hoofd informatiebeveiliging stelt in het Beveiligingsplan vast welke integrale risicoanalyses uitgevoerd moeten worden en in welke periode die zullen plaatsvinden.

PDCA-cyclus
Te nemen maatregelen die voortvloeien uit de risicoanalyses, worden geborgd in een Plan Do Check Act cyclus (PDCA). Informatiebeveiliging is een continu verbeterproces en de PDCA-cyclus vormt het managementsysteem daarvan.

Actie: de privacy en security officer stellen een PDCA-cyclus vast voor privacy- en informatiebeveiliging binnen de Kiesraad, die wordt gehanteerd bij de uitvoering van het Beveiligingsbeleid en -plan.

Volwassenheidsmodel
De focus rondom privacy- en informatiebeveiliging is de laatste jaren meer komen te liggen op risicomanagement in plaats van compliancy 'op basis van lijstjes'. In lijn hiermee wordt binnen het Rijk meer gestuurd op basis van 'volwassenheid' van beheerprocessen. Hiervoor wordt het NBA-volwassenheidsmodel gehanteerd.[4] In 2019 worden delen van dit model ingericht om te sturen op de volwassenheid van IB-processen bij BZK en binnen diens uitvoeringsorganisaties.

Actie: de privacy en security officer stellen vast of, en zo ja welke, onderdelen uit het NBA-volwassenheidsmodel gebruikt gaan worden binnen de Kiesraad en stelt de volwassenheidsniveaus ten aanzien van geselecteerde, relevante beheersprocessen vast.

4 https://www.nba.nl/globalassets/over-de-nba/ledengroepen/lio/handreiking-bij-volwassenheidsmodel-informatiebeveiliging/handreiking_volwassenheidsmodel_informatiebeveiliging.pdf

4. Uitgangspunten

Het kader voor privacy- en informatiebeveiliging binnen de Kiesraad is geformuleerd aan de hand van uitgangspunten. Deze uitgangspunten beschrijven het proces van risicomanagement en verantwoording, inclusief de inrichting van de organisatie. De inrichting van de organisatie is met wat meer toelichting beschreven in het tweede hoofdstuk. De verantwoordelijkheid voor het voldoen aan de uitgangspunten ligt bij het hoofd informatiebeveiliging. Die moet zich, gesteund door de privacy en security officer, ervan vergewissen dat de Kiesraad aan de uitgangspunten voldoet.

De volgende uitgangspunten voor privacy- en informatiebeveiliging worden binnen de Kiesraad gehanteerd:

Bescherming van persoonsgegevens en andere informatie

1. Bij de verwerking van persoonsgegevens wordt voldaan aan de AVG, waaronder de zes in artikel 5 van de AVG genoemde beginselen:
    a. rechtmatigheid, behoorlijkheid en transparantie;
    b. doelbinding;
    c. minimale gegevensverwerking;
    d. juistheid;
    e. opslagbeperking;
    f. integriteit en vertrouwelijkheid.
2. Voor *Departementaal Vertrouwelijke en Staatsgeheime* informatie dient de inrichting van de informatiebeveiliging conform het VIR-BI 2013 te zijn, voor zover van toepassing;
3. Het juiste niveau van privacy- en informatiebeveiliging komt tot stand op basis van risicomanagement (zoals uitwerkt in het VIR 2007 en bedoeld in de AVG). Bestaande kaders en wetgeving bepalen hierbij het minimumniveau, waaronder:
    a. Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR 2007);
    b. Baseline Informatiebeveiliging Overheid, Baseline Informatiebeveiliging Rijksdienst (BIO / BIR 2017[5]);
    c. Besluit Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI 2013);
    d. Algemene Verordening Gegevensbescherming;
    e. Archiefwet 1995.
4. Maatregelen ter bescherming van verwerkingen van persoonsgegevens worden geïntegreerd opgepakt met maatregelen die worden getroffen ter beveiliging van informatie in brede zin. Hierbij wordt er in de volle breedte rekening gehouden met de geldende wet- en regelgeving, zoals de AVG.
5. Elke verwerking of elk informatiesysteem[6] heeft een proceseigenaar[7] die verantwoordelijk is voor het risicomanagement dat op het informatiesysteem wordt toegepast. Over het algemeen zal dit de clustercoördinator of secretaris-directeur zijn, die als opdrachtgever optreedt.
6. In aanvulling op het algemene fysieke toegangsbeleid, dient voor individuele informatiesystemen en verwerkingen, net als voor de algemene ICT, het volgende toegangsbeleid te worden gehanteerd:
    a. De noodzaak voor het verlenen van toegang komt voort uit de functie of rol die iemand vervult. Zodra de noodzaak vervalt, dient de toegang te vervallen.
    b. Indien een informatiesysteem of verantwoordelijkheidsgebied verschillende niveaus van toegang onderscheidt, dient per niveau inzichtelijk te zijn welke eisen er voor het verlenen van toegang worden gesteld.
    c. De verantwoordelijkheid toezicht te houden op het tijdig intrekken van toegangsrechten (autorisaties) ligt bij de proceseigenaar, en dient voor interne systemen gebaseerd te zijn op de life-cycle van de gebruikers zoals wordt beheerd in het Identity Management Systeem.

---

5 Deze zijn voor wat betreft de normen en maatregelen identiek.

6 Volgens het VIR 2007: 'een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.'

7 In het VIR eigenaar van het informatiesysteem genoemd en in de AVG verwerkingsverantwoordelijke genoemd.

d. Om toegangsbeheer sluitend te maken, is het de verantwoordelijkheid van het lijnmanagement om te zorgen dat intern en extern personeel tijdig uitdienst wordt gemeld.
e. De eigenaar van het informatiesysteem kan de werking van het proces van toekennen en intrekken van bevoegdheden aantonen.
f. Informatiesystemen die een generieke toegang voor alle gebruikers hebben (zoals het Rijksportaal) hoeven geen eigen administratie bij te houden. In dit geval wordt gesteund op het toegangsbeheer in de algemene ICT infrastructuur.

Risicomanagement

7. De secretaris-directeur of clustercoördinator die proceseigenaar is van het informatiesysteem of de verwerking, is ervoor verantwoordelijk dat het risicomanagement inzichtelijk en toetsbaar is. Dit betekent in essentie dat:
    a. Betrouwbaarheidseisen voor een informatiesysteem of verwerking expliciet zijn vastgelegd. Dit zijn betrouwbaarheidseisen voortvloeiend uit een risicoanalyse op het te ondersteunen proces en een impactanalyse op privacyaspecten indien van toepassing;
    b. De keuze en implementatie van maatregelen die voortvloeien uit de betrouwbaarheidseisen expliciet zijn gemaakt, vastgelegd en op een passend niveau zijn.[8]
    c. De effectiviteit van de geïmplementeerde maatregelen wordt geëvalueerd en aan de hand hiervan eventueel worden bijgesteld.
8. Bij risicomanagement dienen eerdergenoemde eisen te worden ingevuld.
   Bij verwerkingen van persoonsgegevens met een verhoogd risico, dienen de vragen uit het model PIA Rijksoverheid in de integrale risicoanalyse te worden geadresseerd en beantwoord.[9]
   De quickscan BIR wordt gehanteerd om een eerste inschatting van risico's te maken. Naast het gebruik van bestaande technieken, zoals IRAM (Information Risk Analysis Methodology) wat een geïntegreerde risicomethode is, worden door BZK, directie CIO&IM, sjablonen aangeboden die gebruikt kunnen worden.
9. Bij de uitvoering van ICT-projecten dienen risicoanalyses zoals hiervoor beschreven te zijn uitgevoerd onder verantwoordelijkheid van de proceseigenaar dan wel de projectleider of programmamanager, afhankelijk van de omvang van het ICT-project. Risicoanalyses voor ICT-projecten dienen te worden gevalideerd door het hoofd informatiebeveiliging dan wel door de stuurgroep.
10. Bij de keuze van maatregelen hoeft alleen rekening gehouden te worden met reële dreigingen: tegen dreigingen met een grote impact maar een zeer kleine kans, zoals atoom- en natuurrampen, worden geen specifieke maatregelen getroffen.
    Daarnaast hoeven uitsluitend dreigingen in kaart te worden gebracht die *geen* deel uitmaken van het dreigingenprofiel dat aan de basis van de BIR heeft gelegen. Nota Bene: de constatering dat er geen relevante additionele dreigingen zijn, dient in de risicoanalyse te zijn onderbouwd.
11. Bij het bepalen van maatregelen ter borging van de informatiebeveiliging wordt de relevantie van spionage en een langdurige en doelgerichte cyberaanval (advanced persistent threat), als factor expliciet benoemd (afhankelijk van de gekozen vorm in de risicoanalyses en informatiebeveiligingsplannen).
12. Risicoanalyses dienen actueel te worden gehouden, d.w.z. minimaal elke twee jaar geëvalueerd/bijgesteld, of tussentijds bij (significante) aanpassingen.

Organisatie privacy- en informatiebeveiliging

13. Het hoofd informatiebeveiliging voert regie op de uitvoering van privacy- en informatiebeveiliging over de belangrijkste processen, systemen en verantwoordelijkheidsgebieden van de Kiesraad. Een privacy en security officer zijn aangewezen om nader invulling te geven aan deze taak.
14. Om te bepalen waar de regie zich toe uitstrekt, worden de actuele risico's waarbij de te beschermen belangen een bepaald niveau overschrijden jaarlijks

8 Artikel 32 van de AVG.
9 https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia

geïnventariseerd. De te beschermen belangen waarmee in ieder geval rekening gehouden wordt zijn afhankelijkheden van burgers, bedrijven en medeoverheden, potentiële imagoschade voor de Kiesraad of de overheid, bescherming van staatsgeheimen en risicovolle verwerkingen van persoonsgegevens.

15. Voor de uitvoering van de taken van de privacy en security officer zorgt de Kiesraad ervoor dat deze:
    a. Direct in contact staan met het hoofd informatiebeveiliging, punten kunnen agenderen voor het stafoverleg en onder bijzondere omstandigheden ook voor de Kiesraadvergadering;
    b. Beschikken over inhoudelijke expertise;
    c. Een onafhankelijke positie hebben ten opzichte van onderdelen binnen de organisatie die belast zijn met de ontwikkeling van diensten en producten ten behoeve van de informatievoorziening.
16. Het hoofd informatiebeveiliging heeft inzichtelijk welke activiteiten en plannen met betrekking tot verbeteringen op het gebied van privacy- en informatiebeveiliging moeten worden doorgevoerd en stuurt op de voortgang hiervan. De totstandkoming van het Beveiligingsbeleid en Beveiligingsplan vindt plaats in overleg met het hoofd informatiebeveiliging. De uitvoering van het plan wordt periodiek in het stafoverleg besproken.
17. In aanvulling op bovenstaande hebben de privacy en security officer een eigen verantwoordelijkheid om relevante ontwikkelingen of gebeurtenissen te bespreken met het hoofd informatiebeveiliging.

Risicomanagement en de relatie met toezicht en verantwoording

18. Over privacy- en informatiebeveiliging wordt jaarlijks door het hoofd informatiebeveiliging verantwoording afgelegd via de 'In Control Verklaring Kiesraad' (ICV Kiesraad), waarbij de eerdergenoemde kaders en wetgeving als uitgangspunt dienen. De reikwijdte van de ICV Kiesraad wordt bepaald door de processen/systemen van de Kiesraad met aanmerkelijk te beschermen belangen, aangevuld met de organisatorische aspecten van privacy- en informatiebescherming.
19. Het hoofd informatiebeveiliging heeft hierbij de volgende verantwoordelijkheid:
    a. Voorbereiden van de verantwoording;
    b. Vaststellen en coördineren van vorm en inhoud van de verantwoording;
    c. Erop toezien dat bij afwijking van kaders en richtlijnen uitsluitend verantwoorde risico's worden genomen;
20. De proceseigenaren zijn verantwoordelijk voor de processen die onder hun verantwoordelijkheid worden uitgevoerd.
    a. Proceseigenaren hebben voor hun systeem inzichtelijk gemaakt hoe zij aan de kaders voldoen, met zodanige diepgang dat het te controleren is;
    b. Indien bij een proces uitsluitend gebruikt gemaakt wordt van gedeelde of generieke systemen, kan worden verwezen naar de beheersmaatregelen die voor deze systemen zijn getroffen. De verantwoordelijkheid van de proceseigenaar is dan beperkt tot de zorg dat organisatorische en gebruikersmaatregelen worden nageleefd.
21. De privacy en security officer hebben intern een toezichthoudende taak met betrekking tot de PDCA-cyclus van de Kiesraad.
22. Alle verantwoordingsdocumentatie (d.w.z.: PIA, Risicoanalyses, Informatiebeveiligingsplannen) wordt door privacy en security officer beheerd en zo nodig beschikbaar gesteld.
23. De Kiesraad volgt de interdepartementale lijn voor organisatiesturing en -inrichting op basis van volwassenheidsniveaus.

Inkoop, ontwikkeling en beheer

24. De inkoop van een ICT-dienst, of de start van een ICT-project (diensten en producten ten behoeve van de informatievoorziening), kan pas plaatsvinden als aantoonbaar is dat de privacy en security officer betrokken zijn.
25. Bij de inkoop en totstandkoming van informatiesystemen voor nieuw beleid of nieuwe wetgeving waarbij persoonsgegevens worden verwerkt met significante privacyrisico's, dient er een PIA (privacy impact assessment) te zijn gemaakt.[10]

10 Artikel 35.1 van de AVG.

Hierbij wordt gebruik gemaakt van de leidraad 'model gegevensbeschermings-effectbeoordeling Rijksdienst (PIA)'.[11] Ook bij het vervangen van een bestaand informatiesysteem waarin persoonsgegevens worden verwerkt met significante privacyrisico's, gaat de Kiesraad over tot een PIA of herijking ervan.

26. Bij de inkoop van diensten en producten ten behoeve van de informatievoorziening zijn de betrouwbaarheidseisen (vertrouwelijkheid, integriteit en beschikbaarheid) van de ondersteunde processen mede kaderstellend voor de inkoop. Die eisen moeten dus tijdig worden vastgesteld. Indien betrouwbaarheidseisen (deels) voorvloeien uit wet- en regelgeving (bijvoorbeeld de AVG en het VIR-BI) kan dit gevolgen hebben voor het inkoopproces als potentiële leveranciers aan niet met Nederlandse wet- en regelgeving geharmoniseerde eisen moeten voldoen (bijvoorbeeld de Patriot Act of de Foreign Intelligence Surveillance Amendments Act).
    In het inkoopproces dienen afwegingen in relatie tot het bovenstaande door de proceseigenaar expliciet en inzichtelijk te zijn gemaakt.
    In contracten wordt een beveiligingsparagraaf opgenomen waarin minimaal de relatie met de BIR wordt gelegd en concrete maatregelen rondom informatiebeveiliging worden geformuleerd.
27. Bij de ontwikkeling van diensten en producten ten behoeve van de informatievoorziening zijn de betrouwbaarheidseisen (vertrouwelijkheid, integriteit en beschikbaarheid) van de ondersteunde processen mede kaderstellend in het ontwikkelproces. Deze zogenaamde 'niet-functionele eisen' dienen voorafgaand aan (waterval) of zo vroeg mogelijk (agile/scrum) tijdens de ontwikkeling te worden vastgesteld en eventueel gedurende het traject te worden heroverwogen of bijgesteld.
    Dit geldt tevens voor de risicoanalyse(s) waaruit deze eisen volgen.
28. Voor ingebruikname van een nieuw informatiesysteem of vervanging van een informatiesysteem, dient de proceseigenaar de volgende stappen te doorlopen:
    a. Bij ingebruikname van het informatiesysteem binnen de ICT infrastructuur van SSC-ICT wordt dat aan SSC-ICT voorgelegd, zodat het systeem door SSC-ICT kan worden getoetst op hun criteria. Indien het systeem bij een andere overheidsorganisatie wordt ondergebracht, dient een vergelijkbaar traject te worden doorlopen.
    b. Indien een informatiesysteem extern wordt ondergebracht, verifieert het hoofd informatiebeveiliging in samenspraak met de uitvoerend verantwoordelijken of het basisniveau van beheersmaatregelen op het goede niveau is.
    c. De door het informatiesysteem te beschermen belangen worden door de proceseigenaar inzichtelijk gemaakt. Het niveau van de te beschermen belangen bepaalt of het informatiesysteem geaccrediteerd moet worden.
    d. In het geval dat het systeem geaccrediteerd dient te worden, kan accreditatie verschillende vormen aannemen, afhankelijk van de zwaarte van het informatiesysteem. In oplopende zwaarte kan worden gedacht aan (niet uitputtend):
        i. Uitvoering van een complete risicoanalyse;
        ii. Beoordeling beheersomgeving;
        iii. Technische en/of penetratietesten voorafgaand aan de inproductiename;
        iv. Code review.
29. Voor diensten die verwerkingen van persoonsgegevens inhouden, wordt eveneens een verwerkersovereenkomst met de leveranciers afgesloten. Voor leveranciers binnen de Rijksdienst is er sprake van een verwerkersafspraak.
30. Het gebruik van clouddiensten[12] voor verwerkingen/diensten is toegestaan onder de volgende voorwaarden:
    a. Er is geen sprake van de verwerking van staatsgeheime informatie.
    b. Er is een risicoanalyse uitgevoerd waaruit blijkt dat de risico's van het gebruik van de betreffende clouddienst acceptabel zijn in relatie tot de

11 https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia

12 In dit document wordt onder een 'clouddienst' een ICT-dienst verstaan waarbij gebruik wordt gemaakt van een gedeelde 'pool' van configureerbare computer resources die flexibel kunnen worden ingezet, vaak over meerdere locaties.

verwerking en de voor deze verwerking relevante dreigingen.[13] Hierbij wordt meegewogen of gebruik wordt gemaakt van een public cloud of een private cloud – die laatste in het bijzonder in het geval van een private cloud onder beheer van een overheidsorganisatie.

c. In beginsel – maar afhankelijk van het type verwerking of dienst – zorgt de Kiesraad ervoor dat security en security monitoring, alsmede Identity en access management onder de directe controle van de Kiesraad vallen. Indien noodzakelijk kunnen ook deze IT-functies worden uitbesteed, mits bij een leverancier die geen relatie met de cloudleverancier heeft.
d. Bij het besluit van de proceseigenaar is aantoonbaar het advies van de privacy en security officer is meegewogen.

Incident- en crisisbeheer

31. De privacy en security officer richten het incidentbeheer binnen de Kiesraad in op een niveau dat passend is bij de taken die de Kiesraad uitvoert. Hier hoort een ordelijke registratie bij van incidenten en hun afhandeling.
32. Het proces 'meldplicht datalekken' en de hiertoe ingerichte processen bij de Kiesraad, zijn een bijzondere vorm van het incidentenproces.[14]

Standaarden, baselines en websites

33. Bestaande en nieuwe websites worden, indien dat technisch en functioneel mogelijk is, onder de centrale dienst 'Platform Rijksoverheid Online' (PRO) gebracht.
34. De proceseigenaar is er verantwoordelijk voor te zorgen dat websites die niet onder PRO vallen voldoen aan de standaarden zoals geformuleerd door het Forum Standaardisatie.[15]
35. Het hoofd informatiebeveiliging draagt er zorg voor dat voor werkplekdiensten die *niet* bij SSC-ICT worden afgenomen geldt dat de mailvoorzieningen voldoen aan de veilige standaarden zoals vastgesteld door het Forum Standaardisatie.
36. De proceseigenaar die uitingen via nieuwsbrieven laat verzorgen door derde partijen, draagt er zorg voor dat voldaan wordt aan de veilige standaarden met betrekking tot e-mail.
37. De opvolging van meldingen van het NCSC betreffende de beveiliging van websites in het kader van 'responsible disclosure' is de verantwoordelijkheid van de proceseigenaar.[16]

Verzoeken en rechten van betrokkenen

38. Onder de AVG is het mogelijk voor een burger om een verzoek te doen (inzage, correctie, recht om vergeten te worden). Het beleid rondom de afhandeling van deze verzoeken:
    i. Afhandeling binnen een maand. Indien afhandeling binnen een maand niet mogelijk is, wordt een uitstelbrief gestuurd binnen een maand. De maximale uitsteltermijn is twee maanden.
    ii. Voor de behandeling van een verzoek dient de verzoeker adequaat te worden geïdentificeerd, bijvoorbeeld door het opvragen van een kopie paspoort. Na verificatie van de identiteit moet het bewijs van identificatie worden vernietigd (niet opgeslagen).
    iii. De afhandeling van binnengekomen en afgehandelde verzoeken wordt geregistreerd.
    iv. De bewaartermijn van correspondentie rondom het verzoek is vijf jaar na afhandeling van het verzoek, daarna moeten de stukken vernietigd worden.[17]
    v. De functionaris gegevensbescherming wordt betrokken indien nodig.

---

13 Voor de verwerking van persoonsgegevens moet o.a. worden overwogen of gekeken moet worden of voor het land van opslag de lijst van landen waarvoor een 'adequacy decision' is genomen, van toepassing is. Zie: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

14 http://content.rp.rijksweb.nl/cis/content/media/rijksportaal/bzk_1/organisatie_21/bzk_2/dienstconcernstafenbedrijfsvoeringdcb/dcbbreed/chiefinformationofficercio/bestanden_3583/Fasering_datalekken.pdf

15 https://www.forumstandaardisatie.nl/open-standaarden

16 https://www.ncsc.nl/contact/kwetsbaarheid-melden

17 Deze termijn is gelijkgesteld aan de bewaartermijn t.a.v.de beantwoording van een burgerbrief.

vi. Indien het verzoek ook andere organisaties betreft, stuurt de Kiesraad het verzoek door.

KIESRAAD

Privacy- en informatiebeveiligingsplan Kiesraad

2020

Departementaal vertrouwelijk

Versie 1.0

Dit document wordt beheerd door de privacy en security officer, in naam van het hoofd informatiebeveiliging. De beheerders beoordelen dit document ten minste eenmaal per jaar op onder meer actualiteit, volledigheid en relevantie.

Versie	Omschrijving	Toelichting	Steller	Datum
0.1	Concept 1	Voorstel	5 1 2e	24-12-2019
0.2	Concept 2	Toevoeging hfdst. 3 en 4	5 1 2e	27-01-2019
1.0	Goedkeurig	Voorstel voor stafoverleg	5 1 2e	07-02-2019

Afkortingen

AVG	Algemene Verordening Gegevensbescherming
BIO	Baseline Informatiebeveiliging Overheid
BIR	Baseline Informatiebeveiliging Rijksdienst
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CIO	Chief Information Officer, oftewel het hoofd informatiebeleid
CIO&IM	Directie CIO en Informatiemanagement binnen BZK
CISO	Chief Information Security Officer
CvI	Code voor Informatiebeveiliging
FG	Functionaris voor de Gegevensbescherming
ICV	In Control Verklaring
NDN	Nationaal Detectie Netwerk
NCSC	Nationaal Cyber Security Centrum
PDCA-cyclus	Plan Do Check Act (Learn) cyclus.
PIA	Privacy Impact Assessment
VIR	Voorschrift Informatiebeveiliging Rijksdienst
VIR-BI	Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie

Voorwoord

Voor u ligt het Privacy- en informatiebeveiligingsplan Kiesraad 2020 (hierna: het Beveiligingsplan). De omvang en ernst van de digitale dreiging in Nederland zijn aanzienlijk en blijven zich ontwikkelen. Digitale dreiging rond verkiezingen kreeg de afgelopen jaren in binnen- en buitenland veel aandacht. De Kiesraad, waar in dit document zowel de Raad als diens secretariaat onder verstaan wordt, vervult als centraal stembureau, adviesorgaan en informatiecentrum een belangrijke rol op gebied van verkiezingen en het kiesrecht. Reden te meer om voldoende aandacht te besteden aan de beveiliging van informatie bij de Kiesraad.

Dit Beveiligingsplan bevat maatregelen om de kwaliteit van de privacy- en informatiebeveiliging binnen de Kiesraad te waarborgen. Maatregelen met het oog op de exclusiviteit, integriteit en continuïteit van gegevensverwerkingen binnen de Kiesraad. Strategische uitgangspunten voor privacy- en informatiebeveiliging heeft de Kiesraad vastgelegd in het Privacy- en informatiebeveiligingsbeleid Kiesraad 2019-2022 (hierna: het Beveiligingsbeleid). Dat beleid geldt als richtsnoer voor dit plan. Activiteiten die binnen het tijdsbestek van een jaar nodig zijn om invulling te geven aan het beleid maken deel uit van dit plan.

Het onderhoud van dit Beveiligingsplan is belegd bij de privacy en security officer. Het Beveiligingsplan wordt jaarlijks opnieuw vastgesteld door het hoofd informatiebeveiliging. Tijdens een risicoanalyse worden risico's (opnieuw) bekeken en ingeschat en maatregelen beoordeeld op relevantie en effectiviteit. Indien tussentijds blijkt dat een maatregel uit het plan onvoldoende werkt of dat aanvullende maatregelen nodig zijn, dan wordt het plan hierop aangepast. Inhoudelijke wijzigingen moeten worden goedgekeurd door het hoofd informatiebeveiliging.

Dit Beveiligingsplan is gerubriceerd als departementaal vertrouwelijk en is beschikbaar voor medewerkers van het secretariaat, de Kiesraadleden en voor personen en/of organisaties die hiervoor expliciet toestemming hebben gekregen van het hoofd informatiebeveiliging. Het is niet toegestaan dit plan zonder toestemming aan derden beschikbaar te stellen.

De opbouw van dit Beveiligingsplan is als volgt. Hoofdstuk 1 bevat een inleiding met het doel en de kaders. In hoofdstuk 2 is de context Kiesraad beschreven, waaronder de kerntaken en -waarden. De nummering van de daaropvolgende hoofdstukken begint bij 5 en sluit daardoor aan bij de Baseline Informatiebeveiliging Overheid (BIO). Vanaf dat hoofdstuk worden de maatregelen op het gebied van informatiebeveiliging per domein uitgewerkt. Een volledig overzicht van de handreikingen waarnaar in dit plan verwezen wordt kan teruggevonden worden op de website van de informatiebeveiligingsdienst.

Inhoudsopgave

1. Inleiding

Doel
Het doel van dit Beveiligingsplan is om inzicht te geven in de maatregelen die de kwaliteit van privacy- en informatiebeveiliging binnen de Kiesraad waarborgen. Meer in het bijzonder maatregelen ter beveiliging van verkiezingsprocessen die onder de verantwoordelijkheid van de Kiesraad vallen en de beveiliging van ondersteunende systemen die onder regie van de Kiesraad worden gebruikt of ter beschikking worden gesteld aan ketenpartners. Daarnaast wordt in dit plan en bijgevoegde planning beschreven aan welke maatregelen de Kiesraad in 2020 gaat werken en welke documenten van derden, zoals handreikingen, hierbij worden betrokken.

Kaders
Het Beveiligingsplan sluit aan bij bestaande kaders voor privacy- en informatiebeveiliging. Dit zijn, voor zover van toepassing en relevant:
- Het Voorschrift Informatiebeveiliging Rijk (VIR);
- Het Voorschrift Informatiebeveiliging Rijksdienst-bijzondere informatie (VIR-BI);
- De Code voor Informatiebeveiliging (Cvi) (ISO 27002:2007);
- De Baseline Informatiebeveiliging Overheid (BIO);
- De Richtsnoer Autoriteit Persoonsgegevens: beveiliging van persoonsgegevens (CBP, 1 mei 2013);
- Het beleidskader Privacy- en Informatiebescherming 2019 van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK).

Het VIR stelt eisen aan de organisatie en het opnemen van informatiebeveiliging in de planning en control cyclus van de bedrijfsvoering. Het VIR schrijft voor dat het management een risicoafweging maakt. Als voorbeeld om hieraan invulling te geven, noemt het VIR de Code voor Informatiebeveiliging (Cvi). Het VIR-BI geeft regels voor de beveiliging van bijzondere informatie bij de rijksdienst.

De overheid heeft een eigen Baseline Informatiebeveiliging Rijksoverheid ontworpen, de BIR. De BIR gaat uit van de Code voor Informatiebeveiliging (Cvi), plus een aantal extra maatregelen en aanscherpingen. Vanaf 1 januari 2020 is de opvolger van de BIR van kracht, de BIO. Dit is één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op ISO-normen.

De Algemene verordening gegevensbescherming (AVG) bevat regels voor de verwerking van persoonsgegevens. Voorheen was dat in de Wet bescherming persoonsgegevens (Wbp). Per 1 maart 2013 heeft de Autoriteit Persoonsgegevens de Richtsnoeren beveiliging van persoonsgegevens gepubliceerd, waarin staat hoe deze Autoriteit bij het beoordelen van de beveiliging de normen toepast.

Het beleidskader Privacy- en Informatiebescherming 2019 van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft model gestaan voor het Beveiligingsbeleid van de Kiesraad, dat op zijn beurt dienstdoet als richtsnoer voor dit Beveiligingsplan.

Begrippen
Hieronder is voor een consistent gebruik van begrippen een definitie opgenomen van belangrijke begrippen in dit plan. De definities zijn afkomstig uit de VIR en Cvi.

Informatiebeveiliging is het proces voor het vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit, plus het treffen, onderhouden en controleren van een samenhangend pakket aan bijbehorende maatregelen.

Een informatiesysteem is een samenhangend geheel van gegevensverzamelingen en de daarbij horende personen, procedures, processen en programmatuur, plus de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.

Betrouwbaarheid is de mate waarin de organisatie zich kan verlaten op een informatiesysteem voor zijn informatievoorziening. Betrouwbaarheid geldt als de verzamelterm voor de begrippen vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid.

Vertrouwelijkheid is de mate waarin toegang tot en de kennisname van een informatiesysteem en de informatie daarin is beperkt tot een gedefinieerde groep van gerechtigden. Voor vertrouwelijkheid wordt ook de term 'exclusiviteit' gebruikt.

Integriteit is de mate waarin een informatiesysteem zonder fouten is waardoor de correctheid en volledigheid van informatie en verwerking worden gewaarborgd.

Beschikbaarheid is de mate waarin een informatiesysteem in bedrijf is op het moment dat de organisatie het nodig heeft waardoor geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en bedrijfsmiddelen.

Controleerbaarheid (ook wel benoemd als integriteit) is de mate waarin activiteiten binnen het systeem herleid en traceerbaar zijn zodat fouten en/of ongewenste activiteiten worden geregistreerd, gealarmeerd en geanalyseerd.

Bijlagen

Bijlage 1 bij dit plan bevat een overzicht van de rollen op het gebied van privacy- en informatiebeveiliging binnen de Kiesraad, zoals vastgelegd in het beleid. Bijlage 2 bij dit plan bevat een overzicht van de processen binnen de Kiesraad. Bijlage 3 bij dit plan bevat een legenda voor de inschatting van de betrouwbaarheidseisen beschikbaarheid, integriteit en vertrouwelijkheid.

2. Context

De Baseline Informatiebeveiliging Overheid, oftewel de BIO, geeft ruimte om op basis van een risicoafweging te werken. Het is mogelijk om prioriteiten te stellen in wat binnen de Kiesraad nu gedaan moet worden en wat tot een later moment kan wachten. Het vertrekpunt in dit plan is een inventarisatie van de context en bedrijfsprocessen, om vast te stellen wat de kritieke bedrijfsprocessen en de daarbij horende essentiële informatiesystemen zijn die komend jaar de aandacht verdienen.

Focus
Dit Beveiligingsplan heeft betrekking op de informatie(systemen) van de Kiesraad, al dan niet in eigen beheer, en eventuele voorzieningen die onder de verantwoordelijkheid van de Kiesraad door derden worden beheerd. In dit plan komt overeenkomstig de BIO een breed spectrum aan maatregelen aan bod, van organisatorische en personele tot fysieke beveiligingsmaatregelen.

De organisatie
Om prioriteit aan te brengen in informatiebeveiliging is het belangrijk om vast te stellen wat de context van de Kiesraad is. Waarom bestaat de Kiesraad als organisatie en hoe zit deze in elkaar? Op de website staat hierover het volgende:

De Kiesraad treedt bij verschillende verkiezingen op als centraal stembureau. Verder is de Raad adviesorgaan en informatiecentrum op het gebied van kiesrecht en verkiezingen. De leden van de Kiesraad worden bij hun werkzaamheden ondersteund door een secretariaat. Aan het hoofd van het secretariaat staat de secretaris-directeur. Het secretariaat bestaat uit het cluster Juridische Zaken en Informatiebeleid en het cluster Communicatie, Onderzoek en Ondersteuning.

Processen
Op basis van voorgaande informatie en de in bijlage 1 bij dit plan gevoegde afbeelding met processen, kunnen de volgende domeinen, processen en belanghebbenden onderscheiden worden:

Domein	Proces	Belanghebbenden
Verkiezingen	Registratie politieke partijen	Politieke partijen
Verkiezingen	Uitvoeren kandidaatstelling	Politieke partijen, kandidaten
Verkiezingen	Uitvoeren uitslagvaststelling	Kiezers, politieke partijen, vrtw. orgaan
Verkiezingen	Tussentijdse benoemingen	Kandidaten, vrtw. orgaan
Juridisch	Opstellen adviezen	Wetgever
Juridisch	Wob-verzoeken behandelen	Verzoekers
Juridisch	Bezwaar, beroep en inlichtingen	Procespartijen
Juridisch	Opstellen beleidsregels en regelingen	Kiesraad, politieke partijen
Communicatie	Uitvoeren onderzoek	Wetenschap, geïnteresseerden
Communicatie	Verzorgen communicatie	Kiezers, geïnteresseerden
Communicatie	Informatieverstrekking en -verwerking	Vragenstellers, klachten indieners
ICT	Beheer OSV	Kiesraad en gemeenten
ICT	Beheer Databank	Kiezers, geïnteresseerden
Bedrijfsvoering	Personeel	Kiesraad, personeel
Bedrijfsvoering	Financiën	Kiesraad, personeel
Bedrijfsvoering	Huisvesting	Kiesraad, personeel
Bedrijfsvoering	Automatisering	Kiesraad, personeel
Bedrijfsvoering	Informatiebeleid	Kiesraad, personeel

In onderstaande tabel staat beschreven welk van bovengenoemde processen binnen de Kiesraad als kritiek zijn aan te merken, inclusief de daarbij horende essentiële informatiesystemen. Processen waarop ten minste 3 van de volgende criteria van toepassing zijn merken we aan als zeer belangrijk en bij ten minste 5 criteria als

kritiek: imagoschade, aanzienlijke kostenposten, schade voor de Kiesraad of derden, niet voldoen aan wettelijke termijnen of eisen, niet halen van afgesproken ambities, impact op eigen bedrijfsvoering of die van derden, stokken van de eigen bedrijfsvoering of die van derden, stokken van de dienstverlening.

