PBLQ

De bescherming van persoonsgegevens in Papendrecht

Rekenkamer van Papendrecht
Definitieve versie
23 december 2024

Inhoudsopgave

Bestuurlijke Rapportage

1. Bevindingen, conclusies en aanbevelingen

1.1 Overzicht van de bevindingen

Gemeenten beheren veel gegevens van inwoners. Binnen een gemeente vindt de registratie in het bevolkingsregister plaats, melden inwoners zich voor een vergunning, een uitkering, of vragen om zorg of ondersteuning. Inwoners moeten ervan uit kunnen gaan dat hun gegevens bij de gemeente in veilige handen zijn. Gemeenten moeten dat vertrouwen verdienen, zowel in de directe contacten met de burger als in verantwoording achteraf.

In 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Deze verordening betreft een uitwerking van Europese regelgeving die bedoeld is om de privacy van alle inwoners (beter) te beschermen. Als gevolg van de AVG lopen gemeenten risico op boetes in het geval zij niet conform de geldende normen de beveiliging van persoonsgegevens op orde hebben. Het maatschappelijk en financieel belang van een adequaat privacybeleid is daarom al met al groot. Gemeenten hebben bovendien niet alleen een goed privacybeleid nodig, maar ook een goede uitvoering daarvan.

Korte Inleiding op de Algemene Verordening Gegevensbescherming (AVG)[1]

De *AVG* heeft tot doel om de privacy van burgers te beschermen. Onder meer is in de AVG vastgelegd dat informatie van personen alleen mag worden verzameld als daar een belang mee is gemoeid dat opweegt tegen het feit dat de burgers deze informatie over hunzelf afstaan. De instantie die deze gegevens beheert (de gemeente), heeft de verplichting deze adequaat te beschermen. Gemeenten moeten kunnen aantonen dat ze zich aan de wet houden. Om ervoor te zorgen dat dit inderdaad het geval is, zijn er voor organisaties als gemeenten verschillende waarborgen, procedures en functionarissen van belang. Deze zijn:

- *Privacy bij Design*: Dit houdt in dat al bij het ontwerpen van producten en diensten er wordt gezorgd dat persoonsgegevens goed worden beschermd. Onder meer moet zijn vastgelegd dat gegevens niet langer bewaard worden dan nodig is voor het doel van de verwerking.
- *Functionaris Gegevensbescherming*: Gemeenten zijn verplicht een Functionaris Gegevensbescherming (FG) aan te stellen. Deze functionaris houdt toezicht op de toepassing en naleving van de AVG.
- *Data Protection Impact Assessment*: De AVG verplicht gemeenten om een data protection impact assessment (DPIA) uit te voeren wanneer zij persoonsgegevens gaan verwerken. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen, mede om vervolgens maatregelen te kunnen nemen ter verkleining en beheersing van de risico's. Zolang de gegevensverwerking gaande is, moet een DPIA met enige regelmaat geactualiseerd worden. Hierbij wordt bekeken of er eventueel nieuwe of andere privacyrisico's zijn, en of de maatregelen die zijn genomen ter bescherming van persoonsgegevens nog voldoende effectief zijn.
- *Verwerkingsregisters:* Gemeenten zijn verplicht om een verwerkingsregister bij te houden. Dit register bevat informatie over de persoonsgegevens die door de organisatie worden verwerkt. Het register moet tevens informatie bevatten over:

[1] Zie voor een uitgebreide uitleg voor diverse begrippen en procedures: notendop_avg.pdf (autoriteitpersoonsgegevens.nl)

- de naam en contactgegevens van de organisatie of de vertegenwoordiger van de organisatie,
- eventuele andere organisaties met gezamenlijke doelen en middelen van de verwerking zijn vastgesteld,
- de gegevens van de aangestelde FG,
- eventuele andere organisaties waar persoonsgegevens mee worden gedeeld,
- de doeleinden waarvoor de persoonsgegevens worden verwerkt,
- de categorieën van personen van wie gegevens worden verwerkt,
- de categorieën van persoonsgegevens die worden verwerkt,
- de bewaartermijn van de persoonsgegevens en
- de categorieën van ontvangers aan wie persoonsgegevens worden verstrekt.

- Een veilige omgang met gegevens is ook zeer gediend met het inrichten en naleven van een gedegen *informatiebeveiligingsbeleid*. Gemeenten stellen daartoe vaak een *Chief Information Security Officer (CISO*) aan, die verantwoordelijk is voor het informatiebeveiligingsbeleid. Dit is niet verplicht volgens de AVG, maar wel te doen gebruikelijk. De CISO houdt zich bezig met het implementeren van het informatiebeveiligingsbeleid, en houdt toezicht op de uitvoering ervan. De CISO is ook verantwoordelijk voor de strategie op het gebied van informatiebeveiliging.
- Gemeenten zijn op grond van de AVG verplicht om een *Privacy Officer (PO)* te hebben. Een PO zorgt ervoor dat de AVG wordt nageleefd binnen een organisatie. Ook ziet een PO erop toe dat de privacy en dataverwerking bij elke medewerker die persoonsgegevens verzamelt of verwerkt in veilige handen is. Een PO geeft advies en biedt ondersteuning binnen zijn organisatie, geeft interne trainingen en heeft een rol bij het melden van datalekken. In Papendrecht wordt voor deze functionaris de titel Privacy Coördinator gebruikt.
- Burgers hebben verschillende *rechten om controle uit te oefenen* op de naleving van de AVG. Dit betreft onder meer het *recht op inzage van hun persoonsgegevens.*
- Een gemeente werkt vaak samen met andere organisaties voor het uitvoeren of ondersteunen van taken. Dit kan een bedrijf zijn, een andere gemeente of bijvoorbeeld een gemeenschappelijke regeling. Zo'n andere organisatie heet een *verwerker* van persoonsgegevens. De gemeente blijft in principe zelf eindverantwoordelijk voor de privacy van de persoonsgegevens van zijn inwoners. In AVG termen is de gemeente de *verwerkingsverantwoordelijke.* Wanneer een andere organisatie persoonsgegevens verwerkt moet er altijd een *verwerkersovereenkomst* worden afgesloten tussen beide partijen. Hierin worden afspraken gemaakt over zaken als het doel van de verwerking, geheimhoudingsplicht, beveiliging, verwijderingstermijnen en auditverplichtingen. Het kan ook gebeuren dat de organisatie waarmee de gemeente samenwerkt zelf ook verwerkingsverantwoordelijke is. Dat gebeurt wanneer die organisatie zelf kan bepalen welke persoonsgegevens worden verwerkt, hoe deze gegevens worden verzameld en hoe lang ze worden bewaard. In dat geval is er geen verwerkersovereenkomst nodig ten behoeve van de samenwerking. Of een organisatie waarmee de gemeente samenwerkt verwerkingsverantwoordelijke is, wordt bepaald op basis van de feitelijke omstandigheden.
- De Vereniging van Nederlandse Gemeenten heeft in samenwerking met andere (belangenorganisaties van) overheden de *Baseline Informatiebeveiliging Overheid (BIO)*[2] ingericht. In de BIO is het basisniveau voor informatiebeveiliging beschreven. Er zijn verschillende toetsen en monitoren ontwikkeld waarmee overheden kunnen bepalen of en in

[2] De voorloper van de BIO was de Baseline Informatiebeveiliging Gemeenten (BIG)

welke mate ze voldoen aan de BIO. Dit betreft onder meer de *ENSIA*. Deze afkorting betreft de ‘Eenduidige Normatiek Single Information Audit’.

Voor de verwerking van persoonsgegevens binnen het ambtelijk apparaat van een gemeente is naast de AVG ook de Wet politiegegevens (Wpg) van belang. Deze wet geldt sinds 2018, op basis van de Europese Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn EU 2016/680). Deze richtlijn verplicht lidstaten tot het creëren van nationale wetgeving voor het verwerken van persoonsgegevens die gaan over voorkoming, onderzoek, opsporing en vervolging van strafbare feiten. Voor zover relevant voor gemeenten gaat het hier in de praktijk om het verwerken van persoonsgegevens door Buitengewoon Opsporingsambtenaren (boa’s). Het gaat hierbij om situaties waarin zij hun bevoegdheden op grond van het strafrecht gebruiken, bijvoorbeeld door een verkeersboete op te leggen. De eisen van de Wpg overlappen inhoudelijk voor een aanzienlijk deel met die van de AVG, bijvoorbeeld waar het gaat om de verplichting een verwerkingenregister bij te houden en een Functionaris Gegevensbescherming aan te stellen. Er zijn echter ook verschillen. Bij de Wet politiegegevens is wettelijk bepaald wie verwerkingsverantwoordelijke is, terwijl dit bij de AVG uit de feitelijke omstandigheden moet blijken. Ook kent de Wpg wettelijk vastgestelde bewaartermijnen, en verdergaande verplichtingen met betrekking tot gebruikers van politiegegevens, zoals de verplichting om bij te houden wie welke gegevens bekijkt (logging). Bovendien kent de Wpg de verplichting voor gemeenten om elk jaar een interne audit uit te voeren, en eens per vier jaar een externe audit. Vanwege de overlap in verplichtingen tussen AVG en Wpg is het goed mogelijk en vanuit het oogpunt van synergie zelfs voordelig om tegelijkertijd onderzoek te doen naar de implementatie van beide binnen één gemeente.

1.2 Beantwoording onderzoeksvragen

Bij aanvang van het onderzoek is een centrale probleemstelling geformuleerd. Deze probleemstelling, en het antwoord daarop zijn als volgt:

Centrale onderzoeksvraag

Hoe wordt de privacy van de Papendrechtse inwoners beschermd en wordt er adequaat gebruik gemaakt van de AVG en Wpg, ook gelet op derden aan wie de uitvoering van beleid is uitbesteed, of met wie anderszins persoonsgegevens worden gedeeld? En op welke wijze wordt de gemeenteraad in staat gesteld de privacybescherming periodiek te controleren?

Om deze centrale vraag te kunnen beantwoorden, heeft de rekenkamer een aantal deelonderzoeksvragen opgesteld. Deze vragen en de antwoorden daarop zijn opgenomen in onderstaand overzicht.

