

Uitwerking AVG afdeling Publiekzaken



Inhoud

Uitwerking AVG afdeling Publiekzaken	1
Inleiding.....	2
Aanleiding en doel.....	2
Methode	3
Samenvatting.....	3
Algemene afdronk.....	3
Samenvatting van de gesprekken.	6

Inleiding

Aanleiding en doel

Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. De AVG schrijft voor hoe organisaties om moeten gaan met het verzamelen, verwerken, opslaan en verwijderen van persoonsgevoelige informatie.

De volgende regels moeten worden gevolgd:

- **Transparantie:** de persoon van wie de gegevens verwerkt worden, is hiervan op de hoogte, heeft hiervoor toestemming gegeven en kent zijn rechten.
- **Doelbeperking:** de persoonsgegevens worden voor een welbepaald gewettigd doel verzameld, en mogen niet voor andere zaken gebruikt worden.
- **Gegevensbeperking:** enkel de gegevens die voor het beoogde doel noodzakelijk zijn, mogen worden verzameld.
- **Juistheid:** de persoonsgegevens moeten correct zijn en blijven.
- **bewaarbeperking:** de persoonsgegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel.
- **Integriteit en vertrouwelijkheid:** de persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging.
- **Verantwoording:** de verantwoordelijke moet kunnen aantonen aan deze regels te voldoen.

De afdeling Publiekszaken maakt veel gebruik van persoonsgegevens. Deze gegevens zijn nodig voor alle lopende processen met betrekking tot de BRP. De afgelopen jaren is er steeds meer aandacht voor de vertrouwelijkheid van informatie en de maatregelen die nodig zijn om veilig te handelen. Er wordt steekproefsgewijs gekeken hoe de verschillende bureaus (clusters) hiermee omgaan.

Jaarlijks worden er verschillende controles uitgevoerd. De belangrijkste is het jaarlijkse ENSIA onderzoek van het Ministerie. Dit onderzoek richt zich op de beveiliging van processen, fysieke toegang en de naleving en bestaat uit verschillende onderdelen zoals: zelfevaluatie Basisregistratie; paspoorten/reisdocumenten controle en algemene controle BRP en Burgerlijke Stand.

Daarnaast vindt er door het Ministerie controle plaats bij de gegevensverwerking RNI (Register Niet Ingezetenen) en doorlopend de kwaliteitsmonitor (controle op de verwerkte gegevens).

Om een volledig overzicht te hebben welke gevoelige informatie de afdeling precies heeft en hoe er mee om wordt gegaan is gevraagd om een verkennend onderzoek. Hierbij wordt de afdeling in beeld gebracht.

Doel

Met dit onderzoek willen we verder *in control* komen op het gebied van AVG op de afdeling: we willen weten bij welke processen en/of organisatieonderdelen er binnen Publiekszaken gebruik gemaakt wordt van verschillende persoonsgevoelige gegevens, hoe daar mee om wordt gegaan, wat onzekerheden en risico's zijn en hoe we met deze risico's om moeten of willen gaan (risicobereidheid). Om zo meer inzicht en grip te krijgen op de AVG bij Publiekszaken en te kunnen bepalen welke vervolgstappen er nodig zijn om de afdeling verder AVG-proof te krijgen. Hierbij is gekeken naar gebruikte systemen, processen en gegevens (op hoofdlijnen) en naar welk gedrag en bewustzijn daarvoor nodig is onder medewerkers.

Daarnaast draagt dit onderzoek bij aan de verantwoording van Publiekszaken aan de Functionaris Gegevensbescherming (FG). De afgelopen jaren is de rol van de Functionaris Gegevensbescherming (FG) en de Privacy Officer (PO) steeds meer vormgegeven in de organisatie. Zij hebben een controlerende (FG) en adviserende (PO) rol wat betreft de waarborging van de vertrouwelijkheid van persoonsgegevens.

Methode

De informatie is zoveel mogelijk opgehaald via gesprekken met leidinggevendenden omdat zij een goed overzicht van hun bureau hebben. Waar relevant zijn verdiepende gesprekken met medewerkers gevoerd. De constateringen in dit stuk zijn voornamelijk op basis van indrukken en uitleg van de leidinggevendenden en medewerkers. Omdat dit onderzoek gaat om een verkenning op de afdeling, is niet tot in detail in systemen en correspondentie gekeken of steekproefsgewijs getoetst.