Proces	Eigenaar	Prio	Informatiesystemen	Eigenaar
Registratie politieke partijen	CC JZ	+		
Uitvoeren kandidaatstelling	CC JZ	++	OSV (++), T&T (+)	CC IB
Uitvoeren uitslagvaststelling	CC JZ	++	OSV (++)	CC IB
Tussentijdse benoemingen	CC JZ	+		
Opstellen adviezen	CC JZ			
Wob-verzoeken behandelen	CC JZ			
Bezwaar, beroep en inlichtingen	CC JZ			
Opstellen beleidsregels en regelingen	CC JZ			
Uitvoeren onderzoek	CC CO			
Verzorgen communicatie	CC CO		Website	CC CO
Informatieverstrekking en -verwerking	CC CO		FMP	CC CO
Ontwikkeling en beheer OSV	CC IB	+	OSV (++)	CC IB
Ontwikkeling en beheer Databank	CC CO		Databank	CC CO
Personeel	SD		P-Direkt, Job2	SD
Financiën	SD	?	3F, Webfocus (?)	SD
Huisvesting	SD			
Automatisering	SD	+	iBabs, Office, Digidoc (+), IT-netwerk (+)	SD
Informatiebeleid	SD			SD

Legenda	
Eigenaar	SD = Secretaris-Directeur, CC = Cluster Coördinator
Thema	JZ = Juridische Zaken, COO: Communicatie en Onderzoek, IB = Informatiebeleid
Prioriteit	+ = Zeer belangrijk, ++ = Kritiek

In de tabel hierboven staat ook wie binnen de Kiesraad eigenaar zijn van de processen en informatiesystemen. Het is de verantwoordelijkheid van de eigenaar om ervoor te zorgen dat risico's binnen het proces of het systeem passend worden beheerst op basis van de BIO. Bij systemen waarvoor externen de verantwoordelijkheid dragen is de eigenaar binnen de Kiesraad het hoogste aanspreekpunt waaraan verantwoording dient te worden afgelegd.

Transitie
Bij de Kiesraad zijn organisatorische veranderingen op komst vanwege de transitie. Dit is het programma digitale hulpmiddelen in de verkiezingsketen, dat in mei 2019 is gestart en in 2020 verder zijn beslag zal krijgen. Het programma heeft tot doel om digitale hulpmiddelen te laten ontwikkelen die gebruikt worden in verschillende fasen van het verkiezingsproces. De verantwoordelijkheid voor deze middelen komt op de middellange termijn bij de Kiesraad te liggen. De Kiesraad wordt hierbij omgevormd tot een Verkiezingsautoriteit. In dit plan kijken we waar mogelijk vooruit naar de gevolgen die de transitie in 2020 voor de informatiebeveiliging zal hebben.

Belangrijke toekomstige ontwikkelingen uit het oogpunt van informatiebeveiliging:
- Omvormen van de Kiesraad tot een verkiezingsautoriteit, met gevolgen voor de aard, omvang en samenstelling van de organisatie;
- Ontwerpen en ontwikkelen van digitale hulpmiddelen voor respectievelijk de kandidaatstelling en de vaststelling van de uitslag;
- Benodigde aanpassingen in wet- en regelgeving;
- Bepalen of en zo ja in welke mate het verkiezingsproces of onderdelen daarvan tot de vitale infrastructuur gaan behoren.

3. Risicoanalyse

Door middel van een korte risicoanalyse en een analyse van de onderdelen waarop de Kiesraad de grootste invloed heeft, kan de prioriteit van de te ondernemen activiteiten worden vastgesteld. De in dit hoofdstuk uitgevoerde risicioanalyse is geen volwaardige vervanger van een volledige risicoanalyse/GAP-analyse, maar maakt het wel mogelijk om prioriteit aan te brengen in de doelstellingen binnen dit beveiligingsplan en het beveiligingsbeleid van de Kiesraad.

Te beschermen belangen
In het vorige hoofdstuk heeft een inventarisatie plaatsgevonden van de bedrijfsprocessen en informatiesystemen van de Kiesraad. De gegevens en systemen die relevant zijn voor de uitvoering van de belangrijkste taken van de Kiesraad zijn te betitelen als de kroonjuwelen. In de analyse zijn onderstaande bedrijfsprocessen aangeduid als zijnde "kritiek" of "zeer belangrijk":

Kritieke bedrijfsprocessen
- Uitvoeren kandidaatstelling
- Uitvoeren uitslagvaststelling

Zeer belangrijke bedrijfsprocessen
- Registratie politieke partijen
- Tussentijdse benoemingen
- Beheer OSV
- Automatisering

Dit zijn de als "kritiek" en "zeer belangrijk" aangeduide informatiesystemen:

Kritieke informatiesystemen
- OSV (Ondersteunende Software Verkiezingen)

Zeer belangrijke informatiesystemen
- T&T
- Digidoc
- IT-netwerk (kantoorautomatisering)

Van de volledig uit te voeren risicoanalyse/GAP-analyse in 2020 maken bovengenoemde onderdelen opnieuw deel uit. Ook het onderdeel Financiën en de bijbehorende systemen als 3F, Webfocus die mogelijk als zeer belangrijk moeten worden aangemerkt.

Systeemtypering
In deze paragraaf is per kritiek en zeer belangrijk systeem de typering "nuttig", "belangrijk" of "vitaal" toegekend op basis van de Handreiking Quickscan Information Security versie 1.0.

Typering	Waardering
Nuttig	- Het informatiesysteem geeft support bij de activiteiten binnen het bedrijfsproces en is 'handig om te hebben'.
Belangrijk	- Het informatiesysteem levert een belangrijke bijdrage aan de activiteiten binnen het proces en/of de levering van de producten of diensten. - Slechts met grote, onevenredige inspanning is voortzetting van het proces mogelijk. - Inzet van het informatiesysteem heeft een positief effect op de doeltreffendheid en doelmatigheid van de organisatie. - Het informatiesysteem wordt door veel (interne / externe) medewerkers/burgers gebruikt.
Vitaal	- Het uitvoeren van de bedrijfsprocessen of het tot stand brengen van producten/diensten is (nagenoeg) onmogelijk zonder de inzet van het informatiesysteem. - Inzet van het informatiesysteem is essentieel voor een goede uitvoering van het bedrijfsproces.

Informatie-systeem	Belang	Argumentatie
OSV	Vitaal	Het informatiesysteem is essentieel voor een goede en tijdige verwerking van gegevens bij de kandidaatstelling en uitslagvaststelling.
T&T	Belangrijk	Het informatiesysteem is de toegang voor de Kiesraad tot de GBA-V. Daarmee is dit systeem van zeer groot belang voor een betrouwbaar kandidaatstellings-proces. Indien T&T niet of onjuist werkt, dan kan de tijdigheid en integriteit van de kandidatenlijsten niet worden geborgd. Indien T&T niet beschikbaar is, dan is met aanzienlijke inspanning mogelijk om alternatieven te gebruiken.
Digidoc	Belangrijk	Het informatiesysteem is een Document Management Systeem (DMS) van het Ministerie van BZK. De Kiesraad maakt hier tevens gebruik van, in het bijzonder voor het archiveren van beleidsstukken, adviezen, besluiten etc. Het register van aanduidingen staat onder andere in Digidoc. Derhalve is het van belang dat het systeem operationeel is. Er bestaan terugvalopties, zoals gebruik van lokaal opgeslagen bestanden, echter is dit niet wenselijk. Indien het systeem niet integer is (bijvoorbeeld de spreektekst is ongeautoriseerd gewijzigd), dan kan dat gevolgen hebben in het kader van de uitslagvaststelling.
IT-netwerk	Belangrijk	Onder het IT-netwerk verstaan wij de werkstations (thin clients), besturingssystemen, kantoorapplicaties (tekstverwerkers, e-mail, etc.), printers en netwerkconnectiviteit. De beschikbaarheid en integriteit van het IT-netwerk is van groot belang voor de kritieke bedrijfsprocessen. Bijvoorbeeld: het IT-netwerk (inclusief printers) worden gebruikt om het proces-verbaal af te drukken. Daarnaast wordt het IT-netwerk intensief gebruikt voor communicatie tussen medewerkers van de Kiesraad en naar de buitenwereld. Hoewel er alternatieven bestaan om de belangrijkste processen alsnog uit te voeren (bijv. gebruik van een alternatieve, stand-alone laptop en printer), is het IT-netwerk van zeer groot belang voor een tijdige en correcte verwerking van de uitslag.

Betrouwbaarheidseisen
Aan de hand van bovenstaande proces- en systeemclassificatie is in deze paragraaf een inschatting van de betrouwbaarheidseisen opgenomen. Het betreft een classificatie in termen van beschikbaarheid, integriteit en vertrouwelijkheid:

Beschikbaarheid:	Het niet beschikbaar zijn van deze gegevens en uitval van het systeem levert ernstige schade op voor de organisatie.
Integriteit:	Onjuiste of onvolledige uitvoering van de gegevens en het systeem levert ernstige schade op voor de organisatie.
Vertrouwelijkheid:	Verspreiding van de gegevens en informatie uit het systeem kan ernstige (imago)schade toebrengen aan de organisatie.

Zie bijlage 1 voor de legenda Hoog, Midden, Laag op deze onderdelen.

OSV		
Eis	**Categorie**	**Argumentatie**
Beschikbaarheid	Hoog	Het informatiesysteem moet met name in de week van de verkiezingen beschikbaar zijn om stemaantallen in te voeren en te verwerken. Uitval van het systeem in deze periode kan leiden tot grootschalige publieke verontwaardiging, negatieve publiciteit, vertraging en het verlies van vertrouwen in het verkiezingsproces. Buiten piektijden is de beschikbaarheid van het systeem minder van belang.
Integriteit	Hoog	De juistheid en volledigheid van de informatie verwerkt in het informatiesysteem is van belang om de burger het vertrouwen te kunnen bieden dat het verkiezingsproces niet is gemanipuleerd. Zonder juistheid en volledigheid van de informatie, kan het vertrouwen, transparantie en controleerbaarheid van het verkiezingsproces niet worden geborgd.
Vertrouwelijkheid	Midden	Het informatiesysteem verwerkt verschillende gegevens, waaronder het aantal toegelaten kiezers, het aantal stemmen per lijst, het aantal blanco stemmen, het aantal ongeldige stemmen en (persoons)gegevens van politici. De vertrouwelijkheid van het aantal stemmen is laag: deze informatie is openbaar. Kennisname van (persoons)gegevens van o.a. de politici en eventueel gebruikers van het systeem door onbevoegden is ongewenst en kan een afwijking vormen ten opzichte van de AVG.

T&T		
Eis	**Categorie**	**Argumentatie**
Beschikbaarheid	Laag	Indien T&T niet of onjuist werkt, dan kan de tijdigheid en integriteit van de kandidatenlijsten niet worden geborgd. Indien T&T echter niet beschikbaar is, dan is het mogelijk om op andere wijze dezelfde functionaliteit te raadplegen. Het kost echter aanzienlijke inspanning om alternatieven te gebruiken.
Integriteit	Laag	De juistheid, tijdigheid en volledigheid van de informatie in T&T is belangrijk, maar niet vitaal voor de uitvoering van de bedrijfsprocessen. Een integriteitsschending heeft een negatieve impact, maar kan worden hersteld en leidt bijvoorbeeld niet tot grote verontwaardiging. Er heeft zich, bijvoorbeeld, een incident voorgedaan waarbij door foutief gebruik van T&T een onjuiste aanname is gedaan over een kandidaat. Deze fout kon relatief eenvoudig ambtshalve door de Kiesraad worden in de verzuimperiode.
Vertrouwelijkheid	Midden	T&T biedt toegang tot de BRP, waar veel persoonsgegevens in zijn geregistreerd. Bescherming van deze gegevens is derhalve van belang, ook in het kader van de AVG.

Digidoc		
Eis	**Categorie**	**Argumentatie**
Beschikbaarheid	Laag	Het register van aanduidingen staat onder andere in Digidoc. Het is derhalve van belang dat het systeem operationeel is. Er bestaan terugvalopties, zoals gebruik van lokaal opgeslagen bestanden. Dit is echter niet wenselijk.
Integriteit	Midden	Indien het systeem niet integer is (bijvoorbeeld de spreektekst is ongeautoriseerd gewijzigd), dan kan dat gevolgen hebben in het kader van de uitslagvaststelling.
Vertrouwelijkheid	Midden	Het systeem bevat interne notities, adviezen, beleidsstukken etc. Indien dergelijke informatie door onbevoegden wordt ingezien, heeft dit consequenties voor de reputatie van de Kiesraad/overheid. Dergelijke stukken bevatten wel persoonsgegevens, maar geen staatsgeheimen.

IT-netwerk		
Eis	**Categorie**	**Argumentatie**
Beschikbaarheid	Midden	De beschikbaarheid en integriteit van het IT-netwerk is van groot belang voor de kritieke bedrijfsprocessen. Bijvoorbeeld: het IT-netwerk (inclusief printers) worden gebruikt om het proces-verbaal af te drukken. Daarnaast wordt het IT-netwerk intensief gebruikt voor communicatie. Hoewel er alternatieven bestaan om de belangrijkste processen alsnog uit te voeren (bijv. gebruik van een alternatieve, stand-alone laptop en printer), is het IT-netwerk van zeer groot belang voor een tijdige en correcte verwerking van de uitslag. De maximale hersteltijd van het IT-netwerk is doorgaans 16 werkuren.
Integriteit	Midden	Er bestaat een afhankelijkheid tussen het IT-netwerk en de uitslagvaststelling en publicatie/communicatie van resultaten. Indien de integriteit van het IT-netwerk niet kan worden gewaarborgd, heeft dit grote (reputatie)schade tot gevolg. Zie ook de beschrijving bij beschikbaarheid.
Vertrouwelijkheid	Midden	In het IT-netwerk worden onder andere vertrouwelijke persoonsgegevens verwerkt.

Risico's
In de onderstaande tabel zijn de meest in het oog springende risico's beschreven in relatie tot de hierboven geclassificeerde informatiesystemen.

Risico	**Informatie-systeem**	**Link met BIO-hoofdstuk**
Informatiesysteem wordt gehackt, integriteit en vertrouwelijkheid van de gegevens kan niet worden geborgd.	OSV T&T Digidoc IT-netwerk	Dit risico kan door de Kiesraad worden gemitigeerd met de invulling van: 5. Informatiebeveiligingsbeleid 6. Organiseren van informatiebeveiliging 8. Beheer van bedrijfsmiddelen 9. Toegangsbeveiliging 10. Cryptografie

		11. Fysieke beveiliging en beveiliging van de omgeving 12. Beveiliging bedrijfsvoering 13. Communicatiebeveiliging 14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen 15. Leveranciersrelaties 18. Naleving
Methode voor de zetelberekening is fout, waardoor tot een onjuiste zetelberekening wordt gekomen.	OSV	Dit risico kan door de Kiesraad worden gemitigeerd met de invulling van: 14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen 15. Leveranciersrelaties 18. Naleving
Het informatiesysteem is niet benaderbaar door een fout in de software, een (D)DoS-aanval of een fout bij de hostingpartij.	OSV T&T Digidoc IT-netwerk	Dit risico kan door de Kiesraad worden gemitigeerd met de invulling van: 5. Informatiebeveiligingsbeleid 6. Organiseren van informatiebeveiliging 8. Beheer van bedrijfsmiddelen 12. Beveiliging bedrijfsvoering 14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen 15. Leveranciersrelaties 17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer 18. Naleving
Ongeautoriseerd persoon krijgt toegang tot het informatiesysteem door onzorgvuldig handelen van interne- of externe medewerkers.	OSV T&T Digidoc IT-netwerk	Dit risico kan door de Kiesraad worden gemitigeerd met de invulling van: 5. Informatiebeveiligingsbeleid 6. Organiseren van informatiebeveiliging 7. Veilig personeel 9. Toegangsbeveiliging 11. Fysieke beveiliging en beveiliging van de omgeving 12. Beveiliging bedrijfsvoering 14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen 15. Leveranciersrelaties 18. Naleving

In 2020 worden door de Kiesraad integrale risicoanalyses uitgevoerd op de procedure voor de uitslagvaststelling en kandidaatstelling. Daarin worden risico's ten aanzien van de informatiebeveiliging ingeschaald op basis van kans maal impact. Op basis hiervan worden de beheersmaatregelen in dit plan opnieuw beoordeeld.

Invloed
In de onderstaande tabel zijn de verschillende BIO-hoofdstukken uiteengezet ten opzichte van de controle die de Kiesraad, dienstenleveranciers en ketenpartners hierop hebben.

Hfd. BIO	**Titel**	**Invloed Kiesraad**	**Invloed Diensten Leveranciers**	**Invloed Ketenpartner**
5	Informatiebeveiligingsbeleid	++	-	-
6	Organiseren van informatiebeveiliging	++	-	-
7	Veilig personeel	++	+	+
8	Beheer van bedrijfsmiddelen	+	-	-
9	Toegangsbeveiliging	+	+	+
10	Cryptografie	+	+	+
11	Fysieke beveiliging en beveiliging van de omgeving	+	+	+
12	Beveiliging bedrijfsvoering	+	+	+
13	Communicatiebeveiliging	+	++	+
14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	++	+	+
15	Leveranciersrelaties	++	+	+
16	Beheer van informatiebeveiligingsincidenten	++	+	+
17	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	+	+	+
18	Naleving	++	+	+

Invloed	- = Geen invloed, + = Invloed, ++ = Veel invloed

4. Prioritering

Op basis van de risicoanalyse en de mate van invloed die de Kiesraad heeft, zoals die in het vorige hoofdstuk beschreven zijn, is in dit hoofdstuk een prioritering aangebracht ten aanzien van de BIO. Het uitgangspunt is dat zaken waar de Kiesraad een grote invloed op kan uitoefenen en die tevens een grote impact hebben op het verkleinen van de belangrijkste risico's, prioriteit hebben. Dit, om zogenoemde 'Quick wins' zo snel mogelijk op te pakken. De beheersmaatregelen uit de BIO worden in de navolgende hoofdstukken afzonderlijk behandeld.

Prio	BIO-hoofdstuk	Status
1	**5. Informatiebeveiligingsbeleid**	
	Beveiligingsbeleid en plan vaststellen	
	Beveiligingsbeleid communiceren	
	Beveiligingsbeleid beoordelen	
	Beveiligingsplan 2021 opstellen	
	Beleid en plan voor 2021 vaststellen	
2	**6. Organiseren van informatiebeveiliging**	
	Beoordelen rollenstructuur	
	Vaststellen gewijzigde rollenstructuur	
	Beschrijving taken en controleurs verk.	
	Overzicht contactgegevens opstellen	
	Beoordelen rollenstructuur	
3	**14. Acquisitie, ontwikkeling en onderhoud**	
	Voorwaarden opnemen in testplan	
	Meegeven voor aanbesteding	
4	**15. Leveranciersrelaties**	
	Leidraad IB en leveranciers opstellen	
5	**18. Naleving**	
	Opstellen PDCA-cyclus	
	Opstellen ISMS	
	Audit- en testplan opstellen	
	ICV doorontwikkelde OSV opstellen	
6	**7. Veilig personeel**	
	Informatie indiensttreding beoordelen	
	Bewustwordingsprogramma maken	
	Bewustwordingsdag organiseren	
7	**16. Beheer beveiligingsincidenten**	
	IB incidentenproces opstellen	
	IB incidentenproces vaststellen	

Rest	BIO-hoofdstuk	Status
	8. Verantwoordelijkheid bedrijfsmiddelen	
	Beoordelen inventarisatie bedrijfsm.	
	Eigenaren inventarisatie bedrijfsm.	
	Gedragsregels contracten externen	
	Procedure teruggave bedrijfsmiddelen	
	Classificatie informatie OSV en verk.	
	Classificatieschema ontwerpen	
	Informatie: labelen en procedures	
	Beleid en eisen verwd. transp. media	
	9. Toegangsbeveiliging	
	Beleid toegangsbeveiliging beoordelen	
	Beschrijving rolverdeling OSV bij verk.	
	Na classifcatie inlogprc. beoordelen	
	Na analyse wachtwoordbl. beoordelen	
	10. Cryptografie	
	11. Fysieke beveiliging en van de omgeving	
	Expliciteren interne maatregelen	
	12. Beveiliging bedrijfsvoering	
	Beoordelen doorontwikkeling	
	Meegeven voor aanbesteding	
	13. Communicatiebeveiliging	
	Beoordelen doorontwikkeling	
	Meegeven voor aanbesteding	
	17. Communicatiebeveiliging	
	Inventariseren continuïteitsplannen	

5. Informatiebeveiligingsbeleid

Doelstelling
Het verschaffen van aansturing en steun voor informatiebeveiliging door de staf van de Kiesraad, in overeenstemming met organisatorische eisen en relevante wet- en regelgeving.

Beleidsregels voor informatiebeveiliging

BIO	Maatregel
5.1	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.

Binnen de Kiesraad is Privacy- en informatiebeveiligingsbeleid opgesteld. Het hoofd informatiebeveiliging bespreekt dit beleid begin 2020 samen met de privacy- en de security officer, waarna het ter goedkeuring aan de staf (het MT) wordt voorgelegd en wordt gecommuniceerd met de Kiesraad met behulp van een managementsamenvatting. De medewerkers worden met behulp van de inwerkmap en het bewustwordingsprogramma van het beleid op de hoogte gesteld.

Beoordeling van het informatiebeveiligingsbeleid

BIO	Maatregel
5.2	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.

Vanwege de in gang gezette transitie zal het Privacy- en informatiebeveiligingsbeleid in november 2020 opnieuw tegen het licht gehouden worden, om te beoordelen of dit passend, adequaat en doeltreffend is. De handreiking Informatiebeveiligingsbeleid kan hierbij als uitgangspunt dienen. Tegelijkertijd zal het Privacy- en informatiebeveiligingsplan voor 2021 opgesteld worden.

Actielijst

Beveiligingsbeleid en plan vaststellen

Beveiligingsbeleid communiceren

Beveiligingsbeleid beoordelen

Beveiligingsplan 2021 opstellen

Beleid en plan voor 2021 vaststellen

6. Organiseren van informatiebeveiliging

Doelstelling
Een kader vaststellen om de implementatie en uitvoering van informatiebeveiliging binnen de Kiesraad op te zetten en te beheersen.

Rollen en verantwoordelijkheden

BIO	Maatregel
6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.

Hoofdstuk 2 van het Privacy- en informatiebeveiligingsbeleid bevat de rollen en verantwoordelijkheden op het gebied van privacy- en informatiebeveiliging binnen de Kiesraad, welke gebaseerd zijn op relevante voorschriften. Het hoofd informatiebeveiliging neemt de verantwoordelijkheden op zich die onderdeel uitmaken van het CISO-functieprofiel. In het kader van de transitie wordt een nieuw cluster IT en informatiebeleid in het leven geroepen. Halverwege 2020 zal, op basis van de gewijzigde situatie beoordeeld worden of de rollenstructuur aangepast wordt.

Scheiding van taken

BIO	Maatregel
6.1.2	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

Voor de kandidaatstelling en vaststelling van de verkiezingsuitslag geldt dat in het informatiesysteem rollen zijn beschreven, die taken en verantwoordelijkheden met zich meebrengen die van elkaar gescheiden zijn. Procesmatig geldt voor de landelijke verkiezingen dat er binnen de Kiesraad een projectleider is, die zorgdraagt voor de verdeling van taken. Voor taken als het opstellen van de processen-verbaal, spreekteksten en publicaties in de Staatscourant geldt steevast het meer-ogen principe. Voorafgaand aan toekomstige landelijke verkiezingen zal een beschrijving worden opgesteld met de belangrijkste producten en bijbehorende controleurs.

Contact met overheidsinstanties

BIO	Maatregel
6.1.3	Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.

In het begin van 2020 stellen de privacy- en security officer een overzicht op met contactgegevens van relevante overheidsinstanties, waaronder de Autoriteit Persoonsgegevens. Dit kan door de privacy- en security officer aan de orde worden gesteld in een CISO-overleg, zodat wellicht kan worden aangesloten bij contactgegevens waar het ministerie van BZK reeds over beschikt.

Informatiebeveiliging in projectbeheer

BIO	Maatregel
6.1.5	Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.

Informatiebeveiliging maakt onderdeel uit van de transitie en de doorontwikkeling van de bestaande OSV. De proceseigenaar ziet erop toe dat implicaties van informatiebeveiliging regelmatig worden behandeld en beoordeeld. Informatiebeveiliging in projectbeheer zal aan de orde worden gesteld in het bewustwordingsprogramma dat de privacy en security officer opzetten.

Beleid voor mobiele apparatuur

BIO	Maatregel
6.2.1	Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.

Voor het gebruik van mobiele apparatuur bestaan richtlijnen binnen het ministerie van BZK waar de Kiesraad bij aansluit. SSC-ICT is verantwoordelijk voor het uitrollen van mobiele apparatuur. In dit verband verwijzen wij naar de in control verklaring betreffende SSC-ICT die het ministerie van BZK heeft afgegeven. Het gebruik van mobiele apparatuur zal aan de orde worden gesteld in het bewustwordingsprogramma dat de privacy en security officer opzetten.

Telewerken

BIO	Maatregel
6.2.2	Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.

Voor telewerken bestaan richtlijnen binnen het ministerie van BZK waar de Kiesraad bij aansluit. SSC-ICT is verantwoordelijk voor het faciliteren van telewerken. In dit verband verwijzen wij naar de in control verklaring betreffende SSC-ICT die het ministerie van BZK heeft afgegeven. Telewerken zal aan de orde worden gesteld in het bewustwordingsprogramma dat de privacy en security officer opzetten.

Actielijst

Beoordelen rollenstructuur

Vaststellen gewijzigde rollenstructuur

Beschrijving taken en controleurs verk.

Overzicht contactgegevens opstellen

Bewustwordingsprogramma maken

7. Veilig personeel

Doelstelling
Waarborgen dat medewerkers en contactanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen.

Screening

BIO	Maatregel
7.1.1	Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.

Voor personeel dat in dienst treedt bij de Rijksoverheid – en dus ook bij de Kiesraad – is een verklaring omtrent het gedrag (VOG) nodig. Dit is een verklaring waaruit blijkt dat uw gedrag in het verleden geen bezwaar vormt voor het vervullen van uw functie. De richtlijnen voor indiensttreding bij het ministerie van BZK worden ook gevolgd voor indiensttreding bij de Kiesraad.

Arbeidsvoorwaarden

BIO	Maatregel
7.1.2	De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.

Medio 2020 beoordelen de privacy- en security officer de aanwezige informatie over informatiebeveiliging voor nieuwe interne en externe medewerkers, die zij bij hun aanstelling of functiewisseling ontvangen.

Directieverantwoordelijkheden

BIO	Maatregel
7.2.1	De directie behoort van alle medewerkers en contractanten te eisen dat ze informatie beveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.

Het ministerie van BZK heeft integriteitbeleid en regelingen, waaronder een gedragsregeling digitale werkomgeving, waar de Kiesraad zich bij aansluit. De overheid heeft een klokkenluidersregeling die ook voor de Kiesraad geldt en in 2021 wijzigt. De klokkenluidersregeling zal aan de orde worden gesteld in het bewustwordingsprogramma dat de privacy en security officer opzetten.

Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

BIO	Maatregel
7.2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.

Medewerkers van de Kiesraad doorlopen bij indiensttreding de introductie van het ministerie van BZK. Zij ontvangen een training voor een veilig gebruik van Digidoc en worden in staat gesteld om de e-learningmodules iBewustzijn te volgen. Medio 2020 beoordelen de privacy- en security officer de aanwezige informatie over informatiebeveiliging voor nieuwe interne en externe medewerkers. En iBewustzijn zal aan de orde worden gesteld in het bewustwordingsprogramma dat de privacy en security officer opzetten. Het programma zal bestaan uit jaarlijks ten minste één dag waarop de thema's en informatie zoals beschreven in dit plan worden uitgelegd.

Disciplinaire procedure

BIO	Maatregel
7.2.3	Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.

De disciplinaire procedure van het ministerie van BZK wordt gevolgd en staat beschreven. Dit onderwerp zal aan de orde worden gesteld in het bewustwordingsprogramma dat de privacy en security officer opzetten.

Beëindiging en wijziging van het dienstverband of verantwoordelijkheden

BIO	Maatregel
7.2.4	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht.

De direct leidinggevende van de persoon die vertrekt of wiens rol wijzigt ziet erop toe dat de informatiebeveiligingsaspecten bij uitdiensttreding of een rolwijziging in beschouwing worden genomen. Bij het gebruik van informatiesystemen treedt de direct leidinggevende hierover in overleg met proceseigenaar van de desbetreffende systemen. Personeelszaken is uiteindelijk verantwoordelijk voor de totale beëindigingsprocedure als het een uitdiensttreding betreft. De verantwoordelijkheden bij uitdiensttreding komen aan de orde in het bewustwordingsprogramma dat de privacy en security officer opzetten.

Actielijst

Informatie indiensttreding beoordelen

Bewustwordingsprogramma maken

Bewustwordingsdag organiseren

8. Verantwoordelijkheid voor bedrijfsmiddelen

Doelstelling
Bedrijfsmiddelen van de Kiesraad identificeren en passende verantwoordelijkheden ter bescherming definiëren.

Inventariseren van bedrijfsmiddelen

BIO	Maatregel
8.1.1	Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.

In de handreiking samenhang beheerprocessen staat dat er in het kader van informatieveiligheid diverse beheerprocessen zijn. De inventarisatie van bedrijfsmiddelen in relatie tot het verkiezingsproces bestaat enerzijds (procesmatig) uit de draaiboeken met producten en middelen die worden ingezet ten behoeve van de organisatie van landelijke verkiezingen en anderzijds (softwarematig) uit de architectuur die aan de OSV ten grondslag ligt. Vanwege de transitie zullen deze procesbeschrijvingen en architectuur opnieuw gedefinieerd worden. De privacy- en security officers naar verwachting in 2021 aandacht besteden aan de inventarisatie van bedrijfsmiddelen en de opgeleverde producten in dit licht beoordelen. In bedrijfsmatig opzicht zullen de activa van de Kiesraad hierbij betrokken worden.

Eigendom van bedrijfsmiddelen

BIO	Maatregel
8.1.2	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.

Voor bedrijfsmiddelen die SSC-ICT uitrolt bestaat een toegewezen eigenaar. Tegelijk met de beoordeling van de inventarisatie van bedrijfsmiddelen die de privacy- en security officer verichten, zullen zij ook aandacht hebben voor de vermelding van eigenaren bij die bedrijfsmiddelen naar aanleiding van de inventarisatie.

Aanvaardbaar gebruik van bedrijfsmiddelen

BIO	Maatregel
8.1.3	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.

De gedragscode integriteit Rijk, die ook voor de Kiesraad geldt en staat beschreven op het intranet, bevat een paragraaf (4.3) over het zorgvuldig omgaan met mensen en middelen. De gedragscode zal aan de orde worden gesteld in het bewustwordingsprogramma dat de privacy- en security officer opzetten. De privacy- en security officer controleren bij de verantwoordelijke medewerkers of de gedragsregels in contacten met externen overeenkomstig zijn vastgelegd. Denk hierbij ook aan de afspraken met stagiaris. Voor externen wordt een lichte versie van de inwerkmap gemaakt.

Teruggeven van bedrijfsmiddelen

BIO	Maatregel
8.1.4	Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven.

In de beëindigingsprocedure is het teruggeven van alle eerder verstrekte fysieke en elektronische bedrijfsmiddelen die eigendom zijn van of toevertrouwd aan de Kiesraad een vast onderdeel. De privacy- en security officer beoordelen of ook is voorzien in:
- de overdracht en het verwijderen van relevantie informatie op middelen die eigendom zijn van de medewerker;
- het documenteren/overdragen van relevantie kennis;
- het uitoefenen van controle op het onbevoegd kopiëren van relevante informatie tijdens de opzegtermijn.

Classificatie van informatie

BIO	Maatregel
8.2.1	Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.

De informatie die onderdeel uitmaakt van het verkiezingsproces en de informatie in het door te ontwikkelen OSV zal door middel van een expliciete risicoafweging geclassificeerd worden, gebruikmakend van de handreiking dataclassificatie, zodat duidelijk is welke bescherming nodig is. De risicoanalyse zal, in samenwerking met de privacy- en security officer plaatsvinden halverwege 2020.

Informatie labelen

BIO	Maatregel
8.2.2	Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.

Om classificatie van de informatie mogelijk te maken zal, in samenwerking met de privacy- en security officer, een classificatieschema worden opgesteld, zodat de informatie binnen de organisatie overeenkomstig gelabeld kan worden. Na afronding van risicoanalyse zullen de privacy- en security officer zich buigen over de labeling.

Behandelen van bedrijfsmiddelen

BIO	Maatregel
8.2.3	Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.

Na afronding van risicoanalyse en het labelen zullen de privacy- en security officer zich ook buigen over de procedures voor het gebruik van de informatie, zoals:
- Toegangsbeperkingen
- Verslaglegging erover
- Uitwisseling ervan
- Opslag ervan

Beheer van verwijderbare media

BIO	Maatregel
8.3.1	Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.

De privacy- en security officer controleren, met de handreiking mobiele gegevensdragers, of de wijze waarop vertrouwelijk of hoger geclassificeerde informatie wordt opgeslagen voldoet aan de eisen van het beveiligingsniveau en of er een verwijderinstructie is opgesteld.

Verwijderen van media

BIO	Maatregel
8.3.2	Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.

Voor de afvoer van ICT-middelen verwijzen wij naar de in control verklaring betreffende SSC-ICT. Voor ICT-middelen die niet in beheer zijn bij SSC-ICT wordt handreiking veilige afvoer ICT-middelen geraadpleegd. Het verwijderen van middelen zal aan de orde worden gesteld in het bewustwordingsprogramma dat de privacy- en security officer opzetten. Vernietiging van papier is geregeld via gebouwbeheer. De privacy- en security officer zullen de procedures die daarvoor gelden vergelijken met het op te stellen classificatieschema.