Onderzoeksvragen

1	*Hoe biedt de gemeente Papendrecht bescherming aan inwoners als het gaat om privacy?*
Antw.	Er staat een actuele privacyverklaring op de website van de gemeente, waarin inwoners kunnen lezen wat hun rechten zijn op grond van de AVG en de Wpg. Papendrecht heeft vastgestelde werkprocessen voor de ambtenaren met betrekking tot de rechten van betrokkenen. Er is bijvoorbeeld een werkproces om verzoeken om inzage in persoonsgegevens af te handelen en een werkproces om persoonsgegevens te corrigeren op verzoek van een inwoner. Inwoners doen echter zelden verzoeken op

	grond van de AVG of de Wpg. Er zijn bovendien maar twee bekende klachten over de AVG geweest, die beide ongegrond bleken. Het privacybeleid van de gemeente is bovendien conform de AVG waar het gaat om het waarborgen van de rechten van betrokkenen. Er zijn echter wel de nodige bevindingen geconstateerd met betrekking tot de uitvoering van de werkprocessen van de gemeente in de praktijk. De uitvoeringspraktijk in de gemeente voldoet in de praktijk op een aantal punten nog niet of niet geheel aan de eisen die hiervoor gelden op grond van de AVG en de Wpg. Dit komt mede door gebrek aan capaciteit binnen de ambtelijke organisatie. Hierdoor ontstaan mogelijk risico's voor de bescherming van persoonsgegevens van inwoners van Papendrecht.
2	*Wat is de stand van zaken van de uitvoering AVG en Wpg?*
Antw.	Voor wat betreft de **AVG** heeft Papendrecht zijn processen op papier grotendeels in orde, maar schort het op een aantal punten aan uitvoering in de praktijk. Zo is er door gebrek aan capaciteit bij de Privacy Coördinatoren en bij de uitvoerende teams in de afgelopen jaren een flinke achterstand opgebouwd met betrekking tot het uitvoeren van DPIA's. Dit is al een aantal jaren het geval, en wordt tot op heden niet of nauwelijks ingelopen. Bovendien lijkt het nog geen automatisme binnen de organisatie dat er een DPIA moet worden uitgevoerd bij nieuwe verwerkingen van gegevens. Vaak is de verwerking bovendien al gestart voordat de DPIA is afgerond, en voordat de aanbevolen risicobeperkende maatregelen zijn genomen. Wel is er een standaardaanpak aanwezig voor nieuwe wijzigingen en/of projecten. Ook komt het voor dat de risicobeperkende maatregelen die naar aanleiding van een DPIA worden vastgesteld niet (aantoonbaar) worden genomen. Na afloop van een DPIA wordt niet altijd verslag gedaan aan de FG over de daadwerkelijk genomen risicobeperkende maatregelen, zoals op grond van het door Papendrecht vastgestelde werkproces voor DPIA's verplicht is. DPIA's worden ook niet na de in dit werkproces vastgestelde termijn opnieuw bezien. De samenwerking met de FG is sinds het aantreden van de nieuwe FG's sterk verbeterd, met name op het niveau van de medewerkers en de teamleiders. Wel is de betrokkenheid van de FG op een aantal punten nog *ad hoc* en afhankelijk van de goede wil en het eigen initiatief van betrokkenen. Ook hier is bovendien nog sprake van een achterstand, die mede veroorzaakt is door gebrek aan capaciteit en kennis binnen de gemeentelijke organisatie. Zo lijky een aantal maatregelen dat in drie opeenvolgende jaarlijkse FG-adviezen door twee verschillende FG's werd aanbevolen nog niet genomen, voor zover kon worden vastgesteld op basis van de beschikbare informatie. Ook op het gebied van privacy bewustzijn en kennisborging en -ontwikkeling is er op papier een goede aanpak door middel van een jaarlijkse nascholingsmaand voor de hele organisatie, maar wordt in de praktijk uitgegaan van deelname op basis van vrijwilligheid. Bovendien zijn privacy bewustzijn en kennisborging en -ontwikkeling nog in onvoldoende mate geïntegreerd in de reguliere werkprocessen en overleggen van alle betrokken teams en medewerkers van de gemeente. Het is iets wat medewerkers erbij moeten

	doen naast hun reguliere taken, terwijl het een integraal onderdeel van de uitvoering van hun reguliere taken zou moeten zijn. Wel is in dit onderzoek tevens geconstateerd dat de gemeente recent een heel aantal verbeteringen in gang heeft gezet op het gebied van gegevensbescherming en privacy, waaronder het inzetten van meer capaciteit. Deze verbeteringen hebben in de afgelopen periode ook tot een aantal concrete resultaten geleid, zoals een verbeterd register van verwerkingen. De capaciteit van de Privacy Coördinatoren is recent versterkt, en op korte termijn zal een projectleider aantreden die belast is met het inlopen van de DPIA-achterstand. Of de maatregelen die de gemeente in gang heeft gezet voldoende zijn om in de toekomst wel aan de eisen van de AVG te voldoen kan echter op dit moment niet worden vastgesteld. Voor wat betreft de **Wpg** is in een externe audit in 2022 al geconstateerd dat Papendrecht op een groot aantal punten niet voldoet aan de eisen die deze wet stelt. Ten tijde van dit onderzoek was dit nog steeds het geval voor een deel van de eisen. De belangrijkste oorzaak hiervoor is de grote vertraging die is ontstaan bij het oppakken van de belangrijkste bevinding uit de audit: het aanschaffen van een nieuw Wpg-conform ICT-systeem. Inmiddels is er een nieuw ICT-systeem aangeschaft, dat zich momenteel in de implementatiefase bevindt. Naar verwachting zal dit systeem in de tweede helft van 2024 operationeel worden. Tot die tijd is het voor Papendrecht onmogelijk om aan de Wpg te voldoen, omdat de huidige ICT-systemen hiervoor niet toereikend zijn. Belangrijke redenen voor de opgelopen vertraging bij de aanschaf van nieuwe software waren een traag verlopend inkoopproces en het uitvoeren van een DPIA. Bovendien is er sprake van een risico in verband met de overgang naar het nieuwe ICT-systeem, omdat de leverancier van de oude systemen tot nog toe niet meewerkt aan het overdragen van de in de oude systemen opgeslagen gegevens. Dit betekent dat het risico bestaat dat alle politiegegevens die in de oude systemen zijn opgeslagen verloren gaan, als gevolg van de implementatie van het nieuwe systeem. Dit zou een forse inbreuk zijn op de eisen die gelden op grond van de Wpg.
3	*Op welke wijze is de raad tot nu toe bij de ontwikkeling van het privacybeleid betrokken geweest?*
Antw.	De raad heeft het geldende privacybeleid uit 2020 vastgesteld en heeft recent kennisgemaakt met de nieuwe FG’s, maar is verder beperkt betrokken bij de stand van zaken rond het privacybeleid. De gemeenteraad heeft weinig aandacht voor het onderwerp privacy. Privacy is geen onderwerp van gesprek in de gemeenteraad en beperkt onderwerp van (raads)vragen. Tijdens de raadsbijeenkomst die in het kader van dit onderzoek is georganiseerd hebben de drie aanwezige raadsleden aangegeven dat het onderwerp naar hun weten in de afgelopen twee jaar niet inhoudelijk aan bod is gekomen.
4	*Waar knelt de AVG/Wpg, waar zitten beperkingen en risico's?*
Antw.	De belangrijkste geconstateerde risico’s met betrekking tot de AVG en de Wpg hebben te maken met het feit dat de gemeente het privacybeleid op papier redelijk op orde lijkt te

	hebben, maar in de praktijk niet aan alle eisen op grond van de AVG en de Wpg wordt voldaan. Hierdoor ontstaan risico's op het gebied van de bescherming van persoonsgegevens. Papendrecht heeft op veel punten al wel verbeteringen in gang gezet, maar op dit moment kan niet worden vastgesteld of deze uiteindelijk voldoende zullen zijn om in de praktijk wel helemaal AVG- en Wpg-conform te werken, of per wanneer dit het geval zal zijn.
5	*Zijn de verantwoordelijkheden van de bij de uitvoering AVG betrokken functionarissen duidelijk belegd – bestuurlijk en ambtelijk?*
Antw.	De bestuurlijke en ambtelijke verantwoordelijkheden van de betrokken functionarissen zijn in het concept voor het nieuwe privacybeleid dat in het kader van dit onderzoek is meegenomen duidelijk belegd. In het geldende privacybeleid is dit veel minder het geval, het beoogde nieuwe beleid vormt op dit gebied een duidelijke verbetering.
6	*Wat is de rol van de OR ten aanzien van privacy en is deze duidelijk binnen de organisatie?*
Antw.	De OR heeft in het kader van de privacy instemmingsrecht op de verwerking van persoonsgegevens van medewerkers. Ook heeft de OR een adviesrol als het gaat om belangrijke technologische voorzieningen binnen de gemeente. In de praktijk zijn er in de recente geschiedenis echter niet veel privacy-gerelateerde onderwerpen waar de OR instemmings- of adviesrecht heeft gehad. Medewerkers kloppen bij de OR ook aan met vraagstukken of problemen die binnen de organisatie spelen. Dit kunnen allerlei verschillende zaken zijn (waaronder ook zaken met betrekking tot privacy en informatievoorziening). De OR heeft hierbij een werkwijze waarbij de identiteit en persoonsgegevens van medewerkers die zich bij hen melden verborgen worden gehouden, zodat eventuele belangrijke signalen kunnen worden doorgegeven aan de bestuurder zonder dat dit medewerkers potentieel schaadt of blootstelt. Hoewel er geen formeel protocol is vastgelegd over deze gang van zaken, is er wel een vaste praktijk. Medewerkers weten over het algemeen dat zij bij vragen of problemen bij de OR terecht kunnen. Het advies- en instemmingsrecht van de OR met betrekking tot de persoonsgegevens van medewerkers lijkt minder bekend te zijn binnen de rest van de organisatie.
7	*Wat zijn ongewenste en onnodige neveneffecten van de AVG: gebeurt het bijvoorbeeld dat informatie niet wordt gedeeld met een (oneigenlijk) beroep op de AVG?*
Antw.	Er zijn in het kader van dit onderzoek geen gevallen geconstateerd waarin informatie niet werd gedeeld met een oneigenlijk beroep op de AVG. Wel is een ongewenst neveneffect dat er in de uitvoering vertraging optreedt doordat het lang duurt om aan de op grond van de AVG geldende eisen te voldoen. Dit is bijvoorbeeld gebeurd bij de aanschaf van het nieuwe ICT-systeem ten behoeve van de Wpg, doordat het lang duurde voor hiervoor een DPIA was uitgevoerd en de benodigde maatregelen werden genomen. De belangrijkste oorzaak hiervoor is capaciteits- en kennisgebrek bij de ambtelijke organisatie.

