

Uitwerking AVG afdeling VJB

Inhoud

Uitwerking AVG afdeling VJB	1
Inleiding.....	2
Aanleiding en doel.....	2
Methode	2
Samenvatting.....	3
Algemene afdronk	3
Samenvatting per bureau	3

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 VJB kenmerkt zich door een grote variatie aan van elkaar verschillende processen. Meestal zijn deze processen ondersteunend van aard. Soms maken ze echter deel uit van de uitvoerende taken van onze gemeente. Binnen deze processen wordt gebruik gemaakt van diverse persoonsgegevens. Van o.a. gegevens die nodig zijn voor statistieken, procedures in het kader van de rechtsbescherming, communicatie, vergaderondersteuning, tot gegevens met betrekking tot vergunningen.

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 ermee omgaan, maar een volledig overzicht van welke gevoelige informatie de afdeling precies heeft en hoe er mee om wordt gegaan, ontbreekt. Daarom is gevraagd om een verkennend onderzoek, om dit voor de afdeling in beeld te brengen.

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 VJB 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 VJB 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 jaarlijkse verantwoording van VJB 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 opgehaald bij specifieke medewerkers binnen de afdeling die inzicht hebben in de materie van het bureau waarbinnen ze werkzaam zijn. Zij kunnen een overzicht van hun bureau bieden. De constateringen in dit stuk zijn voornamelijk op basis van indrukken en uitleg van de betrokken medewerkers. Omdat dit onderzoek ging om een verkenning op de afdeling, is niet tot in detail in systemen en correspondentie gekeken of steekproefsgewijs getoetst.

Samenvatting

Algemene afdrong

De afdeling maakt op meerdere plekken gebruik van persoonsgegevens. Het gebruik is divers omdat de bureau's binnen de afdeling zeer uiteenlopende werkzaamheden verrichten. Aan het verwerken van gegevens zitten grofweg twee elementen. Ten eerste het inregelen van veilige systemen, autorisaties en de afspraken daarom heen. Ten tweede 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 binnen de verschillende bureau's en dat de afgelopen jaren de nodige maatregelen zijn getroffen om risico's te minimaliseren. Daarmee lijkt VJB aardig op weg te zijn en in zekere mate *in control* te zijn. Wel is er een aantal maatregelen dat genomen kan/moet worden en blijft het nodig om in de bureaus met herhaling stil te staan bij AVG. Een datalek of onjuist gebruik van persoonsgegevens is niet uit te sluiten en kan relatief eenvoudig voorkomen. 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).

Wellicht een complicerende factor binnen de afdeling is het feit dat de verschillende bureau's zeer van elkaar verschillende werkzaamheden verrichten. Elk bureau heeft daarmee zeer specifieke risico's en vraagt om specifieke acties om die risico's te minimaliseren. Dit neemt echter niet weg dat de bevordering van AVG-bewust handelen continue aandacht vereist binnen de afdeling als geheel.

Voor zover het bewustwording onder medewerkers betreft, hebben wij begrepen dat in 2024 gemeentebreed een herhaalmodule van de leerlijnen privacy, informatiebeheer en informatieveiligheid gepland is. De verschillende bureau's zullen sturen op de deelname van hun medewerkers.

Hieronder volgt een samenvatting van de belangrijkste constatering per bureau.

Samenvatting per bureau

Bureau Juridische Zaken	
Globale stand van zaken	<p>Juridische Zaken (JZ) verzorgt naast juridische advisering, in het kader van de rechtsbescherming voor burgers, de afhandeling van bezwaren, klachten en inzageverzoeken. Daarnaast vertegenwoordigt JZ het college bij gerechtelijke procedures. Bij de afhandeling van de hiervoor genoemde zaken worden persoonsgegevens verwerkt en is sprake van archivering. Voor de behandeling van de procedures wordt een workflowapplicatie, JZ4All gebruikt die alleen NAW-gegevens bevat en soms een BSN. Documenten die bij de procedures gebruikt worden, kunnen meerdere persoonsgegevens bevatten. Ze worden bewaard in de gemeentelijke archiefapplicatie, Corsa. JZ4All biedt de mogelijkheid van een koppeling naar Corsa.</p> <p>Beide genoemde applicaties zijn alleen toegankelijk binnen de Citrix-omgeving indien men daartoe geautoriseerd is (alleen procesjuristen, administratie en manager JZ).</p> <p>Ondanks dat dossiers, zoals hiervoor is aangegeven, digitaal zijn, wordt ook gewerkt met papieren dossiers wanneer sprake is van gerechtelijke procedures. Dit omdat de rechtspraak niet digitaal werkt en stukken op papier dienen te worden aangeleverd.</p> <p>Voor alle procedures, met uitzondering van de inzageverzoeken en klachten, geldt dat de administratie van JZ bij de aanvang een dossier vormt. Dit kan een digitaal of een papieren (gerechtelijke procedures) dossier zijn. Voor de vorming van het dossier worden documenten</p>