Samenvatting

Algemene afdrank

Op 11 juni 2019 is het plan van aanpak voor de afdeling Publiekszaken opgesteld en zijn we aan de slag gegaan met de punten uit dit plan.

Wat is er gebeurd met de actiepunten van het plan van aanpak?

1. Opslag documenten: In de afgelopen jaren zijn er verschillende sloten vervangen en is meubilair aangepast. Verder zijn er verschillende aanpassingen gedaan in de Stadswinkel (sluiten van deuren, vervangen van sloten en aanpassen werkprocessen). Voor de herinrichting van de Stadswinkel zijn wij betrokken en hebben wij onze wensen voor de privacy kenbaar gemaakt.
2. Ontvangen en versturen gegevens algemeen: Aan de bewustwording is veel aandacht besteed en dit is ook het komende jaren het geval. Werkprocessen zijn aangepast en alle medewerkers gebruiken hiervoor nu "Zivver". De automatische vraag in Outlook ondersteunt dit.
3. Telefoon opvragen gegevens: Hier is de afgelopen jaren heel veel aandacht aan besteed. In 2023 organiseren we een extra actie (ID-fraude).
4. Archiveren gegevens: Sinds oktober 2022 zijn we gestart met een project dat past in het informatiebeheer. Samen met alle clusters bekijken we hoe we gegevens bewaren en direct opschonen (mappen en mail). Naast een nieuwe manier van archiveren nemen we direct het AVG-aspect mee. Na de afronding van dit project is er een goede werkbeschrijving beschikbaar en zijn alle mappen/mail vrij van persoonsgegevens.
5. Website: Team online checkt alle formulieren en past aan waar nodig. Dit is geen actie van de afdeling Publiekszaken, maar we houden dit wel in de gaten.
6. Mail en post andere gemeenten, buitenland en externe partijen: De werkprocessen zijn aangepast.
7. AVG en BRP: De behoefte van 2020 (inventarisatie voorafgaande aan Plan van aanpak) door KOI is niet meer van deze tijd. Er is op de afdeling voldoende kennis van de BRP. Verder zijn nog niet lopende processen in beeld. Nieuwe systemen zorgen voor aanpassing.
8. KCC en telefonie: Alleen bij persoonsgebonden vragen we persoonsgegevens. Bij de overige vragen niet. Op dit moment loopt de DPIA KCC nog (wachten op goedkeuring)
9. In- en extern doorzetten vragen KCC: Op 15 mei nemen we een nieuw systeem Tribe (terugbelverzoeken) in gebruik. Dit systeem zorgt ervoor dat er bij terugbelverzoeken niet meer gegevens worden toegevoegd dan is toegestaan. Bij het begin van het project is er gestart met een DPIA. JZ heeft hier bij meegekeken.
10. Ambtseed KCC: Het werkproces is aangepast.

De afdeling Publiekszaken verwerkt dagelijks persoonsgegevens en er is blijvende aandacht nodig voor de AVG/privacy. De afgelopen jaren is er veel energie gestoken om de bewustwording op de afdeling te vergroten en werkprocessen en systemen aan te passen. Dit doen we onder andere door het houden van onze jaarlijkse ronde langs de werkoverleggen. Nemen we regelmatig steekproeven op de afdeling en spreken collega's aan waar nodig. Spreken collega's elkaar aan op gedrag door middel van de Dodo post-it. Heeft Dodo zijn eigen rubriek in de 2 wekelijkse nieuwsbrief. Deze artikelen worden ook dagelijks op de Tv's getoond (afdeling). En organiseren we een jaarlijks terugkerende afdelingsbrede themabijeenkomst met als inzet de Dodo wisseltrofee.

Dodo is bij Publiekszaken ontstaan en wordt inmiddels ook gemeentebreed ingezet.