8	*Op welke manier wordt de gemeenteraad geïnformeerd over de uitvoering van het beleid rondom de bescherming van persoonsgegevens? Welke mogelijkheden heeft de raad om te sturen en te controleren?*
Antw.	De enige manier waarop de gemeenteraad in Papendrecht voor zover bij ons bekend wordt geïnformeerd over de uitvoering van het beleid rondom de bescherming van persoonsgegevens is door middel van een korte paragraaf in de jaarrapportage in het hoofdstuk Bedrijfsvoering, en de vertrouwelijke bespreking van de jaarlijkse ENSIA-rapportage op het gebied van informatiebeveiliging. In de jaarrapportage wordt hoofdzakelijk procesmatig gecommuniceerd over de uitvoering van de AVG en de Wpg, deze bevatte in de onderzochte jaren weinig tot geen inhoudelijke informatie. De raad is daardoor beperkt in de positie om te sturen en te controleren, omdat de raad in onvoldoende mate over de hiervoor benodigde informatie beschikt. Naast deze formele informatievoorziening zijn er ook bijeenkomsten met de raad om hen te informeren over het beleid en de omgang met persoonsgegevens.
9	*Hoe monitort/verifieert de gemeente afspraken in verwerkersovereenkomsten met derden, waar knelt de AVG/Wpg, waar zitten beperkingen en risico's? Denk aan GGD, Veiligheidshuis, sociale wijkteams, werk inkomen en zorg, belastingen, afval, BRP, personeelsadministraties, Smart City toepassingen.*
Antw.	Voor de activiteiten die worden uitgevoerd op grond van de twee belangrijkste Gemeenschappelijke Regelingen waar Papendrecht aan deelneemt (GR Sociaal en GR DG&J), zoals de activiteiten van de GGD, Jeugdzorg, de Sociale Dienst Drechtsteden en Drechtwerk, zijn de gemeenschappelijke regelingen zelf verwerkingsverantwoordelijke. Dit betekent dat Papendrecht geen verwerkersovereenkomst met deze partijen hoeft te sluiten. De beide GR-en hebben een eigen privacybeleid, wat is afgestemd op dat van de deelnemende gemeenten, en een eigen FG. Papendrecht heeft een zetel in het Algemeen Bestuur van deze GR-en. Het bestuurslid namens Papendrecht kan in de gaten houden hoe met de verwerking van persoonsgegevens wordt omgegaan door de uitvoeringsorganisaties die onder de GR-en vallen. Of dit in de praktijk ook daadwerkelijk gebeurt kan op basis van de beschikbare informatie niet worden vastgesteld. Papendrecht heeft daarnaast een zevental verwerkersovereenkomsten met diverse partijen, zoals de Servicegemeente Dordrecht voor (o.a.) ICT, belastingen en personeelsadministratie, een aantal verwerkersovereenkomsten over activiteiten als huisbezoeken en schuldhulpverlening in het kader van Sterk Papendrecht, en een convenant met politie en OM over het delen en verwerken van persoonsgegevens en politiegegevens in het kader van de aanpak van problematische jeugdgroepen. Deze overeenkomsten zijn in lijn met de daarvoor geldende modellen van VNG, maar nadat ze zijn gesloten is ervoor zover bekend geen sprake van monitoring met betrekking tot de uitvoering in de praktijk. Er zijn geen reguliere overleggen met de verwerkers over het onderwerp privacy, en behoudens datalekken worden er door de verwerkers geen reguliere rapportages aan Papendrecht verstrekt. De verwerkersovereenkomsten worden ook niet periodiek geëvalueerd en indien nodig herzien.
10	*Zijn er verschillen en zo ja welke, in de bescherming van persoonsgegevens door de gemeente en door derden?*

Antw.	Op basis van de beschikbare informatie kunnen geen verschillen worden geconstateerd in de bescherming van persoonsgegevens door de gemeente en door derden.

1.3 Toepassing normenkader

Ten behoeve van het onderzoek is een normenkader opgesteld bestaande uit drie onderdelen (beleid, uitvoering en cultuur). De onderbouwing van het normenkader is opgenomen in paragraaf 2.3. Het normenkader wordt gebruikt om de bevindingen mee te waarderen. Per norm wordt aangegeven of de bevindingen uit het onderzoek wel, niet of deels voldoen aan de beschreven norm uit het normenkader. In de onderstaande tabel staat de toelichting bij deze waarderingen:

Waardering	Toelichting
Voldoet niet	Voldoet niet (aantoonbaar) aan de beschreven norm.
Voldoet deels	Voldoet deels wel en deels niet (aantoonbaar) aan de beschreven norm.
Voldoet wel	Voldoet aan de beschreven norm.

Bij de waardering van de normen uit het normenkader van dit onderzoek wordt er niet alleen gekeken naar de praktijk zoals dat in interviews wordt toegelicht, maar ook naar de aantoonbaarheid van deze praktijk. Niet alleen het *materieel* voldoen is van belang, maar ook het *aantoonbaar* voldoen. Dat komt omdat de AVG en de Wpg ook zo in elkaar zitten: je moet als organisatie niet alleen inhoudelijk aan de vereisten van de AVG en Wpg voldoen, maar ook kunnen aantonen dat dat zo is door middel van documentatie. Dat betekent dat bij de waardering van de normen niet alleen gekeken wordt of er in de praktijk in lijn met de norm gewerkt wordt, maar ook of dit in voldoende mate wordt gedocumenteerd. Zoals verder in dit rapport wordt toegelicht is met name het planmatig en structureel vastleggen van activiteiten gerelateerd aan het privacybeleid een tekortkoming van de gemeente Papendrecht, wat zijn reflectie heeft in de waardering op grond van het normenkader los van de (genuanceerde) beantwoording van de onderzoeksvragen.

Onderstaand staat per categorie een waardering van de normen met daaronder een beknopte toelichting van deze waardering.

Beleid	Beoordeling
De gemeente heeft AVG- en Wpg-conforme beleidskaders, regels en richtlijnen met betrekking tot de (juridische) borging van de privacy van inwoners. Voor specifieke (meer risicovolle) domeinen heeft de gemeente aanvullende regels opgesteld.	Voldoet deels

De algemene uitgangspunten en kaders zijn besproken in en vastgelegd door de gemeenteraad. In het gemeentelijk beleid wordt ingegaan op: – Juridische aspecten op basis van de AVG en Wpg – Vertaling naar de beleidskaders privacy – Organisatie, taken en verantwoordelijkheden (met inbegrip van de rol van de OR) – Inrichting werkprocessen – De toepassing van informatiesystemen en ICT – De gegevens- en informatiestromen – De positie van en communicatie met de burger	Voldoet wel voor AVG, voldoet niet voor Wpg
In de verschillende beleidskaders wordt ingegaan op: – Juridische aspecten op basis van de AVG, de Wpg en de materie wetten – Vertaling naar de beleidskaders privacy. – Organisatie, taken en verantwoordelijkheden. – Het toezicht op gebruik van persoonsgegevens is vastgelegd in een controleplan.	Voldoet wel voor AVG, voldoet niet voor Wpg
In bestuursrapportages, programmabegroting en programmarekening wordt expliciet aandacht besteed aan de wijze waarop een correcte omgang met persoonsgegevens is gewaarborgd. Daaraan worden conclusies en maatregelen verbonden op basis van uitgevoerde controles.	Voldoet niet

Papendrecht beschikt over een AVG-conform (vastgesteld) privacybeleid. Voor de Wpg is dit nog niet het geval. Deze is in het geldende privacybeleid niet meegenomen. Er is een Wpg-beleid, maar deze is nog niet vastgesteld en in de praktijk gebracht. Bezien vanuit dit normenkader is het nieuwe concept privacybeleid een duidelijke verbetering ten opzichte van het geldende beleid. Zo bevat het in tegenstelling tot het huidige beleid een duidelijke taak- en rolverdeling met betrekking tot privacy, en is het beter afgestemd op het geldende informatiebeveiligingsbeleid. Het concept Wpg-beleid gaat in op de belangrijkste onderwerpen en is een belangrijke verbetering.

Zoals in antwoord op onderzoeksvraag 8 al is geconcludeerd, wordt er in de bestuursrapportages alleen op procesniveau aandacht besteed aan gegevensbescherming en privacy. De rapportages bevatten geen inhoudelijke conclusies en maatregelen op basis van uitgevoerde controles.

Uitvoering	**Beoordeling**
In de praktijk wordt gehandeld conform de wijze waarop de bescherming van de persoonsgegevens is geregeld in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren van burgers en het vragen van toestemming.	Voldoet deels
De gemeente heeft een leer- en verbetercyclus waar privacy een apart onderdeel van uitmaakt. Hierin is aandacht voor mogelijke (ongewenste) knelpunten.	Voldoet deels
De gemeente heeft een routine voor het meten en verbeteren van de bescherming persoonsgegevens en legt vast wat de bevindingen en maatregelen zijn. Deze routine wordt tenminste één keer per jaar uitgevoerd.	Voldoet deels

De gemeente informeert de burger op een toegankelijke en begrijpelijke wijze over hun privacy-rechten, zowel schriftelijk als mondeling.	Voldoet deels
De gemeente verschaft aan burgers schriftelijk en mondeling begrijpelijke informatie over het gebruik van hun persoonsgegevens, zowel in algemene zin als afgestemd op de verschillende fasen in het dienstverleningsproces. Daarbij wordt aangegeven met welk doel dit gebeurt, wie inzage heeft en wat er vervolgens met de gegevens gebeurt.	Voldoet deels
Als sprake is geweest van een datalek, is conform de vastgelegde procedure gehandeld.	Voldoet wel
De gemeente heeft verwerkersovereenkomsten gesloten met derden die persoonsgegevens namens de gemeente verwerken, zoals de Sociale Dienst Drechtsteden. Binnen deze samenwerking wordt de bescherming van persoonsgegevens afdoende gewaarborgd.	Voldoet deels
De raad wordt geïnformeerd op een manier die hem in staat stelt te sturen en te controleren.	Voldoet niet

Er zijn weinig datalekken bekend, gemiddeld 3 tot 5 per jaar, maar de datalekken die er zijn worden conform de daarvoor geldende procedure afgehandeld. De gemeente heeft een AVG- en Wpg-conforme privacyverklaring op zijn website, die voldoende toegankelijk en begrijpelijk is voor burgers. In hoeverre het verstrekken van informatie aan burgers op individueel niveau afdoende gebeurt, kan op basis van de beschikbare informatie niet bepaald worden. Dit komt omdat het leeuwendeel van de uitvoerende taken waarbij dit aan de orde is buiten de gemeentelijke organisatie is belegd, hetzij bij één van de gemeenschappelijke regelingen, hetzij bij een verwerker. Er zijn zeven verwerkersovereenkomsten gesloten met derden die persoonsgegevens namens de gemeente verwerken. Maar zoals in antwoord op onderzoeksvraag 9 is gemeld, wordt er na het sluiten van de verwerkersovereenkomst geen aandacht besteed aan het waarborgen van de bescherming van persoonsgegevens in de praktijk. De uitvoering van de overeenkomst wordt niet gemonitord, er vinden geen reguliere overleggen of rapportages over privacy plaats, en de overeenkomsten worden niet periodiek geëvalueerd.