Media fysiek overdragen

BIO	Maatregel
8.3.3	Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.

Voor het fysieke transport van media wordt beleid opgesteld en voor het gebruik van koeriers of transporteurs voor vertrouwelijk of hoger geclassificeerde informatie worden betrouwbaarheidseisen opgesteld.

Actielijst

Beoordelen inventarisatie bedrijfsm.

Eigenaren inventarisatie bedrijfsm.

Gedragsregels contracten externen

Procedure teruggave bedrijfsmiddelen

Classificatie informatie OSV en verk.

Classificatieschema ontwerpen

Informatie: labelen en procedures

Beleid en eisen verwd. transp. media

9. Toegangsbeveiliging

Doelstelling
Toegang tot informatie en informatieverwerkende faciliteiten van de Kiesraad beperken.

Beleid voor toegangsbeveiliging

BIO	Maatregel
9.1.1	Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.

Toegangsbeveiliging is geregeld via gebouwbeheer. Het pand is sinds het einde van 2018 eigendom van het Rijksvastgoedbedrijf, met de daarvoor geldende beveiligingseisen. De Kiesraad sluit hierbij aan. De privacy- en security officer zullen het actuele beleid opvragen en beoordelen of extra maatregelen nodig zijn, gebruikmakend van de handreiking beleid logische toegangsbeveiliging.

Toegang tot netwerken en netwerkdiensten

BIO	Maatregel
9.1.2	Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.

De netwerkdiensten houden verband met gebouwbeheer en SSC-ICT. Met behulp van een gebruikersnaam en wachtwoord kan alleen geauthentiseerde apparatuur toegang krijgen tot een vertrouwde zone. Overige gebruikers krijgen alleen toegang tot een overtrouwde zone met een gastaccount.

Registratie en afmelden van gebruikers

BIO	Maatregel
9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.

Ook voor het aanmelden en afmelden gelden de regels van gebouwbeheer. Bezoekers moeten een werkdag van tevoren per mail worden aangemeld. De bezoekers dienen beneden bij de portier te worden opgehaald door de Kiesraad en na afloop van het bezoek te worden afgemeld bij de portier en begeleid naar de uitgang van het pand. De uitgifte en het beheer van de pasjes gaat via de gebouwbeheerder/gebouwmanager van de Zurichtoren die de autorisaties op de passen verzorgt.

Gebruikers toegang verlenen

BIO	Maatregel
9.2.2	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.

In de OSV maakt de beheerder accounts aan voor de daarvoor bestemde personen met de rol van verkiezingsleider of invoerder. Deze functiescheiding is aangebracht op basis van een risicoafweging. Voor elke verkiezing opnieuw worden de verschillende rollen toegekend. De projectleider van de verkiezing bij de Kiesraad kan, in bijvoorbeeld het draaiboek, expliciet vragen om de toegewezen rollen vast te leggen.

Beheren van speciale toegangsrechten

BIO	Maatregel
9.2.3	Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.

Vanwege de beperkte duur van het verkiezingsproces blijven de speciale toegangsrechten in OSV beperkt tot een klein aantal personen en zijn die speciale toegangsrechten van korte duur.

Beheer van geheime authenticatie-informatie van gebruikers

BIO	Maatregel
9.2.4	Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.

Dit is niet aan de orde bij de OSV, vanwege de aard van het gebruik. Voor authenticatie-informatie op bijvoorbeeld de tokens van medewerkers verwijzen wij naar de in control verklaring betreffende SSC-ICT.

Beoordelen toegangsrechten van gebruikers

BIO	Maatregel
9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.

Vanwege de beperkte duur van het verkiezingsproces zijn de toegangsrechten in de OSV van korte duur. Omdat voor iedere verkiezing een nieuwe versie van de OSV wordt opgeleverd, worden de rechten steeds opnieuw toegewezen.

Toegangsrechten intrekken of aanpassen

BIO	Maatregel
9.2.6	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.

Vanwege de beperkte duur van het verkiezingsproces zijn de toegangsrechten in de OSV van korte duur. Omdat voor iedere verkiezing een nieuwe versie van de OSV wordt opgeleverd, worden de rechten steeds opnieuw toegewezen.

Geheime authenticatie-informatie gebruiken

BIO	Maatregel
9.3.1	Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.

De gouden regel vanuit het ministerie van BZK luidt als volgt: Houd wachtwoorden voor jezelf en schrijf ze niet op. Met wachtwoordbeheerder KeePass bewaar je al je gebruikersnamen en wachtwoorden in een digitale kluis. KeePass is te vinden in je Windows startmenu. Dit onderwerp zal aan de orde worden gesteld in het bewustwordingsprogramma dat de privacy en security officer opzetten.

Beperking toegang tot informatie

BIO	Maatregel
9.4.1	Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.

Gebruikers kunnen in de OSV alleen informatie inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak. Het fysiek isoleren van informatie met een specifiek belang zal in aanloop de naar eerstvolgende landelijke verkiezing nader bekeken worden in 2021.

Beveiligde inlogprocedures

BIO	Maatregel
9.4.2	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.

Gebruikers hebben alleen toegang tot de OSV via een inlogprocedure met een gebruikersnaam en wachtwoord. De sterkte van de gebruikersauthenticatie hoort passend te zijn voor de classificatie van de informatie waartoe toegang wordt verleend. Om die reden zal na de classificatie opnieuw beoordeeld worden of de huidige inlogprocedure volstaat.

Systeem voor wachtwoordbeheer

BIO	Maatregel
9.4.3	Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.

In de OSV wordt geen gebruik gemaakt van two-factor authenticatie. Wel wordt een wachtwoordlengte afgedwongen, maar niet met een complexe samenstelling. Het aantal inlogpogingen is begrensd. Het wachtwoordbeleid zal in het kader van de uit te voeren risicoanalyse voor de transitie en door te ontwikkelen OSV opnieuw beoordeeld worden.

Speciale systeemhulpen gebruiken

BIO	Maatregel
9.4.4	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd.

In de productieomgeving van de OSV zijn er geen systeemhulpmiddelen om beheersmaatregelen te omzeilen, behalve die waarvoor een aparte authenticatie nodig is.

Toegangsbeveiliging op programmabroncode

BIO	Maatregel
9.4.5	Toegang tot de programmabroncode behoort te worden beperkt.

De broncode van de OSV is vrijelijk beschikbaar. Voor publicatie ervan zouden aanvullende maatregelen genomen kunnen worden die bijdragen aan het waarborgen van de integriteit ervan, bijvoorbeeld met een digitale handtekening. De leverancier is verantwoordelijk voor de beveiliging van programmabroncodes en samenhangende items onder zijn beheer.

Actielijst

Beleid toegangsbeveiliging beoordelen

Beschrijving rolverdeling OSV bij verk.

Na classifcatie inlogprc. beoordelen

Na analyse wachtwoordbl. beoordelen

10. Cryptografie

Doelstelling
Zorgen voor een correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

Beleid inzake cryptografie

BIO	Maatregel
10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.

Beleid ten aanzien van het gebruik van cryptografie en de verantwoordelijkheid daarvoor zal op termijn worden opgesteld met gebruikmaking van de handreiking encryptiebeleid. Dit is niet voorzien in 2020. Voor het kiezen van de juiste cryptografische maatregelen die voldoen aan de doelstellingen uit het informatiebeveiligingsbeleid wordt, in het kader van de transitie en de doorontwikkeling van de OSV, deskundig advies ingewonnen.

Sleutelbeheer

BIO	Maatregel
10.1.2	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.

PKI-overheid certificaten zijn de maatstaf en daarvoor hanteert de overheid eisen.

11. Fysieke beveiliging en beveiliging van de omgeving

Doelstelling
Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de Kiesraad voorkomen.

Fysieke beveiligingszone

BIO	Maatregel
11.1.1	Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.

Er gelden beveiligingszones, beginnend met een bemande receptie ter controle van de fysieke toegang tot het gebouw. De toegang tot het gebouw is beperkt tot bevoegd personeel. In zonering is voorzien door gebouwbeheer.

Fysieke toegangsbeveiliging

BIO	Maatregel
11.1.2	Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.

In geval van concrete beveiligingsrisico's worden waarschuwingen verzonden naar de alarmcentrale. Toegangsbeveiliging is geregeld via gebouwbeheer.

Kantoren, ruimten en faciliteiten beveiligen

BIO	Maatregel
11.1.3	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.

Voor bedrijfskritische papieren archieven en apparatuur heeft de Kiesraad beveiligingsmaatregelen genomen. De inventarisatie en risicoafweging kan beter expliciet worden gemaakt door deze vast te leggen in een document, waarvoor op zichzelf ook extra beveiligingsmaatregelen zullen moeten gelden. Zie in dit verband de handreiking logische toegangsbeveiliging.

Beschermen tegen bedreigingen van buitenaf

BIO	Maatregel
11.1.4	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.

In bescherming is voorzien via gebouwbeheer en de lokale hulpdiensten. Voor bedrijfskritische papieren archieven en apparatuur heeft de Kiesraad beveiligingsmaatregelen genomen.

BIO	Maatregel
11.1.5	*Werken in beveiligde gebieden* Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.
11.1.6	*Laad- en loslocatie* Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.
11.2.2	*Nutsvoorzieningen* Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.
11.2.3	*Beveiliging van bekabeling* Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.

11.2.7	*Veilig verwijderen of hergebruiken van apparatuur* Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.

Voor de hierboven genoemde maatregelen geldt dat gebouwbeheer en SSC-ICT hierin voorzien.

BIO	Maatregel
11.2.1	*Plaatsing en bescherming van apparatuur* Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.
11.2.4	*Onderhoud van apparatuur* Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.
11.2.5	*Verwijdering van bedrijfsmiddelen* Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.
11.2.6	*Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein* Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.
11.2.8	*Onbeheerde gebruikersapparatuur* Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.
11.2.9	*'Clear desk'- en 'clear screen'-beleid* Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten te worden ingesteld.

SSC-ICT is verantwoordelijk voor de plaatsing, het onderhoud en het verwijderen van grote ICT-apparaten en de bijbehorende beheersmaatregelen. Gaat het om kleine bedrijfsmiddelen en apparaten dan dienen gebruikers er zorgvuldig mee om te springen tijdens het gebruik, waaronder het plaatsen, onderhouden, verwijderen, het meenemen of het achterlaten ervan. Deze onderwerpen zullen aan de orde worden gesteld in het bewustwordingsprogramma dat de privacy en security officer opzetten.

Actielijst

Expliciteren interne maatregelen

12. Beveiliging bedrijfsvoering

Doelstelling
Correcte en veilige bediening van informatieverwerkende faciliteiten van de Kiesraad waarborgen.

Ten aanzien van de werkplekken van medewerkers is SSC-ICT verantwoordelijk voor de bedieningsprocedures en verantwoordelijkheden. De hieronder beschreven maatregelen worden bezien in het licht van de OSV.

BIO	Maatregel
12.1.1	*Gedocumenteerde bedieningsprocedures* Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.
12.1.2	*Wijzigingsbeheer* Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.
12.1.3	*Capaciteitsbeheer* Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.
12.1.4	*Scheiding van ontwikkel-, test- en productieomgevingen* Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.
12.2.1	*Beheersmaatregelen tegen malware* Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.
12.3.1	*Back-up van informatie* Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.
12.4.1	*Gebeurtenissen registreren* Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
12.4.2	*Beschermen van informatie in logbestanden* Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
12.4.3	*Logbestanden van beheerders en operators* Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.
12.4.4	*Kloksynchronisatie* De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.
12.5.1	*Software installeren op operationele systemen* Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.
12.6.1	*Beheer van technische kwetsbaarheden* Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.

12.6.2	*Beperkingen voor het installeren van software* Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.
12.7.1	*Beheersmaatregelen betreffende audits van informatiesystemen* Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.

De OSV wordt doorontwikkeld en in het kader van de transitie wordt een nieuw digitaal hulpmiddel voor de verkiezingsketen ontwikkeld. Op basis van de BIO kunnen bij de aanbesteding van het nieuwe digitale hulpmiddel begin 2020 belangrijke voorwaarden worden meegegeven. En bij de doorontwikkeling kunnen de maatregelen uit de BIO als toetssteen fungeren. In samenwerking met de privacy- en security officer wordt in het kader van de doorontwikkeling beoordeeld aan welk van deze maatregelen op dit moment wel en niet voldaan wordt. Zie in dit verband de handreiking samenhang beheersprocessen en informatiebeveiliging, de handreiking back-up and recovery, de handreiking aanwijzing logging, de handreiking voor implementatie van detectie-oplossingen en de handreiking penetratietesten.

Actielijst

Beoordelen doorontwikkeling

Meegeven voor aanbesteding

13. Communicatiebeveiliging

Doelstelling
De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten van de Kiesraad waarborgen.

Ook voor de netwerken van de kantooromgeving geldt dat SSC-ICT hier verantwoordelijk voor is. De hieronder beschreven maatregelen worden bezien in het licht van de OSV.

BIO	Maatregel
13.1.1	*Beheersmaatregelen voor netwerken* Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.
13.1.2	*Beveiliging van netwerkdiensten* Beveiligingsmechanismen, dienstverleningsniveaus en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
13.1.3	*Scheiding in netwerken* Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.
13.2.1	*Beleid en procedures voor informatietransport* Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.
13.2.2	*Overeenkomsten over informatietransport* Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.
13.2.3	*Elektronische berichten* Informatie die is opgenomen in elektronische berichten behoord passend te zijn beschermd.
13.2.4	*Vertrouwelijkheids- of geheimhoudingsovereenkomst* Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.

De OSV wordt doorontwikkeld en in het kader van de transitie wordt een nieuw digitaal hulpmiddel voor de verkiezingsketen ontwikkeld. De hier beschreven maatregelen als toetssteen fungeren bij de doorontwikkeling en worden meegenomen bij de aanbesteding van het nieuwe digitale hulpmiddel.

Actielijst

Beoordelen doorontwikkeling

Meegeven voor aanbesteding

14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen

Doelstelling
Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen van de Kiesraad in de gehele levenscyclus.

Analyse en specificatie van informatiebeveiligingseisen

BIO	Maatregel
14.1.1	De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.

Voor de aanbesteding van het nieuwe digitale hulpmiddel wordt een risicoanalyse uitgevoerd, zodat de eisen die verband houden met informatiebeveiliging kunnen worden opgenomen in de eisen voor het nieuwe informatiesysteem. De uit te voeren risicoanalyse kan ook tot maatregelen leiden ten aanzien van de begin 2020 door te ontwikkelen OSV. Het raadplegen van de handreiking diepgaande risicoanalyse methode strekt hierbij als voorbeeld tot de aanbeveling.

BIO	Maatregel
14.1.2	*Toepassingen op openbare netwerken beveiligen* Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.
14.1.3	*Transacties van toepassingen beschermen* Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.
14.2.1	*Beleid voor beveiligd ontwikkelen* Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.
14.2.2	*Procedures voor wijzigingsbeheer met betrekking tot systemen* Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.
14.2.3	*Technische beoordeling van toepassingen na wijzigingen besturingsplatform* Als besturingsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.
14.2.5	*Principes voor engineering van beveiligde systemen* Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.
14.2.6	*Beveiligde ontwikkelomgeving* Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.
14.2.7	*Uitbestede softwareontwikkeling* Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.
14.2.8	*Testen van systeembeveiliging* Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.
14.2.9	*Systeemacceptatietests* Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.
14.3.1	*Bescherming van testgegevens* Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.

De hier geformuleerde maatregelen brengen belangrijke eisen met zich mee voor het ontwikkelen van informatiesystemen. Deze kunnen worden meegenomen bij de

aanbesteding van het nieuwe digitale hulmiddel. Voor de testgegevens die de Kiesraad zelf gebruikt gelden een aantal voorwaarden, zoals het niet gebruiken van echte persoonsgegevens. Deze voorwaarden worden gehanteerd, maar zijn niet opgenomen in het huidige testplan. In samenwerking met de privacy- en security officer wordt daar in het nieuw op te stellen testplan voor zorggedragen.

Actielijst

Voorwaarden opnemen in testplan

Meegeven voor aanbesteding

15. Leveranciersrelaties

Doelstelling
De bescherming waarborgen van bedrijfsmiddelen van de Kiesraad die toegankelijk zijn voor leveranciers.

BIO	Maatregel
15.1.1	*Informatiebeveiligingsbeleid voor leveranciersrelaties* Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.
15.1.2	*Opnemen van beveiligingsaspecten in leveranciersovereenkomsten* Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.
15.1.3	*Toeleveringsketen van informatie- en communicatietechnologie* Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.
15.2.1	*Monitoring en beoordeling van dienstverlening van leveranciers* Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.
15.2.2	*Beheer van veranderingen in dienstverlening van leveranciers* Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.

Binnen de Kiesraad dienen medewerkers die zich bezighouden met leveranciersrelaties op te hoogte te zijn van de daaraan te stellen eisen. Bovenstaande maatregelen zullen kort aan de orde worden gesteld in het bewustwordingsprogramma dat de privacy- en security officer opzetten. Hetzelfde geldt voor de uitgangspunten voor Inkoop, ontwikkeling en beheer die de Kiesraad hanteert en die beschreven zijn in hoofdstuk 4, vanaf punt 24, van het Privacy- en informatiebeveiligingsbeleid 2019-2022. Dit beleid en de hieronder vermelde controls, die bij de maatregelen uit de BIO horen, zullen door de privacy- en security officer met de betrokken medewerkers gedeeld en besproken worden. In onderling overleg zal hiervoor een leidraad worden opgesteld die alle maatregelen en eisen omvat. Zie hiervoor ook de handreiking inkoopvoorwaarden en informatiebeveiligingseisen.

BIO	Maatregel
15.1.1.1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden eisen t.a.v. informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd. Deze eisen zijn gebaseerd op een expliciete risicoafweging.
15.1.1.2	Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekken tot leverancierstoegang tot bedrijfsinformatie vastgesteld.
15.1.1.3	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.
15.1.2.1	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.
15.1.2.2	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.
15.1.2.3	In situaties waarin contractvoorwaarden worden opgelegd door leveranciers, is voorafgaand aan het tekenen van het contract met een risicoafweging helder gemaakt wat de consequenties hiervan zijn voor de organisatie.

	Expliciet is gemaakt welke consequenties geaccepteerd worden en welke gemitigeerd moeten zijn bij het aangaan van de overeenkomst.
15.1.2.4	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaard voorwaarden voor inkoop gehanteerd.
15.1.2.5	Voordat een contract wordt afgesloten wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exit-strategie.
15.1.2.6	In inkoopcontracten wordt expliciet de mogelijkheid van een externe audit opgenomen waarmee de betrouwbaarheid van de geleverde dienst kan worden getoetst. Een audit is niet nodig als de contractant d.m.v. certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.
15.1.3.1	Leveranciers moeten hun keten van toeleveranciers bekend maken en transparant zijn over de maatregelen die zij genomen hebben om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers.
15.2.1.1	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatieindicatoren, zoals in het contract opgenomen is.

In de aanbesteding van het nieuwe digitale hulpmiddel voor de verkiezingsketen zullen eisen ten aanzien van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd worden.

Actielijst

Leidraad IB en leveranciers opstellen

16. Beheer van informatiebeveiligingsincidenten

Doelstelling
Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten bij de Kiesraad, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.

BIO	Maatregel
16.1.1	*Verantwoordelijkheden en procedures* Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.
16.1.2	*Rapportage van informatiebeveiligingsgebeurtenissen* Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.
16.1.4	*Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen* Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.
16.1.5	*Respons op informatiebeveiligingsincidenten* Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.
16.1.6	*Lering uit informatiebeveiligingsincidenten* Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.
16.1.7	*Verzamelen van bewijsmateriaal* De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.

Op basis van de hier beschreven maatregelen, de controls uit de BIO en het indicidentenproces zoals BZK dat heeft ingericht en diens ervaringen daarmee, stellen de privacy- en security officer een incidentenproces voor de Kiesraad op. Zie hiervoor ook het voorbeeld incidentmanagement en response beleid. Dit proces wordt vastgesteld door het hoofd informatiebeveiliging, gedeeld met de medewerkers en aan de orde gesteld in het bewustwordingsprogramma dat de privacy- en security officer opstellen. Het opstellen van het incidentenproces houdt nauw verband met de in hoofdstuk 6 vermelde gewijzigde rollenstructuur en het in dat hoofdstuk vermelde contactenoverzicht.

Actielijst

IB incidentenproces opstellen

IB incidentenproces vaststellen

17. Informatiebeveiligingscontinuïteit

Doelstelling
Informatiebeveiligingscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de Kiesraad.

BIO	Maatregel
17.1.1	*Informatiebeveiligingscontinuïteit plannen* De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen.
17.1.2	*Informatiebeveiligingscontinuïteit implementeren* De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.
17.1.3	*Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren* De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.
17.2.1	*Beschikbaarheid van informatieverwerkende faciliteiten* Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.

De privacy- en security officer inventariseren welke continuïteitsplannen er, in het kader van bijvoorbeeld gebouwbeheer en ICT-dienstverlening, reeds bestaan. Zie in dit verband het model continuïteitsstrategie en het modelplan. Op termijn worden op basis van een risicoanalyse eisen opgesteld voor informatiebeveiliging in ongunstige situaties. Dit is niet voorzien voor 2020.

Actielijst

Inventariseren continuïteitsplannen

18. Naleving

Doelstelling
Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.

Beschermen van registraties

BIO	Maatregel
18.1.3	Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.

De bewaartermijnen van informatie die zich bij de Kiesraad bevindt staan in de selectielijsten en het verwerkingenregister. Verder maakt de Kiesraad gebruik van de archiefdiensten van BZK. Het onderscheid tussen openbare en vertrouwelijke informatie in de registers van aanduidingen is gemaakt door de registers op te splitsen in een openbare variant op de website en een interne variant in Digidoc.

Privacy en bescherming van persoonsgegevens

BIO	Maatregel
18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

In overeenstemming met de AVG heeft de Kiesraad een Functionaris Gegevensbescherming (FG) die toeziet op de juiste toepassing van de AVG binnen de Kiesraad, de secretaris-directeur ondersteunt bij zijn ambtelijke verantwoordelijkheid ten aanzien van de beveiliging van persoonsgegevens en de Kiesraad kan adviseren bij het vaststellen van eisen die uit de AVG volgen. De privacy officer controleert op de naleving van de eisen.

Cryptografische beheersmaatregelen

BIO	Maatregel
18.1.5	Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.

Beleid ten aanzien van het gebruik van cryptografie en de verantwoordelijkheid daarvoor zal op termijn worden opgesteld met gebruikmaking van de handreiking encryptiebeleid, zoals beschreven in hoofdstuk 10 van dit plan.

Onafhankelijke beoordeling van informatiebeveiliging

BIO	Maatregel
18.2.1	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.

Zoals vermeld in het Privacy- en informatiebeveiligingsbeleid wordt een PDCA-cyclus ingericht. De privacy- en security officer tuigen in 2020 een information security management system (ISMS) op, waarmee aantoonbaar de gehele plan-do-check-act cyclus op gestructureerde wijze wordt afgedekt. Zie hiervoor de handreiking ISMS.

Het cluster IT en informatiebeleid stelt een audit- en testplan op, waarin jaarlijks keuzes worden gemaakt voor welke systemen welke audits en tests worden uitgevoerd als het gaat om informatiebeveiliging.

Naleving beveiligingsbeleid en -normen

BIO	Maatregel
18.2.2	De directie behoort regelmatig de naleving van de informatieverwerking en - procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.

Voor het doorontwikkelde OSV en het nieuwe digitale hulpmiddel wordt, mits de Kiesraad daar de opdrachtgever/eigenaar van is, jaarlijks een in control verklaring (ICV) afgegeven op basis de rapportage uit de PDCA-cyclus, die onderdeel is van de reguliere verantwoording. Voor het doorontwikkelde OSV wordt in 2020 een eerste ICV opgesteld door het cluster IT en informatiebeleid, in samenwerking met de security officer.

Beoordeling van technische naleving

BIO	Maatregel
18.1.5	Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.

Het team IT en informatiebeleid stelt een audit- en testplan op, waarin jaarlijks keuzes worden gemaakt voor welke systemen welke audits en tests worden uitgevoerd als het gaat om informatiebeveiliging. Informatiesystemen worden daardoor periodiek gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid.

Actielijst

Opstellen PDCA-cyclus

Opstellen ISMS

Audit- en testplan opstellen

ICV doorontwikkelde OSV opstellen

Resterend uit het Privacy- en informatiebeveilgingsbeleid

De focus rondom privacy- en informatiebeveiliging is de laatste jaren meer komen te liggen op risicomanagement in plaats van compliancy 'op basis van lijstjes'. In lijn hiermee wordt binnen het Rijk meer gestuurd op basis van 'volwassenheid' van beheerprocessen. Hiervoor wordt het NBA-volwassenheidsmodel gehanteerd. In 2019 worden delen van dit model ingericht om te sturen op de volwassenheid van IB-processen bij BZK en binnen diens uitvoeringsorganisaties.

De privacy en security officer stellen vast of, en zo ja welke, onderdelen uit het NBA-volwassenheidsmodel gebruikt gaan worden binnen de Kiesraad en stelt de volwassenheidsniveaus ten aanzien van geselecteerde, relevante beheersprocessen vast. Dit is niet in 2020 voorzien.

19. Bijlage 1

Binnen de Kiesraad zijn de volgende taken en verantwoordelijkheden relevant met betrekking tot privacy- en informatiebeveiliging:

Hoofd informatiebeveiliging (secretaris directeur, in toekomst mogelijk de cluster coördinator IT en Informatiebeleid)

- stelt het Beveiligingsbeleid en het Beveiligingsplan vast, in samenspraak met de andere stafleden;
- rapporteert aan de Kiesraad over de vaststelling van het Beveiligingsbeleid en -plan;
- is verantwoordelijk ervoor te zorgen dat voldoende kennis en kunde op het gebied van privacy- en informatiebeveiliging binnen de Kiesraad aanwezig is;
- rapporteert aan de Kiesraad over de uitvoering van het Beveiligingsbeleid en -plan;
- draagt zorg voor de naleving van het Beveiligingsbeleid en -plan en de uitvoering ervan, onder meer met betrekking tot bij de Kiesraad aanwezige informatiesystemen en verwerkingen;
- wijst vanuit zijn/haar verantwoordelijkheid een privacy en security officer aan, met een onafhankelijke rol (zie uitgangspunten nrs. 15 en 16), voor de ondersteuning van privacy- en informatiebeveiliging;
- geeft de privacy en security officer aandachtspunten mee bij de toetsing van de uitvoering van het Beveiligingsbeleid en -plan;
- zorgt voor de totstandkoming van de jaarlijkse verantwoording over de privacy- en informatiebeveiliging;

Proceseigenaar (secretaris-directeur en clustercoördinatoren)

- is proceseigenaar van de onder hem of haar verantwoordelijkheid vallende verwerkingen, informatiesystemen en diensten;
- legt bij de beheersing van ICT-projecten nadruk op het tijdig opleveren van essentiële producten, zoals risicoanalyses en privacy impact analyses;
- stelt, overeenkomstig de planning in het Beveiligingsbeleid- en plan en met assistentie van de privacy en security officer, de betrouwbaarheidseisen vast voor de systemen, verwerkingen en werkprocessen op basis van een integrale risicoanalyse;
- draagt, met assistentie van de privacy en security officer, zorg voor een adequaat stelsel van gedocumenteerde en verifieerbare beheersmaatregelen naar aanleiding van gehouden risicoanalyses;
- evalueert en actualiseert, met assistentie van de privacy en security officer, aanwezige integrale risicoanalyses minimaal iedere twee jaar, of eerder indien wijzigingen in proces of beheersomgeving dit vereisen.
- stimuleert dat medewerkers tot deelname aan het bewustwordingsprogramma van de Kiesraad rondom privacy- en informatiebeveiliging;

Privacy officer

- aanspreekpunt op het gebied van privacybescherming;
- adviseren over privacybescherming;
- uitvoeren van taken die voortvloeien uit het Beveiligingsbeleid- en plan;
- bewaken naleving van de geldende wet- en regelgeving;
- agenderen onderwerpen op het gebied van privacybescherming bij het hoofd informatiebeveiliging en de staf;
- verzorgen communicatie over privacybescherming;
- zorgt dat medewerkers zorgvuldig met (persoons)gegevens, informatiesystemen en overige hulpmiddelen omgaan en de daarvoor vastgestelde reglementen naleven;
- vertegenwoordigen van de Kiesraad op het gebied van privacybescherming in het CISO-overleg bij BZK;
- inventariseert jaarlijks actuele risico's waarbij de te beschermen belangen een bepaald niveau overschrijden (zie uitgangspunt nr. 14);
- richt een planning en control cyclus in voor de verantwoording over privacybescherming;

- richt een incidentenprocedure in voor privacybescherming;
- toezien op naleving van de incidentenprocedure binnen de Kiesraad;
- afhandelen incidenten en hierover rapporteren aan het hoofd informatiebeveiliging.

Security officer
- aanspreekpunt op het gebied van informatiebeveiliging;
- adviseren over informatiebeveiliging;
- uitvoeren van taken die voortvloeien uit het Beveiligingsbeleid- en plan;
- bewaken naleving van de geldende wet- en regelgeving;
- agenderen onderwerpen op het gebied van informatiebeveiliging bij het hoofd informatiebeveiliging en de staf;
- verzorgen communicatie over informatiebeveiliging;
- zorgt dat medewerkers zorgvuldig met (persoons)gegevens, informatiesystemen en overige hulpmiddelen omgaan en de daarvoor vastgestelde reglementen naleven;
- vertegenwoordigen van de Kiesraad op het gebied van informatiebeveiliging in het CISO-overleg bij BZK;
- inventariseert jaarlijks actuele risico's waarbij de te beschermen belangen een bepaald niveau overschrijden (zie uitgangspunt nr. 14);
- richt een planning en control cyclus in voor de verantwoording over informatiebeveiliging;
- richt een incidentenprocedure in voor informatiebeveiliging;
- toezien op naleving van de incidentenprocedure binnen de Kiesraad;
- afhandelen incidenten en hierover rapporteren aan het hoofd informatiebeveiliging.

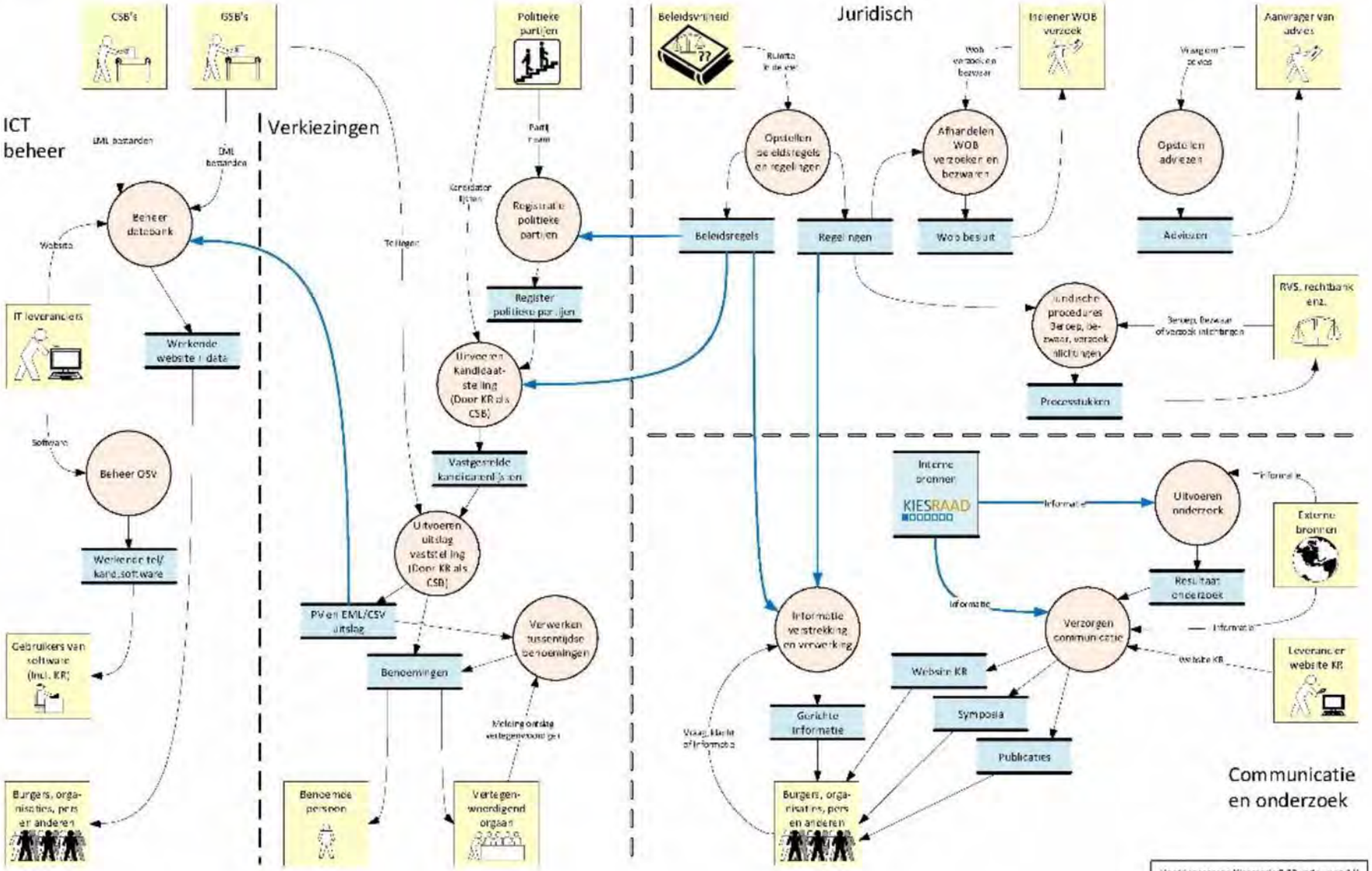
Buiten de Kiesraad zijn de volgende taken en verantwoordelijkheden relevant met betrekking tot privacy- en informatiebeveiliging:

CIO bij BZK
- stelt namens de SG de kaders voor privacy- en informatiebeveiliging van BZK op en evalueert deze periodiek;
- adviseert en ondersteunt de Kiesraad desgewenst over risicomanagement;
- zorgt voor de totstandkoming van de jaarlijkse verantwoording over de privacy- en informatiebeveiliging voor de verwerkingen en systemen die onderdeel zijn van de risicokaart BZK.