	bij andere afdelingen opgevraagd (en eventueel digitaal gemaakt indien nodig) of uit Corsa gehaald. Papieren dossiers worden door het bureau bewaard in afsluitbare archiefkasten. Stukken worden gedeeld met bezwaarden, vergunninghouders, advocaten en gemachtigden. Indien persoonsgegevens per mail worden verzonden, dan wordt hiervoor veilig mailen gebruikt. Medewerkers zijn bekend met deze mogelijkheid en kunnen deze inzetten. Soms wordt gebruik gemaakt van Nextcloud als er grotere bestanden moeten worden verzonden.
Belangrijkste systemen	JZZ4All (workflowapplicatie) Corsa (archiefapplicatie) Mail (Outlook)
Belangrijkste risico's	<ul style="list-style-type: none"> - gebruik van papieren dossiers (gerechtelijke procedures) die ook door medewerkers mee naar huis en naar de rechtszittingen worden genomen. Risico van onbeheerd achterlaten, verlies, in verkeerde handen vallen; - Onbedoeld delen van persoonsgegevens met derden in brieven en documentverkeer. Bijvoorbeeld het delen van meer dan naam en adres van bezwaarden met een vergunninghouder, het versturen van de verkeerde stukken aan bezwaarden, vergunninghouders, advocaten en/of gemachtigden; - Onbedoeld delen van persoonsgegevens door onbeheerd achterlaten van laptop en daarmee toegang verschaffen aan onbevoegden; - Verzuimen persoonsgegevens via onbeveiligde mail te verzenden; - Bij gebruik van Nextcloud verzuimen om de aangemaakte mappen daarna te verwijderen.
Mogelijke acties	<p>Voorname risico's zien allemaal op houding en gedrag en menselijk handelen. Om de risico's te minimaliseren is het zaak om bij medewerkers voldoende i-bewustzijn te creëren en te onderhouden. Hiertoe volgen nieuwe medewerkers verplichte online onboardingsleerlijnen op dit gebied. Ook zijn deze met regelmaat organisatiebreed verplicht voor zittende medewerkers. In de werkoverleggen is het goed om het onderwerp levend te houden en ook incidenten die zich voordoen steeds te bespreken en te benoemen om hiervan te leren.</p> <p>Verder valt nog te vermelden dat bij JZ in januari twee nieuwe medewerkers gaan starten die zich onder andere met Privacy bezig gaan houden.</p>

Bureau Strategie, Public Affairs, Onderzoek en Statistiek	
Globale stand van zaken	<p>Binnen het bureau worden bij het onderdeel Onderzoek en Statistiek (O en S) persoonsgegevens verwerkt. De werkwijze houdt in dat voor statistiekdoeleinden met een vast frequentie (meestal jaarlijks) basisbestanden worden verzameld en bewerkt. Denk hierbij bijvoorbeeld aan bevolkingsbestand, WOZ-bestanden, Leerlingengegevens. Daarnaast worden voor specifieke onderzoeken of informatievragen incidenteel databestanden gemaakt/verkregen/gebruikt. Tot slot is sprake van de benadering en informatieverzameling bij respondenten in het kader van allerlei onderzoeken.</p> <p>Men conformeert zich aan de Gedragsregels voor Onderzoek van de VSO (Vereniging voor Statistiek en Onderzoek), MOA (Center for Information Based Decisionmaking and Marketing Research) en VBO (Vereniging voor Beleidsonderzoek). Deze zijn in 2021 voorgelegd aan de Autoriteit Persoonsgegevens. In specifieke onderzoekssituaties bieden deze regels soms onvoldoende houvast. Daarom worden handelingsgerichte protocollen geschreven voor veelvoorkomende onderzoekssituaties. Daarbij wordt ook gebruik gemaakt van de input van specialisten bij Juridische Zaken. De protocollen worden bewaard op de gemeenschappelijke schijf van O en S. Wanneer gebruik gemaakt wordt van enquetebureau's worden gegevens nodig voor benadering gedeeld via een beveiligde omgeving en verwerkingsovereenkomsten afgesloten.</p> <p>Er is een privacyambassadeur aangewezen binnen het onderdeel.</p>
Belangrijkste systemen	SPS6 (bewerkingstool) R (bewerkingstool) MWM2 (enquetetool)