De medewerkers van de gemeente zetten zich in om aan AVG en Wpg te voldoen, maar door capaciteits- en kennisgebrek is in de afgelopen jaren een flinke achterstand opgebouwd, bijvoorbeeld met betrekking tot het uitvoeren van DPIA's. Er wordt geen jaarlijkse meting van de bescherming van persoonsgegevens uitgevoerd, anders dan het FG-verslag. De aanbevelingen uit de FG-verslagen (2020-2022) zijn niet allemaal opgevolgd. Er is wel een jaarlijks nascholingsprogramma, maar deelname hieraan geschiedt op basis van vrijwilligheid. Er is nog geen sprake van een (aantoonbaar) functionerende Plan-Do-Check-Act-cyclus (PDCA-cyclus) met betrekking tot gegevensbescherming en privacy, in het bijzonder ten aanzien van de 'check' fase. Het blijvend leren en verbeteren is onvoldoende ingebed in de reguliere werkprocessen.

De gemeenteraad wordt met name op procesniveau geïnformeerd over privacy en gegevensbescherming, en beschikt daardoor over onvoldoende informatie om adequaat te kunnen sturen en controleren. Met betrekking tot informatiebeveiliging beschikt de raad door middel van de ENSIA-rapportages wel over voldoende sturingsinformatie.

Cultuur	Beoordeling
De medewerkers van de gemeente zijn bekend met het gemeentelijk beleid met betrekking tot de bescherming van persoonsgegevens en worden van aanpassingen op de hoogte gehouden.	Voldoet wel
In hun dagelijks functioneren geven de medewerkers er blijk van het gemeentelijk privacybeleid na te leven.	Voldoet wel
In de relatie met inwoners zijn de medewerkers proactief en transparant over de wijze waarop de gemeente omgaat met hun gegevens	Voldoet niet
In de relatie met ketenpartners bewaken de medewerkers actief dat deze ketenpartners zich conformeren aan de regels, standaarden en procedures van de gemeente	Voldoet niet

Alle medewerkers die hebben deelgenomen aan het onderzoek zijn op de hoogte van het gemeentelijke privacybeleid, de meesten kennen ook het nieuwe concept-beleid al. In hun dagelijks functioneren tonen de medewerkers zich betrokken en verantwoordelijk. Zij zijn zich bewust van de noodzaak privacy-conform te handelen en doen daar ook hun best voor. Het ontbreekt hen echter regelmatig aan capaciteit en kennis om alle op grond van de AVG en de Wpg vereiste maatregelen tijdig uit te voeren. In de relatie met de inwoners is Papendrecht voor zover bekend eerder reactief dan proactief. Er wordt vooral vertrouwd op de informatie die inwoners op de site van de gemeente kunnen vinden, maar er wordt weinig aan actieve informatieverstrekking gedaan. In de relatie met samenwerkingspartners gaat Papendrecht vooral uit van vertrouwen. Er wordt niet actief op gelet dat ook de ketenpartners zich houden aan de gemeentelijke eisen die voortvloeien uit het privacybeleid en de AVG.

1.4 Toepassing privacy volwassenheidsmodel

Op verzoek van de rekenkamer is Papendrecht tevens getoetst aan het Privacy Volwassenheidsmodel van het Centrum voor Informatiebeveiliging en Privacybescherming (CIP)[3], voor zover dit binnen de beantwoording van de onderzoeksvragen past. Dit model sluit inhoudelijk aan bij het Toetsingskader AVG Borging van de Informatie Beveiligingsdienst van VNG. Het model kent vijf volwassenheidsniveaus, namelijk:

Niveau	Toelichting
1	**Informeel**: de organisatie werkt alleen situationeel op verwerkingsniveau aan privacy.
2	**Beheerst**: er zijn door meerdere personen vastgestelde processen, maar conformiteit aan wet- en regelgeving kan niet altijd worden aangetoond.
3	**Gedefinieerd**: de organisatie werkt organisatiebreed aan privacy en kan dit aantonen. NB: dit is het vereiste minimumniveau om AVG/Wpg-conform te zijn.
4	**Voorspelbaar**: er wordt ook actief op wijzigingen in wet- en regelgeving geanticipeerd, de organisatie investeert in continue verbetering van beleid en medewerkers en rapporteert regelmatig over de voortgang.

[3] Privacy Volwassenheidsmodel, CIP

5	**Geoptimaliseerd**: de organisatie heeft een volledig geïntegreerd privacybeleid, dat actueel is en voldoet aan wettelijke eisen en best practices. Er zijn procedures geïmplementeerd om de naleving te garanderen en daar is ook toezicht op, de voortgang en stand van zaken worden voortdurend gemonitord en gerapporteerd aan/door het management. Privacy is een speerpunt op alle niveaus binnen de organisatie geworden en krijgt ook aandacht in communicatie-uitingen naar publiek of klanten.

Papendrecht voldoet op dit moment aan **niveau 2** van dit privacy-volwassenheidsmodel. Er zijn vastgestelde processen en het beleid is op papier op orde. In de praktijk wordt echter niet altijd (aantoonbaar) conform de geldende privacyregels en vastgestelde processen gewerkt – of wordt dit niet adequaat vastgelegd. Bovendien is er onvoldoende sprake van een functionerende PDCA-cyclus binnen de gehele organisatie met betrekking tot privacy, en is privacy en gegevensbescherming nog onvoldoende ingebed in de reguliere werkprocessen van de gehele organisatie. Het is van belang om op te merken dat onze beoordeling aan de hand van dit volwassenheidsmodel niet betekent dat alle activiteiten ten aanzien van de bescherming van persoonsgegevens op volwassenheidsniveau 2 worden uitgevoerd: het gaat om een algemene en brede beoordeling.

1.5 Conclusies en aanbevelingen

De invulling van de probleemstelling, de beantwoording van de onderzoeksvragen en de toepassing van het normenkader resulteren in de onderstaande conclusies.

Het privacybeleid van de gemeente Papendrecht voldoet niet op alle punten aan de eisen uit de AVG en de Wpg. Hoewel het beleid op papier in grote mate voldoet (voor de AVG) wordt er in de praktijk niet altijd aantoonbaar gewerkt volgens dit beleid. Ook zijn er achterstanden in de uitvoering van het beleid, in het bijzonder ten aanzien van DPIA's. Als laatste worden verbetermaatregelen, bijvoorbeeld op basis van het FG-verslag, niet of pas na langere tijd opgevolgd. Kortom, de gemeente moet nog belangrijke verbeteringen doorvoeren in de uitvoering van het beleid.

De grootste tekortkomingen zijn er ten aanzien van de Wpg, zoals vastgesteld in de Wpg audit uit 2022. Voor deze tekortkomingen is er beperkte aandacht en sturing geweest vanuit directie, College en gemeenteraad. De gemeente heeft de nodige verbeteringen in gang gezet om tijdens de volgende audit wel te voldoen, waarvan de belangrijkste een nieuw informatiesysteem en het Wpg-beleid zijn.

Als laatste concluderen we dat er beperkte betrokkenheid is van de gemeenteraad bij het onderwerp. De gemeenteraad wordt met name op procesniveau geïnformeerd over privacy en gegevensbescherming en beschikt over onvoldoende informatie om adequaat te kunnen sturen en controleren.

Op basis van de bevindingen in het onderzoek doet de rekenkamer de volgende aanbevelingen

Aanbevelingen aan de gemeenteraad

1	Neem een pro-actievere (kaderstellende) rol aan ten aanzien van de bescherming van persoonsgegevens en het privacy- en Wpg-beleid en besluit mee over strategische uitgangspunten en ambitieniveaus.
2	Zorg voor een betere informatiepositie door het beleid en de verbeteringen van de gemeente periodiek te beoordelen.

3	Spreek minimaal jaarlijks over privacy (AVG én Wpg).

Aan het College van B&W zijn er de volgende aanbevelingen:

	Aanbevelingen aan het College van B&W
1	Zet de reeds ingezette verbeteringen, waaronder het nieuwe privacy- en Wpg-beleid en het uitvoeren van DPIA's, onverminderd door. Zorg daarbij voor voldoende capaciteit.
2	Zorg voor een periodieke rapportage over de voortgang met betrekking tot het privacy- en Wpg-beleid, de uitvoering van DPIA's en het opvolgen van FG-adviezen, en stuur bij waar nodig.
3	Beoordeel en evalueer het privacy- en Wpg-beleid jaarlijks en leg de resultaten hiervan vast.
4	Besteed meer aandacht aan de bescherming van persoonsgegevens bij gemeenschappelijke regelingen, samenwerkingspartners of verwerkers in de praktijk door afspraken en waarborgen uit verwerkersovereenkomsten periodiek te toetsen door middel van rapportage of onderzoeken.

Feitenrapportage

2. Inleiding

2.1 Aanleiding

Gemeenten beheren veel gegevens van inwoners. Binnen een gemeente vindt de registratie in het bevolkingsregister plaats, melden inwoners zich voor een vergunning of een uitkering, of vragen zij om zorg of ondersteuning. Inwoners moeten ervan uit kunnen gaan dat hun gegevens bij de gemeente in veilige handen zijn. Gemeenten moeten dat vertrouwen verdienen, zowel in de directe contacten met de burger als in verantwoording achteraf. Het is voor gemeenten lastig zich in het veld van privacy en informatiebeveiliging te begeven, gezien de snelle veranderingen en de samenwerkingsverbanden op regionaal niveau die vaak aan de orde zijn. De bescherming van (persoons)gegevens wordt steeds belangrijker en het niet op orde hebben van de informatiebeveiliging en privacy kan grote gevolgen hebben, waaronder bestuurlijke sancties.