CISO bij BZK (Chief Information Security Officer)
- voert taken uit voor de bescherming van privacy en informatie, onder de verantwoordelijkheid van de CIO-BZK.
- onderhoudt contact met de CISO's en privacy-officers van de diverse BZK-onderdelen en met de privacy en security officer van de Kiesraad;
- zit het CISO-overleg voor.

Functionaris gegevensbescherming (FG)
- ziet toe op de juiste toepassing van de AVG binnen de Kiesraad;
- ondersteunt hiermee de secretaris-directeur bij zijn ambtelijke verantwoordelijkheid ten aanzien van de beveiliging van persoonsgegevens;
- kan de Kiesraad adviseren bij het vaststellen van eisen die uit de AVG volgen.

Hoofdprocesmodel Kiesraad



21. Bijlage 3

Beschikbaarheid: Het niet beschikbaar zijn van deze gegevens en uitval van het systeem levert ernstige schade op voor de organisatie.

Categorie	*Maximale schade*
Laag	Het informatiesysteem mag incidenteel uitvallen voor maximaal twee weken (ook inpiekperiodes) en heeft nauwelijks of geen gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: • financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de • begroting van het ministerie of uitvoeringsorganisatie; leidt nog niet uit het niet • krijgen van een accountants verklaring; of • beperkt verlies van management control; of • irritatie en ongemak bij burgers geventileerd in de media; of • interne negatieve publiciteit (imagoschade).Deze gevolgen worden als volgt gekwantificeerd: • Kantoorautomatisering en dienstspecifieke systemen hebben tijdens openingstijden • een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; • maximaal dataverlies 28 uur; • maximale hersteltijd in geval van incidenten is binnen 40 werkuren (5 werkdagen van 8 uur) in 85% van de gevallen.
Midden	Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en heeft voelbare gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: • politieke schade aan een bewindspersoon: bewindspersoon moet voor verantwoording naar de Tweede Kamer, bijvoorbeeld n.a.v. Kamervragen; of • diplomatieke schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van het ministerie of • uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of • verlies van publiek respect; klachten van burgers; of • Rijksbrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers.De beschikbaarheid wordt als volgt gekwantificeerd: • Kantoorautomatisering en dienstspecifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; • maximaal dataverlies 24 uur; • maximale hersteltijd in geval van incidenten is binnen 16 werkuren (2 dagen van 8 uur).
Hoger dan midden	Ernstigere schade dan het bij “Midden” beschreven schadescenario.De beschikbaarheideis overstijgt het standaard niveau dat een dienstenleverancier op dit moment kan leveren. In overleg met een dienstenleverancier moeten specifiek voor de situatie benodigde maatregelen worden afgesproken.

Integriteit: Onjuiste of onvolledige uitvoering van de gegevens en het systeem levert ernstige schade op voor de organisatie.

Categorie	*Maximale schade*
Laag	Er zijn geen bijzondere maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR definitie) te waarborgen. Het verlies van integriteit kan leiden totbeperkte schade, bijvoorbeeld:• financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de

	begroting van het ministerie of uitvoeringsorganisatie; leidt nog niet uit het niet krijgen van een accountants verklaring; of• beperkt verlies van management control; of• irritatie en ongemak bij burgers geventileerd in de media; of• interne negatieve publiciteit (imagoschade).
Midden	Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR definitie) te waarborgen. Het verlies van integriteit kan leiden tot forse schade, bijvoorbeeld:• politieke schade aan een bewindspersoon: bewindspersoon moet voor verantwoording naar de Tweede Kamer, bijvoorbeeld n.a.v. Kamervragen; of• diplomatieke schade te herstellen door ambtelijke opschaling; of• financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van het ministerie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of• belangrijk verlies van management control; of• verlies van publiek respect; klachten van burgers; of• Rijksbrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers.
Hoger dan midden	Ernstigere schade dan het bij “Midden” beschreven schadescenario. De integriteitseis overstijgt het standaard niveau dat een dienstenleverancier op dit moment kan leveren. In overleg met een dienstenleverancier moeten specifiek voor de situatie benodigde maatregelen worden afgesproken.

Vertrouwelijkheid: Verspreiding van de gegevens en informatie uit het systeem kan ernstige (imago)schade toebrengen aan de organisatie.

Categorie	*Maximale schade*
Laag	Kennisname van informatie door ongeautoriseerden (buitenstaanders) is niet gewenst, maar leidt niet tot schade van enige omvang. Het gaat hier om ongerubriceerde informatie.Het openbaar worden van deze informatie kan leiden tot: • financiële gevolgen: op te vangen binnen de begroting van het ministerie of uitvoeringsorganisatie; of • irritatie en ongemak bij burgers geventileerd in de media; of • interne negatieve publiciteit (imagoschade).
Midden	Bescherming van gegevens en andere te beschermen belangen in de processen van de Rijksdienst, waar o.a. vertrouwelijkheid aan de orde is, omdat het om gevoelige informatie gaat. Het openbaar worden van de gegevens, kan leiden tot: • politieke schade aan een bewindspersoon: bewindspersoon moet voor verantwoording naar de Tweede Kamer, bijvoorbeeld n.a.v. Kamervragen; of • diplomatieke schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de begroting van het ministerie of uitvoeringsorganisatie; geen accountants-verklaring afgegeven; of • verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers; of • bindende aanwijzing van de AP in verband met schending van de privacy; of • directe imagoschade, bijvoorbeeld door negatieve publiciteit.
Hoog	• Verlies van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3; • informatie wordt door derden geleverd met een rubricering (niet zijnde BBN2); of • aansluiting op een infrastructuur vereist (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen) BBN3 om informatie te kunnen verwerken op deze infrastructuur; of • weerstand tegen statelijke actoren is noodzakelijk.

From: "5.1.2.e "
Sent: Tue, 16 Oct 2018 15:54:16 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: AVG

Beste 5.1.2.e

Best al weer geruime tijd geleden stuurde jij de staf een notitie met een aantal bijlagen. Ik bn jou nog een tergkoppeling verschuldigd van de besprekingen hiervan in twee achtereenvolgende stafvergaderingen.

Bijlage 1
Voorstel 1.1.: Publiceer de namen van gemachtigden en plv. gemachtigden niet langer ook op de website van de Kiesraad. - Akkoord
Voorstel 1.2.: Stuur politieke partijen drie maanden vóór de dag van kandidaatstelling van elke verkiezing een brief met daarin de namen van degenen die namens de vereniging zijn aangewezen als gemachtigde en plaatsvervangend gemachtigde. - Akkoord
Voorstel 1.3: De Kiesraad moet de stukken die politieke partijen overleggen in het kader van een verzoek tot registratie van een aanduiding c.q. aanwijzing van een (plv.) gemachtigde vernietigen zodra deze niet meer relevant zijn. - Akkoord (wel nog een vraag: het kan relevant zijn te weten of een politieke partij een voortzetting is van een partij waarvan de aanduiding al eerder geregistreerd was; hoe stel je dat vast wanneer de stukken zijn vernietigd? Of moet je de bewijslast daarvoor simpelweg en alleen leggen bij verzoekers?)
Voorstel 1.4: De kopieën van stukken betreffende de registratie van aanduidingen die aan de Kiesraadstukken worden toegevoegd, dienen op het in art. G 1, negende lid, bedoelde moment eveneens vernietigd te worden. - Akkoord (ook hier een vraag: wat te doen met op cd-rom - verstrekte stukken?)
Voorstel 1.5: De notitie van het secretariaat bij registratieverzoeken kan beter geen persoonsgegevens bevatten - Akkoord
Voorstel 2.1: Geef een ieder die een kandidatenlijst inlevert niet alleen een ontvangstbevestiging, maar ook schriftelijk informatie over de verwerking van zijn persoonsgegevens in het verkiezingsproces, tenzij betrokkene hier expliciet geen prijs op stelt. - Akkoord
Voorstel 2.2: Beperk het verstrekken van informatie over de verwerking van persoonsgegevens niet tot de verwerking van de persoonsgegevens. - Akkoord
Voorstel 2.3: Vernietig alle kandidatenlijsten en bijkomende stukken, met uitzondering van de instemmingsverklaringen, na de vaststelling van de verkiezingsuitslag. - Akkoord
Voorstel 2.4: Verleng de terinzagelegging van kandidatenlijsten en - Akkoord
ondersteuningsverklaringen niet. I
Voorstel 2.5: Waarborg in het draaiboek voor de kandidaatstelling dat OSV-bestanden die op de dag van kandidaatstelling op een digitale gegevensdrager worden ingeleverd, niet alleen veilig worden bewaard, maar ook op tijd worden vernietigd. Vernietiging moet plaatsvinden op hetzelfde moment als de vernietiging van de papieren equivalent van de gegevens. - Akkoord
Voorstel 2.6: Wees erop attent dat een reactie op een verzoek van een natuurlijk persoon die een beroep doet op in de AVG neergelegde rechten gelijk is gesteld met een appellabel besluit, ook als deze rechten in de verordening of de Kieswet buiten toepassing zijn verklaard.
Voorstel 3.1: De AVG heeft geen gevolgen voor de wijze waarop de Kiesraad, in zijn hoedanigheid van centraal stembureau, ingevolge de Kieswet de verkiezingsuitslag vaststelt. - Akkoord
Voorstel 3.2: De Kiesraad mag het geslacht van een kandidaat niet zelf opzoeken, ook niet voor statistische doeleinden. - Akkoord (vraag: het geslacht zal veelal volgen uit identiteitsbewijs dan wel instemmingsverklaring. Mogen wij die gegevens overnemen op de kandidatenlijst als de inleveraar expliciet aangeeft daar geen problemen mee te hebben?)
Voorstel 4.1: Vernietig documenten die samenhangen met de (tussentijdse) - Akkoord
(tijdelijke) benoeming van leden in EK, TK en EP nadet de zittingstermijn van het vertegenwoordigend orgaan is afgelopen.

Met vriendelijke groet,
5.1.2.e

5.1.2.e
5.1.2.e
KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag
T 5.1.2.e / 5.1.2.e
E 5.1.2.e @kiesraad.nl
W www.kiesraad.nl

FOLLOW US ON twitter

100 JAAR KIESRECHT

From: "5.1.2.e "
Sent: Tue, 16 Oct 2018 16:39:41 +0200
To: "5.1.2.e " <5.1.2.e @kiesraad.nl>
Subject: AVG

Bijlage 2

Voorstel 1: Beslis of de Kiesraad en de minister van BZK gezamenlijk verwerkingsverantwoordelijk zijn voor het Informatiepunt Verkiezingen - Besluit: alleen de KR moet worden gezien als verwerkingsverantwoordelijk.
Voorstel 2: Er hoeft geen verandering plaats te vinden in de categorieën van persoonsgegevens die worden verwerkt voor het Informatiepunt Verkiezingen of de Postbus Kiesraad. - Akkoord
Voorstel 3: Maak een keuze tussen:

a. Ook bij vragen die per email binnenkomen wordt niet de integrale inhoud van de email in FMP geplaatst, maar formuleert de medewerker met eigen woorden in het kort wat de te beantwoorden vraag is.
b. Het blijft mogelijk om de inhoud van emails integraal in FMP op te nemen, maar medewerkerskrijgen de aanwijzing mee daarbij het 'onderschrift' niet te kopiëren. - Besluit:

keuze voor b, tenzij een binnengekomen email meer persoonsgegevens bevat (bedoeld is: van andere personen dan de verzender van de email.
Voorstel 4: Medewerkers van het Informatiepunt Verkiezingen krijgen als aandachtspunt mee in het veld 'aantekening' in FMP geen persoonsgegevens te vermelden. - Akkoord
Voorstel 5: De auto-responder op emails aan Kiesraad@Kiesraad.nl en Informatiepunt@Kiesraad.nl wordt aangepast - Akkoord, met dien verstande dat de door 5.1.2.e voorgestelde tekst als volgt wordt geamendeerd:

1. De woorden in behandeling nemen" worden gewijzigd in: af te handelen en
2. De tweede alinea wordt in zijn geheel geschrapt. In de plaats daarvan wordt voor wat betreft informatie over ons privacybeleid een link opgenomen naar de betreffende pagina op onze website. Er zal niet expliciet worden gewezen op de mogelijkheid van het indienen van bezwaar. Die mogelijkheid staat reeds vermeld op de betreffende webpagina.

Voorstel 6: Het Informatiepunt Verkiezingen wordt permanent beschikbaar. Onderzocht moet worden op welke wijze dit technisch te realiseren is. - Besluit: is geen AVG-punt en zal te zijner tijd nog wel eens worden bezien.
Voorstel 7: De tekst op het meldingsbandje van het Informatiepunt Verkiezingen wordt gewijzigd. - Besluit: De huidige mededeling wordt aangevuld met een verwijzing naar ons privacybeleid, opgenomen onder 'Privacy' op onze website www.kiesraad.nl.
Voorstel 8: Gegevens die in FMP worden ingevoerd worden vijf kalenderjaren bewaard. - Akkoord
Voorstel 9: Voor in- en uitgaande emails geldt dezelfde bewaartermijn in FMP. - Akkoord
Voorstel 10: Introduceer een nieuw systeem om in FMP emails te registreren. Streef naar een 'clean and mean'-structuur. - Akkoord om in overleg met 5.1.2.e en 5.1.2.e nog eens goed naar de huidige structuur te kijken; deze lijkt inderdaad niet erg transparant en consistent.

Met vriendelijke groet,
5.1.2.e

5.1.2.e
5.1.2.e

KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag

T 5.1.2.e / 5.1.2.e
E 5.1.2.e @kiesraad.nl
W www.kiesraad.nl

From: "5.1.2.e"
Sent: Tue, 16 Oct 2018 17:04:31 +0200
To: "5.1.2.e" <5.1.2.e@kiesraad.nl>
Subject: AVG

Bijlage 3

De staf kan instemmen met de in deze bijlage, onder 3 en 4, besproken punten.

Bijlage 4

Voorstel 1: Kiest de Kiesraad ervoor dezelfde persoon als Functionaris voor Gegegevensbescherming aan te wijzen als het ministerie van BZK?	- Besluit: vooralsnog wel (de betreffende functionaris zal hierover worden benaderd en bij instemming zal zijn naam worden doorgegeven aan de Autoriteit Persoonsgegevens)
Voorstel 2: Maak een emailadres aan voor de FG (fg@kiesraad.nl) en stuur alle emails die daarop binnenkomen automatisch door naar het emailadres van deze functionaris.	- Akkoord, zodra er groen licht is.
Voorstel 3:Ga na of de FG het heel belangrijk vindt dat de Kiesraad gebruik	- Akkoord, zodra er groen licht is.
Voorstel 4: Als de Kiesraad gebruik maakt van een digitaal register van verwerkingen, voorkom dan dat uittreksels daarvan op rijksoverheid.nl worden geplaatst	- Akkoord
Voorstel 5: De Kiesraad en de voorzitter van de Kiesraad zijn ieder een bestuursorgaan en zijn ieder verwerkingsverantwoordelijke in de zin van de AVG. In het door BZK aangeboden register is het evenwel niet mogelijk om de voorzitter als verwerkingsverantwoordelijke aan te wijzen.	- Akkoord met voorgestelde 'oplossing'
Voorstel 6: De secretaris-directeur is bevoegd om de opname van een verwerkingsproces in het register te accorderen.	- Akkoord (vraag: er zijn er drie 'in behandeling'; hoe staat het daarmee en welke zouden er nog bij moeten komen?

Dat was de terugkoppeling uit de staf 5.1.2.e Sorry dat het er niet eerder van is gekomen. Zoals jou al eerder is gevraagd, zouden wij graag zien dat je nu – als een volgende stap – een presentatie verzorgt voor de medewerkers van het secretariaat.

Heel veel dank voor al jouw inspanningen 5.1.2.e! Je bent er wat mij betreft ruim in geslaagd om de concreetheid te leveren waar wij behoefte aan hebben. Nogmaals dank daarvoor!

Met vriendelijke groet,
5.1.2.e

5.1.2.e
5.1.2.e

KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 2511WB Den Haag
Postadres: Postbus 20011, 2500 EA Den Haag

T 5.1.2.e / 5.1.2.e
E 5.1.2.e@kiesraad.nl
W www.kiesraad.nl

KIESRAAD

Notitie

Onderwerp
Handtekeningen op internet

Datum
5 juni 2019

Kenmerk
2019-0000293617

Onderdeel
Kiesraad

Blad
1 van 4

Aan
Leden van de Kiesraad
Van
5:1.2e

In de Kiesraadvergadering van 4 juni heeft u gesproken over de openbaarmaking van handtekeningen onderaan het proces-verbaal U 16 (en vergelijkbaar het proces-verbaal P 22). Aanleiding hiervoor was een bericht van de gemeente Zwolle (tevens hoofdstembureau) dat het vreemd was dat de handtekeningen onder de processen-verbaal N 10 en O 3 door gemeenten verwijderd moeten worden, terwijl de Kiesraad deze laat staan bij het eigen proces-verbaal.

Besloten is toen een notitie voor te bereiden over het wettelijk kader en de overwegingen die aan de huidige werkwijze ten grondslag liggen. Deze notitie geeft daaraan uitvoering. In de notitie is gemeend nog een verdiepingsslag te moeten maken. Uw handtekeningen komen namelijk niet alleen in de processen-verbaal met uitslagen terug, maar ook in processen-verbaal omtrent de kandidaatstelling en in adviezen. Ook ten aanzien van deze stukken is het goed te overwegen of het al dan niet wenselijk is de handtekeningen op internet te publiceren.

Publicatie processen-verbaal met uitslagen
De processen-verbaal met uitslagen van stembureaus, hoofdstembureaus en centraal stembureaus dienen sinds december 2018 allemaal op internet te worden gepubliceerd. Deze publicatieplicht gold al langer voor hoofd- en centraal stembureaus. Door deze publicatie kunnen derden uitslagen controleren en de brondocumenten raadplegen, iets wat vanuit het oogpunt van transparantie in de uitslagvaststelling belangrijk wordt geacht. Tegelijk is, ook voor hoofd- en centraal stembureaus geregeld dat publicatie dient plaats te vinden met weglating van de ondertekening daarvan.[1] Artikel P 23 van de Kieswet luidt:

> *Het centraal stembureau maakt zijn proces-verbaal* ***met weglating van de ondertekening*** *onverwijld op een algemeen toegankelijke wijze elektronisch openbaar […].*

[1] De Raad is niet om advies gevraagd over dit wetsvoorstel. De reden was dat de Raad eerder al geconsulteerd was over de kern van dit voorstel (publicatie processen-verbaal van stembureaus).

Ook voor alle andere instanties in de verkiezingsketen is een vergelijkbare regeling opgenomen als het gaat om de openbaarmaking van de processen-verbaal voor de vaststelling van de uitslag.[2] Het is m.a.w. wettelijk uniform geregeld voor alle onderdelen in de verkiezingsketen.

Een uitzonderingsgrond hierop is niet in de wet opgenomen, De regering overwoog destijds:

> *"Hoewel derhalve het algemeen belang bij de elektronische openbaarmaking van de processen-verbaal in beginsel zwaarder weegt dat het individuele belang van betrokkenen, neemt de regering in aanmerking dat de elektronische openbaarmaking van handtekeningen – mede gelet op het grote bereik van de publicatie op het internet – de kans op oneigenlijk gebruik van dit persoonsgegeven vergroot. Gelet hierop en nu de publicatie van de ondertekening op het internet niet zonder meer noodzakelijk is om het beoogde doel van transparantie in de procedure van uitslagvaststelling te bereiken, wordt voorgesteld bij de elektronische openbaarmaking van de stukken de ondertekening daarvan weg te laten."*[3]

De wetgever heeft zich dus op het standpunt gesteld dat bij de publicatie op internet, het recht van de ondertekenaars om beschermd te blijven van oneigenlijk gebruik van hun handtekeningen, zwaarder dient te wegen dan het belang van volledige openbaarmaking. De namen van de ondertekenaars worden wel gepubliceerd, iets wat in de regeling van het model gefaciliteerd wordt door deze ook op een andere pagina dan de handtekeningen te plaatsen.[4]

Een andere relevante overweging heeft betrekking op de aanleiding voor deze notitie; de melding van een gemeente. Gemeenten hebben relatief veel werk aan het verwijderen van de handtekeningen, zeker in relatie tot de mate waarin de processen-verbaal geraadpleegd worden. Het lijkt onwenselijk als de Kiesraad in tegenspraak met de wet zou menen dat de handtekeningen toch gepubliceerd mogen worden. Gemeenten kunnen dan de indruk krijgen dat het met deze bepaling niet zo nauw genomen hoeft te worden. Of, zo mogelijk nog erger, dat dat dan misschien ook wel geldt voor andere bepalingen uit de Kieswet. De voorbeeldfunctie van de Raad brengt met zich mee dat het de voorkeur verdient de wet te volgen.

Vanuit juridisch oogpunt is er derhalve geen ruimte voor de Kiesraad om te besluiten om de handtekeningen te laten staan op het afschrift van het proces-verbaal dat op internet gepubliceerd wordt, of dat nu wenselijk wordt geacht of niet. Dat de Raad dit eigenlijk liever anders ziet, is bekend. Zo is bij bespreking in uw Raad van het conceptadvies over het proces-verbaal voor de toewijzing van de Brexitzetels, de opmerking geschrapt dat het model het weglaten van de handtekeningenpagina niet faciliteert. Overeenkomstig artikel P 23 van de Kieswet zou dat wel moeten. De meerderheid van de Raad wenste de transparantie van het verkiezingsproces te laten prevaleren boven de privacy van de leden.[5] Desondanks dat het model bij mogelijke toewijzing van de Brexitzetels hier dus niet op is toegespitst, geldt ook

---

[2] Zie hiervoor de artikelen N 12, tweede lid, O 4, T 11en U 16 van de Kieswet.
[3] *Kamerstukken II* 2017/18, 35011, 3, p. 6.
[4] *Kamerstukken II* 2017/18, 35011, 3, p. 7.
[5] Verslag van de Kiesraadvergadering van 14 januari 2018.

voor dat proces-verbaal de wettelijke plicht om de ondertekening van de internetpublicatie weg te laten.[6]

Voorgesteld wordt om in lijn hiermee voortaan de handtekeningen op de internetversie van het proces-verbaal waarin een uitslag wordt vastgesteld weg te laten en dat ook met terugwerkende kracht alsnog te doen in de op internet gepubliceerde processen-verbaal van de recent gehouden EK- en EP-verkiezingen. Op die manier handelen we in lijn met de wetsaanpassing die in 2018 van kracht is geworden.

Publicatie overige ondertekende stukken
Voor de processen-verbaal m.b.t. de kandidaatstelling (I 1 en I 4) en de adviezen van de Raad is niet bepaald dat deze verplicht, met weglating van de handtekeningen, op internet moeten worden gepubliceerd. Kieswettelijk is er daarom eveneens geen verplichting om de ondertekening van deze stukken weg te laten, al kunnen er overwegingen zijn dat toch te doen. De processen-verbaal I 1 en I 4 liggen wel verplicht ter inzage (artikel I 18 van de Kieswet).

De ondertekening van stukken is van oudsher een manier om de authenticiteit van de stukken te benadrukken. Uitgaande brieven en adviezen worden daarom altijd ondertekend en in die vorm in het archief opgeslagen. Bij publicatie van een stuk op internet gaat het feitelijk om een afschrift van dat origineel. De ondertekening van dat stuk voegt op zichzelf echter niets toe aan de betrouwbaarheid van het stuk. Ter vergelijking; online gepubliceerde besluiten van overheidswege bevatten daarom ook geen handtekening maar enkel een vermelding van de tekeningsbevoegde.[7]

Tegenover het belang om met een ondertekening de authenticiteit van een stuk te bevestigen, staat het belang van het voorkomen van misbruik van deze persoonsgegevens. De mogelijkheid van identiteitsfraude met handtekeningen is niet ondenkbaar. De handtekeningen kunnen misbruikt worden door personen die zich als iemand anders voordoen. De Autoriteit Persoonsgegevens stelt dat handtekeningen (net als burgerservicenummers) een zodanige bescherming vereisen, dat zij nooit op internet geplaatst mogen worden.[8] Met het voorkomen van identiteitsfraude als oogmerk, is het niet publiceren van handtekeningen op internet begrijpelijk.

Er staan hier dus twee principiële belangen tegenover elkaar, waartussen een afweging gemaakt moet worden.

Er is ook nog een overweging van meer praktische aard. Het verdient namelijk de voorkeur om een consistente lijn te hanteren met betrekking tot de publicatie van handtekeningen. Aangezien er op basis van de wet geen ruimte is om de handtekening op het proces-verbaal van de vaststelling van de uitslag op internet te publiceren, zou dit met zich meebrengen dat de handtekeningen ook niet op de overige stukken vermeld dienen te worden. Het zou vreemd zijn als dezelfde handtekeningen de ene keer wel beschermd worden, en de andere keer niet. In plaats van de handtekeningen zou eventueel de tekst 'was getekend' aan het afschrift kunnen worden toegevoegd.

---

[6] Artikel 3 van de Wet van 12 december 2018, houdende regeling van de mogelijke toewijzing van extra zetels voor Nederland in het Europees Parlement
[7] https://www.officielebekendmakingen.nl/
[8] https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/persoonsgegevens-op-internet

Voorstel
Om te komen tot een praktische werkwijze waarin de bovengenoemde belangen zijn afgewogen, wordt voorgesteld op de website geen stukken te publiceren waarin handtekeningen zijn opgenomen. Het betreft hier:

Document	Authentieke versie	Versie op internet
PROCESSEN-VERBAAL MET UITSLAGEN (P 22 en U 16)	Ondertekend in openbare zitting, na verloop van tijd gearchiveerd	Niet-ondertekend omdat de wet dit vergt
PROCESSEN-VERBAAL VOOR DE KANDIDAATSTELLING (I 1 en I 4)	Ondertekend ter inzage, na verloop van tijd gearchiveerd	Niet-ondertekend
ADVIEZEN	Ondertekend naar de adressant, na verloop van tijd gearchiveerd	Niet ondertekend

Aangezien er voor de adviezen en de processen-verbaal I 1 en I 4 geen model is dat het weglaten van de handtekeningen faciliteert, wordt voorgesteld om in de internetversie van deze stukken de vermelding ‘was getekend’ toe te voegen.

Notitie

Onderwerp

Implementatie van de Algemene verordening gegevensbescherming (AVG)

Datum
28 mei 2018

Kenmerk
2018-0000271742

Inlichtingen
5.1.2.e
T 070 426 6266
F 070 751 7078

Aan
Voorzitter en leden van de Kiesraad
Van
Secretariaat

1. Inleiding

Op 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing geworden.[1] Deze is ook van toepassing op de Kiesraad, want ook de Kiesraad verwerkt persoonsgegevens. Bijvoorbeeld in het kader van zijn taken als centraal stembureau bij nationale verkiezingen en referenda, bij het beantwoorden van maatschappelijke correspondentie, en bij het voeren van het beheer over zijn secretariaat.

In deze notitie staat het proces centraal; niet de inhoud. De notitie is bedoeld om u te informeren over de procedurele stappen die door het secretariaat zijn gezet om de Kiesraad voor te bereiden op de van toepassingwording van de AVG. Uiteraard roept de implementatie van de AVG ook inhoudelijke vragen van diverse aard op: praktisch, juridisch en/of technisch. Het secretariaat heeft een notitie voor uw Raad in voorbereiding waarin op een aantal vraagstukken nader wordt ingegaan. Deze wordt op een later moment met u gedeeld. Op dit moment is de implementatie van de AVG nog niet voltooid. In de komende maanden zal de implementatie van de AVG dan ook aandacht van het secretariaat blijven vragen.

2. Voorbereiding

Bewustwording
Eén van de aandachtspunten voor een juiste implementatie van de AVG binnen een organisatie, is dat er in de breedte van de organisatie voldoende kennis moet zijn

[1] 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)

over de verordening en de rechten die derden daaraan kunnen ontlenen. Dat wil niet zeggen dat iedereen AVG-specialist moet worden. Wel is het nodig dat medewerkers van het secretariaat sensitief zijn voor het feit dat zij met persoonsgegevens werken en dat dit zekere verantwoordelijkheden met zich meebrengt. Ook moeten medewerkers ervan op de hoogte zijn dat personen van wie zijn persoonsgegevens verwerken op grond van de Algemene verordening gegevensbescherming bepaalde rechten hebben, zoals: het recht op inzage, het recht op rectificatie en het recht op verwijdering van gegevens. Met dit doel is op 17 juli 2017 een goed bezochte lunchlezing georganiseerd voor medewerkers van het secretariaat.

Inventarisatie
Het secretariaat heeft een inventarisatie gemaakt van alle werkprocessen waarin persoonsgegevens worden verwerkt. Het gaat daarbij zowel om werkprocessen waarbij de Kiesraad persoonsgegevens van derden verwerkt (externen) als om werkprocessen waarin persoonsgegevens van leden en medewerkers van de Kiesraad worden gebruikt (intern). Voorbeelden van werkprocessen waarbij de Kiesraad persoonsgegevens van derden verwerkt zijn: ons relatiebestand, de kandidaatstellingsprocedure en burgerbrieven. Voorbeelden van werkprocessen waarbij de Kiesraad persoonsgegevens van internen verwerkt zijn: verjaardagkalender medewerkers, het jaarverslag en verlofregistratie.

Daarna zijn deze werkprocessen geprioriteerd. Dit is gedaan op basis van de gevoeligheid van de persoonsgegevensverwerking. Daarbij is gebruik gemaakt van een door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties opgesteld document met daarin een opsomming van achttien indicatoren die kunnen helpen verschillende werkprocessen ten opzichte van elkaar te prioriteren. Bij de implementatie van de AVG heeft het secretariaat de werkprocessen met de hoogste prioriteit voorrang gegeven. Het gaat daarbij om werkprocessen die in verhouding tot andere werkprocessen van de Kiesraad, relatief gevoelig zijn en/of waarin veel persoonsgegevens worden verwerkt. Concreet betreft het de volgende vijf processen:

1. De kandidaatstellingsprocedure.
2. De vaststelling van de verkiezingsuitslag.
3. De benoeming van (tijdelijke) (plaatsvervangende) volksvertegenwoordigers.
4. De registratie van aanduidingen van politieke partijen.
5. Inleidende en definitieve verzoeken tot het houden van een referendum.

Kennisontwikkeling
Sinds 20 juni 2017 is het secretariaat, waar mogelijk, steeds aangeschoven bij de maandelijkse bijeenkomsten van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties ter voorbereiding van de implementatie van de AVG. Dit gaf met name inzicht in de interne werkprocessen van BZK en de gevolgtrekkingen die onderdelen van BZK uit de verordening maken. Daarnaast heeft het secretariaat deelgenomen aan verschillende zogenoemde AVG leerateliers. Tijdens deze bijeenkomsten stond de inhoud van de verordening centraal. De focus lag vaak evenwel op de inhoudelijke tekst van de verordening; meer dan op de concrete toepassing in de praktijk. Op vrijdag 25 mei 2018 vond een rijksbrede conferentie

plaats over de AVG. Sprekers waren onder andere 5.1.2.e 5.1.2.e en 5.1.2.e 5.1.2.e 5.1.2.e). Beiden zijn goed in de materie thuis en hadden inhoudelijk zeer interessant verhaal. Laatstgenoemde spreker heeft o.a. een klein boekje gepubliceerd waarin wordt uitgelegd hoe 'privacy by design' – artikel 25 van de AVG – in de praktijk concreet kan worden toegepast met behulp van acht privacyontwerpstrategieën. Dit digitale boekje is binnen het secretariaat verspreid onder de medewerkers voor wie deze informatie relevant kan zijn. Daarnaast is het boekje ook in DigiDoc opgenomen.

Kennisontwikkeling heeft niet alleen plaatsgevonden door het bijwonen van bijeenkomsten. Er zijn ook twee notities geschreven. Eén over de verplichtingen van de verwerkingsverantwoordelijke (kenmerk: 2017-0000469416) en één over de verantwoordelijkheidsverdeling tussen de verwerkingsverantwoordelijke en verwerker(s) onder de AVG (kenmerk: 2018-0000147364).

3. Merkbare gevolgen

De voorloper van de Algemene verordening gegevensbescherming, de Europese Privacyrichtlijn[2], was geïmplementeerd in de Wet bescherming persoonsgegevens.[3] Die wet was niet van toepassing op verwerkingen van persoonsgegevens ter uitvoering van de Kieswet.[4] Wel is bij wijzigingen in de Kieswet rekening gehouden met de richtlijn.[5] Andere verwerkingen van persoonsgegevens door de Kiesraad vielen wel onder de Wet bescherming persoonsgegevens. Daarvan is in het verleden binnen het secretariaat mogelijk niet iedereen zich altijd voldoende bewust geweest. De implementatie van de AVG geeft dan ook aanleiding om te evalueren of sommige (interne) werkprocessen aanscherping behoeven. Die evaluatie maakt onderdeel uit van het vervolg van het implementatietraject.

De implementatie van de Algemene verordening gegevensbescherming heeft vooralsnog niet geleid tot grote wijzigingen in de bestaande werkprocessen. Dat is goed verklaarbaar, want de materiële normen waaraan de verwerking van persoonsgegevens volgens de AVG moet voldoen is in grote lijnen gelijk gebleven aan die uit de Europese Privacyrichtlijn en de Wet bescherming persoonsgegevens.[6] Met andere woorden: het soort persoonsgegevens dat verwerkt mag worden, de voorwaarden waaronder persoonsgegevens verwerkt mogen worden en de wijze waarop persoonsgegevens verwerkt mogen worden, zijn niet heel ingrijpend gewijzigd. Grote wijzigingen in bestaande werkprocessen zijn, in organisaties die de privacyregelgeving al netjes naleefden, dan ook niet erg waarschijnlijk. Meer informatie over de regelgeving omtrent de verwerking van persoonsgegevens die op

[2] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
[3] Wet bescherming persoonsgegevens (Stb. 2000, 302).
[4] Art. 2 onder f Wet bescherming persoonsgegevens (van 1 september 2001 (Stb. 2001, 337) tot 24 mei 2018 (Stb. 2018, 145).
[5] Zie bijvoorbeeld: Kamerstukken II 2015/16, 34 384, nr. 3, p. 14 (MvT).
[6] Kamerstukken II 2017/18, 34 851, nr. 3, p. 5 (MvT).

de Kiesraad van toepassing is, kunt u vinden in een separate notitie over dit onderwerp (kenmerk: 2018-0000319432).