	Mail (Outlook)
Belangrijkste risico's	<ul style="list-style-type: none"> - Toegang tot gegevens door onbevoegden (via mail of niet afsluiten computer); - Delen verkeerde of andere gegevens met enquetebureau; - Taken en verantwoordelijkheden privacyambassadeur onvoldoende duidelijk.
Mogelijke acties	<ul style="list-style-type: none"> - Voor basisbestanden worden persoonsgegevens gescheiden bewaard van overige gegevens. Op termijn volledige verwerking in datawarehouse; - Voor incidentele databestanden de werkwijze aanpassen door ook hier persoonsgegevens en inhoud apart te bewaren, zodat geen koppeling aanwezig is; - Oude incidentele databestanden (waar geen scheiding is tussen persoonsgegevens en inhoud) opruimen; - Taken en verantwoordelijkheden privacyambassadeur helder maken en positie binnen bureau verankeren; - Bewustwording onder medewerkers realiseren en onderhouden.

Bureau Communicatie	
Globale stand van zaken	<p>Binnen het bureau wordt gebruik gemaakt van een beeldbank waar foto's in worden opgeslagen. Voor deze tool is er in samenwerking met Juridische zaken een verwerkersovereenkomst opgezet. Daar staan regelmatig ook personen op. Men wil graag dat deze personen toestemming geven om op de foto te gaan. Daar wordt een toestemmingsformulier voor gebruikt. Op social media worden ook foto's geplaatst waar mensen opstaan. Mochten er inwoners op een foto staan die dit niet willen dan hebben is het beleid om deze foto bij een melding te verwijderen van de social media kanalen. Hiervoor is in overleg met Juridische Zaken gekozen. Onder journalistieke vrijheid is het niet verplicht om van iedereen een verklaring te hebben. Er wordt echter wel geprobeerd zoveel mogelijk expliciete toestemming te krijgen.</p> <p>Het Bureau geeft voorts een corporate nieuwsbrief uit. Deze bestond al vóór de invoering van de AVG. Bij het aanmelden voor de nieuwsbrief gaven inwoners verschillende gegevens op. Bij de invoering van de AVG zijn deze (niet noodzakelijke) aanvullende gegevens van de abonnees verwijderd. Er wordt scherp op gelet alleen de noodzakelijke gegevens te verzamelen.</p> <p>Het Team online houdt zich bezig met Nijmeegse websites. Wanneer een afdeling een nieuwe website wil ontwikkelen dan gaan ze een intakeproces in. In dit intakeproces is de AVG als onderdeel meegenomen.</p>
Belangrijkste systemen	<ul style="list-style-type: none"> - Beeldbank - Social Mediakanalen gemeente Nijmegen - Mail (Outlook)
Belangrijkste risico's	<ul style="list-style-type: none"> - Delen/publiceren van foto's van personen zonder dat zij hiervoor toestemming hebben gegeven; - Toegang tot gegevens door onbevoegden (via onbeveiligde mail, niet afsluiten computer).
Mogelijke acties	<ul style="list-style-type: none"> - Voor het gebruik van de beeldbank is een verwerkingsovereenkomst opgezet. Daarnaast zoveel mogelijk werken met toestemmingsverklaringen. Gebruik maken van de journalistieke vrijheid binnen de marges van redelijkheid, zoals in ieder geval het verwijderen van foto's al hierom wordt verzocht; - Bewustwording onder medewerkers realiseren en onderhouden.

Bureau's Veilige & Weerbare Stad en Veilige & Zorgzame Stad	
Globale stand van zaken	<p>Veiligheid kent meerdere basisprocessen, verdeeld over de twee bureaus. Er is bij beide bureaus de afgelopen jaren merkbaar meer aandacht en bewustzijn gekomen voor naleving van de AVG. Zo is er hard gewerkt aan het (ook met terugwerkende kracht) op orde brengen van</p>