In 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden.[4] De verordening is bedoeld om de persoonsgegevens van betrokkenen (beter) te beschermen. De Autoriteit Persoonsgegevens houdt toezicht op de uitvoering van de AVG in Nederland. Wanneer gemeenten de bescherming van persoonsgegevens niet op orde hebben, riskeren zij een boete van de Autoriteit Persoonsgegevens. Het maatschappelijk en financieel belang van een adequaat privacybeleid daarvan is al met al groot. Gemeenten hebben niet alleen een goed privacybeleid nodig, maar ook een goede uitvoering daarvan. Beide zijn verplicht op grond van de AVG. Bij dit onderzoek zijn daarom zowel de inrichting van het beleid als de uitvoering ervan beschreven en beoordeeld.

Voor de verwerking van persoonsgegevens binnen het ambtelijk apparaat van een gemeente is naast de AVG ook de Wet politiegegevens (Wpg) van belang. Deze wet geldt sinds 2018, op basis van de Europese Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn EU 2016/680). Deze richtlijn verplicht lidstaten van de EU tot het creëren van nationale wetgeving voor het verwerken van persoonsgegevens die gaan over voorkoming, onderzoek, opsporing en vervolging van strafbare feiten. Voor gemeenten gaat het in de praktijk om het verwerken van persoonsgegevens door Buitengewoon Opsporingsambtenaren (boa's). Dit geldt in situaties waar zij hun bevoegdheden gebruiken en politiegegevens verwerken, bijvoorbeeld bij het opleggen van een verkeersboete. De eisen van de Wpg overlappen voor een aanzienlijk deel met die van de AVG, bijvoorbeeld waar het gaat om de verplichting een verwerkingenregister bij te houden en een Functionaris Gegevensbescherming aan te stellen. Er zijn echter ook verschillen, zoals op het gebied van bewaartermijnen en verplichte logging van o.a. het bijhouden welke personen in welke gegevens kijken. Bovendien kent de Wpg de verplichting voor gemeenten om elk jaar een interne audit uit te voeren, en eens per vier jaar een externe audit. Vanwege de overlap in verplichtingen tussen AVG en Wpg is het goed mogelijk en vanuit het oogpunt van synergie zelfs voordelig om tegelijkertijd onderzoek te doen naar de implementatie van beide binnen één gemeente.

2.2 Centrale onderzoeksvraag

De rekenkamer van de gemeente Papendrecht heeft een onderzoek laten verrichten naar de bescherming van persoonsgegevens en de toepassing van de AVG en de Wpg in deze gemeente. Hiertoe heeft de rekenkamer de volgende probleemstelling geformuleerd:

[4] Een compacte beschrijving van de essentiële onderdelen van de AVG en de Wpg is opgenomen in de bestuurlijke rapportage.

Centrale onderzoeksvraag

Hoe wordt de privacy van de Papendrechtse inwoners beschermd en wordt er adequaat gebruik gemaakt van de AVG en Wpg, ook gelet op derden aan wie de uitvoering van beleid is uitbesteed, of met wie anderszins persoonsgegevens worden gedeeld? En op welke wijze wordt de gemeenteraad in staat gesteld de privacybescherming periodiek te controleren?

Deze centrale vraag is uitgewerkt in de volgende onderzoeksvragen:

	Onderzoeksvragen
1	Hoe biedt de gemeente Papendrecht bescherming aan inwoners als het gaat om privacy?
2	Wat is de stand van zaken van de uitvoering AVG en Wpg?
3	Op welke wijze is de raad tot nu toe bij de ontwikkeling van het privacybeleid betrokken geweest?
4	Waar knelt de AVG/Wpg, waar zitten beperkingen en risico's?
5	Zijn de verantwoordelijkheden van de bij de uitvoering AVG betrokken functionarissen duidelijk belegd – bestuurlijk en ambtelijk?
6	Wat is de rol van de OR ten aanzien van privacy en is deze duidelijk binnen de organisatie?
7	Wat zijn ongewenste en onnodige neveneffecten van de AVG: gebeurt het bijvoorbeeld dat informatie niet wordt gedeeld met een (oneigenlijk) beroep op de AVG?
8	Op welke manier wordt de gemeenteraad geïnformeerd over de uitvoering van het beleid rondom de bescherming van persoonsgegevens? Welke mogelijkheden heeft de raad om te sturen en te controleren?
9	Hoe monitort/verifieert de gemeente afspraken in verwerkersovereenkomsten met derden, waar knelt de AVG/Wpg, waar zitten beperkingen en risico's? Denk aan GGD, Veiligheidshuis, sociale wijkteams, werk inkomen en zorg, belastingen, afval, BRP, personeelsadministraties, Smart City toepassingen.
10	Zijn er verschillen en zo ja welke, in de bescherming van persoonsgegevens door de gemeente en door derden?

2.3 Normenkader

Bij onderzoeken van rekenkamers is het gebruikelijk om de bevindingen aan de hand van een normenkader te waarderen. Als het gaat om de bescherming van persoonsgegevens door gemeenten heeft PBLQ ondertussen de nodige ervaring opgedaan. Met gebruikmaking van die ervaringen is in afstemming met de rekenkamer van Papendrecht voor dit onderzoek een normenkader opgesteld.

Aan het gehanteerde normenkader liggen een aantal overwegingen ten grondslag.

- Privacy en de correcte omgang met persoonsgegevens binnen gemeenten worden vaak - ten onrechte - als juridische en ICT-technische onderwerpen gezien. Daarmee wordt het al gauw beschouwd als een onderwerp behorend bij het domein van de afdeling Juridische Zaken en de afdeling ICT. In het normenkader is verwerkt dat een zorgvuldige omgang met persoonlijke gegevens idealiter een kernwaarde moet zijn van elke medewerker in een overheidsorganisatie. De menselijke factor en de dagelijkse uitvoeringspraktijk horen een organisatiebreed aandachtspunt te zijn.

- Lang niet alle gemeenten hebben de bescherming van persoonsgegevens goed ingebed in hun dienstverlening. Er is doorgaans wel een vastgesteld privacybeleid, maar het ontbreekt geregeld aan praktische uitvoeringskaders. Medewerkers zijn zich niet altijd voldoende bewust van wat er op dit gebied van hen gevraagd wordt. Goed privacybeleid heeft aandacht voor alle belangrijke aspecten: de positie van de inwoner, hoe gegevens worden vastgelegd en wie welke gegevens met welk doel mag verwerken of delen met anderen, hoe de kwaliteit van gegevens gewaarborgd wordt en hoe het juridische kader van de AVG en de Wpg wordt vertaald naar werkprocessen en ICT-systemen.
- Het gedrag van medewerkers in de praktijk bepaalt daarbij in hoge mate of de gemeente risico's loopt op bovenmatige verzameling of onzorgvuldig gebruik van persoonsgegevens, een datalek, of het combineren van gegevens terwijl dat eigenlijk niet is toegestaan. Dit gedrag bepaalt dus eveneens of aan de AVG en de Wpg wordt voldaan. Daarom hoort het juist omgaan met persoonsgegevens ook een onderwerp te zijn bij functioneringsgesprekken, werkoverleggen en interne communicatie.
- Gemeenten delen regelmatig (persoons-)gegevens met andere (uitvoerings-)instanties. Met die andere organisaties moeten gezamenlijke afspraken worden gemaakt over een veilige omgang met die gegevens.
- Voor het geval er sprake is van zogenaamde datalekken is de externe communicatie van belang. Omdat de gemeente financiële en imago-risico's loopt, is het cruciaal dat er bij een datalek adequaat wordt gehandeld. Medewerkers moeten weten wat zij moeten doen en escalatielijnen moeten zijn ingeregeld. Ook over de communicatie met de mensen van wie de data is gelekt en met de pers moet vooraf zijn nagedacht.

Deze overwegingen hebben bijgedragen tot het inrichten en toepassen van onderstaande normenkader:

Gemeentelijk beleid

- De gemeente heeft AVG- en Wpg-conforme beleidskaders, regels en richtlijnen met betrekking tot de (juridische) borging van de privacy van inwoners. Voor specifieke (meer risicovolle) domeinen heeft de gemeente aanvullende regels opgesteld.
- De algemene uitgangspunten en kaders zijn besproken in en vastgelegd door de gemeenteraad. In het gemeentelijk beleid wordt ingegaan op:
  - Juridische aspecten op basis van de AVG en Wpg
  - Vertaling naar de beleidskaders privacy
  - Organisatie, taken en verantwoordelijkheden (met inbegrip van de rol van de OR)
  - Inrichting werkprocessen
  - De toepassing van informatiesystemen en ICT
  - De gegevens- en informatiestromen
  - De positie van en communicatie met de burger
- In de verschillende beleidskaders wordt ingegaan op:
  - Juridische aspecten op basis van de AVG, de Wpg en de materie wetten
  - Vertaling naar de beleidskaders privacy.
  - Organisatie, taken en verantwoordelijkheden.
  - Het toezicht op gebruik van persoonsgegevens is vastgelegd in een controleplan.

- In bestuursrapportages, programmabegroting en programmarekening wordt expliciet aandacht besteed aan de wijze waarop een correcte omgang met persoonsgegevens is gewaarborgd. Daaraan worden conclusies en maatregelen verbonden op basis van uitgevoerde controles.

Uitvoeringspraktijk

- In de praktijk wordt gehandeld conform de wijze waarop de bescherming van de persoonsgegevens is geregeld in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren van burgers en het vragen van toestemming.
- De gemeente heeft een leer- en verbetercyclus waar privacy een apart onderdeel van uitmaakt. Hierin is aandacht voor mogelijke (ongewenste) knelpunten.
- De gemeente heeft een routine voor het meten en verbeteren van de bescherming persoonsgegevens en legt vast wat de bevindingen en maatregelen zijn. Deze routine wordt tenminste één keer per jaar uitgevoerd.
- De gemeente informeert de burger op een toegankelijke en begrijpelijke wijze over hun privacy-rechten, zowel schriftelijk als mondeling.
- De gemeente verschaft aan burgers schriftelijk en mondeling begrijpelijke informatie over het gebruik van hun persoonsgegevens, zowel in algemene zin als afgestemd op de verschillende fasen in het dienstverleningsproces. Daarbij wordt aangegeven met welk doel dit gebeurt, wie inzage heeft en wat er vervolgens met de gegevens gebeurt.
- Als sprake is geweest van een datalek, is conform de vastgelegde procedure gehandeld.
- De gemeente heeft verwerkersovereenkomsten gesloten met derden die persoonsgegevens namens de gemeente verwerken, zoals de Sociale Dienst Drechtsteden. Binnen deze samenwerking wordt de bescherming van persoonsgegevens afdoende gewaarborgd.
- De raad wordt geïnformeerd op een manier die hem in staat stelt te sturen en te controleren.