Naast dat de materiële normen in de privacyregelgeving niet ingrijpend gewijzigd zijn, is er nog een tweede reden waarom de implementatie van de AVG vooralsnog niet heeft geleid tot ingrijpende wijzigingen in bestaande werkprocessen. Die reden houdt verband met de gekozen prioriteitsstelling. De vijf werkprocessen waarvoor de AVG met voorrang wordt geïmplementeerd, volgen allemaal rechtstreeks uit de Kieswet. De verkiezingsregelgeving is zeer gedetailleerd waar het de te volgen procedures betreft. De AVG brengt in die procedures nauwelijks een wijziging. Alleen waar de Kiesraad meer doet dan wettelijke noodzakelijk, of waar eigen keuzes gemaakt worden, zal heroverweging daarvan moeten plaatsvinden. Op een later moment wordt u hier nader over geïnformeerd.

Het belangrijkste verschil met de situatie van voor de van toepassingwording van de AVG, is dat de rechten van betrokkenen – personen van wie de Kiesraad persoonsgegevens verwerkt – in de AVG zijn versterkt. Samenhangend daarmee zijn verplichtingen van de verwerkingsverantwoordelijken – de Kiesraad – strenger geworden. Ook wordt van de verwerkingsverantwoordelijke meer transparantie en verantwoording gevraagd dan onder het oude regime. Zo moet de Kiesraad bijvoorbeeld, in het kader van het afleggen van verantwoording, een register van de verwerkingsactiviteiten bijhouden. De implementatie van de AVG bestaat voor een groot deel uit het invullen van dit register. Daarom is daar in het implementatietraject de nodige aandacht naar uitgegaan. Hoewel dat vooralsnog weinig zichtbaar resultaat oplevert, is het wel één van de kernvereisten voor een correcte en volledige implementatie van de verordening.

Zoals eerder in deze paragraaf gesteld verwacht het secretariaat niet dat de implementatie van de AVG tot grote veranderingen in de werkprocessen van de Kiesraad zal leiden. Dat wil natuurlijk niet zeggen dat alles hetzelfde blijft. Bij de twee laatstgehouden openbare zittingen van de Kiesraad, in diens hoedanigheid als centraal stembureau voor het houden van een referendum, zijn bezoekers er bijvoorbeeld al vooraf, en tijdens de zitting, duidelijk op attent gemaakt dat deze bijeenkomst via internet werd gestreamd. Dat gebeurde zowel visueel – bij binnenkomst stond een symbool op de monitoren – als auditief – in de door de voorzitter uitgesproken spreektekst. Het is een kleine aanpassing, maar illustreert wel dat de Kiesraad de implementatie van de AVG serieus neemt.

4. Toekomstige ontwikkelingen

AVG-register: verantwoording
Zoals eerder gemeld is de Kiesraad verplicht een register bij te houden van alle verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden. Dit register is niet openbaar, maar moet desgevraagd aan de Autoriteit Persoonsgegevens ter beschikking kunnen worden gesteld. Op dit moment staan nog niet alle verwerkingsactiviteiten van de Kiesraad in het register. Hier zal de komende tijd aan doorgewerkt blijven worden.

Privacyverklaringen: transparantie
In navolging van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft de Kiesraad een (tijdelijke) nieuwe algemene privacyverklaring op zijn website gepubliceerd. Deze is voor verbetering vatbaar. Het onderdeel 'transparantie' is in het implementatietraject onderbelicht gebleven en krijgt de komende tijd meer aandacht. Op grond van de AVG is de Kiesraad voorts gehouden om, waar hij persoonsgegevens verwerkt die hij rechtstreeks van de betrokkene heeft ontvangen, de betrokkene daarover te informeren.[7] Voor het symposium 'De verkiezing van de toekomst', dat op vrijdag 29 juni plaatsvindt, is daar al rekening mee gehouden. Voor andere processen wordt op een later moment de noodzakelijkheid opnieuw bekeken.

Verwerkersafspraken: verantwoording
Voor zover de Kiesraad gebruikmaakt van verwerkers bij de verwerking van persoonsgegevens, moet de Kiesraad met deze verwerkers afspraken maken over de privacyaspecten van deze verwerking. Het aantal verwerkers is beperkt: DICTU (i.v.m. de Referendum Applicatie) en de belastingdienst (i.v.m. de digitalisering en verwerking van verzoeken tot het houden van een referendum en verklaringen ter ondersteuning van een inleidend verzoek). Op dit moment zijn nog niet alle nodige verwerkersafspraken gemaakt. Met de belastingdienst en DICTU is het secretariaat hierover nog in gesprek. Daarnaast wordt bezien of een concept-verwerkersovereenkomst met IVU kan worden gesloten. IVU is de producent van OSV en is in beginsel geen verwerker voor de Kiesraad. Er is evenwel een scenario denkbaar waarin IVU wel een verwerker wordt; namelijk het scenario dat zich bij de afgelopen gemeenteraadsverkiezing in Amsterdam heeft voorgedaan. In dat geval moet de Kiesraad OSV-bestanden met persoonsgegevens met IVU kunnen delen. Bij een dergelijke calamiteit zou het fijn zijn als de noodzakelijke verwerkersovereenkomst al gereed is, zodat alle energie kan uitgaan naar het oplossen van het probleem.

[7] Art. 13 AVG.

Notitie

Onderwerp
Van Wbp naar AVG: welke regelgeving omtrent de verwerking van persoonsgegevens is wanneer op de Kiesraad van toepassing?

Datum
30 mei 2018

Kenmerk
2018-0000319432

Inlichtingen
s.1.2.e
T 070 426 6266
F 070 751 7078

Aan
Voorzitter en leden van de Kiesraad
Van
Secretariaat

1. Inleiding

In deze notitie wordt ingegaan op de voor de Kiesraad relevante regelgeving voor de verwerking van persoonsgegevens. Allereerst volgt een schets van het juridisch kader (§ 2). Vervolgens wordt kort ingegaan op de belangrijkste veranderingen die de AVG heeft meegebracht (§ 3). Lastig daarbij is dat de Aanpassingswet Algemene verordening gegevensbescherming nog niet gereed is. Welke consequenties dat heeft, wordt daarna geschetst (§ 4). In die paragraaf wordt ook aandacht gevraagd voor een probleem dat vooralsnog niet door de wetgever lijkt te worden opgelost. Tot slot volgt een beknopt overzicht (§ 5).

2. Kader van regelgeving

Op 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing geworden.[1] Verordeningen van de Europese Unie hebben een vergelijkbare status als nationale wetten. De rechten en plichten die in een verordening zijn vastgelegd, gelden dus ook voor burgers en bedrijven. Zij kunnen zich daar onderling direct op beroepen. De AVG vervangt de Europese Privacyrichtlijn.[2] Richtlijnen van de Europese Unie bevatten opdrachten aan de lidstaten op een bepaald resultaat te bereiken, maar moeten door de lidstaten altijd nog in hun nationale wet- en regelgeving worden uitgewerkt. Pas als een richtlijn in de nationale wet- en regelgeving is geïmplementeerd, kunnen burgers en bedrijven zich op deze uitwerking van de richtlijn in het nationale recht beroepen. Burgers en

[1] 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) (Publicatieblad Nr. L 119 van 04/05/2016 blz. 0001-0088).
[2] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Publicatieblad Nr. L 281 van 23/11/1995 blz. 0031 - 0050).

bedrijven kunnen zich onderling dus niet rechtstreeks op een richtlijn beroepen. In Nederland was de Europese Privacyrichtlijn[3] uitgewerkt in de Wet bescherming persoonsgegevens.[4] Omdat de AVG op 25 mei 2018 de Europese Privacyrichtlijn heeft vervangen, is ook de Wet bescherming persoonsgegevens per die datum komen te vervallen.[5]

Ondanks dat een verordening van de Europese Unie een vergelijkbare status heeft als een nationale wet, laat de AVG op sommige punten nog wel ruimte voor nationale keuzes en nadere regels. Nederland heeft deze ruimte ingevuld in de Uitvoeringswet Algemene verordening gegevensbescherming,[6] die eveneens op 25 mei 2018 in werking is getreden. Uiteraard moet ook de bestaande wetgeving worden aangepast aan de terminologie van de AVG en het wegvallen van de Wet bescherming persoonsgegevens als de algemene wet voor bescherming van persoonsgegevens. Dit zal gebeuren met de inwerkingtreding van de Aanpassingswet Algemene verordening gegevensbescherming. Het wetsvoorstel dat tot die wet moet leiden, is op het moment van schrijven nog aanhangig bij de Tweede Kamer.[7]

3. Belangrijkste veranderingen

De materiële normen waaraan de verwerking van persoonsgegevens op grond van de AVG moet voldoen, zijn in grote lijnen gelijk gebleven aan die uit de Europese Privacyrichtlijn en de Wet bescherming persoonsgegevens. De belangrijkste verschillen zien vooral op de rechten van betrokkenen, die versterkt zijn, en op de daarmee samenhangende verplichtingen van de verwerkingsverantwoordelijken, die strenger zijn worden. Hoewel er in materieel opzicht geen sprake is van substantiële wijzigingen, is er wel een wijziging die voor de Kiesraad van groot belang is. De verwerking van persoonsgegevens ten behoeve van de uitvoering van de Kieswet, viel niet onder de Wet bescherming persoonsgegevens.[8] Dergelijke verwerkingen vallen sinds 25 mei 2018 echter wel onder de AVG. Andere verwerkingen van persoonsgegevens door de Kiesraad, bijvoorbeeld ter uitvoering van de Wet raadgevend referendum, hebben altijd al onder de Wet bescherming persoonsgegevens gevallen.

4. Gevolgen vertraging Aanpassingswet

Voor zover de Algemene verordening gegevensbescherming ruimte laat voor nationale keuzes en nadere regels, zijn deze in de Uitvoeringswet Algemene verordening gegevensbescherming gemaakt. Daarop bestaat echter een belangrijke uitzondering. Drie wetten op het terrein van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties zijn van die wet uitgezonderd: de Wet basisregistratie

---

[3] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Publicatieblad Nr. L 281 van 23/11/1995 blz. 0031 - 0050).
[4] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) (Stb. 2000, 302).
[5] Art. 51 Uitvoeringswet Algemene verordening gegevensbescherming (Stb. 2018, 144).
[6] Wet van 16 mei 2018, houdende regels ter uitvoering van 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) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming) (Stb. 2018, 144).
[7] Kamerstukken 2017/18, 34 939, nrs. 1-5.
[8] Art. 2 lid 2 onder f Wet bescherming persoonsgegevens.

personen, de Kieswet en de Wet raadgevend referendum.[9] De AVG zal expliciet in die wetten worden geïmplementeerd. De keuze voor een zelfstandige uitvoering in de Kieswet en de Wet raadgevend referendum is gelegen in het gedetailleerde en bijzondere karakter van het verkiezingsproces en het referendumproces. Deze processen vragen op enkele onderdelen om keuzes die specifiek op deze processen zijn afgestemd.[10]

De expliciete implementatie van de AVG in de Kieswet en de Wet raadgevend referendum wordt geregeld in de Aanpassingswet Algemene verordening gegevensbescherming. Zoals in paragraaf 2 van deze notitie al is gemeld, is dat vooralsnog een wet in wording. De consequentie hiervan is dat alle in de AVG opgenomen rechten en verplichtingen op dit moment onverkort van toepassing zijn op de verwerking van persoonsgegevens bij de uitvoering van de Kieswet en de Wet raadgevend referendum. Ook waar die zich slecht verhouden tot het in de Kieswet c.q. de Wet raadgevend referendum neergelegde systeem. Is dit een probleem?

Kieswet
Er is geen acuut probleem; er is wel sprake van een potentieel toekomstig probleem. Gelet op het gedetailleerde en bijzondere karakter van het verkiezingsproces kunnen niet alle in de Algemene verordening gegevensbescherming neergelegde rechten van natuurlijke personen onverkort worden gegarandeerd bij de verwerking van persoonsgegevens ter uitvoering van de Kieswet. Een voorbeeld. In het verkiezingsproces worden kandidatenlijsten ingeleverd bij het centraal stembureau. Het centraal stembureau onderzoekt de geldigheid van de kandidatenlijsten. De Kieswet kent een imperatief en limitatief aantal gronden op basis waarvan het centraal stembureau tot schrapping van de naam van een voorgedragen kandidaat moet overgaan. Is een kandidatenlijst eenmaal onherroepelijk vastgesteld, dan is deze onveranderbaar. De onmogelijkheid om een onherroepelijk vastgestelde kandidatenlijst nog te wijzigen is noodzakelijk, omdat op basis van deze lijst de stemming – o.a. het drukken van stembiljetten – en de stemopneming – o.a. het drukken van het hiervoor noodzakelijke proces-verbaal – wordt voorbereid. Artikel 18 van de AVG bevat echter een recht op beperking van de verwerking. Het biedt kandidaten het recht het centraal stembureau te vragen hun persoonsgegevens niet verder te verwerken. Als iemand dit recht inroept lopende de verzuimherstelperiode, dan ontstaat een dilemma. Natuurlijk kan de kandidatenlijst, in weerwil van de Kieswet, worden vastgesteld zonder de naam van de betreffende kandidaat, maar wat te doen als een kandidaat een beroep doet op artikel 18 van de AVG nadat de kandidatenlijst officieel is vastgesteld? Voor deze situaties beoogt de regering in de Kieswet een bepaling op te nemen – artikel H 16 Kieswet – waarin wordt bepaald dat artikel 18 van de AVG niet van toepassing is op de verwerking van persoonsgegevens in het kader van de kandidaatstellingsprocedure. Het probleem wordt daarmee opgelost. Zover is het evenwel nog niet. Totdat de Kieswet door de Aanpassingswet is aangepast, is de AVG onverkort van toepassing en heeft, als hogere regeling, ook voorrang op de Kieswet. Op dit moment is dat geen acuut probleem. Er vindt op dit moment immers geen verwerking van persoonsgegevens plaats op basis van de Kieswet. Later dit jaar vinden er in diverse gemeenten wel

[9] Art. 2 lid 2 Uitvoeringswet Algemene verordening gegevensbescherming.
[10] Kamerstukken II 2017/18, 34 939, nr. 3, p. 3 en 7 (MvT).

herindelingsverkiezingen plaats. Dan kan het wel een probleem worden. Ambtenaren van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties gaan er evenwel vooralsnog vanuit dat de Aanpassingswet tegen die tijd in werking is getreden. Het is belangrijk dat de Kiesraad hier een vinger aan de pols houdt.

Wet raadgevend referendum
Er is een acuut probleem. Als de Aanpassingswet met terugwerkende kracht in werking treedt, wordt dit probleem op een later moment gedeeltelijk opgelost. Het secretariaat is hierover op ambtelijk niveau in overleg met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Het volgende is het geval. De regering is voornemens de artikelen 16[11] en 18[12] van de AVG niet van toepassing te verklaren op de verwerking van persoonsgegevens in het kader van de uitvoering van de inleidende[13] en definitieve fase[14] van het raadgevend referendum. Volgens de regering verhouden deze artikelen zich slecht tot het in de Wet raadgevend referendum neergelegde systeem. Die constatering lijkt juist.

Het niet uitsluiten van artikel 15 van de AVG, betekent dat burgers wel een recht op inzage hebben (en houden!) als de voorzitter van de Kiesraad persoonsgegevens verwerkt ter uitvoering van de Wet raadgevend referendum. Het recht op inzage houdt in dat de voorzitter: moet aangeven of hij hun persoonsgegevens verwerkt – dus van de aanvrager, niet in zijn algemeenheid – en welke persoonsgegevens het betreft, moet informeren over de verwerkingsactiviteit en een kopie moet verstrekken van de persoonsgegevens die worden verwerkt. In de voorbereidende fasen kunnen kiesgerechtigden bij de voorzitter van het centraal stembureau een verzoek indienen tot het houden van een referendum óf een verklaring ter ondersteuning van een inleidend verzoek. Buiten discussie staat dat de voorzitter in deze procedure persoonsgegevens verwerkt in de zin van de AVG. De voorzitter verstuurt geen ontvangstbevestigingen. Via de band van artikel 15 van de AVG kan een natuurlijk persoon proberen om alsnog een soort van ontvangstbevestiging af te dwingen.

Het feit dat artikel 15 van de Algemene verordening gegevensbescherming van toepassing is op de inleidende en definitieve fase van het raadgevend referendum, leidt tot twee problemen. Het eerste probleem is van praktische aard. Ontvangen verzoeken en ondersteuningsverklaringen zijn niet op naam doorzoekbaar in de Referendum Applicatie. Het terugvinden van reeds ontvangen documenten is dan ook praktisch onuitvoerbaar. Met de huidige Referendum Applicatie kan de voorzitter van de Kiesraad niet voldoen aan verzoeken die op grond van artikel 15 van de AVG worden ingediend. Het tweede probleem houdt verband met de periode nadat de op het inleidend c.q. definitief verzoek is besloten. Vanaf dat moment blijven de ingediende verzoeken c.q. ondersteuningsverklaringen nog enige tijd in verzegelde pakketten bewaard.[15] Het systeem van de Wet raadgevend referendum staat niet toe dat in die periode uitvoering wordt gegeven aan artikel 15 van de AVG. Waar het

[11] Recht op rectificatie.
[12] Recht op beperking van de verwerking.
[13] Art. 39a Wet raadgevend referendum
[14] Art. 54a Wet raadgevend referendum.
[15] Art. 36 lid 1 jo. 39 Wrr. En art. 51 lid 1 jo. 54 Wrr.

eerste probleem met een investering in ICT mogelijk nog kan worden opgelost, volgt het tweede probleem direct uit het systeem van de Wet raadgevend referendum zelf. Daarom had het naar de mening van het secretariaat meer voor de hand gelegen ook artikel 15 van de AVG in de Wet raadgevend referendum uit te sluiten. Zoals eerder in deze paragraaf is gemeld, is het secretariaat op ambtelijk niveau met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties in gesprek over dit probleem. In een volgende vergadering wordt u over de voortgang hiervan geïnformeerd.

5. Overzicht
In deze notitie is ingegaan op de voor de Kiesraad relevante regelgeving voor de verwerking van persoonsgegevens. Het soort verwerking bepaalt welke regelgeving op deze verwerking van toepassing is.

Verwerking ter uitvoering van de Kieswet:
Op deze verwerking is de Algemene verordening gegevensbescherming en de Kieswet van toepassing. Laatstgenoemde zal op een later moment door de Aanpassingswet aan de verordening worden aangepast. Tot die tijd is de verordening onverkort van toepassing.

Verwerking ter uitvoering van de Wet raadgevend referendum:
Op deze verwerking is de Algemene verordening gegevensbescherming en de Wet raadgevend referendum van toepassing. Laatstgenoemde zal op een later moment door de Aanpassingswet aan de verordening worden aangepast. Tot die tijd is de verordening onverkort van toepassing.

Verwerkingen op andere gronden:
In alle andere situaties waarin de Kiesraad persoonsgegevens verwerkt wordt het juridisch kader bepaald door de Algemene verordening gegevensbescherming en de Uitvoeringswet algemene regels gegevensbescherming.

Notitie

Onderwerp
Vraagstukken bij de implementatie van de Algemene verordening gegevensbescherming (AVG)

Datum
28 mei 2018

Kenmerk
2018-0000271978

Onderdeel
Kiesraad

Aan
Voorzitter en leden van de Kiesraad
Van
Secretariaat

1. Inleiding

Op 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing geworden. Deze is ook van toepassing op de Kiesraad. Voor informatie over de voorbereiding van de Kiesraad op deze van toepassingwording, wordt op deze plaats kortheidshalve verwezen naar een eerdere notitie (kenmerk: 2018-0000271742). In deze notitie worden enkele vraagstukken besproken die zich bij de implementatie van de verordening hebben voorgedaan en de keuze die het secretariaat u hierbij voorstelt.

2. Het AVG-register

a) Algemeen

De Kiesraad moet – als verwerkingsverantwoordelijke – alle verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden noteren in het zogenoemde 'register van verwerkingsactiviteiten'.[1] Daarvoor wordt gebruikgemaakt van een elektronisch register. Dit elektronische register wordt ook door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en negen andere ministeries gebruikt. De techniek wordt gedeeld; de inhoud niet. Ambtelijk is gemeld dat het register van de Kiesraad dus niet voor derden leesbaar is.

b) Openbaarheid

Het register van verwerkingsactiviteiten is in beginsel niet openbaar. De AVG verplicht de verwerkingsverantwoordelijke slechts het register desgewenst ter beschikking te stellen aan de Autoriteit Persoonsgegevens.[2] Desalniettemin is het denkbaar dat (een deel van) de in het register opgenomen informatie op een later moment openbaar gemaakt moet worden als gevolg van een verzoek op basis van

---

[1] Art. 30 lid 1 AVG.
[2] Art. 30 lid 3 AVG.

de Wet openbaarheid van bestuur. Ambtelijk is vernomen dat op enig moment rijksbreed gesproken zal worden over het nut van pro-actieve openbaarmaking van (een deel van) het register. Daarbij is ook mondeling toegezegd dat de Kiesraad op dat moment zelf de keuze houdt om daar, al dan niet onder voorwaarden, aan mee te doen.

c) De verwerkingsverantwoordelijke
In het register van verwerkingsactiviteiten moet onder andere worden genoteerd wie verwerkingsverantwoordelijke is. Vanuit juridisch perspectief is dat op het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties altijd de minister. Om inzichtelijker te maken bij wie de verantwoordelijkheid voor een verwerkingsactiviteit in de praktijk is belegd, is de minister in het AVG-register van BZK echter nergens aangewezen als verwerkingsverantwoordelijke. Die verantwoordelijkheid is lager – op directeursniveau en hoger – belegd. De Kiesraad is zo'n kleine organisatie, dat een soortgelijke aanpak overbodig is. In de huidige opzet van het AVG-register kan echter alleen de voorzitter van de Kiesraad als verwerkingsverantwoordelijke worden aangewezen. Voor sommige verwerkingen is hij dit inderdaad. Denk bijvoorbeeld aan de benoeming van plaatsvervangende Kamerleden. In andere gevallen is het bestuursorgaan Kiesraad als geheel verwerkingsverantwoordelijke en zou het juister zijn de Kiesraad ook als zodanig in het register met verwerkingsactiviteiten op te nemen. Het secretariaat is voornemens deze mogelijkheid op haalbaarheid te onderzoeken.

d) Status
Bij het aanmaken van een verwerkingsactiviteit in het register van verwerkingsactiviteiten heeft deze de status 'In bewerking'. Als de verwerkingsactiviteit volledig is ingevuld, kan de status worden gewijzigd in 'vastgesteld'. Dit roept de vraag op of de verwerkingsverantwoordelijke zelf de wijze waarop de verwerkingsactiviteit in het AVG-register is opgenomen moet accorderen. Het secretariaat gaat er vanuit dat dit niet het geval is. De term 'vastgesteld' wil in casu alleen zeggen dat de registermelding volledig en 'officieel' is, in de zin dat de Autoriteit Persoonsgegevens uit mag gaan van de daarin opgenomen informatie. Instemming van de secretaris-directeur is daarvoor voldoende.

0

, nu het Besluit mandaat en machtiging Kiesraad (Stb. 2016, 19763) hierin niet voorziet. Dit zou voor verwerkingen waarbij de Kiesraad verwerkingsverantwoordelijke is betekenen, dat op alle registermeldingen in een vergadering van de Kiesraad besloten moet worden. Dat zouden waarschijnlijk hamerstukken zijn, want een registermelding is geen besluit en wijzigt op geen enkele manier de huidige procedures. Daarom verzoekt het secretariaat u ermee in te stemmen dat de secretaris-directeur de registermeldingen mag vaststellen. Uiteraard kunnen de vastgestelde registermeldingen daarna ter kennis van uw Raad worden gebracht en, indien nodig, worden gewijzigd.

Privacyverklaring Kiesraad

De Kiesraad functioneert als centraal stembureau bij nationale verkiezingen op grond van de Kieswet, is een adviesorgaan van de regering en het parlement en beantwoordt vragen van ambtenaren, politieke partijen en burgers over de Kieswet en het Nederlandse verkiezingsproces. Meer daarover leest u hier. Soms maakt de Kiesraad bij het uitvoeren van bovengenoemde taken gebruik van uw persoonsgegevens. De Kiesraad respecteert daarbij uw privacy en gaat zorgvuldig om met uw persoonsgegevens. Meer hierover, leest u op deze pagina.

1. Wat zijn persoonsgegevens?
Onder 'persoonsgegeven' wordt alle informatie verstaan die over iemand gaat of tot iemand te herleiden is. Voorbeelden zijn uw naam, adres, telefoonnummer en e-mailadres.

2. Welke persoonsgegevens verwerkt de Kiesraad?
De Kiesraad heeft een aantal (wettelijke) taken en verplichtingen. Om deze taken en verplichtingen goed uit te kunnen voeren, is het soms noodzakelijk om persoonsgegevens te gebruiken. De Kiesraad verzamelt en gebruikt deze persoonsgegevens voor specifieke doeleinden, die afgestemd zijn op zijn taken en verplichtingen. Deze algemene privacyverklaring is daarbij altijd van toepassing. Daarnaast heeft de Kiesraad verschillende specifieke privacyverklaringen opgesteld. Daarin is per thema meer informatie te vinden over de verwerking van persoonsgegevens door de Kiesraad.

Commented [ ]: Is het per taak?

Commented [ ]: Er zijn verwerkingen die niet onder de geformuleerde taken van de Kiesraad zijn terug te brengen.

Specifieke privacyverklaringen:

- Test
- Test

3. Wie is verantwoordelijk voor het gebruik van persoonsgegevens?
De Kiesraad, en zijn voorzitter, zijn verwerkingsverantwoordelijken in de zin van de Algemene verordening gegevensbescherming. Dit houdt in dat zij beslissen welke persoonsgegevens worden gebruikt, voor welk doel en op welke wijze.

4. Hoe beschermt de Kiesraad mijn privacy?
De Kiesraad:

- verwerkt persoonsgegevens op een rechtmatige, behoorlijke en transparante manier;
- verzamelt en gebruikt persoonsgegevens alleen voor vooraf bepaalde, duidelijk omschreven en gerechtvaardigde doeleinden.
- verwerkt alleen de voor het doel noodzakelijke persoonsgegevens;
- draagt er zorg voor dat persoonsgegevens correct en juist zijn en zo nodig worden geactualiseerd;

- bewaart persoonsgegevens niet langer dan noodzakelijk; en
- treft passende organisatorische en technische maatregelen voor de bescherming van persoonsgegevens. Hier zijn rijksbreed afspraken over gemaakt.

5. Heeft de Kiesraad een functionaris voor gegevensbescherming?
De Kiesraad heeft dezelfde functionaris voor gegevensbescherming als het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Deze functionaris is een externe toezichthouder en adviseur voor de bescherming van persoonsgegevens. U kunt contact opnemen met de deze functionaris via: postbusfg@minbzk.nl.

6. Welke rechten heb ik?
Op grond van de Algemene verordening gegevensbescherming kunt u mogelijk beroep doen op één of meer van de onderstaande rechten:

- Inzage in uw gegevens.
  U hebt er recht op te weten of de Kiesraad persoonsgegevens van u verwerkt. Als dit het geval is, geeft de Kiesraad u desgevraagd inzage in deze gegevens.
- Correctie van uw gegevens.
  Als uw persoonsgegevens onjuist zijn verwerkt, dan hebt u er recht op dat deze worden gerectificeerd. Voorts hebt u het recht om uw persoonsgegevens aan te vullen als deze onvolledig blijken te zijn.
- Verwijdering van uw gegevens.
  U hebt er recht op dat uw persoonsgegevens zonder onredelijke vertraging worden verwijderd als u daarom vraagt.
- Beperking van het gebruik van uw gegevens.
  In sommige situaties hebt u er recht op dat de verwerking van uw persoonsgegevens, inclusief de verwijdering, tijdelijk wordt gestaakt of uitgesteld.
- bezwaar tegen de gegevensverwerking;
  Als de verwerking van uw persoonsgegevens plaatsvindt op grond van een taak van algemeen belang, hebt u er recht op om, indien er specifiek op uw situatie ziende redenen daarvoor zijn, bezwaar te maken tegen de verwerking van uw persoonsgegevens.

Er kunnen echter redenen zijn waarom uw verzoek niet kan worden ingewilligd. Als dat het geval is, dan legt de Kiesraad dit aan u uit.

7. Hoe kan ik mijn rechten uitoefenen?
U kunt uw rechten uitoefenen door een verzoek, vergezeld van een kopie van uw rijbewijs, paspoort of identiteitskaart aan de Kiesraad te sturen. Dit kan per post: Kiesraad, t.a.v. Behandelaar AVG-verzoek, Postbus 20011, 2500 EA Den Haag. U kunt uw verzoek ook per e-mail aan ons sturen: kiesraad@kiesraad.nl. De Kiesraad beslist binnen een maand op uw verzoek.

8. Waar kan ik terecht met vragen of klachten?

Commented [s17e]: Ik vind dit punt veel categorischer geformuleerd dan de andere. Komt ook denk ik omdat je hier een grond mist van het verzoek. Kan het wellicht gecombineerd worden met het voorafgaande punt?

Commented [A18e]: Nee, want het is een zelfstandig recht.

Commented [s19e]: Dus iemand zou bezwaar kunnen maken tegen verwijdering van zijn gegevens…?

Commented [s20e]: Jazeker, daar kan iemand belang bij hebben. M.n. bij juridische procedures.

Commented [s21e]: Erg cryptisch… maar los daarvan: is dat ook bij ons mogelijk aan de orde? Als dat niet zo is, hoeven we het ook niet te noemen, zou ik denken.

Commented [s22e]: Ja, speelt ook bij de Kiesraad.

Als u vragen hebt over de bescherming van uw persoonsgegevens, dan kunt u hierover contact opnemen met het secretariaat van de Kiesraad. Dit kan telefonisch (070 426 62 66) of per e-mail (kiesraad@kiesraad.nl).

Hebt u een klacht over de wijze waarop wij uw persoonsgegevens werken of u hierover informeren? U kunt een klacht indienen bij de Autoriteit Persoonsgegevens. Kijk voor meer informatie op de website van de Autoriteit Persoonsgegevens of bel: 088 - 1805 250.

Kandidaatstellingsprocedure

Dit is de privacyverklaring van de Kiesraad over de kandidaatstellingsprocedure. Deze privacyverklaring is een aanvulling op de algemene privacyverklaring van de Raad.

Doel:
De Kiesraad is in de Kieswet aangewezen als centraal stembureau bij Tweede Kamerverkiezingen, Eerste Kamerverkiezingen en Europees Parlementsverkiezingen. In deze hoedanigheid ontvangt de Kiesraad kandidatenlijsten en neemt een besluit over de geldigheid van ingediende kandidatenlijsten en de handhaafbaarheid van daarop voorkomende kandidaten.

Grondslag:
De Kiesraad verwerkt deze persoonsgegevens op basis van een wettelijke grondslag; met name de hoofdstukken H en I van de Kieswet.

Categorieën persoonsgegevens:
Voor het bovengenoemde doel gebruikt de Kiesraad de volgende categorieën persoonsgegevens.

Indiener kandidatenlijst:
Achternaam, voorletters, postadres, postcode, gemeente, handtekening, telefoonnummer, e-mailadres.

Vervanger(s) voor herstel verzuimen:
Achternaam, voorletters, postadres, postcode, gemeente.

Kandidaten:
Achternaam, voorletters, geboortedatum, -plaats, postadres, postcode, gemeente, roepnaam, sekse, burgerservicenummer, handtekening, kopie identiteitsdocument.

Kandidaten bij Europees Parlementsverkiezing:
Zie onder 'kandidaten'. Daarnaast ook: eerste officiële voornaam.

Kandidaten bij Europees Parlementsverkiezing die niet beschikken over de Nederlandse nationaliteit:
Zie onder 'kandidaten'. Daarnaast ook: eerste officiële voornaam, nationaliteit, laatste adres en woonplaats in EU-lidstaat van herkomst.

Gemachtigden door kandidaten aangewezen:
Achternaam, voorletters, postadres, postcode, gemeente.

Gemachtigden van politieke groeperingen:
Achternaam, voorletters, handtekening.

Personen die een ondersteuningsverklaring hebben afgelegd:
Achternaam, voorletters, gemeente, kieskring, handtekening.

Bewijs van betaling waarborgsom (betaler):
Achternaam, voorletters, IBAN-rekeningnummer, gemeente.

Bewijs van betaling waarborgsom (behandelend ambtenaar):
Achternaam, voorletters, naam werkgever, handtekening.

Indiener van een bezwaar:

Achternaam, roepnaam, sekse, woonplaats.

Ontvangers:
Ten behoeve van een transparant en controleerbaar verkiezingsproces schrijft de Kieswet voor dat de ingediende formulieren met kandidatenlijsten en, indien van toepassing, ondersteuningsverklaringen voor een ieder ter inzage liggen bij het centraal stembureau. Van de formulieren met kandidatenlijsten wordt ook een kopie aan de hoofdstembureaus verstrekt, opdat ook zij kunnen voldoen aan de hen door de Kieswet opgelegde verplichting om de formulieren met kandidatenlijsten voor een ieder ter inzage te leggen. De onherroepelijk geldig verklaarde kandidatenlijsten worden in de Staatscourant gepubliceerd. De Kiesraad maakt daarbij gebruik van de diensten van KOOP.

Doorgifte aan derde landen en internationale organisaties:
Bij Europees Parlementsverkiezingen kan de Kiesraad informatie uitwisselen met verkiezingsautoriteiten in andere EU-lidstaten. Als EU-burgers uit een andere lidstaat in Nederland kandidaat willen staan, moeten zij op grond van in de Kieswet geïmplementeerde Europese regelgeving op een formulier verklaren in hun EU-lidstaat van herkomst niet uit het kiesrecht te zijn ontzet. Dit formulier wordt, ter verificatie, met de EU-lidstaat van herkomst gedeeld. Andersom verstrekt de Kiesraad aan verkiezingsautoriteiten in andere EU-lidstaten op verzoek ook informatie over de kiesgerechtigdheid van Nederlanders die zich in een andere EU-lidstaat kandidaat hebben gesteld voor de Europees Parlementsverkiezing. Informatie over Nederlanders die zich in Nederland kandidaat hebben gesteld voor de Europees Parlementsverkiezing wordt niet met derde landen gedeeld.