	<p>DPIA's van verwerkingen.¹ Jaarlijks vindt terugkoppeling over de naleving hiervan richting de FG plaats. Bij de (door)ontwikkeling van nieuwe systemen wordt gewerkt vanuit het principe privacy-by-design. Tot slot is er in de periode 2022/2023 een interne audit uitgevoerd bij het Zorg- en Veiligheidshuis Gelderland-Zuid en is het 'Privacy protocol meldpunt ondermijning' vastgesteld.</p> <p>Bureau Veilige en Weerbare Stad kent een aantal teams/basisprocessen:</p> <ul style="list-style-type: none"> • De integrale en bestuurlijke aanpak van ondermijning • Uitvoering van Wet Bibob • De aanpak i.r.t. veilige wijken • Vergunningverlening i.r.t. veilige horeca en evenementen • Werkzaamheden i.r.t. openbare orde en bestuursadvisering <p>Bureau Veilige en Zorgzame Stad kent een aantal teams/basisprocessen:</p> <ul style="list-style-type: none"> • De diverse tafels binnen het Zorg- en Veiligheidshuis • De aanpak i.r.t. de Jeugdcoaches • De aanpak i.r.t. de Regieteams • De Doorbraakaanpak & KOT
Belangrijkste systemen	<ul style="list-style-type: none"> - PGAx (Veilige & Zorgzame Stad) - VIP (Veilige horeca en evenementen) - Tableau (Veilige wijken) - G-schijf & gemeenschappelijke schijf - Extra beveiligde schijf Veiligheid - RIECIS portal (Integrale aanpak van ondermijning) - Analyst's Notebook (Integrale aanpak van ondermijning) - Khonraad/BOPZ Online (landelijk systeem Wet Wvvgz, Wet Wzd en Wet Tijdelijk huisverbod) - LCMS (landelijk crisismanagementsysteem) - Microsoft (Word, Outlook, Excel etc.) - iPhone
Belangrijkste risico's	<p>Autorisaties</p> <p>Voor verwerkingen geldt dat het risico op een datalek of diefstal van gegevens nooit geheel valt uit te sluiten. Deze risico's zitten vooral op het niveau van medewerkers. Er worden maatregelen genomen om de risico's te verkleinen, bijvoorbeeld door slechts een beperkt aantal medewerkers te autoriseren voor een systeem, mailbox of map. Het autoriseren van medewerkers voor netwerkmappen, mailboxen en systemen gebeurt (gemeente breed) nog veelal handmatig. Hierin schuilt een risico: het is een kwestie van oplettendheid van managers en medewerkers om autorisaties op te heffen wanneer iemand bijvoorbeeld van functie wisselt. Dit risico wordt in meerdere DPIA's benoemd. Hier is nog geen passende oplossing voor.</p> <p>Bewaren en archiveren</p> <p>De managers van de twee bureaus zijn eindverantwoordelijk voor het bewaken van de vastgestelde termijnen en afspraken met betrekking tot gegevensvernietiging, -archivering en -opslag. Voor een aantal werkprocessen is het archiveren en/of vernietigen van gegevens geautomatiseerd, bijvoorbeeld omdat dit in het desbetreffende systeem is ingericht. Echter geldt dit niet voor alle werkprocessen.</p> <p>Eerder heeft er een audit informatie- en archiefbeheer afdeling Veiligheid plaatsgevonden op de onderdelen gezagsdriehoek, ondermijning en Bibob. Hieruit bleek dat in sommige werkprocessen buiten het centrale archiefsysteem Corsa om wordt gewerkt, omdat door de werking van systemen als Corsa en soortgelijke oplossingen (bijv. ook Sharepoint) de toegang tot bestanden niet voldoende goed te beveiligen is. In plaats daarvan wordt gewerkt op</p>

¹O.a. DPIA's Woninginbraak, DPIA's Hennep, DPIA VIK, DPIA MOR-meldingen Overlast, DPIA Kaartviewer Jaarwisseling, DPIA IGP, DPIA Veiligheid anonieme accounts, DPIA Zorg- en Veiligheidshuis, DPIA Jeugdcoaches, DPIA Regieteams.