Cultuur van de organisatie met betrekking tot privacy

- De medewerkers van de gemeente zijn bekend met het gemeentelijk beleid met betrekking tot de bescherming van persoonsgegevens en worden van aanpassingen op de hoogte gehouden.
- In hun dagelijks functioneren geven de medewerkers er blijk van het gemeentelijk privacybeleid na te leven.
- In de relatie met inwoners zijn de medewerkers proactief en transparant over de wijze waarop de gemeente omgaat met hun gegevens.
- In de relatie met ketenpartners bewaken de medewerkers actief dat deze ketenpartners zich conformeren aan de regels, standaarden en procedures van de gemeente.

Daarnaast is Papendrecht op verzoek van de rekenkamer getoetst aan het Privacy Volwassenheidsmodel van het Centrum voor Informatiebeveiliging en Privacybescherming (CIP)[5], voor zover dit binnen de beantwoording van de onderzoeksvragen past. Dit model sluit inhoudelijk aan bij het Toetsingskader AVG Borging van de Informatie Beveiligingsdienst van VNG. Waar nodig wordt de uitvoering van de AVG en de Wpg apart beoordeeld. Dit model kent vijf volwassenheidsniveaus, 1 t/m 5. Deze niveaus behelzen het volgende:

Niveau	Toelichting
1	**Informeel**: de organisatie werkt alleen situationeel op verwerkingsniveau aan privacy.

[5] Privacy Volwassenheidsmodel, CIP

2	**Beheerst**: er zijn door meerdere personen vastgestelde processen, maar conformiteit aan wet- en regelgeving kan niet altijd worden aangetoond.
3	**Gedefinieerd**: de organisatie werkt organisatiebreed aan privacy en kan dit aantonen. NB: dit is het vereiste minimumniveau om AVG/Wpg-conform te zijn.
4	**Voorspelbaar**: er wordt ook actief op wijzigingen in wet- en regelgeving geanticipeerd, de organisatie investeert in continue verbetering van beleid en medewerkers en rapporteert regelmatig over de voortgang.
5	**Geoptimaliseerd**: de organisatie heeft een volledig geïntegreerd privacybeleid, dat actueel is en voldoet aan wettelijke eisen en best practices. Er zijn procedures geïmplementeerd om de naleving te garanderen en daar is ook toezicht op, de voortgang en stand van zaken worden voortdurend gemonitord en gerapporteerd aan/door het management. Privacy is een speerpunt op alle niveaus binnen de organisatie geworden en krijgt ook aandacht in communicatie-uitingen naar publiek of klanten.

2.4 Werkwijze

Ten behoeve van dit onderzoek hebben we de volgende onderzoeksactiviteiten uitgevoerd:

- Het onderzoek is aangekondigd bij de gemeentelijke organisatie. Hierna is een startbijeenkomst gehouden om een algemene toelichting op het onderzoek te geven, de te interviewen functionarissen vast te stellen en de te bestuderen documentatie door te spreken.
- Er is een bureaustudie uitgevoerd naar de relevante beleidsdocumenten die door de gemeentelijke organisatie in delen zijn toegestuurd. Waar relevant heeft het onderzoeksteam om aanvullende documentatie gevraagd gedurende de looptijd van het onderzoek. Een overzicht van de bestudeerde documentatie is opgenomen in Bijlage B.
- Bij verschillende functionarissen zijn er interviews afgenomen, waarop is ingegaan op de achtergrond en overwegingen van het privacybeleid van de gemeente. Ook is er gesproken over hoe het beleid in de praktijk uitpakt en uitgevoerd wordt. In Bijlage A is een overzicht opgenomen van de geïnterviewde personen.
- Om meer inzicht in de dagelijkse uitvoeringspraktijk met betrekking tot (de bescherming van) persoonsgegevens te krijgen, is er een mini-Privacy Impact Assessment[6] uitgevoerd voor het thema Wpg met betrekking tot de verwerking van persoonsgegevens en het gebruik van (nieuwe) informatievoorziening door boa's van de gemeente.
  - Het was bij de aanvang van dit onderzoek de bedoeling om een tweede mini-PIA uit te voeren met betrekking tot het sociaal domein en het thema AVG. In de startbijeenkomst van dit onderzoek is besloten dat deze mini-PIA betrekking zou hebben op (de samenwerking met) Sterk Papendrecht. Het is niet gelukt om binnen de voor dit onderzoek beschikbare tijd deze tweede mini-PIA te organiseren. In overleg met de rekenkamer is besloten om deze achterwege te laten en in plaats daarvan een aanvullend interview te houden. Dit was wel mogelijk binnen de afgesproken planning voor dit onderzoek. De verwachting was bovendien dat dit meer relevante informatie voor de uitkomsten van dit onderzoek zou opleveren.

[6] Bij een PIA wordt stap voor stap de inrichting van de bescherming van persoonsgevoelige informatie geïnventariseerd en beoordeeld. Voor de goede orde moet benadrukt worden dat in het kader van het rekenkameronderzoek geen volledige PIA is uitgevoerd. Gekozen is voor een beperkte variant (aangeduid als mini-PIA) waarbij met enkele direct bij de uitvoeringspraktijk van de boa's betrokken medewerkers gesproken is over de wijze waarop zij in hun dagelijkse praktijk de veiligheid van persoonsgegevens bewaken.

- De gemeenteraad is bij het onderzoek betrokken in een raadssessie. Het doel van deze raadssessie was om inzicht te krijgen in de rol en positie van de gemeenteraad. Dit is uitgevoerd aan de hand van een fictieve casus die de aanwezige raadsleden heeft doen reflecteren op hun eigen rol en positie..
- Op basis van de inzichten die in de bovenstaande onderzoeksactiviteiten zijn opgedaan, is er een gesprek gevoerd met een vertegenwoordiging van de ambtelijke organisatie[7] in een convergentiesessie. Het doel van deze sessie was om de beelden en interpretaties van de onderzoekers te bespreken met de ambtelijke organisatie en te toetsen en zo nodig in een vroeg stadium aan te scherpen.
- Het onderzoeksteam heeft op basis van de verzamelde informatie een feitenrapportage opgesteld (voorliggend).

2.5 Indeling rapport

Dit hoofdstuk vormt samen met de hoofdstukken 3 en 4 het feitenrelaas van dit onderzoek. In het derde hoofdstuk ligt de nadruk in de beschrijving van de bevindingen op het geldende beleid van Papendrecht met betrekking tot de bescherming van persoonsgegevens. In het vierde hoofdstuk gaat de aandacht uit naar de uitvoeringspraktijk.

[7] Ook deze functionarissen zijn vermeld in Bijlage A.

3. De uitgangspunten van het privacybeleid

3.1 Het beleid van Papendrecht

In dit hoofdstuk zijn de uitgangspunten van het beleid aan de orde. Aangegeven wordt wat het startpunt vormde voor dat beleid, bij de inwerkingtreding van de AVG in 2018. Vervolgens wordt aangegeven welke documenten nadien door het gemeentebestuur zijn op- en vastgesteld met betrekking tot het privacybeleid.

In dit hoofdstuk komen de volgende documenten aan de orde:

Document	Status / belang
Privacybeleid Drechtsteden 2020	Dit is het geldende privacybeleid van de gemeente Papendrecht, zoals dat door de gemeenteraad, het college en de burgemeester van Papendrecht is vastgesteld.
Concept-privacybeleid gemeente Papendrecht 2024	Papendrecht heeft een nieuwe versie van het privacybeleid in concept gereed. Deze is nog niet vastgesteld en dus nog niet geldend.
Strategisch informatiebeveiligingsbeleid Drechtsteden 2020-2024	Informatiebeveiliging is een randvoorwaarde voor een veilige omgang met gegevens. Daartoe verschaft dit document de uitgangspunten.

Privacybeleid Drechtsteden 2020
Dit beleid is op dit moment het geldende privacybeleid voor de gemeente Papendrecht. Het is een geactualiseerde versie van het beleid zoals dat kort na inwerkingtreding van de AVG in 2018 is vastgesteld. Dit geldende beleid uit 2020 volgt de hoofdlijnen van de AVG en bevat op een aantal punten een nadere concretisering voor de Drechtsteden, waaronder de gemeente Papendrecht. Het beleid geeft aan hoe de Drechtsteden voornemens zijn aan de AVG te voldoen. De uitvoering van de Wpg is **geen** onderdeel van dit beleid. Hier is nog geen separaat beleid voor vastgesteld binnen de gemeente Papendrecht, een concept is wel gereed. Het geldende privacybeleid ziet er op hoofdlijnen als volgt uit:

- In paragraaf 2.4 van het privacybeleid wordt gesteld dat alle maatregelen die het privacybeleid bevat cyclisch zijn, en dat het de bedoeling is om op de verschillende verantwoordelijke niveaus binnen de organisatie steeds een PDCA-cyclus te doorlopen. Ook is het de bedoeling dat het onderwerp privacy periodiek aan de orde komt door het vast op de agenda's van de verantwoordelijken in de regio te plaatsen. Binnen de gemeente Papendrecht is deze maatregel voor zover bij ons bekend niet nader geoperationaliseerd: er zijn ons geen vastgelegde afspraken bekend om het onderwerp privacy periodiek bij (werk)overleggen binnen de gemeente Papendrecht te agenderen.
- Alle deelnemende gemeenten dienen op hun website helder aan te geven hoe van de rechten voor betrokken personen op grond van de AVG gebruik kan worden gemaakt. De gemeente Papendrecht heeft dit ook opgenomen op haar website[8]. De rechten van betrokkenen zijn samengevat weergegeven in het privacybeleid. Voor de gemeente Papendrecht zijn

[8] Website Papendrecht

werkprocessen vastgesteld met betrekking tot de rechten van betrokkenen, deze komen in paragraaf 3.2 aan de orde.