Werkprocessen en systemen worden bekeken en zo nodig aangepast. We reageren op signalen. Zo is er direct contact opgenomen met de privacy- officer n.a.v. een signaal van een klant in ons klantcontactmonitor (KCM). Klanten krijgen na afloop van hun bezoek een link om mee te doen aan een klantonderzoek. Een klant signaleerde dat hij

door een derden partij hiervoor werd benaderd zonder dat hij toestemming had gegeven. Het webformulier kan helaas niet worden aangepast met een mogelijkheid om al of niet toestemming te geven aan de deelname. Na advies te hebben gevraagd bij JZ is het wel mogelijk om toch zonder toestemming te vragen de klant te laten deelnemen aan het onderzoek (overweging 47 AVG). Op de uitnodiging om deel te nemen aan het onderzoek is nu een uitleg opgenomen.

Mede door onze aandacht voor de privacy in de Stadswinkel loopt er op dit moment een herinrichtingsproject. We geven gerichte verbeterpunten voor deze herinrichting.

Aan het verwerken van gegevens zitten grofweg drie elementen.

Ten eerste is de BRP leidend. De regels die zijn opgenomen in de BRP gaan vaak verder dan die genoemd in de AVG. Ten tweede het inregelen van veilige systemen, autorisaties en de afspraken daarom heen. En ten derde het gedrag van medewerkers: wordt er aan afspraken gehouden, zijn medewerkers zich bewust van AVG en hun rol daarin?

Voor zowel het inregelen van veilige systemen als voor gedrag is de indruk dat er rekening gehouden wordt met AVG en dat de afgelopen jaren de nodige maatregelen zijn getroffen. Ook vindt er een jaarlijkse controle plaats m.b.t. de BRP. Daarmee lijkt Publiekszaken aardig op weg te zijn en in zekere mate *in control* te zijn. Wel zijn er een aantal maatregelen dat genomen kan/moet worden en blijft het nodig om in de bureaus regelmatig stil te staan bij AVG. Een datalek of onjuist gebruik van persoonsgegevens zit in een klein hoekje. Daarnaast blijft het altijd zoeken naar de balans tussen risico's volledig afdekken (bv. slechts één of twee personen ergens toegang toe geven) en het werkbaar houden (bv. elkaar kunnen vervangen bij uitval).

In de gesprekken is gevraagd naar voorvallen en klachten met de AVG de afgelopen jaren. Deze zijn weinig genoemd en als ze zijn genoemd, is hiervoor ook een oplossing gekomen. We zeggen daarmee niet dat alles al goed geregeld is, maar ondersteunt de indruk uit de gesprekken: dat in veel processen, systemen en werkzaamheden rekening gehouden wordt met AVG.

Afdeling Publiekszaken algemeen	
Globale stand van zaken afdeling	<p>Bij de afdeling Publiekszaken is er blijvende aandacht voor de AVG. Werkprocessen en systemen worden bekeken en zo nodig aangepast. Wordt er adequaat gereageerd op signalen die worden ontvangen via medewerkers en/of vanuit ons KCM (Klant Contact Monitor).</p> <p>We besteden regelmatig aandacht aan de bewustwording d.m.v. onze vaste rubriek in de nieuwsbrief (DoDo – AVG, wat moet je ermee?). Worden er artikelen en aandachtspunten op de TV schermen op de afdeling getoond. Is er regelmatig aandacht in de werkoverleggen en hebben we ons jaarlijks terugkerende (afdelingsbrede) themabijeenkomst met als inzet de DoDo wisseltrofee.</p> <p>We hebben oog voor het vergroten van de verantwoordelijkheid van medewerkers doordat we sinds 2022 bezig zijn met het opleiden van onze medewerkers. Dit gebeurt door middel van het NVVB opleidingsplan. Een medewerker die beschikt over voldoende kennis, is beter in staat om sneller te signaleren.</p>
Systemen	<ul style="list-style-type: none">- Laptop- Microsoft office pakket (Word/ Outlook)- iPhone en vaste telefoons- G-schijf