Geautomatiseerde besluitvorming:
Er vindt geen geautomatiseerde besluitvorming plaats.

Bewaartermijn:
De Kiesraad bewaart ingediende kandidatenlijsten en bijbehorende verkiezingsbescheiden tot na de vaststelling van de verkiezingsuitslag. Daarna worden deze documenten, vernietigd. Er geldt een uitzondering voor instemmingsverklaringen. Deze blijven tijdens de zittingsperiode van het orgaan waarvoor de verkiezing plaatsvond bewaard, en worden daarna vernietigd.

Registratie van aanduidingen, logo's en gemachtigden van politieke partijen

Dit is de privacyverklaring van de Kiesraad over de registratie van aanduidingen, logo's en (plaatsvervangend) gemachtigden van politieke partijen. Deze privacyverklaring is een aanvulling op de algemene privacyverklaring van de Raad.

Doel:
De Kiesraad verwerkt persoonsgegevens bij het nemen van een besluit over een verzoek tot registratie, of een verzoek tot wijziging, van een aanduiding, logo of gemachtigde van een politieke groepering ten behoeve van Tweede Kamerverkiezingen, Eerste Kamerverkiezingen en Europees Parlementsverkiezingen. De Raad gaat na of het verzoek is ingediend door degene(n) die bevoegd is/zijn om de politieke partij te vertegenwoordigen. Ook wordt vastgelegd wie (plaatsvervangend) gemachtigd is om, namens de politieke partij, toestemming te verlenen de geregistreerde aanduiding boven een kandidatenlijst te plaatsen. In situaties waarin geregistreerde aanduidingen voor doorwerking in aanmerking komen, maakt de Kiesraad, naast deze aanduidingen, ook de namen, voorletters en sekse van (plaatsvervangend) gemachtigden openbaar in de Staatscourant.

Grondslag:
De Kiesraad verwerkt deze persoonsgegevens op basis van een wettelijke grondslag; de artikelen G 1 en Q 6 van de Kieswet.

Categorieën persoonsgegevens:
Voor de bovengenoemde doelen gebruikt de Kiesraad de volgende categorieën persoonsgegevens.

Van bestuurders van politieke partijen:
Achternaam, voorletters, functie binnen de vereniging, handtekening.

Van (plaatsvervangend) gemachtigden van politieke partijen:
Achternaam, voorletters, sekse, adres, postcode, woonplaats.

Ontvangers:
De Kiesraad wisselt in het kader van de registratie van aanduidingen, logo's en (plaatsvervangend) gemachtigden geen persoonsgegevens uit met anderen.
Een uitzondering hierop vormen de namen, voorletters en sekse van personen die als (plaatsvervangend) gemachtigden staan vermeld ten behoeve van aanduidingen die doorwerken naar decentrale verkiezingen op basis van de Kieswet. Zij worden in de Staatscourant gepubliceerd. De Kiesraad maakt daarbij gebruik van de diensten van KOOP.

Doorgifte aan derde landen en internationale organisaties:
De Kiesraad wisselt in het kader van de registratie van aanduidingen, logo's en (plaatsvervangend) gemachtigden geen persoonsgegevens uit met derde landen of internationale organisaties.

Geautomatiseerde besluitvorming:
Er vindt geen geautomatiseerde besluitvorming plaats.

Bewaartermijn:
De Kiesraad bewaart ingediende verzoekschrift en de daarbij overgelegde documenten totdat een aanduiding onherroepelijk uit het register van aanduidingen is geschrapt. Een verklaring waarin een (plaatsvervangend) gemachtigde wordt aangewezen wordt vernietigd zodra deze is vervangen door een andere.

Vaststelling verkiezingsuitslag

Dit is de privacyverklaring van de Kiesraad over de kandidaatstellingsprocedure. Deze privacyverklaring is een aanvulling op de algemene privacyverklaring van de Raad.

Doel:
De Kiesraad is in de Kieswet aangewezen als centraal stembureau bij Tweede Kamerverkiezingen, Eerste Kamerverkiezingen en Europees Parlementsverkiezingen. In deze hoedanigheid ontvangt de Kiesraad de processen-verbaal van de hoofdstembureaus om de uitslag van de verkiezing vast te stellen. Onder dit doel wordt mede begrepen het vastleggen van bezwaren die bij de vaststelling van de verkiezingsuitslag door kiesgerechtigden zijn ingebracht en het, indien nodig, uitvoeren van een nieuwe stemopneming. Teneinde te kunnen beoordelen of een nieuwe stemopneming noodzakelijk is, ontvangt de Kiesraad ook kopieën van de processen-verbaal van stembureaus.

Grondslag:
De Kiesraad verwerkt deze persoonsgegevens in hoofdzaak op basis van een wettelijke grondslag; met name hoofdstuk P van de Kieswet. De verwerking van persoonsgegevens die voorkomen in de processen-verbaal van stembureaus vindt plaats op grond van een taak van algemeen belang.

Categorieën persoonsgegevens:
Voor de bovengenoemde doelen gebruikt de Kiesraad de volgende categorieën persoonsgegevens.

Kandidaten:
Achternaam, voorletters, roepnaam, geslacht, gemeente.

Indiener van een bezwaar:
Achternaam, roepnaam, sekse, woonplaats.

Leden van het centraal stembureau / hoofdstembureau / stembureau:
Achternaam, voorletters, handtekening.

Ontvangers:
Ten behoeve van een transparant en controleerbaar verkiezingsproces schrijft de Kieswet voor dat het proces-verbaal van het centraal stembureau, inclusief bijlagen, onverwijld op een algemeen toegankelijke wijze elektronisch openbaar wordt gemaakt. De Kiesraad doet dit door het proces-verbaal op zijn website te publiceren. Voorts wordt een kopie van het proces-verbaal toegezonden aan het vertegenwoordigend orgaan waarvoor de verkiezing plaatsvond. Bij Europees Parlementsverkiezingen wordt een kopie van het proces-verbaal toegezonden aan de Tweede Kamer. De vastgestelde verkiezingsuitslag wordt ook in de Staatscourant gepubliceerd. De Kiesraad maakt daarbij gebruik van de diensten van KOOP.

Doorgifte aan derde landen en internationale organisaties:
De Kiesraad wisselt in het kader van de vaststelling van de verkiezingsuitslag geen persoonsgegevens uit met derde landen of internationale organisaties.

Geautomatiseerde besluitvorming:
Er vindt geen geautomatiseerde besluitvorming plaats.

Bewaartermijn:
De door de Kiesraad ontvangen papieren processen-verbaal van de hoofdstembureaus en stembureaus worden bewaard tot drie maanden nadat over de toelating van de gekozenen is beslist. Het proces-verbaal van het centraal stembureau blijft online beschikbaar.

Informatie over de verwerking van uw persoonsgegevens

De Kiesraad behandelt de door hem ontvangen persoonsgegevens in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG) en gaat zorgvuldig met uw persoonsgegevens om. Uw persoonsgegevens worden niet met derden gedeeld.

Lees meer over de verwerking van uw persoonsgegevens

Waarom worden deze gegevens gevraagd?

Het symposium is alleen toegankelijk voor personen die zich hiervoor hebben aangemeld.

Op welke manier worden uw gegevens verwerkt?

Om uw aanmelding voor het symposium te kunnen verwerken, heeft de Kiesraad uw voor- en achternaam nodig en uw e-mailadres. Wij gebruiken uw e-mailadres alleen om u te kunnen informeren als er een wijziging in het programma optreedt of als het symposium onverhoopt niet doorgaat.

Hoe lang bewaren wij uw gegevens?

De Kiesraad vernietigt de persoonsgegevens die hem zijn verstrekt ten behoeve van deelname aan het symposium binnen een week nadat het symposium heeft plaatsgevonden.

Wat zijn uw rechten?

Voor meer informatie over uw rechten met betrekking tot de verwerking van persoonsgegevens verwijzen wij u naar de over 'Privacy' op deze website. Deze opent in een nieuw tabblad.

Privacyverklaring aanmelding symposium De verkiezing van de toekomst

De Kiesraad behandelt de door hem ontvangen persoonsgegevens in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG) en gaat zorgvuldig met uw persoonsgegevens om.

Verwerkingsdoeleinden: [Art. 13 lid 1 onder c & art. 13 lid 2 onder e AVG]
Het symposium is alleen toegankelijk voor personen die zich hiervoor hebben aangemeld. Om uw aanmelding voor het symposium te kunnen verwerken, heeft de Kiesraad uw voor- en achternaam nodig. Het invullen van uw e-mailadres is optioneel. Als u uw e-mailadres meldt, dan kunnen wij u informeren als er bijvoorbeeld een wijziging in het programma optreedt of als het symposium onverhoopt niet doorgaat. Met uw aanmelding geeft u de Kiesraad toestemming voor de verwerking van deze persoonsgegevens.

Gegevensbeheerder: [Art. 13 lid 1 onder d AVG]
De gegevens die u aan de Kiesraad verstrekt bij uw aanmelding voor de conferentie worden niet met derden gedeeld.

Bewaartermijn: [Art. 13 lid 2 onder a AVG]
De Kiesraad vernietigt de persoonsgegevens die hem zijn verstrekt ten behoeve van deelname aan het symposium binnen een week nadat het symposium heeft plaatsgevonden.

Meer informatie: [Art. 13 lid 1 onder a AVG]
Mocht u meer informatie willen over de verwerking van uw persoonsgegevens, dan kunt u contact opnemen met het secretariaat van de Kiesraad.
Postadres: Postbus 20011, 2500 EA Den Haag
E-mail: kiesraad@kiesraad.nl
Tel.: 070 426 6266

Functionaris voor de Gegevensbescherming: [Art. 13 lid 1 onder b AVG]
Naam: 5.1.2e
Postadres: Postbus 20011, 2500 EA Den Haag

Klachten: [Art. 13 lid 2 onder d AVG]
Hebt u een klacht over de verwerking van uw persoonsgegevens ten behoeve van het symposium door de Kiesraad? In dat geval verzoeken wij u deze klacht eerst bij ons in te dienen. Bent u daarna ontevreden over de wijze waarop wij uw klacht hebben afgehandeld, dan kunt u een klacht indienen bij de Autoriteit Persoonsgegevens.

Commented [5.1.2e]:
De elementen genoemd in artikel 13 lid 2 onder b en c van de AVG komen in deze privacyverklaring nog niet terug. Dat is strikt genomen niet in lijn met de AVG. Het opnemen ervan leidt echter tot een ridicule tekst. Welk risico lopen wij door deze onderdelen niet te melden? Kunt u zich voorstellen dat wij ervoor kiezen om deze elementen niet op te nemen? Zo nee, welke tekstsuggestie zou u ons doen?

From: "5.1.2.e"
Sent: Tue, 30 Oct 2018 11:46:54 +0100
To: "5.1.2.e" <5.1.2.e@minbzk.nl>
Cc: "5.1.2.e" <5.1.2.e@kiesraad.nl>
Subject: 5.1.2.e voor de 5.1.2.e
Attachments: 5.1.2.e voor de Kiesraad.pdf

Geachte 5.1.2.e

Op 28 september 2018 heeft de 5.1.2.e u een brief gestuurd. Tot op heden hebben wij van u helaas nog geen reactie op deze brief ontvangen. Kunt u aangeven op welke termijn wij een reactie van u tegemoet kunnen zien? Zekerheidshalve stuur ik een kopie van de verzonden brief als bijlage bij deze e-mail mee.

Met vriendelijke groet,
5.1.2.e

5.1.2.e

KIESRAAD
Bezoekadres: Zurichtoren, Muzenstraat 85, 5.1.2.e Den Haag
Postadres:: 5.1.2.e 20011, 5.1.2.e Den Haag

T: 5.1.2.e
E: 5.1.2.e@kiesraad.nl
W: www.kiesraad.nl

KIESRAAD

Ministerie van Justitie en Veiligheid
T.a.v. Functionaris voor Gegevensbescherming
Postbus 20301
2500 EH Den Haag

KIESRAAD

Datum
28 september 2018

Ons kenmerk
2018-0000794826

Inlichtingen
5.1.2.e
T 070 426 6266
F 070 751 7078

Uw kenmerk

Blad
1 van 1

Bezoekadres
Zurichtoren, 14 etage
Muzenstraat 85
2511 WB Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

Internetadres
www.kiesraad.nl

E-mailadres
kiesraad@kiesraad.nl

Onderwerp
FG voor de Kiesraad

Geachte 5.1.2.e

Op 25 mei 2018 is de Algemene verordening gegevensbescherming van toepassing geworden, ook op de Kiesraad. Bij de implementatie van deze verordening heeft de Kiesraad mede gebruikgemaakt van de expertise die binnen het ministerie van Binnenlandse Zaken en Koninkrijksrelaties op dit terrein is opgebouwd.

Tot nog toe is er, zowel door het ministerie alsook door de Kiesraad, altijd vanuit gegaan dat de Kiesraad dezelfde Functionaris voor Gegevensbescherming (FG) heeft als het ministerie. In het verleden hebt u ons ook geadviseerd over privacygerelateerde onderwerpen, zoals de Privacy Impact Assessments voor de toenmalige Referendumapplicatie van de Kiesraad (Rapp) en de website met verkiezingsuitslagen. Afspraken daarover zijn evenwel nog niet formeel vastgelegd, hetgeen gelet op artikel 37, eerste lid, onderdeel a, van de verordening wel wenselijk is. Met deze brief wil ik u dan ook officieel vragen schriftelijk te bevestigen dat u ook voor de Kiesraad als FG wilt blijven optreden. In dat geval maak ik dienaangaande graag enkele praktische afspraken met u en zal de Kiesraad ervoor zorgdragen dat u beschikt over zijn register van verwerkingen.

In afwachting van uw reactie,

hoogachtend,

5.1.2.e

From: "5.1.2.e" <5.1.2.e@autoriteitpersoonsgegevens.nl>
Sent: Mon, 4 Feb 2019 11:49:27 +0100
To: "Postbus Kiesraad" <Kiesraad@kiesraad.nl>
Subject: Aanmelding Functionaris voor de gegevensbescherming

Geachte heer/mevrouw,

U heeft een functionaris voor de gegevensbescherming (FG) voor uw organisatie Kiesraad aangemeld. Hartelijk dank voor deze aanmelding. Het aan u toegekende FG-nummer is **FG009394**.

Meer informatie over de FG vindt u op https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming. Zoekt u aanvullende informatie? Dan kunt u hiervoor terecht bij het Nederlands Genootschap voor de Functionaris voor de Gegevensbescherming, het NGFG. Meer informatie over het NGFG vindt u op www.ngfg.nl.

Graag geven wij u nog aanvullende informatie over de positie van de FG binnen uw organisatie:

- u moet de FG genoeg middelen ter beschikking stellen om zijn taken goed te vervullen.
- u mag de FG geen instructies geven over het uitvoeren van de FG-taken; de FG voert zijn taken en verplichtingen onafhankelijk uit.
- de FG mag naast zijn FG-taken eventueel andere taken of functies vervullen, maar er mag geen sprake zijn van belangenverstrengeling.
- u bent verplicht de contactgegevens van uw FG openbaar te maken.

Met vriendelijke groet,

5.1.2.e

FG@autoriteitpersoonsgegevens.nl
autoriteitpersoonsgegevens.nl

From: "5.1.2.e" <5.1.2.e@autoriteitpersoonsgegevens.nl>
Sent: Fri, 19 Nov 2021 14:29:06 +0100
To: "5.1.2.e" <5.1.2.e@kiesraad.nl>
Subject: Uw wijziging is verwerkt!

Geachte heer/mevrouw,

Wij hebben de wijziging van uw FG aanmelding voor de organisatie **Kiesraad** verwerkt. Het aan uw melding toegekende FG-nummer blijft **FG009394**.

Meer informatie over de FG vindt u op https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming. Zoekt u aanvullende informatie? Dan kunt u hiervoor terecht bij het Nederlands Genootschap voor de Functionaris voor de Gegevensbescherming, het NGFG. Meer informatie over het NGFG vindt u op www.ngfg.nl.

Graag geven wij u nog aanvullende informatie over de positie van de FG binnen uw organisatie:

- u moet de FG genoeg middelen ter beschikking stellen om zijn taken goed te vervullen.
- u mag de FG geen instructies geven over het uitvoeren van de FG-taken; de FG voert zijn taken en verplichtingen onafhankelijk uit.
- de FG mag naast zijn FG-taken eventueel andere taken of functies vervullen, maar er mag geen sprake zijn van belangenverstrengeling.
- u bent verplicht de contactgegevens van uw FG openbaar te maken.

Met vriendelijke groet,

5.1.2.e

FG@autoriteitpersoonsgegevens.nl
T 5.1.2.e - F 5.1.2.e
Prins Clauslaan 60, 2595 AJ Den Haag
Postbus 93374, 2509 AJ Den Haag
autoriteitpersoonsgegevens.nl

Notitie

Onderwerp
Actief informatierecht

Datum
26 juni 2018

Kenmerk
2018-0000498825

Inlichtingen
5.1.2.e
T 070 426 6266
F 070 751 7078

Blad
1 van 3

Aan
Staf
Van
5.1.2.e

1. Inleiding

Artikel 12, tweede lid, van de Algemene verordening gegevensbescherming (AVG)[1] verplicht de Kiesraad de in de AVG neergelegde rechten te faciliteren. De AVG bevat twee soorten rechten: een actief informatierecht en een passief informatierecht. Deze notitie ziet uitsluitend op het actief informatierecht. Over het passief informatierecht is al eerder een notitie in de staf besproken.[2] In deze notitie wordt besproken welke informatie verstrekt moet worden, op welke termijn en welke uitzonderingen op deze regel bestaan.

2. Actief informatierecht

De rechten die vallen onder de categorie 'actief informatierecht', komen ieder natuurlijk persoon van wie de Kiesraad persoonsgegevens verwerkt van rechtswege toe. Van de Kiesraad wordt verwacht dat hij uit eigen beweging, dus proactief, deze rechten faciliteert.

De inhoud

Het actief informatierecht is neergelegd in de artikelen 13 en 14 van de AVG. Artikel 13 ziet op de situatie waarin de Kiesraad de te verwerken persoonsgegevens direct van de betrokkene heeft verkregen. Artikel 14 ziet op de situatie waarin de Kiesraad persoonsgegevens indirect, dus van een derde, heeft verkregen. Hierna volgt een tabel met daarin de informatie die de Kiesraad moet verstrekken om, in beide gevallen, aan de actief informatierecht uit de AVG te voldoen.

---

[1] 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).
[2] Notitie d.d. 31 mei 2018 over 'Werkprocedure AVG-rechten', kenmerk: 2018-0000325158.

Te verstrekken informatie	Art. 13 AVG Direct verkregen	Art. 14 AVG Indirect verkregen
Identiteit en contactgegevens van de verwerkingsverantwoordelijke (= Kiesraad)	√	√
Contactgegevens functionaris voor gegevensbescherming	√	√
Verwerkingsdoeleinden & Rechtsgrond verwerking	√	√
Categorieën van persoonsgegevens die verwerkt worden.		√
Uitleg over de 'gerechtvaardigde belangen' bij verwerking	√	√
De ontvangers of categorieën van ontvangers van persoonsgegevens.	√	√
Voornemen doorgifte persoonsgegevens aan derde landen of internationale organisaties.	√	√
Bewaartermijn. Anders: criteria ter bepaling van deze termijn.	√	√
Rechten van betrokkenen. Verzoek om: inzage, rectificatie, wissing, beperking verwerking.	√	√
Mogelijkheid tot intrekking toestemming voor verwerking.	√	√
Recht klacht indienen bij Autoriteit Persoonsgegevens	√	√
Bron van persoonsgegevens.		√
Bestaan van wettelijke/contractuele verplichting tot verstrekking persoonsgegevens. Gevolgen …	√	
Geautomatiseerde besluitvorming: profilering, onderliggende logica, belang & verwachtte gevolgen.	√	√

Legenda:

	= Deze eis is niet altijd van toepassing.
	= Deze eis is altijd van toepassing.
√	= Deze eis is van toepassing.

De termijn
Als de Kiesraad de persoonsgegevens die hij verwerkt direct van de betrokkene verkrijgt, moet de bovenvermelde informatie direct bij de verkrijging van de persoonsgegevens worden verstrekt.

Als de Kiesraad de persoonsgegevens die hij verwerkt niet direct van de betrokkene heeft gekregen, maar van een derde, dan moet hij degene wiens persoonsgegevens verwerkt de bovenvermelde informatie binnen een redelijke termijn geven. Dat is in elk geval binnen een maand, maar ook:

- Als de ontvangen persoonsgegevens worden gebruikt voor communicatie met de betrokkene: uiterlijk bij het eerste contact.
- Als wordt overwogen de ontvangen persoonsgegevens aan een derde te verstrekken: uiterlijk het tijdstip waarop de gegevens voor het eerst worden verstrekt.

De uitzonderingen
Als de Kiesraad de persoonsgegevens die hij verwerkt direct van de betrokkene verkrijgt, geldt de actieve informatieplicht alleen niet als de betrokkene deze informatie al bezit. In dat geval hoeft de informatie niet nog een keer verstrekt te worden.

Als de Kiesraad de persoonsgegevens die hij verwerkt niet direct van de betrokkene heeft gekregen, maar van een derde, zijn er meer redenen op grond waarvan de actieve informatieplicht niet van toepassing is, namelijk:

a. als de betrokkene reeds in het bezit is van de informatie.
b. als het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen. In deze situatie moet de Kiesraad wel passende maatregelen nemen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie.
c. als de verwerking nadrukkelijk in de wet- en regelgeving is voorgeschreven.
d. als de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim.

Notitie

Onderwerp
De verantwoordelijkheidsverdeling tussen verwerkingsverantwoordelijke en verwerker(s) onder de AVG

Datum
2 maart 2018

Kenmerk
2018-0000147364

Inlichtingen
5.1.2.e
T 070 426 6266
F 070 751 7078

Aan
Staf
Van
5.1.2.e

1. Inleiding

In september 2017 heb ik een notitie[1] geschreven over de verplichtingen van de verwerkingsverantwoordelijke onder de Algemene Verordening Gegevensbescherming (AVG).[2] In de onderhavige notitie wordt één aspect nader belicht, namelijk: de verantwoordelijkheidsverdeling tussen de verwerkingsverantwoordelijke en de eventueel door hem ingeschakelde verwerkers. Meer precies wordt ingegaan op de voorwaarden waaronder een verwerkingsverantwoordelijke een verwerker mag inschakelen, de risico's die daarbij ontstaan en de manier waarop deze risico's juridisch afgedekt kunnen worden.

2. Verwerkingsverantwoordelijke versus verwerker

2.1 Definities

Verwerkingsverantwoordelijke:
Ingevolge artikel 4, onder 7, van de AVG wordt onder een verwerkingsverantwoordelijke verstaan: "Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald

[1] Notitie d.d. 22 september 2017 (kenmerk: 2017-0000469416) over de verplichtingen van een verwerkingsverantwoordelijke.
[2] 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.

wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen."

Verwerker:
Ingevolge artikel 4, onder 8, van de AVG wordt onder een verwerker verstaan: "Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt."

2.2 Het inschakelen van een verwerker

In alle situaties waarin persoonsgegevens als bedoeld in de AVG worden verwerkt, is er een verwerkingsverantwoordelijke. Deze verwerkingsverantwoordelijke draagt de (eind)verantwoordelijkheid voor de verwerking van persoonsgegevens. Als de verwerkingsverantwoordelijke wil, dan kan hij voor de verwerking andere partijen inschakelen: verwerkers. Het delegeren van (een deel van) de verwerking van persoonsgegevens aan een verwerker, verandert overigens niets aan de eindverantwoordelijkheid van de verwerkingsverantwoordelijke. De AVG bepaalt namelijk expliciet dat de verwerkingsverantwoordelijke alleen gebruik mag maken van verwerkers "die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden".[3] Die garantie moet zodanig zijn dat "de technische en organisatorische maatregelen beantwoorden aan de voorschriften van deze verordening, mede wat de beveiliging van de verwerking betreft."[4] Een verwerker moet dus niet alleen deskundig en betrouwbaar zijn, maar ook aantoonbaar de middelen hebben om een AVG-conforme verwerking te kunnen garanderen. Daartoe sluiten de verwerkingsverantwoordelijke en verwerker een contract met elkaar af. Daarover meer in paragraaf 4 van deze notitie.

3. Financiële risico's

Ook als de verwerkingsverantwoordelijke gebruikmaakt van de faciliteiten c.q. diensten van een verwerker, blijft de eerstgenoemde ervoor (eind)verantwoordelijk dat de verwerking van persoonsgegevens plaatsvindt in overeenstemming met de verordening. Met het delegeren van (een deel van) de verwerking aan een verwerker moeten er afspraken worden gemaakt die waarborgen dat de verwerking conform de AVG plaatsvindt, zowel organisatorisch als technisch. Als dat niet, of onvoldoende, gebeurt, ontstaat een reputatie risico – slechte publiciteit – en een financieel risico voor de verwerkingsverantwoordelijke. In deze paragraaf wordt nader ingegaan op twee mogelijke financiële risico's.

Schadevergoeding:
Op grond van de verordening heeft een ieder die materiële of immateriële schade heeft geleden als gevolg van een inbreuk op de Algemene Verordening Gegevensbescherming (AVG) recht op schadevergoeding.[5] De verordening laat het aan de burger om zelf te kiezen wie hij wil aanspreken: de verwerkingsverantwoordelijke of de verwerker. Hun verantwoordelijkheden verschillen echter.

---

[3] Art. 28 lid 1 AVG.
[4] § 81 Onderdeel van de toelichting bij de AVG.
[5] Art. 82 lid 1 AVG.

- Verwerker: Een verwerker is alleen aansprakelijk voor schade die door de verwerking is veroorzaakt als:
  a. bij de verwerking niet is voldaan aan de specifiek tot verwerkers gerichte verplichtingen uit de AVG; of
  b. de schade het gevolg is van handelen buiten dan wel in strijd met de rechtmatige instructies van de verwerkingsverantwoordelijke.
- Verwerkingsverantwoordelijke: De verwerkingsverantwoordelijke is en blijft altijd volledig aansprakelijk voor de schade die wordt veroorzaakt door verwerking die inbreuk maakt op de verordening. Ook als zijn rechtmatige instructies door de verwerker zijn geschonden.

Het voorgaande laat zien hoe belangrijk het is dat de verwerkingsverantwoordelijke zich er bij het sluiten van een verwerkingsovereenkomst van bewust is dat hij een taak overdraagt, maar geen verantwoordelijkheid. Weliswaar is de verwerker verantwoordelijk voor wat hij doet, maar de verwerkingsverantwoordelijke blijft eindverantwoordelijk voor de bescherming van persoonsgegevens door de verwerker en financieel aansprakelijk voor schade die bij derden kan ontstaan als gevolg van een inbreuk op de verordening. Daarom moet een verwerkingsovereenkomst duidelijke afspraken bevatten over de verwerking van persoonsgegevens. Voorts is het zo dat de verwerkingsverantwoordelijke en de verwerker beiden voor het gehele bedrag van de schade van de betrokkene aansprakelijk zijn.[6] Achteraf kan de verwerkingsverantwoordelijke wel proberen het deel van de schadevergoeding op de verwerker te verhalen dat overeenkomt met diens deel van de verantwoordelijkheid.

Administratieve geldboetes:
Financiële aansprakelijkheid speelt niet alleen wanneer een burger materiële of immateriële schade heeft geleden als gevolg van een inbreuk op de verordening. Het speelt ook als de verwerkingsverantwoordelijke een administratieve geldboete krijgt opgelegd door de Autoriteit Persoonsgegevens vanwege een schending van de verordening. Een dergelijke geldboete kan oplopen tot wel 20 miljoen euro.[7] De verwerkingsverantwoordelijke heeft er belang bij om een dergelijke boete te kunnen verhalen op de verwerker.

4. Contracten met verwerkers

Eerder in deze notitie is ingegaan op de voorwaarden waaronder een verwerkingsverantwoordelijke een verwerker mag inschakelen (§ 2) en de risico's die hij daarmee loopt (§ 3). Daarbij kwam ook al kort het contract te sprake dat de verwerkingsverantwoordelijke en de verwerker met elkaar moeten afsluiten. In deze paragraaf wordt daar dieper op ingegaan. Eerst wordt ingegaan op het type document (§ 4.1), daarna op de noodzakelijke inhoud (§ 4.2).

4.1 Twee soorten contracten

Op het Rijksportaal zijn twee soorten standaardcontracten te vinden voor het maken van afspraken tussen de verwerkingsverantwoordelijke en de verwerker. Eén

[6] Art. 82 lid 4 AVG.
[7] Art. 83 lid 5 en 6 AVG.

contract – de zogenoemde 'verwerker' afspraken' – wordt gebruikt als beide partijen privaatrechtelijk onder de Staat der Nederlanden vallen. Dit is bijvoorbeeld het geval als de Kiesraad (verwerkingsverantwoordelijke) een contract wil afsluiten met de belastingdienst (verwerker). Het andere contract – de zogenoemde 'verwerkersovereenkomst' wordt gebruikt als een orgaan dat tot de Staat der Nederlanden behoort afspraken moet maken met een orgaan dat daar niet onder valt. Dit is bijvoorbeeld het geval als de minister van Binnenlandse Zaken en Koninkrijksrelaties (verwerkingsverantwoordelijke) met de gemeente Den Haag (verwerker) afspreekt dat de gemeente kiesgerechtigde Nederlanders in het buitenland hun stembiljet per e-mail toestuurt.[8] Gemeenten zijn immers zelfstandige rechtspersonen.[9] Om te voldoen aan de AVG is het belangrijk altijd de meest recente versie van de modeldocumenten te gebruiken.

4.2 Inhoud van het contract

Een verwerkingsverantwoordelijke mag alleen gebruik maken van verwerkers die voldoende garanties bieden, met name op het gebied van deskundigheid, betrouwbaarheid en middelen, om ervoor te zorgen dat de technische en organisatorische maatregelen beantwoorden aan de vereisten die de AVG stelt ten aanzien van de verwerking van persoonsgegevens. De vraag rijst hoe de verwerkingsverantwoordelijke dat concreet moet toetsen. Dat is lastig te zeggen. Het ligt echter voor de hand dat de verwerkingsverantwoordelijke bepaalt aan welke eisen de verwerker moet voldoen en dit in het contract vastlegt. Hij is immers opdrachtgever en draagt ook de eindverantwoordelijkheid voor de verwerking. Daarnaast kan een verwerker zich aansluiten bij een goedgekeurde gedragscode of bij een goedgekeurde certificatieregeling. Een gedragscode of certificatieregeling kan worden gebruikt als een element om aan te tonen dat de verwerker aan de verplichtingen van de verwerkingsverantwoordelijke voldoet.

Het contract tussen de verwerkingsverantwoordelijke en de verwerker moet ingevolge de AVG de volgende elementen bevatten:[10]

– Het onderwerp van de verwerking: wat wordt er verwerkt?
– De duur van de verwerking: contractduur.
– Aard en doel van de verwerking.
– Het soort persoonsgegevens (gewoon / bijzonder / strafrechtelijk) en categorieën betrokkenen.
– Rechten en verplichtingen van de verwerkingsverantwoordelijke.

Het staat de verwerkingsverantwoordelijke en verwerker niet helemaal vrij om zelf de inhoud van het tussen hen geldende contract te bepalen. De verordening schrijft (kort gezegd) voor dat in het contract minimaal afgesproken moet worden dat de verwerker:

a. de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke. Dit is alleen anders als op de verwerker krachtens het nationale recht of het Europees recht een plicht

[8] Art. 5 lid 2 Tijdelijk experimentenbesluit stembiljetten en centrale stemopneming.
[9] Vgl. art. 2:1 BW.
[10] Art. 28 lid 3 AVG.

rust om persoonsgegevens te verwerken. In dat geval dient de verwerker de verwerkingsverantwoordelijk, voorafgaand aan de verwerking, in kennis te stellen van dat wettelijke voorschrift.

b. waarborgen dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe verbinden vertrouwelijkheid in acht te nemen. Het kan ook voldoende zijn als de bedoelde personen onder een passende wettelijke regeling tot vertrouwelijkheid gebonden zijn.

c. alle maatregelen nemen als bedoeld in artikel 32 van de verordening. Kortom: passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. Deze maatregelen moeten, waar passend, onder meer het volgende bevatten:
   a. Pseudonimisering en versluiting van persoonsgegevens.
   b. De mogelijkheid om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen.
   c. Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen.
   d. Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

d. geen derde verwerker inschakelt om een deel van de aan hem opgedragen verwerking te verrichten. Tenzij de procedure uit artikel 28, tweede en vierde lid, van de AVG wordt gevolgd.

e. Voor zover mogelijk bijstand verleent aan de verwerkingsverantwoordelijke bij het vervullen van diens plicht om verzoeken om uitoefening van de rechten van betrokkenen – Hoofdstuk III van de AVG – te beantwoorden. Het gaat dan onder andere om:
   – Art. 15 AVG: Recht op inzage.
   – Art. 16 AVG: Recht op rectificatie.
   – Art. 17 AVG: Recht op gegevenswissing.
   – Art. 18 AVG: Recht op beperking van de verwerking.

f. Bijstand verleent aan de verwerkingsverantwoordelijke bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 t/m 36 van de AVG. Uit dit voorschrift volgt bijvoorbeeld dat de verwerker de verwerkingsverantwoordelijke moet informeren als er een inbreuk wordt gemaakt op de bescherming van persoonsgegevens, zoals bijvoorbeeld wanneer ongeautoriseerden zich toegang verschaffen tot de persoonsgegevens.

g. Na afloop van de verwerkingsdienst alle persoonsgegevens wist of aan de verwerkingsverantwoordelijke teruggeeft en bestaande kopieën vernietigt.

h. De verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de nakoming van vorengenoemde verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke mogelijk maakt en daaraan bijdraagt.

Notitie

Onderwerp
Persoonsgegevens, categorieën van persoonsgegevens en bijzondere categorieën van persoonsgegevens.