- De deelnemende gemeenten, waaronder Papendrecht, zijn ieder zelf verantwoordelijk voor de privacy-bewustwording van hun eigen personeel. Zij dienen ervoor te zorgen dat werknemers die werken met persoonsgegevens, weten wat hun verantwoordelijkheid is en hoe zij zorgvuldig om dienen te gaan met persoonsgegevens. Zij moeten in staat zijn om te beoordelen welke gegevens nodig zijn voor het uitvoeren van de werkprocessen. Werknemers worden getraind in privacy-bewust functioneren door middel van presentaties, workshops en trainingen, leermodules in de e-learningomgeving en het altijd voor handen hebben van een interne of externe vraagbaak.
- Alle gemeenten moeten een procedure inrichten voor datalekken en incidentbeheer, inclusief het informeren van betrokkenen. Papendrecht heeft deze procedure ingericht (zie paragraaf 3.2).
- Alle gemeenten moeten ervoor zorgen dat alle gegevensverwerkingen waarin persoonsgegevens worden verwerkt in beeld zijn gebracht en zijn vastgelegd in het Register van verwerkingen. Waar nodig c.q. vereist dient een DPIA te zijn uitgevoerd, hiervan dient een aantekening te worden vastgelegd in het Register van verwerkingen. Dit is momenteel niet gerealiseerd. Er staat een actualisatie van het Register op de planning voor de tweede helft van 2024. Dit is belangrijk om te kunnen sturen op actualisatie en het kunnen uitvoeren van maatregelen.
- Met verwerkers dienen verwerkersovereenkomsten te worden gesloten. Hierbij moet de modelovereenkomst van VNG als uitgangspunt worden gebruikt. In verwerkersovereenkomsten moeten minimaal afspraken worden gemaakt over:
  - De doeleinden waarvoor de gegevens mogen worden verwerkt.
  - Hoe de verwerker met de persoonsgegevens moet omgaan.
  - Welke beveiligingsmaatregelen moeten worden genomen.
  - Welke vormen van toezicht de eigenaar mag uitoefenen.
  - Geheimhoudingsplicht.
  - Inschakeling van derden en onderaannemers.
  - Locatie van de data.
  - Aansprakelijkheid van schade door het niet naleven van regelgeving.
  - Exit-strategie.
- Voor persoonsgegevens waarvoor geen wettelijk vastgestelde bewaartermijnen gelden, moeten alle deelnemende gemeenten zelf besluiten over de bewaartermijn. De bewaartermijnen dienen vermeld te worden in het Register van verwerkingen. Het is op basis van de beschikbare informatie niet duidelijk in hoeverre binnen gemeente Papendrecht persoonsgegevens worden verwerkt waarvoor geen wettelijke bewaartermijn is vastgesteld, en zo ja, of er een eigen besluit over de bewaartermijnen is genomen. De bewaartermijnen zijn vastgelegd in aparte tooling (‘i-navigator’), van waaruit de archivaris overzichten kan geven voor vernietiging conform het beleid.
- Op de website van Papendrecht dient een privacyverklaring te zijn opgenomen waarin op hoofdlijnen wordt aangegeven welke persoonsgegevens met welke doeleinden worden verwerkt. Dit is het geval.
- Het College van B&W dient de gemeenteraad in het kader van de jaarlijkse planning- en controlcyclus te informeren over de toepassing van het privacybeleid. Deze stukken zijn erg procesmatig en bevatten weinig inhoudelijke punten.
- De deelnemende organisaties hebben een gezamenlijke FG. De positie van de FG is door Dordrecht nader vastgelegd in het Reglement Functionaris voor de Gegevensbescherming Drechtsteden 2022. In paragraaf 3.2 zal hier nader op worden ingegaan.
- Proceseigenaren zijn verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens binnen de processen van de eenheid waaraan zij leidinggeven. Zij zijn daarom ook

verantwoordelijk om te monitoren of persoonsgegevens zorgvuldig worden verwerkt en dit zo nodig bij te sturen. Proceseigenaren zorgen ervoor dat zij kunnen aantonen op welke wijze uitvoering is gegeven aan de privacywetgeving binnen hun werkprocessen. Conform het privacy- en het informatiebeveiligingsbeleid is binnen de i-navigator genoteerd dat teamleiders de proceseigenaren voor hun eigen werkprocessen zijn. Hoe de monitoring moet worden uitgevoerd en hoe moet worden aangetoond op welke wijze uitvoering wordt gegeven aan de privacywetgeving met betrekking tot een proces is, voor zover bij ons bekend, niet nader geoperationaliseerd op basis van dit beleid.

Concept-privacybeleid gemeente Papendrecht 2024

Inmiddels wordt door Papendrecht gewerkt aan een nieuw privacybeleid. Dit is in conceptvorm beschikbaar en het is de bedoeling om dit beleid in 2024 vast te laten stellen door het college, de burgemeester en de gemeenteraad. Ook dit nieuwe privacybeleid gaat alleen over de AVG. Wat betreft de Wpg wordt in dit conceptbeleid nu verwezen naar een ‘Privacybeleid Wet politiegegevens’, dat ook op de website van de gemeente Papendrecht ter beschikking zal worden gesteld. Ook dit beleid (Privacybeleid Wet politiegegevens) is in conceptversie gereed. We gaan hieronder kort op dit beleid in.

Het concept-privacybeleid van Papendrecht is gebaseerd op het model-privacybeleid van de Informatiebeveiligingsdienst (IBD) van VNG. Waar het beleid aansluit op c.q. overeenkomt met de AVG is het inhoudelijk gelijk aan het geldende beleid. Ten opzichte van het geldende beleid bevat het concept-beleid de volgende aanvullingen c.q. wijzigingen:

- Een evaluatiebepaling: het beleid dient minimaal eens per drie jaar te worden beoordeeld en indien nodig herzien.
- Het beleid ziet uitdrukkelijk op alle gegevensverwerkingen door of namens de gemeente, ook wanneer deze zijn uitbesteed of op een andere manier zijn georganiseerd, zoals door deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht.
- Het beleid bevat de verplichting een bewaartermijn vast te stellen voor persoonsgegevens waarop geen wettelijke bewaartermijn van toepassing is.
- De gemeente moet bij de ontwikkeling van nieuwe diensten, systemen of processen rekening houden met aspecten van privacy en gegevensbescherming, om zo te komen tot een zo optimaal mogelijke bescherming van Persoonsgegevens (*Privacy by Design)*. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente *Privacy by Default* als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.
- Uitsluitend geautoriseerde personen hebben toegang tot persoonsgegevens. De gemeente controleert periodiek of bevoegdheden nog correct zijn toebedeeld, en moet gebruik maken van logging (bijhouden wie welke gegevens bekijkt) en andere maatregelen om ongeautoriseerde toegang zo veel mogelijk te voorkomen.
- De gemeente werkt samen met andere (overheids)organisaties om een taak van algemeen belang uit te voeren, hierover is een uitgebreidere tekst opgenomen in het concept-beleid. Hierbij kan men bijvoorbeeld denken aan de samenwerking binnen de Gemeenschappelijke regeling Sociaal, waarbinnen de Sociale Dienst Drechtsteden valt, of aan de Gemeenschappelijke regeling Dienst Gezondheid & Jeugd. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt en wie waarvoor verantwoordelijk is. In paragraaf 3.4 wordt hier nader op ingegaan.

- Het concept-beleid bevat een nadere vastlegging van rollen en verantwoordelijkheden binnen de gemeentelijke organisatie. Ten opzichte van het VNG-model bevat het concept-beleid van Papendrecht de volgende gemeentespecifieke bepalingen:
  - De gemeentesecretaris/algemeen directeur van de gemeentelijke organisatie is operationeel eindverantwoordelijk voor de naleving van de privacywetgeving binnen de organisatie, alsmede voor de uitvoering van het privacybeleid.
  - De teamleiders zijn verantwoordelijk voor de naleving van de privacywetgeving en het privacybeleid binnen het eigen team. Zij zijn als proceseigenaar verantwoordelijk voor het voldoen aan de AVG van de eigen processen, waaronder het uitvoeren van een DPIA waar nodig. Zij zijn verantwoordelijk voor het trainen van hun personeel met betrekking tot privacy, het autoriseren van nieuw personeel, het intrekken van de autorisatie van scheidend personeel, en het bevorderen van een duurzame privacycultuur. Ook dienen zij de privacycoördinator en via deze de FG in een vroeg stadium te betrekken bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.
- Er wordt een aantal interne en regionale overleggen genoemd waar het onderwerp privacy aan de orde dient te komen, te weten:
  - Interne werkoverleggen
  - Privacy coördinatoren overleg (PCO)
  - Periodiek overleg met adviseurs informatiebeveiliging
  - Periodiek overleg met informatiemanagers
  - Periodiek overleg met het Juridisch Kenniscentrum (JKC) van de Servicegemeente Dordrecht
  - Periodiek overleg met de Functionaris Gegevensbescherming (FG).

De gemeente werkt in regionaal verband aan de praktische uitwerking van het privacybeleid. Dit wordt gedaan aan de hand van actieplannen waarop acties met betrekking tot privacy en de verdere uitwerking van het beleid worden uitgewerkt. Deze actieplannen worden continue en gedurende het jaar bijgewerkt. Voorbeelden van acties in de actieplannen zijn het opstellen van standaardbrieven voor rechten van betrokkenen, de evaluatie van het datalekkenproces of de afstemming van uit te voeren DPIA's.

Concept Privacybeleid Wet politiegegevens

In het concept Privacybeled Wet politiegegevens van de gemeente Papendrecht zijn de verplichtingen uit de Wpg en aanverwante regelgeving[9] in beleid vastgelegd. Dit beleid is aanvullend op het privacybeleid, dat toeziet op de AVG maar niet op de Wpg. Het doel van het beleid is om te beschrijven hoe de gemeente binnen de wettelijke kaders (verantwoordelijk) omgaat met persoonsgegevens. In het conceptbeleid staat verder dat onder andere wordt beoogd te bereiken dat boa's "zich ten volle bewust zijn van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met politiegegevens" en "de rechten van betrokkenen respecteren en werken volgens de vastgestelde procedures"[10].

In het concept Privacybeleid Wet politiegegevens worden onder andere de volgende onderwerpen geadresseerd:

[9] Zoals het Besluit politiegegevens (Bpg), het Besluit politiegegevens boa's en de Regeling periodieke audit politiegegevens.
[10] Concept Privacybeleid Wet politiegegevens, pagina 2

- Het algemene beleidskader voor de Wpg met de belangrijkste verplichtingen zoals het scheiden van op feiten gebaseerde gegevens en op persoonlijk oordeel gebaseerde gegevens, het loggen van invoeren en verwerken van persoonsgegevens (in het informatiesysteem BRS) en de specifieke eisen uit het Besluit politiegegevens.
- De rechten van betrokkenen, waarvan de procedures op hoofdlijnen gelijk zijn met hetgeen er in het privacybeleid voor de AVG is opgenomen.
- Bewustwording en training van medewerkers die te maken krijgen met politiegegevens en BRS, waaronder een Wpg e-learning voor nieuwe medewerkers en een aanvullende extern belegde training voor Boa's die al in dienst zijn.