	afgeschermd netwerksschijven. Hiervoor geldt dat documenten wel goed worden afgeschermd, maar niet altijd goed beschermd: de verkenner mist essentiële archieffunctionaliteiten als documenten bevriezen, metadata over documenten toevoegen, versiebeheer of vernietiging. Correcte archivering (incl. naleving bewaartermijnen) is bij deze werkprocessen afhankelijk van oplettendheid en discipline van de betrokken medewerkers en managers. Er wordt nader onderzocht of er voor de desbetreffende werkprocessen een passende oplossing bestaat.												
Mogelijke acties	<ul style="list-style-type: none"> • Halfjaarlijkse check op autorisaties van systemen, netwerkmappen en mailboxen door managers. • Halfjaarlijkse opschoonactie netwerkmappen per werkproces door medewerkers. • Gemeentebrede afspraken over opschonen van mail en telefoon, vb. halfjaarlijks opschoonactie telefoon en mailboxen per werkproces door medewerkers. • Opfrissen afspraken over archivering van data per werkproces. • Er lopen gesprekken met I&A, omdat er voor een aantal werkprocessen die, zoals eerder genoemd, geen gebruik kunnen maken van Corsa, behoefte is aan een ICT oplossing die ondersteuning biedt in a) Veilige en overzichtelijke opslag van bestanden; b) Goed geborgde en gemakkelijke archivering; c) Gemakkelijk genereren van managementinfo; en d) Minimale workflow (status van een zaak en bestanden kunnen voorzien van metadata). • Het uitvoeren van DPIA's op nieuwe werkprocessen. • Bewustwording onder medewerkers realiseren en onderhouden. <table border="1"> <tr> <td>Halfjaarlijkse check op autorisaties van systemen, netwerkmappen en mailboxen door managers.</td><td>Elk halfjaar</td></tr> <tr> <td>Halfjaarlijkse opschoonactie netwerkmappen per werkproces door medewerkers.</td><td>Elk halfjaar</td></tr> <tr> <td>Gemeentebrede afspraken over opschonen van mail en telefoon, vb. halfjaarlijks opschoonactie telefoon en mailboxen per werkproces door medewerkers.</td><td>Afhankelijk van gemeentelijke ontwikkelingen</td></tr> <tr> <td>Opfrissen afspraken over archivering van data per werkproces.</td><td>Nader te bepalen</td></tr> <tr> <td>Er lopen gesprekken met I&A, omdat er voor een aantal werkprocessen die, zoals eerder genoemd, geen gebruik kunnen maken van Corsa, behoefte is aan een ICT oplossing die ondersteuning biedt in a) Veilige en overzichtelijke opslag van bestanden; b) Goed geborgde en gemakkelijke archivering; c) Gemakkelijk genereren van managementinfo; en d) Minimale workflow (status van een zaak en bestanden kunnen voorzien van metadata).</td><td>Q1-Q2 2024</td></tr> <tr> <td>Het uitvoeren van DPIA's op nieuwe werkprocessen.</td><td>Doorlopend</td></tr> </table>	Halfjaarlijkse check op autorisaties van systemen, netwerkmappen en mailboxen door managers.	Elk halfjaar	Halfjaarlijkse opschoonactie netwerkmappen per werkproces door medewerkers.	Elk halfjaar	Gemeentebrede afspraken over opschonen van mail en telefoon, vb. halfjaarlijks opschoonactie telefoon en mailboxen per werkproces door medewerkers.	Afhankelijk van gemeentelijke ontwikkelingen	Opfrissen afspraken over archivering van data per werkproces.	Nader te bepalen	Er lopen gesprekken met I&A, omdat er voor een aantal werkprocessen die, zoals eerder genoemd, geen gebruik kunnen maken van Corsa, behoefte is aan een ICT oplossing die ondersteuning biedt in a) Veilige en overzichtelijke opslag van bestanden; b) Goed geborgde en gemakkelijke archivering; c) Gemakkelijk genereren van managementinfo; en d) Minimale workflow (status van een zaak en bestanden kunnen voorzien van metadata).	Q1-Q2 2024	Het uitvoeren van DPIA's op nieuwe werkprocessen.	Doorlopend
Halfjaarlijkse check op autorisaties van systemen, netwerkmappen en mailboxen door managers.	Elk halfjaar												
Halfjaarlijkse opschoonactie netwerkmappen per werkproces door medewerkers.	Elk halfjaar												
Gemeentebrede afspraken over opschonen van mail en telefoon, vb. halfjaarlijks opschoonactie telefoon en mailboxen per werkproces door medewerkers.	Afhankelijk van gemeentelijke ontwikkelingen												
Opfrissen afspraken over archivering van data per werkproces.	Nader te bepalen												
Er lopen gesprekken met I&A, omdat er voor een aantal werkprocessen die, zoals eerder genoemd, geen gebruik kunnen maken van Corsa, behoefte is aan een ICT oplossing die ondersteuning biedt in a) Veilige en overzichtelijke opslag van bestanden; b) Goed geborgde en gemakkelijke archivering; c) Gemakkelijk genereren van managementinfo; en d) Minimale workflow (status van een zaak en bestanden kunnen voorzien van metadata).	Q1-Q2 2024												
Het uitvoeren van DPIA's op nieuwe werkprocessen.	Doorlopend												