	<ul style="list-style-type: none"> - Gemeenschappelijke schijf - Zivver - Website (afspraken/vragen/klachten e.a.) - Tribe
Aanvullende systemen	<p>Coda. In dit systeem worden relaties aangemaakt. Dit is het gemeentebrede financiële systeem.</p> <p>Gouw. In dit systeem worden relaties aangemaakt en gebruikt voor aanslagen leges, huwelijken en uittreksels. De belasting gebruikt dit systeem en wij kunnen hierin kijken.</p> <p>Ky2betalen. Gebruikt door financiën. Dit is een kassa systeem. Hierin staan geen persoonsgegevens.</p> <p>Corsa. Het gemeentebrede archief en registratie systeem. Hierin staan wel persoonsgegevens vermeld.</p> <p>JCC. Dit is ons centrale afsprakensysteem. Hierin worden alle afspraken verwerkt.</p> <p>Vrij BRP (Procura). In dit systeem worden alle persoonsgegevens verwerkt.</p> <p>KCM. Dit is onze klantcontact monitor. Meting klanttevredenheid en bevatten persoonsgegevens.</p> <p>Disc systeem. Hierin staan alle akten van de burgerlijke stand, bestemd voor de landelijke registratie.</p> <p>Kennisbank (Britannica). Hierin staan alle werkprocessen en benodigde informatie beschreven.</p> <p>Scanner (Oribi en Security Tach) Dit systeem zorgt voor de security check.</p> <p>UV lamp en loep. Worden gebruikt om de ID bewijzen te controleren.</p> <p>Telefoonsysteem (Detron). Dit is het systeem dat bij het KCC (Klant Contact Centrum) wordt gebruikt.</p>
Belangrijkste risico's afdeling	<p>De geïnventariseerde risico's zijn:</p> <ul style="list-style-type: none"> • De openheid van de afdeling. • Het opvangen van privacygevoelige informatie (SW en afdeling). • Stembureau manager en ROS lijst (verkiezingen). • Borging afspraken en het beheer van accounts en e-herkenning. • Centrale opslag paspoortgegevens.
Hoe heb ik de informatie opgehaald.	<p>Een ronde langs alle clusters gehouden om nog bestaande knelpunten m.b.t. de AVG op te halen. Deze gesprekken heb ik gevoerd met de leidinggevenden.</p> <p>Gesprekken gevoerd met individuele medewerkers en teams om meer zicht te krijgen op de verschillende werkprocessen en systemen (stafmedewerkers, team dienstverlening, I-medewerker, financiën en verkiezingen).</p> <p>Hieronder een korte samenvatting van de gesprekken.</p>

Nog op te pakken acties	In onze jaarlijkse terugkoppeling AVG in het MT PU (januari) wordt de actielijst gepresenteerd voor het komende jaar. De acties en aandachtspunten die voortkomen uit deze inventarisatie zijn aangevuld op de bestaande actielijst (<i>zie bijlage</i>)
Waar gaan we mee door (standaard)	<ul style="list-style-type: none"> • Constante aandacht voor de bewustwording AVG door Dodo. Wat mag wel, wat mag niet? Waar loopt men tegenaan, wat zijn nog vragen? • Steekproeven nemen om te kijken of er in de clusters nog gewerkt wordt zoals we hebben afgesproken. • Jaarlijks terugkerende themabijeenkomst of andere activiteit voor de gehele afdeling (Dodo wisseltrofee). • Het oppakken van alle acties die zijn opgenomen in de actielijst.
Gemeentebrede aandachtspunten	<ul style="list-style-type: none"> • Afspraken over opschonen van mail en telefoon is een vraagstuk dat voor de gehele gemeente geldt. Dit punt is op een eerder moment al aangegeven en afgesproken: <i>Hiervoor wordt een gemeentebrede visie opgesteld door JZ.</i> • Wanneer medewerkers thuis aan het werken zijn maken zij gebruik van hun privé laptop en privé telefoon. Persoonsgegevens zijn daardoor openbaar op privé apparaten van medewerkers. Dit punt is al op een eerder moment aangegeven en afgesproken: 5.1.2e en 5.1.2e nemen dit mee naar de stuurgroep. • Gebruik mobiele telefoon: Wat zijn de afspraken voor het gebruik van de mobiele telefoon? Deze worden door veel mensen zowel privé als zakelijk gebruikt. Mensen nemen deze telefoon overal mee naartoe, ook op vakantie. Het risico op een datalek door het verlies van de telefoon wordt hierdoor groter. • Gebruik zakelijk mailadres: Wat zijn de afspraken m.b.t. het gebruik van je zakelijke mailadres voor privédoeleinden. Mensen koppelen hun zakelijke mailadres aan apps en/of websites. Wat zijn de gemeentebrede afspraken? • Verloop personeel: Gemeentebreed is er ook een groot verloop van nieuwe medewerkers. De vraag is of het bewustzijn van de AVG altijd even hoog is als je tijdelijk of net in dienst bent. • Werkbare kaders: We moeten er wel voor zorgen dat we met elkaar een werkzame situatie creëren en nadenken over wat de gevolgen echt zijn. Hiervoor zouden kaders moeten komen.