Datum
1 juni 2018

Kenmerk
2018-0000326948

Inlichtingen
5.1.2.e
T 070 426 6266
F 070 751 7078

Aan
Staf
Van
5.1.2.e

1. Inleiding

De Algemene verordening gegevensbescherming (AVG)[1] gebruikt de termen 'persoonsgegevens', 'categorieën van persoonsgegevens' en 'bijzondere categorieën van persoonsgegevens'. In deze notitie wordt uitgelegd wat het onderscheid is tussen deze begrippen. Eerst komt het verschil tussen 'persoonsgegevens' en 'categorieën van persoonsgegevens' aan bod (§ 2), daarna het verschil tussen 'categorieën van persoonsgegevens' en 'bijzondere categorieën van persoonsgegevens' (§ 3). Tot slot wordt nog kort ingegaan op de samenstelling 'categorieën van ontvangers' (§ 4).

2. 'Persoonsgegevens' v. 'categorieën van persoonsgegevens'

In de verordening worden de begrippen 'persoonsgegevens' en 'categorieën van persoonsgegevens' ogenschijnlijk door elkaar gebruikt. Eerstgenoemde komt bijvoorbeeld voor in de artikelen 1, 2 en 3; laatstgenoemde bijvoorbeeld in de artikelen 14, 15 en 23. Is er een verschil in betekenis?

Persoonsgegevens:
De term 'persoonsgegevens' wordt in de verordening zelfstandig gebruikt, als het om de persoonsgegevens in abstracta gaat. Bijvoorbeeld in artikel 21 lid 2 van de verordening: "Wanneer persoonsgegevens ten behoeve van direct marketing worden verwerkt, heeft de betrokkene te allen tijde het recht bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens voor dergelijke marketing, met inbegrip van profilering die betrekking heeft op direct marketing." Het bezwaar van de betrokkene richt zich hier niet op één persoonsgegeven in het bijzonder, maar op

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

de verwerking van zijn persoonsgegevens in zijn algemeenheid. Om het even welke persoonsgegevens voor direct marketing worden gebruikt – naam, adres, e-mailadres of telefoonnummer – de betrokkene wil het niet meer en maakt daar bezwaar tegen.

Categorieën van persoonsgegevens:
De term 'categorieën van persoonsgegevens' wordt in de verordening gebruikt als het om concrete persoonsgegevens gaat. Zo bepaalt artikel 14, eerste lid, onder d, van de verordening dat een organisatie die via een derde persoonsgegevens heeft gekregen van de betrokkene, de betrokkene moet informeren over de betrokken categorieën van persoonsgegevens. Het is dan niet voldoende dat de ontvanger meldt persoonsgegevens te hebben ontvangen. Er moet concreet gemeld worden welke persoonsgegevens zijn ontvangen. Voorbeelden van categorieën van persoonsgegevens zijn: achternaam, straat en huisnummer, telefoonnummer.

Bij de term 'categorieën van persoonsgegevens' gaat het dus – anders dan de naam doet vermoeden – niet om groepen persoonsgegevens.

3. 'categorieën van persoonsgegevens' v. 'bijzondere categorieën van persoonsgegevens'

Uit de in de vorige paragraaf gegeven uitleg volgt dat de term 'categorieën van persoonsgegevens' gelezen mag worden als 'persoonsgegevens'; een term waarvoor de verordening ook een definitie geeft. Daarnaast komt in de verordening ook de term 'bijzondere categorieën van persoonsgegevens' voor. Bijvoorbeeld in de artikelen 6, 9 en 22 van de verordening. Dit zijn de gegevens die in Nederland voorheen als 'bijzondere persoonsgegevens' werden aangeduid.

Persoonsgegevens:
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.[2]

Bijzondere categorieën van persoonsgegevens:[3]
Gevoelige gegevens, zoals iemands: ras, godsdienst, politieke opvatting en lidmaatschap van een vakbond. Nieuw onder de AVG is dat ook genetische gegevens – DNA[4] – en biometrische gegevens – vingerafdruk, stem, handschrift, geometrie van de handomtrek, scans van netvlies, iris en gelaat[5] – als bijzondere persoonsgegevens worden aangemerkt. Pasfoto's zijn in het verleden ook aangemerkt als bijzonder persoonsgegeven, maar zijn dit onder de AVG meestal niet meer.[6]

---

[2] Art. 4 onder 1 AVG.
[3] Art. 13 AVG.
[4] Zie voor een definitie van 'genetische gegevens' art. 4 onder 13 AVG.
[5] Zie voor een definitie van 'biometrische gegevens' art. 4 onder 14 AVG.
[6] Zie overweging 51 van de AVG. De verwerking van foto's is alleen te beschouwen als een verwerking van een bijzonder persoonsgegeven als zij – m.b.t. van daaruit af te leiden biometrische gegevens –

4. Categorieën van ontvangers?

Het woord ‘categorie’ komt in de verordening ook in andere samenstellingen voor. Bijvoorbeeld in artikel 15, eerste lid, onder e, waar gesproken wordt over ‘ontvangers of categorieën van ontvangers’. In deze samenstelling heeft het woord ‘categorie’ wel zijn gebruikelijke betekenis. Een organisatie die persoonsgegevens met alle gemeenten deelt, kan met deze algemene melding volstaan en hoeft niet alle gemeenten in Nederland bij naam te noemen.

---

worden verwerkt om met behulp van technische middelen de unieke identificatie of authenticatie van een natuurlijk persoon mogelijk te maken.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

NOTA ACTIEF OPENBAAR
Nee

Onze referentie
2025

Datum
24-06-2025

Opgesteld door
5.1.2.e

Bijlage(n)
2

Kopie voor
postbusFG@minbzk.nl

Aan Kiesraad
Directeur IT en Uitvoering

Van FG office BZK en VRO

nota

FG-advies inzake DPIA Klantcontact (binnenkomende vragen beantwoorden) versie 1.0

Inleiding

De Algemene verordening gegevensbescherming (AVG) stelt dat de verwerkingsverantwoordelijke[1], wanneer een verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, vóórdat de verwerking start, een Data Protection Impact Assessment (DPIA) uitvoert.[2]

Daarnaast stelt het Rijksbrede privacybeleid dat voor alle verwerkingen van persoonsgegevens (projecten, beleid en regelgeving) met een hoog risico voor de rechten en vrijheden van betrokkenen een DPIA moet worden uitgevoerd.[3]

De Functionaris voor Gegevensbescherming (FG) ondersteunt de verwerkingsverantwoordelijke door een nader advies te geven op de DPIA. Het inwinnen van dit advies is een verplichting voor de verwerkingsverantwoordelijke.[4]

Onderstaand advies heeft betrekking op de DPIA Klantcontact (binnenkomende vragen beantwoorden) versie 1.0 d.d. 13 februari 2024, ontvangen op 24 februari 2025.

[1] De verwerkingsverantwoordelijke is verantwoordelijk voor het uitvoeren van een DPIA. Formeel is de betreffende minister de verwerkingsverantwoordelijke voor gegevensverwerkingen door een onderdeel van de rijksdienst (bestuursorgaan). In de praktijk zal de bevoegdheid om te beslissen of en op welke wijze persoonsgegevens worden verwerkt zijn gemandateerd, bijvoorbeeld aan een directeur-generaal of een directeur van een (beleids-)directie of dienstonderdeel.
[2] Zie artikel 35, lid 1 AVG. Rijksbreed wordt nu de term DPIA gebruikt in plaats van de termen Privacy Impact Assessment (PIA) en Gegevensbeschermingseffectbeoordeling (GEB).
[3] Data Protection Impact Assessment | Kenniscentrum voor beleid en regelgeving (kcbr.nl)
[4] Zie artikel 35, lid 2 AVG en artikel 39, lid 1c AVG.

Uitgangspunten advies FG

Bij deze review is uitgegaan van een risicogerichte benadering, de privacybeginselen volgens de AVG en een zo laag mogelijk privacyrisico voor betrokkenen. Dat wil zeggen dat de opzet, inrichting en het gebruik van de persoonsgegevens een zo laag mogelijke impact op de persoonlijke levenssfeer van de betrokkenen hebben. Ook is gekeken naar de bestuurlijke- en politieke risico's die een eventueel onrechtmatige verwerking met zich meebrengen.

In bijlage 1 is Europese en nationale wetgeving vermeld welke betrekking heeft op de bescherming van persoonsgegevens.

In bijlage 2 heeft de functionaris voor gegevensbescherming de belangrijkste uitgangspunten van deze review vermeld.

Werkwijze FG

De FG geeft, op basis van het *model gegevensbeschermingseffect-beoordeling Rijksdienst*, advies op de DPIA Klantcontact (binnenkomende vragen beantwoorden) versie 1.0. Toetsing vindt altijd plaats op alle elementen van de DPIA.[5]

De FG adviseert de (gedelegeerd) verwerkingsverantwoordelijke onderstaande adviezen over te nemen en invulling te geven aan de opmerkingen.

Indien de voorgestelde adviezen niet worden overgenomen of opmerkingen geen invulling krijgen dan moet in de definitieve versie van de DPIA beargumenteerd en duidelijk naar voren komen waarom deze adviezen niet zijn overgenomen of opmerkingen invulling hebben gekregen (*'comply or explain'*).

De FG ontvangt ter kennisgeving graag de door u vastgestelde DPIA en een afschrift van het besluit dat u mede op basis daarvan heeft genomen.

Het advies van de FG is het definitieve advies op de DPIA.

[5] Zie Data Protection Impact Assessment | Kenniscentrum voor beleid en regelgeving

Advies FG[6]

De FG heeft geen (inhoudelijke) opmerkingen bij de DPIA en adviseert het voorstel uit te voeren zoals beschreven in de DPIA.

Algemeen

De FG merkt in algemene zin op dat de DPIA goed leesbaar is en inzicht geeft in de verschillende afwegingen die zijn gemaakt om tot de voorgelegde (sub)verwerking(en) te komen.

Een DPIA is een 'levend' proces dat helpt de risico's van de verwerking en de genomen maatregelen voortdurend te beheren en te herzien. Het is noodzakelijk deze aan te passen bij significante wijzigingen in de verwerkingen van persoonsgegevens, zoals het implementeren van webformulieren op de website van de Kiesraad en de persoonsgegevens via een Application Programming Interface (API) uitwisselen met TOPdesk.

De FG adviseert om, conform verplichting in de AVG, de voorgenomen verwerking op te nemen in het BZK verwerkingenregister.[7]

[6] Advies is conform werkwijze Raad van State: Werkwijze - Raad van State.

[7] Zie artikel 30 AVG.

bijlage

De belangrijkste regels voor het verwerken van persoonsgegevens in Nederland zijn vastgelegd in de AVG. Naast de AVG draagt diverse andere Europese regelgeving bij aan de bescherming van persoonsgegevens.

- Artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM):

  Op grond van dit artikel is geen inmenging van enig openbaar gezag toegestaan in de uitoefening van het recht op respect voor zijn privéleven, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

- Artikel 8 van het Handvest van de grondrechten van de Europese Unie (Handvest):

  Dit artikel bepaalt onder meer dat persoonsgegevens eerlijk en voor bepaalde doeleinden moeten worden verwerkt, en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet.

- Artikel 16 van het Verdrag betreffende de werking van de Europese Unie (VWEU):

  Dit artikel bepaalt dat eenieder in de Europese Unie recht heeft op bescherming van zijn persoonsgegevens.

- Artikel 10, lid 1 Grondwet:

  Dit artikel bepaalt dat eenieder recht heeft op eerbiediging van zijn persoonlijke levenssfeer, behoudens bij of krachtens de wet te stellen beperkingen.

bijlage

De belangrijkste uitgangspunten waaraan de DPIA moet voldoen zijn in hoeverre:

- Het nut en de noodzaak van de (voorgenomen) verwerking voldoende aantoonbaar aanwezig is;
- De gehele keten voldoende op privacy risico's bekeken is;
- De verantwoordelijkheden en rollen van de verschillende stakeholders duidelijk en inzichtelijk beschreven zijn (*verwerkingsverantwoordelijke, (sub)verwerker, verstrekker* en *ontvanger)*;
- De persoonsgegevens verwerkt worden op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (*„rechtmatigheid*, *behoorlijkheid* en *transparantie"*);
- De persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt (*„doelbinding"*);
- De *proportionaliteit*- en *subsidiariteitsbeginselen* toegepast zijn en aantoonbaar zijn;
- De persoonsgegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (*„minimale gegevensverwerking"*);
- De opzet en inrichting er voor zorgt dat de juistheid van de gegevens gewaarborgd is (*„juistheid"*);
- De persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is (*„opslagbeperking"*);
- De risico's van de gegevensverwerking (zowel voor gegevensuitwisseling, opslag en het gebruik ervan) voor de rechten en vrijheden van de betrokkenen inzichtelijk en aantoonbaar en onderbouwd zijn;
- Door het nemen van passende technische of organisatorische maatregelen de persoonsgegevens op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (*„integriteit en vertrouwelijkheid"*);
- De principes van *privacy-by-design* en *privacy-by-default* voldoende gehanteerd worden;
- Een veilige en betrouwbare gegevensuitwisseling, opslag en verwerking in lijn is met wet- en regelgeving en relevante standaarden zoals de Code voor Informatiebeveiliging (ISO 27001/2) en de Baseline Informatiebeveiliging Overheid (BIO);
- Opslagbeperking ten aanzien van *bewaartermijnen* dan wel dataminimalisatie aantoonbaar toegepast is;

Let wel, voorgaande uitgangspunten zijn slechts enkele uitgangspunten voor het beoordelen van de DPIA en dient niet als een afvinklijst gehanteerd te worden maar geeft een illustratie waaraan een kwalitatief goed uitgevoerde DPIA moet voldoen.

Naast voorgaande uitgangspunten wordt ook het proces van het tot stand komen van de DPIA beoordeeld. Aspecten die hierbij een rol spelen zijn onder andere: door wie is het proces begeleid, is er voldoende expertise betrokken bij de totstandkoming van de DPIA, op welk moment in het proces is de DPIA uitgevoerd?

Kiesraad

DPIA

Van 5.1.2.e
Aan 5.1.2.e 5.1.2.e

Datum
13 februari 2024

Onderwerp DPIA Klantcontact (binnenkomende vragen beantwoorden)

Vaststelling
Verwerkingsverantwoordelijke:
Naam: 5.1.2.e 5.1.2.e

Advies functionaris gegevensbescherming:
Naam: 5.1.2.e functionaris gegevensbescherming BZK

Versie: 1.0
Status: Definitief

Revisie:

Versie	Datum	Toelichting
Versie 0.1	24-1-2024	Concept omschrijving voorstel, persoonsgegevens en gegevensverwerkingen.
Versie 0.2	2-2-2024	Verwerking feedback en eerste aanzet verwerkingsdoeleinden en betrokken partijen.
Versie 0.7	7-2-2024	Workshop met stakeholders
Versie 0.8	12-2-2024	Feedbackronde
Versie 0.9	12-2-2024	Concept definitief ter review door CISO
Versie 1.0	13-2-2024	Feedback verwerkt tot definitieve versie

Rapportagemodel DPIA Rijksdienst
Versie 3.0

Contact Ministerie van BZK, directie CIO-Rijk
PAR-team: 5.1.2.i @minbzk.nl
Datum 25 juli 2023
Status Definitief

Inhoudsopgave

Inleiding

Dit is het rapportagemodel van het Rijksmodel DPIA. Een DPIA wordt uitgevoerd door de 17 paragrafen in de navolgende pagina's zo helder en nauwkeurig mogelijk in te vullen en te beschrijven.

Dit rapportagemodel staat niet op zichzelf. Het is aan te raden om het Rijksmodel DPIA (delen I tot en met III) bij de hand te houden bij het schrijven van een DPIA. Met name deel III, de toelichting, is van belang bij het schrijven van de DPIA. Hierin wordt per paragraaf beschreven wat wordt verwacht qua invulling van desbetreffende onderdeel. Ook worden definities uitgebreid uitgelegd en worden handige voorbeelden gegeven.

Het Rijksmodel DPIA is hier te vinden.

Binnen de Kiesraad verzorgt het informatiepunt (IP) het aannemen en afhandelen van vragen van burgers, overheidspartijen en politieke groeperingen/partijen rondom de kieswet, (lopende) verkiezingen en alles dat hiermee te maken heeft.

Er wordt een servicemanagement tool gebruikt ter ondersteuning van dit proces. Tot op heden was de gebruikte tool 'Filemaker Pro (FMP)' maar deze DPIA is met name geïnitieerd vanwege het plan om een nieuwe tool in te zetten. De beoogde tool is TOPdesk in de Cloud (ofwel SaaS) variant.

In deze situatie is een DPIA verplicht omdat er wordt voldaan aan twee criteria[1]:

1. *Wanneer er gebruik gemaakt wordt van een publieke cloudvoorziening (in specifieke omstandigheden);*
2. *Bij gegevensverwerkingen van persoonsgegevens die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.*

In deze situatie wordt er een cloudoplossing ingezet en er worden persoonsgegevens verwerkt van gevoelige aard en waar de politieke opvatting uit blijkt. Dit laatste behoort qua gegevens tot de categorie 'bijzondere persoonsgegevens'[2] en betekent een verhoogd risico voor de rechten en vrijheden van de betrokken; dit laatste onderschrijft de verplichting tot een DPIA nog verder. Ter bevestiging is een pre-scan DPIA[3] ingevuld en die geeft als conclusie ook dat een DPIA noodzakelijk is.

Deze DPIA is opgesteld met ondersteuning van verschillende stakeholders binnen de Kiesraad. De scope van de DPIA betreft de verwerkingen 'Binnenkomende vragen afhandelen' door het informatiepunt en de sub-verwerkingen daarbij. Hierbij wordt uitgegaan van de SOL-situatie waarbij de TOPdesk SaaS-oplossing wordt gebruikt.

---

[1] Model DPIA Rijksdienst BZK v3.0, paragraaf 1.1
[2] AVG, artikel 9
[3] Pre-scan DPIA | CIP-overheid

Managementsamenvatting

Voeg hier de managementsamenvatting toe na afronding rapportagemodel. De managementsamenvatting dient de belangrijkste punten te omvatten van de DPIA-rapportage, met name de geïdentificeerde risico's en (voorgenomen) maatregelen om de risico's te mitigeren]

Binnen de Kiesraad verzorgt het informatiepunt (IP) het aannemen en afhandelen van vragen van burgers, overheidspartijen en politieke groeperingen/partijen rondom de kieswet, (lopende) verkiezingen en alles dat hiermee te maken heeft.

Het IP wil de servicemanagement tool TOPdesk inzetten om de afhandeling van deze vragen te ondersteunen. Omdat de beoogde tool een publieke cloudtool is en er gevoelige informatie en bijzondere persoonsgegevens worden verwerkt binnen het IP is deze Data Privacy Impact Assessment (DPIA) uitgevoerd.

De scope van de verwerking van persoonsgegevens in dit kader omvat die persoonsgegevens die nodig zijn om de vragen die binnenkomen te kunnen afhandelen. Dat betekent concreet: het formuleren van (juridische) antwoorden op die vragen, communiceren met de vragensteller via mail of telefoon en het binnen de Kiesraad routeren van meldingen tussen het IP en de Backoffice.

Het is in veel gevallen niet nodig om veel persoonsgegevens te verwerken. Wat deze situatie daarom uitdagend maakt is dat er aan de ene kant – ongevraagd - overbodige persoonsgegevens worden geleverd door de vragenstellers en aan de andere kant, dat informatie is af te leiden uit andere informatie die is meegeleverd. Dit is zo omdat deze informatie onlosmakelijk verbonden is met de soort vragen die gesteld worden of de personen die de vragen stellen. Het is geen doel van de Kiesraad om deze informatie te verwerken; dit moet worden gezien als 'bijvangst'. De Kiesraad doet niets met deze informatie. Het is niet te voorkomen dat dit gebeurt, omdat anders het IP het werk niet goed kan uitvoeren.

Er is in januari 2024 een aparte risicoanalyse uitgevoerd waar ook dit proces in scope was. Het gros van de risico's met een hoge score waren gerelateerd aan het verkrijgen van toegang door onbevoegden tot de verzamelde informatie of het lekken van die informatie. Het tot uiting komen van die risico's zou potentieel impact hebben op de rechten en vrijheden van de betrokken, omdat daarbij ook (gevoelige) persoonsgegevens voor onbevoegden beschikbaar zouden kunnen raken.
In diezelfde risicoanalyse is ook nagedacht over mitigerende maatregelen. Er zijn voldoende maatregelen bedacht die de kans op het tot uiting komen van die risico's tot een aanvaardbaar niveau kunnen terugbrengen. Belangrijke maatregelen hierbij hebben tot doel het zo veel mogelijk minimaliseren van de informatie die verwerkt wordt. Voorbeelden zijn het inrichten van pseudonimisering en het verwijderen van de gevoelige informatie. Relevant in dit kader is dat hoewel TOPdesk een cloudtool is, deze ook hulp biedt bij deze zaken omdat deze tool functionaliteiten biedt om dit soort zaken te automatiseren.

Alles in overweging nemende kan worden geconcludeerd dat de Kiesraad er niet aan ontkomt om (een klein deel) gevoelige en bijzondere persoonsgegevens te verwerken om haar taak goed uit te kunnen voeren. De Kiesraad stelt hierbij alles in het werk om de risico's tot een aanvaardbaar niveau terug te brengen en de privacybelangen van de betrokkenen te waarborgen.

Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de DPIA: een overzicht van alle relevante feiten van de voorgenomen gegevensverwerkingen. Essentieel is dat de feiten helder en volledig zijn, want het resterende deel van de DPIA is gebaseerd op wat in dit onderdeel is beschreven.

1 Voorstel

Beschrijf het voorstel waar de DPIA op toeziet op hoofdlijnen en benoem hoe het voorstel tot stand is gekomen en wat de beweegredenen zijn achter de totstandkoming van het voorstel.

Aanleiding | *Binnen de Kiesraad bestaat het Informatiepunt (IP) dat verantwoordelijk is voor het proces 'binnenkomende vragen beantwoorden'. Het informatiepunt is een loket waar burgers, politieke- groeperingen/partijen en overheidsinstanties (met name gemeentes) telefonisch of per mail vragen kunnen stellen over de kieswet, (lopende) verkiezingen en alles dat daarmee te maken heeft.*

Er worden binnen het IP twee 'soorten' vragen behandeld:
1. *Reguliere vragen | Dit zijn vragen van burgers en overheidsinstellingen (voornamelijk gemeentes) over verkiezingen en/of de Kieswet. Ook gemeenteambtenaren leggen vragen bij de Kiesraad neer.*
2. *Vragen van politieke groeperingen/-partijen | Dit zijn diverse vragen. Meestal gaat het over het voorbereiden van registratie verzoeken of het maken van afspraken voor bijvoorbeeld het inleveren van kandidatenlijsten.*

Binnen de Kiesraad is er een behoefte aan een tool die kan ondersteunen bij dit werkproces. Er is hier gekozen voor de inzet van een servicemanagement tool in de vorm van een publieke Cloud-oplossing (TOPdesk). Cloud-beleid verplicht het uitvoeren van een DPIA voor bij het inzetten van publieke Cloud-oplossingen. Zeker in dit geval omdat er verwerkingen zijn van gevoelige informatie en bijzondere persoonsgegevens.

De scope van deze DPIA omvat de gegevensverwerking 'binnenkomende vragen behandelen' door het informatiepunt (IP) van de Kiesraad. Het gaat binnen dit proces om:
1. *Registreren van relevante informatie over de vraag en van de vragensteller;*
2. *Bijhouden van de voortgang van de afhandeling van de vraag;*
3. *Intern routeren van de vraag;*
4. *Kennisborging;*
5. *Integrale rapportages in het kader van de efficiëntie van de afhandeling van de vragen.*

De (sub)gegevensverwerkingen binnen dit kader zijn:
- *Verzamelen | Informatie wordt aangeleverd per mail of telefonisch verzameld.*
- *Vastleggen (opslaan) | Relevante informatie wordt vastgelegd in de servicemanagement tool. Mails worden opgeslagen in de mailbox (server).*
- *Ordenen | Informatie wordt in de overeenkomstige velden in de servicemanagementtool genoteerd.*
- *Bijwerken | later aangeleverde aanvullende informatie wordt toegevoegd indien relevant.*

- *Wijzigen | Foutieve informatie wordt gewijzigd als nodig.*
  Informatie wordt waar mogelijk gepseudonimiseerd.
- *Opvragen | Aanvullende informatie nodig voor de afhandeling wordt opgevraagd bij de vragensteller.*
- *Raadplegen | Informatie wordt geraadpleegd voor het beantwoorden van vragen of het communiceren met de vragensteller.*
  Informatie wordt geraadpleegd in de vorm van geaggregeerde rapportages.
- *Gebruiken | Relevante informatie wordt gebruikt bij het beantwoorden van vragen of de communicatie met de vragensteller.*
- *Doorzenden | Relevante informatie wordt doorgezonden naar interne collega's of afdelingen die betrokken zijn bij het beantwoorden van de vragen.*
- *Afschermen | Informatie wordt afgeschermd voor interne en externe onbevoegden.*
- *Wissen | Informatie die ouder is dan de vastgesteld bewaartermijn wordt verwijderd.*

Veel communicatie verloopt via de mailbox (informatiepunt@kiesraad.nl). Het komt voor dat de vragenstellers ongevraagd (gevoelige) informatie leveren die niet altijd nodig is voor de beantwoording; dit gaat zo ver als foto's van stempassen, legitimatiebewijzen of BSN-nummers.
De informatie die in de servicemanagement tooling wordt geregistreerd is zo veel mogelijk geschoond voordat deze daarin wordt geregistreerd. Het is wel bedoeling dat in de toekomst volledige mails in de tool geïmporteerd zullen worden (en daarmee zullen ook de bijlagen meegenomen worden). In de huidige situatie blijven de mail en bijlagen ook opgeslagen in de mailbox op de mailserver (Office365). In de toekomstige situatie zullen er maatregelen genomen worden om zowel de tooling als mailbox te schonen van die bijlagen.

Persoonsgegevens over de vragensteller worden alleen geregistreerd voor zover dit nodig is voor de communicatie of wanneer deze informatie nodig is voor de beantwoording van de vraag. In gevallen waar er vragen zijn van politieke groeperingen is voor de beantwoording wel bepaalde aanvullende (gevoelige) informatie relevant. Dit betreft voornamelijk informatie van de categorie 'politieke opvattingen' en dat is volgens de AVG informatie uit de categorie 'bijzondere informatie' waarbij er verhoogde risico's zijn voor de rechten en vrijheden van de betrokkenen. Deze informatie wordt letterlijk gedeeld met de Kiesraad of deze is indirect af te leiden uit de andere informatie die meegeleverd is. Volledige anonimiseren is niet mogelijk vanwege deze herleidbaarheid.

Er zullen rapportages over geaggregeerde data worden gecreëerd. Dit zullen rapportages zijn over de efficiëntie van de afhandeling of over totalen van soorten vragen. Rapportages gaan nooit over personen of zijn daaruit te herleiden.

***Situatie** | Het betreft een bestaande situatie. Alleen de potentiële inzet van TOPdesk (SAAS) ter ondersteuning van de registratie en routering binnen de Kiesraad is nieuw.*

***Privacy by design (PBD) en by default (PBD)** | Deze principes worden in de huidige situatie nog onvoldoende toegepast. Een van de opbrengsten van de inzet van TOPdesk bij het ondersteunen van dit proces is dat PBD en PBD beter invulling krijgen (d.m.v. bijv. encryptie, toegangsbeheer, mogelijkheden voor configuratie en uitschakelen van modules, pseudonimisering, dataminimalisatie en automatische verwijdering van data)*

***Redenen totstandkoming voorstel** | Voortschrijdende inzicht: Dit voorstel is geïnitieerd doordat de Kiesraad een nieuwe softwaretool wil gaan inzetten bij het informatiepunt. Omdat de beoogde tool een Cloud-oplossing is er en er ook bijzondere persoonsgegevens verwerkt worden is het vereist dat er kritisch naar de verwerking wordt gekeken.*

2 Persoonsgegevens

Beschrijf alle persoonsgegevens die worden verwerkt. Classificeer deze persoonsgegevens naar type: gewoon, gevoelig, bijzonder, strafrechtelijk en wettelijk identificatienummer. Geef per categorie persoonsgegevens aan welke persoonsgegevens worden verzameld en geef aan wat de bron is van deze persoonsgegevens.

Categorie betrokkenen	Categorie persoons gegevens	Persoonsgegevens	Type persoons gegeven	Bron
		Reguliere vragen burgers		
Burgers	Contactgegevens	Voornaam vragensteller	Gewoon	Vraagsteller
Burgers	Contactgegevens	Achternaam vragensteller	Gewoon	Vraagsteller
Burgers	Contactgegevens, Arbeidsinformatie	E-mail vragensteller	Gewoon	Vraagsteller
Burgers	Contactgegevens	Telefoonnummer vragensteller	Gewoon	Vraagsteller
Burgers	Demografisch, Politieke voorkeur, Identificatie-nummer Biometrisch	Informatie en bestanden (word, pdf, foto's, ...) m.b.t. de gestelde vragen over zaken gerelateerd aan de kieswet, verkiezingen of de kiesraad.	Gevoelig	Vraagsteller
Burgers	Demografisch Identificatie-nummer	Foto's van ID-bewijzen	Gevoelig	Vraagsteller
Burgers	Identificatie, Contactgegevens, Politieke voorkeur	Stempassen (met volledige naam en adres)	Gewoon, gevoelig, bijzonder	Vraagsteller
Burgers	Politieke voorkeur	Partijvoorkeur	Bijzonder	Vraagsteller
Burgers	Identificatie-nummer	BSN nummer	Wettelijk identificatie nummer	Vraagsteller
Burgers	Identificatie, Biometrisch	Stempel of scan vingerafdruk	Gevoelig	Vraagsteller
Burgers	Politieke voorkeur	Lidmaatschap PG of PP	Bijzonder	Vraagsteller
		Overheidsambtenaren (vooral gemeente)		
Overheidsamb tenaren	Arbeidsinformatie	Naam gemeente / overheidsinstelling	Gewoon	Vraagsteller
Overheidsamb tenaren	Arbeidsinformatie	Functie en rol	Gewoon	Vraagsteller
		Kiesraad medewerker		
Kiesraad-medewerker	Contactgegevens	Voornaam Kiesraadgebruiker	Gewoon	Kiesraad
Kiesraad-medewerker	Contactgegevens	Achternaam Kiesraadgebruiker	Gewoon	Kiesraad
Kiesraad-medewerker	Contactgegevens	E-mail Kiesraadgebruiker	Gewoon	Kiesraad

Kiesraad-medewerker	Contactgegevens	Telefoonnummer Kiesraadgebruiker	Gewoon	Kiesraad
Kiesraad-medewerker	Account	accountgegevens TOPdesk	Gevoelig	TOPdesk
		Vragen PG en PP		
Medewerker PG/PP	Contactgegevens	Voornaam vragensteller	Gewoon	Medewerker PG/PP
Medewerker PG/PP	Contactgegevens	Achternaam vragensteller	Gewoon	Medewerker PG/PP
Medewerker PG/PP	Contactgegevens	E-mail vragensteller	Gewoon	Medewerker PG/PP
Medewerker PG/PP	Contactgegevens	Telefoonnummer vragensteller	Gewoon	Medewerker PG/PP
Medewerker PG/PP	Contactgegevens	Naam gemeente melder	Gewoon	Medewerker PG/PP
Medewerker PG/PP	Politieke opvatting	Naam politieke partij of groepering	Bijzonder	Medewerker PG/PP
Medewerker PG/PP	Arbeidsinformatie	Rol / Functie	Gewoon	Medewerker PG/PP
Medewerker PG/PP	Politieke opvatting	Registratieverzoek[4]	Gevoelig	Medewerker PG/PP
Medewerker PG/PP	Politieke opvatting	Statuten van partijen?	Gevoelig	Medewerker PG/PP
Medewerker PG/PP	Politieke opvatting	invulformulier met adres van de partij en de namen en handtekeningen van de bestuurders van de vereniging	Gevoelig	Medewerker PG/PP
Medewerker PG/PP	Politieke opvatting, Identificatie	Handtekeningen	Gevoelig	Medewerker PG/PP
		Divers		
Kiesraad-medewerker, Burgers, gemeente ambtenaren, Medewerker PG/PP	Metadata	Metadata over de afhandeling van de vragen (tijdstippen, header info import mail (e-mail, IP-adressen, tijdstippen e.d.)	Gevoelig	TOPdesk
Kiesraad-medewerker, Burgers, gemeente ambtenaren, Medewerker PG/PP	Loggegevens	Loggegevens TOPdesk (toegang tot TOPdesk, wijzigingen, ...)	Gewoon	TOPdesk

[4] Op dit moment wordt de formele afhandeling en administratie van registratieverzoeken niet gedaan door het IP. Het IP beantwoordt wel algemene vragen over registratieverzoeken.

In de kern gaat het om de (basis)contactgegevens, maar vanwege de aard van de vragen en de betrokken personen wordt er ook gevoelige en bijzondere persoonsgegevens verwerkt binnen dit proces.
Veel van de communicatie gaat per mail en de vragenstellers leveren vaak (ongevraagd en ongewenst) informatie op die niet altijd nodig is voor de beantwoording. Dit is informatie die gevoelig van aard kan zijn (BSN of vingerafdrukken) of van de categorie 'bijzondere persoonsgegevens' zoals door de AVG bepaalt (zoals politieke voorkeur). Met informatie die niet nodig is wordt niks gedaan behalve dat deze opgeslagen is in de mailbox.

3 Gegevensverwerkingen

Geef alle gegevensverwerkingen weer en geef aan welke categorieën persoonsgegevens worden verwerkt per gegevensverwerking. Desgewenst kan een stroomschema van de gegevensverwerkingen worden toegevoegd.