Globale stand van zaken	<p>Binnen dit bureau wordt gebruik gemaakt van iBabs. iBabs wordt gebruikt ter ondersteuning van de vergaderprocessen van zowel de organisatie, college, raad en rekenkamer. Daarnaast worden de agenda's vanuit iBabs (geautomatiseerd) gearcheveerd wat zorgt voor een beter archiveerproces.</p> <p>iBabs verwerkt en beheert persoonsgegevens van gebruikers, zoals namen, e-mailadressen en andere relevante informatie die nodig is voor het beheren van vergaderingen en documenten. Als zodanig moet de verwerking van deze persoonlijke gegevens voldoen aan de wettelijke vereisten en principes van gegevensbescherming.</p> <p>Er worden persoonsgegevens verwerkt die alleen zichtbaar zijn voor (geautoriseerde) gebruikers van iBabs maar ook gegevens die worden gepubliceerd op de website (laatste na expliciete toestemming van betrokkene). Het gaat hierbij om namen, woonadressen, emailadressen, geboortedatums.</p> <p>Persoonsgegevens worden nooit gepubliceerd op de website, uitgezonderd namen van insprekers of schrijvers van een brief nadat toestemming van publicatie is verkregen.</p> <p>Met het oog op bovenstaande is een DPIA gemaakt. Hierbij is onlangs geoordeeld dat de risico's aanvaardbaar zijn.</p>
Belangrijkste systemen	iBabs
Belangrijkste risico's	<p>Ongeoorloofde toegang: Er bestaat een risico dat onbevoegde personen toegang krijgen tot de gegevens in iBabs. Dit kan leiden tot ongeautoriseerd gebruik, misbruik of onthulling van persoonsgegevens, wat de privacy en vertrouwelijkheid van betrokkenen in gevaar kan brengen.</p> <p>Datalekken: Ondanks de beveiligingsmaatregelen kunnen er nog steeds risico's bestaan op datalekken. Dit kan bijvoorbeeld optreden als gevolg van technische storingen, menselijke fouten, cyberaanvallen of andere beveiligingsincidenten. Datalekken kunnen leiden tot ongeautoriseerde toegang tot persoonsgegevens en het risico van identiteitsdiefstal, fraude of andere vormen van schade voor betrokkenen.</p> <p>Onjuiste gegevensverwerking: Er bestaat een risico dat de gegevens in iBabs onjuist of onvolledig worden verwerkt. Dit kan leiden tot foutieve besluitvorming, onnauwkeurige rapportage of andere negatieve gevolgen voor betrokkenen.</p> <p>Gegevensbewaartermijn: Als de gegevens in iBabs langer worden bewaard dan noodzakelijk, kan dit een risico vormen voor betrokkenen. Langdurige opslag van persoonsgegevens verhoogt het potentieel voor ongeoorloofde toegang, datalekken of ongeoorloofd gebruik van gegevens.</p> <p>Gebruik van derde partijen: Als iBabs gebruikmaakt van derde partijen voor gegevensverwerking, bestaat er een risico op ongeoorloofde toegang of onjuiste verwerking van gegevens door deze partijen.</p>

Mogelijke acties	<p>Het is noodzakelijk om een autorisatiestructuur op te zetten met het daar bijhorende toezicht daarop. Op dit moment is deze structuur er niet. Dit wordt in gang gezet.</p> <p><u>Planning:</u> De autorisatiestructuur is inmiddels beschikbaar. Het toezicht wordt begin 2024 in gang gezet.</p> <p>De logging in iBabs is onvoldoende. Er is slechts te zien wie als laatste een agenda heeft gepubliceerd. Van belang is om terug te kunnen zien welke wanneer de agenda heeft gepubliceerd maar ook welke gebruiker wanneer welk document heeft geopend. Hierin moeten ook externe gebruikers worden meegenomen.</p> <p><u>Planning:</u> Dit wordt meegenomen in een gesprek met de leverancier medio januari 2024. Men is echter wel volledig afhankelijk van de medewerking van de leverancier.</p> <p>Het is risico op een onrechtmatige gegevensverwerking wordt minimaal geacht. In de digitale wereld is geen enkel risico volledig uit te sluiten. Hetzelfde geldt voor gebruik van iBabs.</p>
-------------------------	---