Samenvatting van de gesprekken.

Ronde langs alle clusters om nog bestaande knelpunten m.b.t. de AVG op te halen m.b.t. de AVG.

Vragen:

- ✚ Wat is de algemene indruk van de stand van zaken m.b.t. de AVG voor jouw bureau?
- ✚ Zijn er afspraken gemaakt/vastgelegd over het opvragen/verstrekken van persoonsgegevens (aanvullende afspraken nodig)?
- ✚ Zijn alle werkprocessen binnen jouw cluster voldoende AVG proef en vastgelegd?
- ✚ Waar zitten nog de risico's?
- ✚ Waar ervaar je nog knelpunten binnen jouw cluster?
- ✚ Voor welke werkprocessen zouden wij nog een DPIA moeten uitvoeren?
- ✚ Waar moeten we nog extra aandacht voor hebben (afdelingsbreed)?
- ✚ Waar moeten we nog extra aandacht voor hebben (gemeentebreed)?

PU00 - 5.1.2e (31/1/2023):

(Staf – team dienstverlening – verkiezingen – algemeen)

Er zal aandacht moeten blijven voor de BRP monitor (de zelfevaluatie en het werken aan de verbeterpunten) . 5.1.2e is tevreden over de stijgende lijn van het bewustzijn van de medewerkers, maar verwacht dat dit ook weer snel wegzakt als de aandacht hiervoor afneemt. Hiervoor blijven dus acties nodig.

Soms slaan we ook door. In het rooster zouden we niet meer mogen vermelden waarom iemand afwezig is (verlof of ziek). We moeten er wel voor zorgen dat we met elkaar een werkzame situatie creëren en nadenken over wat de gevolgen echt zijn. Hiervoor zouden kaders moeten komen.

Scherp blijven op welke normen we vragen en situaties die zich voordoen (datalek – kasten – laptop – papieren enz). De gang (langs backoffice) wordt nog door teveel mensen gebruikt. Het risico op het prijsgeven van informatie blijft aanwezig.

Actie P&O voor toestemming adresgegevens. Benieuwd hoeveel actieve toestemmingen er komen. Aan het eind van het jaar een lijst opvragen bij P&O hoeveel mensen deze toestemming hebben gegeven.

Wat doen we nu met toegang BRP van medewerkers die afscheid nemen maar nog wel op de loonlijst blijven staan? De toegang tot de BRP zou geblokkeerd moeten worden. Inmiddels hebben we hier advies over ingewonnen en weten we hoe we kunnen handelen

PU20 - 5.1.2e (15/2/2023) - 5.1.2e (21/4/2023) - 5.1.2e (21/4/2023):

(KCC – Specialisten – RNI – Financieel – Content)

De werkprocessen bij de specialisten, Financieel en Content zijn goed in beeld en worden voldoende gemonitord. Vanuit de BRP is er ook een jaarlijkse controle.

Specialisten:

De openheid van de afdeling is een aandachtspunt. Deuren staan open en mensen die niet op de afdeling horen lopen langs de backoffice richting het restaurant. In de brandkasten (achter de specialisten) liggen de brondocumenten. Voor de werkbaarheid moeten deze kasten open blijven overdag, echter kunnen hier documenten uitgehaald worden door een derde. Dit geldt ook voor de gegevens die de specialisten printen op de speciale printer.

Een aantal werkprocessen worden al nader bekeken: printen (direct ophalen/Dodo); proces brondocumenten doornemen en aanpassen; telefoneren (gehoorigheid/meeluisteren);

KCC/RNI:

We hebben te maken met veel doorstroming, dus veel nieuwe medewerkers.