Gegevens verwerking	Categorieën persoonsgegevens
Verzamelen	Accountinformatie, Arbeidsinformatie, Biometrisch, Contactgegevens, Demografisch, Identificatie, Identificatienummer, Loggegevens, Metadata, Politieke voorkeur
Vastleggen / opslaan	Accountinformatie, Arbeidsinformatie, Contactgegevens, Demografisch, Identificatie, Identificatienummer, Loggegevens, Metadata, Politieke voorkeur
Ordenen	Arbeidsinformatie, Contactgegevens, Demografisch, Politieke opvatting
Bijwerken	Accountinformatie, Arbeidsinformatie, Contactgegevens, Demografisch.
Wijzigen	Accountinformatie, Arbeidsinformatie, Contactgegevens, Demografisch.
Opvragen	Arbeidsinformatie, Contactgegevens, Demografisch, Politieke voorkeur
Raadplegen	Arbeidsinformatie, Contactgegevens, Demografisch, Loggegevens, Metadata, Politieke voorkeur
Gebruiken	Arbeidsinformatie, Contactgegevens, Demografisch, Politieke opvatting
Doorzenden	Arbeidsinformatie, Contactgegevens, Demografisch, Politieke opvatting
Afschermen	Accountinformatie, Arbeidsinformatie, Biometrisch, Contactgegevens, Demografisch, Identificatie, Identificatienummer, Loggegevens, Metadata, Politieke voorkeur
Wissen	Accountinformatie, Arbeidsinformatie, Biometrisch, Contactgegevens, Demografisch, Identificatie, Identificatienummer, Loggegevens, Metadata, Politieke voorkeur

De gegevensverwerking 'afhandelen van vragen' kent verschillende (sub)verwerkingen zoals aangegeven in de tabel. De Kiesraad gebruikt maar een klein deel van deze (opgeleverde) gegevens voor het afhandelen van vragen; de contactgegevens en de gegevens die relevant zijn voor het beantwoorden van de vragen.
Er wordt overbodige informatie meegestuurd, maar daar wordt niets mee gedaan. Uit bepaalde informatie of de context van de vraag is in bepaalde gevallen bijzondere informatie herleidbaar (politieke opvatting).

Het is niet altijd mogelijk om de gegevens die niet nodig zijn of die leiden tot herleidbare andere informatie te verwijderen omdat daarmee informatie verloren gaat die wel nodig is.

De samenhang tussen gegevensverwerkingen (ter inzicht):

4 Technieken en methoden van de gegevensverwerkingen

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem, bijvoorbeeld, of sprake is van bijvoorbeeld (semi-) geautomatiseerde besluitvorming, profilering, een cloudoplossing of big dataverwerkingen en, zo ja, beschrijf waaruit dat bestaat.

Kiesraadmedewerkers werken op de Digitale werkplek Rijk (DWR next, Citrix werkplek geleverd door SSC-ICT).
Er wordt een servicemanagement tool gebruikt ter ondersteuning van het klantcontact proces. Dit was tot op heden de tool 'filemaker pro' maar deze DPIA is met name geïnitieerd vanwege de wens om een nieuwe tool in te zetten. De beoogde tool is TOPdesk als cloudoplossing (ofwel SaaS). Binnen dit proces zijn verder relevante technische middelen: telefoon en e-mail. In de toekomst mogelijk ook webformulieren op de site van de Kiesraad.

Binnen dit proces beperkt de ondersteuning door deze tool(s) zich tot registratie en opslag van informatie en interne routering. De tool zal niet worden gebruikt voor (semi-) geautomatiseerde besluitvorming of profilering. Bij het verwerken van persoonsgegevens wordt zo veel mogelijk aan dataminimalisatie gedaan maar voor bepaalde vragen is het niet te voorkomen dat gevoelige of bijzondere persoonsgegevens verwerkt worden.
De persoonsgegevens zullen zo veel mogelijk gepseudonimiseerd worden (na afhandeling van de vragen) maar er blijft veelal nog een bepaalde mate van herleidbaarheid uit de context mogelijk.

5 Verwerkingsdoeleinden

Beschrijf de doeleinden van alle gegevensverwerkingen.
Voeg aanvullende informatie toe in het tekstveld.

Gegevensverwerking	Verwerkingsdoeleinde	Oorspronkelijk verwerkingsdoeleinde
Verzamelen	Binnenkomende vragen behandelen	n.v.t.
Vastleggen / opslaan	Binnenkomende vragen behandelen Archivering	n.v.t.
Ordenen	Binnenkomende vragen behandelen Dataminimalisatie	n.v.t.
Bijwerken	Binnenkomende vragen behandelen Aanvullen	n.v.t.
Wijzigen	Binnenkomende vragen behandelen Corrigeren	n.v.t.

Gegevensverwerking	Verwerkingsdoeleinde	Oorspronkelijk verwerkingsdoeleinde
Opvragen	Binnenkomende vragen behandelen	n.v.t.
Raadplegen	Binnenkomende vragen behandelen Rapporteren	n.v.t.
Gebruiken	Binnenkomende vragen behandelen Communiceren met de vragensteller	n.v.t.
Doorzenden	Binnenkomende vragen behandelen Tweedelijn inschakelen	n.v.t.
Afschermen	Binnenkomende vragen behandelen Waarborgen van privacy en lekken informatie	n.v.t.
Wissen	Binnenkomende vragen behandelen Waarborgen van privacy Voldoen aan wetgeving	n.v.t.

Alle verwerkingen hebben betrekking op het doeleinde 'Binnenkomende vragen behandelen'. De gegevens worden niet voor andere doeleinden gebruikt.

6 Betrokken partijen

Benoem alle partijen die betrokken zijn en deel deze in per gegevensverwerking. Deel deze partijen in onder de rollen: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker, sub-verwerker, verstrekker, ontvanger, betrokkene(n) en derde. Wanneer bekend, benoem ook welke functionarissen/afdelingen binnen deze partijen toegang krijgen tot welke categorieën persoonsgegevens. Voeg aanvullende informatie toe in het tekstveld.

Naam partij	Rol partij	Functies/ afdelingen	Persoonsgegevens
Kiesraad	Verwerkings-verantwoordelijke, ontvanger	JKA	Contactgegevens, Demografisch
Kiesraad	Verwerkings-verantwoordelijke, ontvanger	IP-medewerker	Accountinformatie, Arbeidsinformatie, Biometrisch, Contactgegevens, Demografisch, Identificatie, Identificatienummer, Loggegevens, Metadata, Politieke opvatting
Kiesraad	Verwerkings-verantwoordelijke, ontvanger	IP-coördinator	Accountinformatie, Arbeidsinformatie, Biometrisch, Contactgegevens, Demografisch, Identificatie, Identificatienummer,

Naam partij	Rol partij	Functies/ afdelingen	Persoonsgegevens
			Loggegevens, Metadata, Politieke voorkeur
Kiesraad	Verwerkings-verantwoordelijke, ontvanger	D&T - Functioneel beheerder	Accountinformatie, Contactgegevens
Kiesraad	Verwerkings-verantwoordelijke, ontvanger	Management	Rapportages
Burgers	Betrokkene	n.v.t.	Arbeidsinformatie, Biometrisch, Contactgegevens, Demografisch, Identificatie, Identificatienummer, Politieke voorkeur
Overheidsambtenaren (gemeente ambtenaren)	Betrokkene	n.v.t.	Arbeidsinformatie, Biometrisch, Contactgegevens, Demografisch, Identificatie, Identificatienummer, Politieke voorkeur
Medewerkers PG/PP	Betrokkene	n.v.t.	Contactgegevens, partijlidmaatschap
SSC-ICT	Betrokkene (DWR)	n.v.t	Geen
SSC-ICT	Verwerker (Filemaker Pro / Mail / telefonie)		Accountinformatie, Arbeidsinformatie, Biometrisch, Contactgegevens, Demografisch, Identificatie, Identificatienummer, Loggegevens, Metadata, Politieke voorkeur
TOPdesk	Verwerker	n.v.t.	Contact- en contract gegevens Kiesraadmedewerkers

De Kiesraad is de enige verwerkersverantwoordelijke.

7 Belangen bij de gegevensverwerkingen

Beschrijf alle belangen die de betrokken partijen hebben bij de gegevensverwerkingen. Vraag betrokkenen of hun vertegenwoordigers ook naar hun mening over de verwerking indien relevant. Licht deze mening toe onder het belang van de betrokkenen.

Betrokken Partij	Belangen
Kiesraad medewerkers	Efficiënt en effectief werken, traceerbaarheid (bewijsvoering)
Burgers (waaronder ook kandidaten)	Goede hulp en correcte (juridische) antwoorden op de gestelde vragen. Dat privacy niet geschonden wordt en persoonlijke informatie goed wordt beschermd.
Ambtenaren (gemeenteambtenaren)	Goede hulp en correcte (juridische) antwoorden op de gestelde vragen. Dat privacy niet geschonden wordt en persoonlijke informatie goed wordt beschermd.
Medewerker PG/PP	Goede hulp en correcte (juridische) antwoorden op de gestelde vragen. Dat privacy niet geschonden wordt en persoonlijke informatie goed wordt beschermd.
Kiesraad	Onderdeel van primaire proces en uitvoeren wettelijke taak
SSC-ICT	Uitvoeren van Contractuele verplichting
TOPdesk	Uitvoeren van Contractuele verplichting

In het kader van deze DPIA zijn de belangrijkste belangen dat de Kiesraad haar taken goed uit kan voeren en er daarbij zo min mogelijk (gevoelige) persoonsgegevens worden verwerkt ten behoeve van het waarborgen van de privacy van de betrokkenen.

---

8 Verwerkingslocaties

Benoem in welke landen de gegevensverwerkingen plaatsvinden. Beschrijf het doorgiftemechanisme dat van toepassing is wanneer verwerkingslocaties buiten de Europese Economische Ruimte bevinden en noem of en welke aanvullende maatregelen van toepassing zijn. Voeg aanvullende informatie toe in het tekstveld.

Zie deel III van het Rijksmodel DPIA voor meer informatie over de doorgiftemechanismen.

Gegevens verwerkingen	Verwerkingslocaties	Doorgifte mechanisme	Maatregelen
Alle (Filemaker Pro)	Nederland, binnen SSC-ICT datacenter in Nederland	n.v.t.	n.v.t.
Alle (TOPdesk)	Nederland, Amsterdam	n.v.t.	Bij aanvang contract wordt gekozen voor servers binnen de EER.
Opslag SSC-ICT (DWR en mail)	Nederland, binnen SSC-ICT datacenter in Nederland	n.v.t.	n.v.t.

Alle gegevensverwerkingen vinden plaats binnen de Kiesraad (grotendeels binnen het informatiepunt), op dit moment gebruik makend van de tool Filemaker pro die draait on premisse binnen de DWR-infra.
In de toekomst wordt gebruik gemaakt van een TOPdesk-oplossing in de SaaS-variant die volledig gehost wordt op Nederlandse servers en valt onder de EER (en de AVG is van toepassing).

9 Juridisch en beleidsmatig kader

Benoem alle wet- en regelgeving en beleid met mogelijke gevolgen voor de gegevensverwerkingen. De AVG en de Richtlijn[5] hoeven niet genoemd te worden. Voeg aanvullende informatie toe in het tekstveld.

Gegevensverwerkingen	Juridisch en/of beleids-matig kader	Wetsartikelen
Persoonsinformatie van individuen is in principe niet opvraagbaar volgens de WOO. Deze informatie zal eruit gehaald worden bij WOO-verzoeken.	Wet Open Overheid (WOO)	5.1.1 | Het openbaar maken van informatie ingevolge deze wet blijft achterwege voor zover dit: 5.1.1.D | persoonsgegevens betreft als bedoeld in paragraaf 3.1 onderscheidenlijk paragraaf 3.2 van de Uitvoeringswet Algemene verordening gegevensbescherming, tenzij de betrokkene uitdrukkelijk toestemming heeft gegeven voor de openbaarmaking van deze persoonsgegevens of deze persoonsgegevens kennelijk door de betrokkene openbaar zijn gemaakt;
De verwerkingen die betrekking hebben op het bewaren (opslag) van (persoons)gegevens.	Archiefwet	De archiefwet bepaalt dat er een lijst moet zijn voor selectie en waardering archiefbescheiden (de zogeheten selectielijst) ofwel welke informatie in het archief opgenomen moeten worden en onder welke voorwaarden. Hierin staan ook bewaartermijnen waaraan je gebonden bent (de Kiesraad valt onder de selectielijst BZK (1-1-2003)[6]. Pag. 29 Categorie 5, en dan vooral proces 5.1 en 5.2 > Waardering v5 ofwel vernietigen na 5 jaar.
Alle verwerkingen die betrekking hebben op de	Baseline Informatie-	Verplicht kader voor de Rijksoverheid voor informatiebeveiligingsmaatregelen. Gevolgen

[5] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

[6] Selectielijst BZK 2003

Gegevensverwerkingen	Juridisch en/of beleids-matig kader	Wetsartikelen
toegang, transport en opslag van de informatie.	beveiliging overheid (BIO	zijn niet zozeer op de verwerkingen zelf maar wel op de bescherming van de informatie die verwerkt wordt.

Uitvoeringswet AVG artikel 2, lid 2: 'In afwijking van het eerste lid, is deze wet niet van toepassing op de verwerking van persoonsgegevens voor zover daarop de Wet basisregistratie personen, de Kieswet of de Wet raadgevend referendum van toepassing is.'

Voor zover de Kieswet de Kiesraad zaken laat doen waarbij persoonsgegevens moeten worden verwerkt (denk aan kandidaatstellingsprocedure) is de AVG niet van toepassing. De werkzaamheden van het Informatiepunt vallen niet onder specifieke werkzaamheden die door de Kieswet voor worden geschreven (die volgen meer indirect of in de geest van de wet). De AVG is dus, in principe, wel van toepassing.

De Kieswet maakt verder uitzonderingen op de rechten van de betrokkenen maar niet specifiek over dat wat hier in scope is.

---

10 Bewaartermijnen

Bepaal de bewaartermijnen van de persoonsgegevens aan de hand van de gegevensverwerkingen en de verwerkingsdoeleinden. Motiveer waarom deze bewaartermijnen niet langer zijn dan strikt noodzakelijk ten opzichte van de verwerkingsdoeleinden. Beschrijf wie toeziet op de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn. Voeg aanvullende informatie toe in het tekstveld.

Gegevens-verwerking	Verwerkings-doeleinde	Categorie Persoons-gegevens	Bewaar termijn	Motivatie bewaartermijn
Afhandelen vragen burgers	Alle	Alle	5 jaar	Waardering v5 in de selectielijst BZK.
(bijzondere) Persoonsgegevens	Alle	Alle	5 jaar	Zo veel mogelijk geschoond of gepseudonimiseerd. Wat over blijft volgt dezelfde bewaartermijn als de rest van de informatie. Zie toelichting.

Er wordt zo veel mogelijk aan dataminimalisatie gedaan. Waar mogelijk worden gegevens die niet nodig zijn verwijderd en waar ze wel nodig zijn gepseudonimiseerd. Er blijf echter altijd gevoelige of bijzondere informatie achter die nodig is voor het doeleinde 'beantwoorden van vragen' of 'communiceren met de vraagsteller' of die informatie is af te leiden uit de andere informatie. Dit kan niet altijd los van elkaar worden getrokken dus voor de persoonsgegevens die 'achterblijven' geldt dezelfde bewaartermijn als voor de rest. Na de bewaartermijn dienen alle gegevens te worden vernietigd.

Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel de rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen en rechten van de betrokkene.

11 Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd. Iedere rechtsgrond moet aan bepaalde voorwaarden voldoen, voeg in de toelichting op de rechtsgrond toe hoe aan deze voorwaarden wordt voldaan. Voeg aanvullende informatie toe in het tekstveld.

De rechtsgronden zijn:

Rechtsgrond	Toelichting	Van toepassing?
Toestemming	Voor toestemming is nodig dat deze op ondubbelzinnige wijze vrij wordt gegeven voor een specifieke verwerking. Licht toe hoe hieraan wordt voldaan.	Nee
Noodzakelijk voor de uitvoering van de overeenkomst	Hier moet sprake zijn van een overeenkomst met de betrokkene, geef aan van wat voor overeenkomst sprake is	Nee
Noodzakelijk om te voldoen aan een wettelijke verplichting	Geef aan welke EU- of Nederlandse wetsbepalingen van toepassing zijn	Nee
Noodzakelijk om de vitale belangen van de betrokkene of een ander te beschermen	Hiervan kan sprake zijn wanneer iemands leven of gezondheid in gevaar is en die persoon niet in staat is om toestemming te geven	Nee
Noodzakelijk voor de vervulling van een taak van algemeen belang.	Geef aan welke EU- of Nederlandse wetsbepalingen van toepassing zijn.	**Ja**
Noodzakelijk voor de behartiging van een gerechtvaardigd belang	Deze grondslag is niet van toepassing op gegevensverwerkingen die worden uitgevoerd in het kader van de publieke taak van een overheidsorgaan. Voor deze grondslag is een belangenafweging nodig, voeg deze toe aan de toelichting op de rechtsgrond.	Nee

Gegevensverwerking	Rechtsgrond	Toelichting op de rechtsgrond
Afhandelen vragen	Taak van algemeen belang	Gerechtvaardigd belang is geen grondslag die voor de overheid te gebruiken is.[7] Er is geen wettelijke verplichting om deze gegevens te verwerken.

De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkings-verantwoordelijke rust; de verantwoordelijkheid van de Kiesraad om vragen van burgers te beantwoorden, valt onder de algemene, publieke taak om als informatief en adviserend orgaan op te treden, en minder als een specifieke verplichting die in de Kieswet is vastgelegd. De Kiesraad zet zich in voor de bevordering van de transparantie van het verkiezingsproces en het informeren van het publiek, wat indirect ook het beantwoorden van vragen van burgers omvat.

12 Bijzondere persoonsgegevens

Het verwerken van bijzondere of strafrechtelijke persoonsgegevens is in principe verboden. Verwerking is pas mogelijk wanneer een uitzonderingsgrond van toepassing is. Beoordeel of een van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een nationaal identificatienummer, beoordeel of dit is toegestaan.
Voeg aanvullende informatie toe in het tekstveld.

Gegevens verwerking	Type bijzondere persoons gegevens	Uitzonderingsgrond
Afhandelen vragen	Politieke opvattingen	**AVG artikel 9** **Lid 1.** Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden. **Lid 2.** Lid 1 is niet van toepassing wanneer aan een van de onderstaande voorwaarden is voldaan: **g.** de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene;

[7] https://autoriteitpersoonsgegevens.nl/uploads/imported/normuitleg_gerechtvaardigd_belang.pdf

De Kiesraad heeft niet tot doel het verwerken van bijzondere persoonsgegevens. Het zit echter in de aard van het werkgebied van de Kiesraad en daarmee dat de vragen die gesteld worden aan politiek raken en dat de vragenstellers een politieke rol of functie bekleden. Het is hierdoor niet te voorkomen dat de Kiesraad – direct of indirect - te maken krijgt met informatie over politieke opvattingen.
Deze informatie is onlosmakelijk verbonden met bepaalde stakeholders en hoewel dus niet altijd nodig is het niet altijd mogelijk om die bijzondere informatie niet mee te verwerken.

13 Doelbinding

Als de persoonsgegevens voor een ander doeleinde worden verwerkt dan het doeleinde waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, beoordeel of deze (nieuwe) verdere verwerking toelaatbaar is op grond van Unie- of lidstaatrechtelijk recht, dan wel verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Voeg in het tekstveld de verenigbaarheidstoets en aanvullende informatie toe.

Gegevensverwerking	Persoonsgegevens	Doeleinde	Oorspronkelijk doeleinde
N.v.t.			

De gegevens worden uitsluitend verwerkt voor het doeleinde 'afhandelen van vragen' door de Kiesraad.

14 Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk en evenredig zijn voor het verwezenlijken van de verwerkingsdoeleinden.
Ga hierbij in ieder geval in op:

a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt?

De gegevens die verzameld worden zijn nodig voor het beantwoorden van de vragen of het communiceren met de vragenstellers.

Er worden minimaal gegevens gevraagd/verwerkt voor dat doeleinde echter:

- *de gegevens worden veelal door de vragensteller (ongevraagd) opgegeven; en/of*
- *de informatie is af te leiden uit de andere informatie die verstrekt wordt.*

Niet verwerken van deze (minimale) gegevens is geen optie omdat daarmee de vragen niet correct beantwoord kunnen worden en/of communicatie niet mogelijk is.

Er is geen andere mogelijkheid om de vragen af te handelen dan wel de gegevens te verwerken die nodig zijn voor het beantwoorden van de vragen of erover te kunnen communiceren.

Waar mogelijk wordt dataminimalisatie toegepast om de nadelige gevolgen zo veel mogelijk te beperken.

15 Rechten van betrokkenen

Beschrijf de procedure waarmee invulling wordt gegeven aan de rechten van de betrokkenen Als de rechten van de betrokkene worden beperkt, beschrijf op grond van welke wettelijke uitzondering dat is toegestaan.

Rechten van betrokkene	Procedure ter uitvoering	Beperking op grond van wettelijke uitzondering
Recht van inzage	Er is een privacyverklaring op de Kiesraad website.	Kieswet, diverse artikelen/hoofdstukken: *De artikelen 15, 16 en 18 van de Algemene verordening gegevensbescherming zijn niet van toepassing op verwerking van persoonsgegevens bij of krachtens dit hoofdstuk.*
Recht op rectificatie en aanvulling		
Recht op vergetelheid		
Recht op beperking van de verwerking		
Recht op dataportabiliteit		
Recht niet onderworpen te worden aan geautomatiseerde besluitvorming		
Recht om bezwaar te maken		
Recht op duidelijke informatie		

De operationele uitvoering van deze rechten gebeurt 'handmatig'. Een van de voordelen die bereikt worden met het inzetten van TOPdesk is dat aan een aantal van deze rechten meer structureel en geautomatiseerd invulling gegeven kan worden (zoals automatische verwijdering, ophalen van informatie, rectificatie).

Zo veel mogelijk van de persoonsinformatie wordt geschoond of gepseudonimiseerd.

Beschrijving en beoordeling risico's voor de betrokkenen

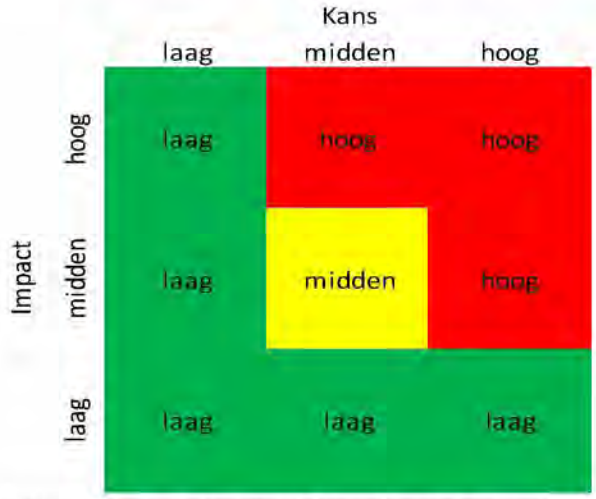
Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen.

16 Risico's voor betrokkenen

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie;
b. de oorsprong van deze gevolgen;
c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Gebruik voor de inschatting van de kans, impact en het risico de niveaus 'laag', 'gemiddeld' en 'hoog'. De kans wordt bepaald aan de hand van de formule kans x impact. Gebruikmaken van de bijbehorende kleuren is aan te raden. De onderstaande matrix kan worden gebruikt voor het vaststellen van de risico's voor betrokkenen.



*De bovenstaande risicomatrix is illustratief. Risico's met een lage impact of lage kans worden als laag ingeschat indien het risico niet verder kan worden gemitigeerd. Zo kan bijvoorbeeld de impact van ransomware hoog zijn, maar door het nemen van de juiste technische maatregelen de kans (zeer) laag. Het risico kan dan ten behoeve van de risico-acceptatie als laag beschouwd worden.

Voeg aanvullende informatie in het tekstveld toe.

Beschrijving risico	Kans	Impact	Risico-inschatting
Kwaadwillende verkrijgen toegang tot Topdesk door het gebruik van herbruikte wachtwoorden, welke zijn gelekt bij datalekken los van Topdesk	H	H	H
Medewerkers kunnen na uitdiensttreding nog bij hun TopDesk account en maken daar misbruik van.	H	H	H
Er wordt gevoelige informatie in Topdesk opgeslagen (zoals BSN) of zelfs bijzondere persoonsgegevens (zoals	H	H	H

Beschrijving risico	Kans	Impact	Risico-inschatting
stemvoorkeur) of die informatie is af te leiden uit de andere informatie uit een melding. Deze informatie kan lekken of worden ingezien door onbevoegden.			
Er is geen of onvoldoende functioneel beheer ingericht (waardoor bijvoorbeeld iedereen hoge rechten heeft of mensen die er geen verstand van hebben de verkeerde configuraties implementeren)	H	H	H
SSC ICT kan/wil SPF records niet aanpassen waardoor er misbruik van ons domeinnaam gemaakt kan worden.	H	H	H
Medewerker wordt gephisht met vals inlogportaal van TopDesk en geven credentials + 2FA code.	M	H	H
Er wordt door Topdeskgebruikers misbruik gemaakt door informatie van derden op te zoeken die niet voor de betreffende persoon toegankelijk zou moeten zijn.	M	H	H
Er wordt gebruik gemaakt van zwakke wachtwoorden waardoor onbevoegden makkelijk toegang tot Topdesk kunnen krijgen.	M	H	H
Beheerders hebben onvoldoende kennis en ervaring en maken daardoor fouten in de configuratie/instellingen waardoor onbevoegde toegang tot Topdesk of informatie mogelijk is.	M	H	H
Kwaadwillende maakt misbruik van de SPF records kwetsbaarheid om mails namens @Kiesraad.nl te versturen en zo phishing te proberen of desinformatie te verspreiden.	M	H	H
Kwaadwillende verkrijgen toegang tot Topdesk door het gebruik van herbruikte wachtwoorden, welke zijn gelekt bij datalekken los van Topdesk	H	H	H
Medewerkers kunnen na uitdiensttreding nog bij hun TopDesk account en maken daar misbruik van.	H	H	H
Er wordt gevoelige informatie in Topdesk opgeslagen (zoals BSN) of zelfs bijzondere persoonsgegevens (zoals stemvoorkeur) of die informatie is af te leiden uit de andere informatie uit een melding. Deze informatie kan lekken of worden ingezien door onbevoegden.	H	H	H
Er is geen of onvoldoende functioneel beheer ingericht (waardoor bijvoorbeeld iedereen hoge rechten heeft of mensen die er geen verstand van hebben de verkeerde configuraties implementeren)	H	H	H
SSC ICT kan/wil SPF records niet aanpassen waardoor er misbruik van ons domeinnaam gemaakt kan worden.	H	H	H

Er is in januari 2024 een risicoanalyse (MAPGOOD) uitgevoerd voor TOPdesk waarbij dit proces ('afhandelen van vragen') in scope was. De focus van die analyse was breed en omvatte risico's op de verschillende themagebieden.

De risico's uit die analyse kunnen in potentie negatieve gevolgen hebben voor de rechten en vrijheden van de betrokkenen, zoals:

- *Ongeautoriseerde toegang tot gevoelige informatie leidt tot identiteitsdiefstal en het misbruik van iemands identiteit(sgegevens);*
- *Ongeautoriseerde toegang tot gevoelige informatie leidt tot datalekken, verkopen en/of misbruik van informatie;*
- *Informatie wordt gemanipuleerd dat leidt tot desinformatie en foutieve antwoorden;*
- *Onbevoegde toegang of lekken van informatie leidt tot discriminatie van betrokkenen (bijv. bij sollicitatie);*
- *Onbevoegde toegang of lekken van informatie leidt tot stigmatisering of uitsluiting voor individuen (bijv. vanwege politieke voorkeur);*
- *Onbevoegde toegang of lekken van informatie leidt tot imago schade voor PG/PP;*
- *Informatie wordt online beschikbaar gesteld of verkocht;*
- *Er wordt desinformatie verspreid over betrokkene;*
- *Desinformatie of phishing wordt verspreid uit naam van betrokkene;*
- *Desinformatie of phishing wordt verspreid naar betrokkene;*

In bovenstaande tabel zijn de top 10 risico's uit de risicoanalyse met de hoogste risicoscore opgenomen. Dit gaat om de bruto risicoschattingen (dus vóór het nemen van maatregelen).

Maatregelen en restrisico's

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen.
Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de DPIA is in het bijzonder expertise over informatiebeveiliging belangrijk.

17 Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt. Voeg aanvullende informatie in het tekstveld onder de tabellen toe.

Beschrijf ook de resterende risico's die nog aanwezig zijn na de uitvoering en/of implementatie van de geïdentificeerde maatregelen. Geef per resterend risico aan wat het niveau is van dit risico.

Geef tot slot een conclusie over de restrisico's. Zijn deze acceptabel? En is er een voorafgaande raadpleging bij de Autoriteit Persoonsgegevens nodig?

Gebruik voor de inschattingen van de risico's de niveaus 'laag', 'gemiddeld' en 'hoog'. Gebruikmaken van de bijbehorende kleuren is aan te raden.

Risico	Maatregelen	Restrisico en risico-inschatting	Beheerder van maatregelen
Kwaadwillende verkrijgen toegang tot Topdesk door het gebruik van herbruikte wachtwoorden, welke zijn gelekt bij datalekken los van Topdesk	Single sign on	L	Implementatieteam
Medewerkers kunnen na uitdiensttreding nog bij hun TopDesk account en maken daar misbruik van.	Procedure on- en off-boarding (aanvraag rechten en uitschakelen accounts) Periodieke checks accounts en rechten	L	Functioneel beheer
Er wordt gevoelige informatie in Topdesk opgeslagen (zoals BSN) of bijzondere persoonsgegevens (zoals stemvoorkeur) of die informatie is af te leiden uit de andere informatie uit een melding. Deze informatie kan lekken of worden ingezien door onbevoegden.	Waar mogelijk dataminimalisatie; (automatisch) pseudonimiseren; Rechtenbeheer (informatie afschermen (filters), rollen en autorisaties, intrekken delete rechten);	L	Functioneel beheer

Risico	Maatregelen	Restrisico en risico-inschatting	Beheerder van maatregelen
	Uitschakelen (niet gebruikte/niet te gebruiken) functionaliteiten; Afspraken/procedure m.b.t. registratie en opslaan van data (dataminimalisatie)		
Er is geen of onvoldoende functioneel beheer ingericht (waardoor bijvoorbeeld iedereen hoge rechten heeft of mensen die er geen verstand van hebben de verkeerde configuraties implementeren)	Formeel beleggen en inrichten van FB voor Topdesk bij team D&T binnen de Kiesraad; Support vanuit Topdesk tijdens de implementatiefase bij het installeren en configureren van Topdesk.	L	Opdrachtgever Consultant
SSC ICT kan/wil SPF records niet aanpassen waardoor er misbruik van onze domeinnaam gemaakt kan worden.	Dit risico is niet meer van toepassing; SSC-ICT werkt mee.	L	Implementatieteam
Medewerker wordt gephisht met vals inlogportaal van TopDesk en geven credentials + 2FA code.	Single Sign on	L	Implementatieteam
Er wordt door Topdeskgebruikers misbruik gemaakt door informatie van derden op te zoeken die niet voor de betreffende persoon toegankelijk zou moeten zijn.	Waar mogelijk dataminimalisatie; (automatisch) pseudonimiseren; Rechtenbeheer (informatie afschermen (filters), rollen en autorisaties, intrekken delete rechten); Uitschakelen (niet gebruikte/niet te gebruiken) functionaliteiten; Afspraken/procedure m.b.t. registratie en opslaan van data (dataminimalisatie)	L	Functioneel beheer

Risico	Maatregelen	Restrisico en risico-inschatting	Beheerder van maatregelen
	Logging van zoekopdrachten (indien mogelijk)		
Er wordt gebruik gemaakt van zwakke wachtwoorden waardoor onbevoegden makkelijk toegang tot Topdesk kunnen krijgen.	Single sign on	L	Implementatieteam
Beheerders hebben onvoldoende kennis en ervaring en maken daardoor fouten in de configuratie/instellingen waardoor onbevoegde toegang tot Topdesk of informatie mogelijk is.	Rechtenbeheer (informatie afschermen (filters), rollen en autorisaties, intrekken delete rechten) Training en opleiding.	L	Implementatieteam
Kwaadwillende maakt misbruik van de SPF records kwetsbaarheid om mails namens @Kiesraad.nl te versturen en zo phishing te proberen of desinformatie te verspreiden.	Dit risico is niet meer van toepassing; SSC-ICT werkt mee.	L	Implementatieteam
Geen toepassing van dataminimalisatie door afwezigheid geautomatiseerde verwijdering	Implementatieteam regelt dat in Topdesk de persoonsgegevens gepseudonimiseerd worden.	L	Implementatieteam

Overzicht van de maatregelen

Technische maatregelen tool:

1. *Toegangsbeheer (SSO en complexe credentials, accounts op naam)*
2. *Rechtenbeheer (informatie afschermen (filters), rollen en autorisaties, intrekken delete rechten)*
3. *Privacy by design en default (uitschakelen (niet gebruikte/niet te gebruiken) functionaliteiten)*
4. *Backup en restore van data*
5. *Mailfunctionaliteit beschermen (middels DMARC, DKIM en SPF)*
6. *Pseudonimisering van data (automatisch)*
7. *Opschoning mailbox en tool (automatisch)*
8. *Logging*

Organisatorische maatregelen:

1. *Inrichten Functioneel beheer*
2. *Afspraken/procedure m.b.t. registratie en opslaan van data (dataminimalisatie)*
3. *Training en opleiding (behandelaars en functioneel beheerders)*

4. *Afspraken leverancier(s):*
    a. *Contract (overdragen van informatie, …)*
    b. *SLA (minimale prestatieafspraken, …)*
    c. *Verwerkersovereenkomst (verwerkingen, melden van incidenten, opslaglocaties, …)*
5. *Procedure on- en offboarding (aanvraag rechten en uitschakelen accounts)*
6. *Periodieke check accounts en rechten*

Het gros van de risico's voor de rechten en vrijheden van de betrokken zijn een gevolg van het lekken van informatie of door oneigenlijke toegang tot de data in de systemen van de Kiesraad. De maatregelen zijn er in het algemeen op gericht om de vertrouwelijkheid te waarborgen en lekken en onbevoegde toegang tot een minimum te beperken.

Door het implementeren van deze technische- en organisatorische maatregelen wordt de kans dat de risico's tot uiting komen verlaagd. De impact blijft veelal hetzelfde maar het risico kan daarmee tot een aanvaardbaar niveau worden teruggebracht.

Ondertekening

Om de DPIA formeel vast te stellen is het noodzakelijk deze te ondertekenen, zodat het duidelijk is dat de DPIA door de verantwoordelijke(n) akkoord is bevonden.

Naam verantwoordelijke(n)	5.1.2.e
Directie/afdeling verantwoordelijke(n)	
Functie verantwoordelijke(n)	5.1.2.e
Datum ondertekening	
Handtekening	