Bij het KCC ontvangen wij nog wel eens klachten die betrekking hebben op het verstrekken van persoonsgegevens aan de telefoon. De werkbeschrijvingen en kennisbank zijn op orde, echter moet er wel naar

gekeken en gehandeld worden. Deze procedure is inmiddels geborgd door een intensieve inwerkperiode. De nieuwe medewerkers zijn verplicht om de e-learning Privacy binnen 2 weken te doorlopen. Daarnaast is er veel aandacht voor coaching op de vloer. Dit blijft wel een aandachtspunt.

De tijdelijke locatie van de RNI is niet optimaal. In dit gebouw worden ook Oekraïners opgevangen en de ruimte is erg open. Wel wordt de ruimte altijd afgesloten als de medewerkers niet aanwezig zijn.

Met JZ is afgesproken dat het KCC een lijst gaat aanleveren van afdelingen die specifiek vragen om een BSN nummer. JZ gaat dan in gesprek met de betreffende afdelingen. 5.1.2e is al met deze lijst bezig en pakt dit verder op.

Daarnaast is de vraag of het teveel opvragen van persoonsgegevens met het nieuwe systeem Tribe verholpen is of kan worden. KCC-er vult de kaart in en kiest uit de opties een afdeling. Dan vraagt het systeem zelf om BSN of niet (AVG is meegenomen bij de ontwikkeling van Tribe. Vooraf is er een DPIA gedaan via I&A).

De DPIA van het KCC is gemaakt en na aanvullingen toegestuurd aan JZ. We wachten nog op goedkeuring.

Voor KCC geldt ook dat de gehorigheid en meeluisteren een rol speelt. Iedere medewerker die naar het restaurant gaat via de ingang tegenover KCC kan vertrouwelijke informatie opvangen. Daarnaast blijft het grote verloop van de medewerkers een risico.

De risico's bij de RNI zijn er niet omdat hier volgens systematiek van Ministerie gewerkt en gecontroleerd wordt.

Algemeen:

Op de afdeling maken we veel gebruik van inhuur. Welke autorisaties krijgen deze medewerkers en welke afspraken maak je m.b.t. integriteit. De afdeling bevindt zich op meerdere locaties. Hoe worden deze locaties gecontroleerd op naleving?

Er lopen veel collega's via het KCC naar het restaurant en vergaderruimten. Dit komt doordat collega's via de gangen van de backoffice lopen, dus niet AVG proof. De ideale situatie zou zijn als de gehele 1^e verdieping in gebruik genomen wordt door PU zodat er geen enkele loop meer over de afdeling is, anders dan medewerkers PU.

De deur van de ruimte die in gebruik is bij de Belastingdienst (belastingloket) staat heel vaak open omdat zij aangeven dat het hok te benauwd is. Deze deur bevindt zich in de gang bij de backoffice (huwelijken). Het is niet wenselijk dat deze deur open staat omdat er informatie opgevangen kan worden vanuit de backoffice. Na herhaaldelijk vragen om deze deur dicht te doen komt hierop geen reactie en blijven zij deze deur open doen. We zijn al in gesprek met 5.1.2e (projectleider) om hier een oplossing voor te zoeken.

PU10 - 5.1.2e (31/1/2023):

(Publieksdienstverlening – Gastvrouwen – Burgerzaken – Babs – Roostering – adresonderzoek)

Het bewustzijn onder de medewerkers is zeker toegenomen. Wel is hier blijvende aandacht nodig, ook in verband met nieuwe medewerkers. In de betreffende werkoverleggen en op de vloer wordt regelmatig aandacht gevraagd voor de AVG.

Een aandachtspunt blijft de papieren op de bureaus. Er lopen regelmatig collega's van andere afdelingen in gang bij de backoffice. Daarnaast is het opvragen van persoonsgegevens per mail is ook een terugkerend aandachtspunt.

De werkprocessen zijn goed ingericht. De indruk is dat deze werkprocessen ook voldoende worden nageleefd, dan wel bijgesteld als blijkt dat een proces niet voldoet.

De werkwijze m.b.t. adresonderzoek zal nog eens nagelopen moeten worden om te bekijken of dit op alle vlakken, ook buitendienst AVG proof is. Dit is nog onvoldoende in beeld.

Er zou meer aandacht kunnen komen voor de gehorigheid van de gesprekken die op de afdeling gevoerd worden. Zowel bij specialisten en adresonderzoek is het opvangen van persoonsgegevens van toepassing.

Er wordt weinig tot niet thuis gewerkt.

Team Verkiezingen (17/2/2023):

Er is extra aandacht voor de stembureau manager (administratiesysteem verkiezingen). In dit systeem staan de gegevens in van rond de 4000 mensen die ieder jaar worden aangeschreven. We gaan met JZ bekijken of deze gegevens wel bewaard mogen worden en/of dat zij hiervoor toestemming moeten verlenen.

Verder is er een risico bij het meegeven van de ROS-lijst aan de voorzitters aan de vooravond van de verkiezingen. Op deze lijst staan persoonsgegevens.

Tijdens de verkiezingen bleek dat de berichten via de I-pad niet goed gingen. Hierop wilde team verkiezingen een app-groep in het leven roepen. Dit was echter niet mogelijk omdat er vooraf geen toestemming is gegeven door de voorzitters. Hoe voorkomen we dit bij een volgende keer.

Team Staf (21/2/2023):

Stuk uit nieuwsbrief Autoriteit persoonsgegevens:

Het kabinet wil een centrale database maken met alle persoonsgegevens die mensen aanleveren voor een paspoortaanvraag, zoals vingerafdrukken, handtekeningen en pasfoto's. Zo'n database met gegevens van heel veel Nederlanders brengt grote privacyrisico's mee die het kabinet niet goed meeweegt. Ook kan er onduidelijkheid ontstaan over wie verantwoordelijk is voor de veiligheid van de gegevens. De Autoriteit Persoonsgegevens (AP) adviseert dan ook de plannen grondig aan te passen of anderszins in te trekken. Nu slaat de gemeente waar iemand een paspoort of identiteitskaart aanvraagt zelf de benodigde persoonsgegevens op. In een eigen decentrale database. Het kabinet wil nu met een [wijziging van de Paspoortwet](#) overgaan naar één centrale opslag.

5.1.2e : N.a.v. het bovenstaande stuk is, bij invoering, het risico de centrale opslag paspoortgegevens. Dit wordt dan een landelijke afspraak. Als dit niet goed beveiligd wordt dan liggen alle gegevens op straat. Het is belangrijk dat mijn opvolger dit in de gaten houdt en JZ hierop laat meekijken.

5.1.2e : We gaan extra aandacht besteden aan ID fraude. Vanaf komende maandag (27/2) gaan we in gesprek om extra scanners en nieuwe ontwikkelingen te bespreken.

5.1.2e geeft aan dat er extra aandacht moet zijn voor:

- Herinrichting Stadswinkel. Hierop kijkt zij al mee, maar de omgeving en meubilair zijn niet nu niet AVG proof.
- Persoonsgegevens blijven op de tafels liggen; praktisch onuitvoerbaar om steeds in kasten overdag op te ruimen. Wel blijven we hier aandacht voor vragen.
- Nonchalante houding/afspraken niet nakomen. Ook hier blijf ik aandacht voor houden.

Team informatiebeheer (20/02/2023):|

Sinds oktober 2022 loopt er een project in het kader van informatiebeheer. Hierbij bekijken we hoe gegevens bewaard worden en wordt er direct opgeschoond (mappen en mail).

Naast een nieuwe manier van archiveren wordt ook direct het AVG aspect meegenomen. Hierbij kijken we samen met het betreffende cluster naar de gegevens die worden opgeslagen in de verschillende mappen. Persoonsgegevens die in de centrale systemen worden bijgehouden worden direct verwijderd uit deze mappen. Indien noodzakelijk worden –in overleg met JZ - werkafspraken gemaakt over bewaartermijn en/of het niet meer opslaan van deze gegevens.

Na de afronding van dit project hebben met elkaar de werkafspraken vastgelegd.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	6, 7, 8, 9