Strategisch informatiebeveiligingsbeleid Drechtsteden 2020-2024

Ook het strategisch informatiebeveiligingsbeleid voor de Drechtsteden sluit aan bij het VNG-model wat hiervoor beschikbaar is, alleen dan wel bij een eerdere versie hiervan. Het huidige VNG-model is recenter dan het geldende beleid. Ook het informatiebeveiligingsbeleid wordt momenteel geactualiseerd, de verwachting is dat hiervoor het meest recente model wordt gevolgd. Het huidige beleid bevat de volgende gemeente specifieke bepalingen ten opzichte van het gehanteerde model:

- Als specifieke resultaatgebieden voor de Drechtsteden worden gedefinieerd:
  - Risicomanagement: de organisaties in staat stellen om een duidelijk beeld te krijgen op informatiebeveiligingsrisico's en hoe de risicobereidheid door maatregelen kunnen worden afgedekt.
  - Kennis en kunde: alle verantwoordelijk medewerkers en dan met name de informatiebeveiligingsadviseurs moeten voldoende kennis en kunde hebben om hun taak te kunnen uitvoeren. De CISO en de informatiebeveiligingsadviseurs dragen zorg voor kennisoverdracht en bewustwording binnen de rest van de organisatie.
  - Compliance management: er dient gecontroleerd te worden of systemen en applicaties voldoen aan gestelde eisen en welke risico's voortkomen uit discrepanties.
  - Klantbeleving: andere medewerkers voelen zich gesteund door informatiebeveiliging en hebben hier een positief oordeel over.
  - Innovatiemanagement: er wordt gezorgd dat Papendrecht toekomstbestendig blijft.
- Leveranciersmanagement: er is een transitie gaande naar inkoop vanuit het transitieplan en de inkoop strategie. Hierdoor is het nodig om op strategisch niveau contacten te hebben en onderhouden met de belangrijke leveranciers.
    - Informatiemanagement: zorgen dat er in de beginfase van het voortbrengingsproces al aandacht gevestigd wordt op *Privacy by Design* en *Security by Design*.
    - Ondersteunen bij crisis- en incidentenmanagement.
    - Gevraagd en ongevraagd advies geven vanuit het CISO-team.
    - Security governance: het duidelijk neerzetten van een security governance structuur. De organisatie moet eigenaarschap hebben belegd en verantwoordelijkheid nemen op de risico's die worden gelopen en de maatregelen die worden getroffen.
- Specifiek voor gemeente Papendrecht is een rol- en taakverdeling opgenomen die afwijkt van het VNG-model en van de hoofdtekst van het beleid. Samengevat ziet deze er als volgt uit:
  - Het college van B&W stelt driejaarlijks het beleid vast;
  - De gemeentesecretaris stelt een informatiebeveiligingsplan vast, en is verantwoordelijk voor het opstellen en uitvoeren van aanvullende tactische beleidsregels en hiermee ook de juiste toepassing van de BIO;

- De lokale informatiebeveiligingsadviseur ondersteunt vanuit een onafhankelijke positie de gemeente en rapporteert rechtstreeks aan de gemeentesecretaris;
- In de planning- en controldocumenten moet er aandacht zijn voor informatiebeveiliging, risicovolle onderwerpen dienen ook te worden geadresseerd in auditplannen;
- De proceseigenaren zijn verantwoordelijk voor de informatiebeveiliging van hun processen, inclusief de autorisaties van hun medewerkers;
- Beveiligingsmaatregelen worden genomen op basis van risicomanagement, hiertoe moet de proceseigenaar een quickscan informatiebeveiliging en privacy uitvoeren o.b.v. BIO;
- Alle werknemers worden getraind in het gebruik van beveiligingsprocedures en moeten online nascholingsmodules volgen op het gebied van informatiebeveiliging.

Op dit moment wordt door Servicegemeente Dordrecht gewerkt aan een actualisatie van het Strategisch Informatieveiligheidsbeleid Drechtsteden. Dit beleidsstuk zal lokaal worden vastgesteld. . Een vast evaluatiemoment van het beleid of het proces tot vaststelling en actualisatie hiervan is op dit moment niet afgesproken binnen de Drechtsteden.

Digitaliseringsagenda
Het college werkt aan een nieuwe digitaliseringsagenda. Deze agenda is nog niet vastgesteld maar al wel besproken in het college. De agenda zal meer nadruk leggen op de ethische kant van digitalisering, gebaseerd op waarden zoals betrouwbaarheid. Het doel van de agenda is om meer te sturen op digitaliseringsvraagstukken en fundamenteel na te denken over de betekenis van digitale ontwikkelingen in plaats van alleen de technische kant. De insteek van de agenda is daarnaast om het onderwerp minder ICT-technisch te benaderen en vooral als een politiek en bestuurlijk vraagstuk. De bestuurlijke discussie op basis van de agenda raakt vaak aan privacy en het privacybeleid, omdat dit één van de waarden/thema's is die aan bod komt bij digitaliseringsvraagstukken. Getracht wordt het nadenken over en werken aan de digitaliseringsagenda vooral ook regionaal vorm te geven en daarmee te anticiperen op de veranderende wet- en regelgeving die gemeenten vanaf 2026 opgelegd wordt vanuit Europa.

3.2 Processen

In dit hoofdstuk wordt bezien of en hoe de werkprocessen binnen de gemeente zijn verankerd, waarbij in het bijzonder wordt gekeken naar de processen op het gebied van gegevensbescherming en privacy. Papendrecht werkt al geruime tijd aan het programma 'Processen op orde', dat als doel heeft alle werkprocessen van de gemeente goed vast te leggen, inclusief bijbehorende beveiligingsmaatregelen.

In dit onderzoek is geconstateerd dat de volgende werkprocessen zijn vastgelegd op het gebied van gegevensbescherming en privacy:

Proces	Titel	Inhoud
Opstellen DPIA	Hoe komt een DPIA tot stand binnen de Drechtsteden	◥ Wanneer en hoe maak je een DPIA ◥ Rol FG en Privacy Coördinator bij DPIA ◥ Verplichting om uiterlijk 3 maanden na uitvoering DPIA de daadwerkelijk genomen maatregelen te melden aan de FG

		◥ Verplichting DPIA te wijzigen als verwerking wijzigt, minstens 1x per 2 jaar moet de DPIA sowieso opnieuw worden beoordeeld en indien nodig herzien (PDCA-cyclus)
Datalek afhandelen	Werkwijze bij ingekomen melding: datalekmelding	Beschrijft het werkproces wat wordt gevolgd nadat een medewerker een datalek heeft gemeld door gebruik te maken van de knop ‘melden beveiligingsincident’ op SID (een intern systeem). Het proces omschrijft zowel de informatie die de melder moet leveren als de opvolging van de melding door de Privacy Coördinator.
Overdracht persoonsgegevens op verzoek betrokkene (recht op dataportabiliteit, oftewel het kunnen meenemen van je gegevens naar een andere organisatie)	Werkinstructie Persoonsgegevens verzoek overdracht in gemeenten die niet samenwerken met Dienstverlening Drechtsteden en Zaaktype Persoonsgegevens dataportabliteit verzoek	Beschrijft het proces wat gevolgd wordt nadat een betrokkene via de website van de gemeente een verzoek om de overdracht van zijn persoonsgegevens heeft gedaan. Hiervoor is een formulier op de site beschikbaar. De Privacy Coördinator neemt het voortouw bij de afhandeling.
Verwijderen persoonsgegevens op verzoek betrokkene (recht om vergeten te worden)	Werkinstructie Persoonsgegevens verwijderingsverzoek gemeenten die niet samenwerken met Dienstverlening Drechtsteden en Zaaktype Persoonsgegevens verwijderingsverzoek	Betrokkenen kunnen via een formulier op de site van de gemeente een verzoek tot verwijdering van persoonsgegevens indienen. De Privacy Coördinator neemt het voortouw bij de inhoudelijke afhandeling. Er is daarnaast een ‘Notitie m.b.t. inzageverzoek en verwijderingsverzoek’ die nadere inhoudelijke kaders stelt.
Verzoek tot inzage persoonsgegevens	Werkinstructie Persoonsgegevens inzageverzoek gemeenten die niet samenwerken met Dienstverlening Drechtsteden art 15 AVG	Betrokkenen kunnen via een formulier op de site van de gemeente een verzoek tot inzage van de hun persoonsgegevens indienen. De Privacy Coördinator neemt het voortouw bij de inhoudelijke afhandeling. Er is daarnaast een ‘Notitie m.b.t. inzageverzoek en verwijderingsverzoek’ die nadere inhoudelijke kaders stelt.
Verzoek tot beperken verwerking persoonsgegevens	Werkinstructie Persoonsgegevens verzoek tot beperken verwerking in gemeenten die niet samenwerken met Dienstverlening Drechtsteden art 18 AVG en Zaaktype Persoonsgegevens beperking verwerking verzoek	Betrokkenen kunnen via een formulier op de site van de gemeente een verzoek tot het beperken van de verwerking van de hun persoonsgegevens indienen. De Privacy Coördinator neemt het voortouw bij de inhoudelijke afhandeling.

Verzoek tot correctie van persoonsgegevens	Werkinstructie Persoonsgegevens correctieverzoek gemeenten die niet samenwerken met Dienstverlening Drechtsteden art 16 AVG en Zaaktype Persoonsgegevens correctieverzoek	Betrokkenen kunnen via een formulier op de site van de gemeente een verzoek doen tot de correctie van persoonsgegevens. De Privacy Coördinator neemt het voortouw bij de inhoudelijke afhandeling.
Afhandelen bezwaar tegen verwerking van persoonsgegevens	Werkinstructie bezwaar verwerking persoonsgegevens in gemeenten die niet samenwerken met Dienstverlening Drechtsteden art 21 AVG en Zaaktype Persoonsgegevens verwerking bezwaar	Betrokkenen kunnen via een formulier op de site van de gemeente bezwaar maken tegen de verwerking van hun persoonsgegevens. De Privacy Coördinator neemt het voortouw bij de inhoudelijke afhandeling.

Deze processen zijn in regionaal verband opgesteld en het is de verantwoordelijkheid van de privacy coördinator om lokaal te zorgen voor borging proces en het actueel houden op de website. Dit is in het nieuwe privacybeleid expliciet opgenomen. Het is op basis van de aangeleverde informatie niet duidelijk of deze werkprocessen periodiek geëvalueerd worden.

3.3 Organisatorische inbedding van het beleid

In deze paragraaf wordt beschreven hoe in Papendrecht het beleid organisatorisch is uitgewerkt. Daarbij is aandacht voor de positionering van enkele sleutelfunctionarissen. Dat betreft de Functionaris Gegevensbescherming (FG), de Chief Information Security Officer (CISO) en de Privacy Coördinator (PC).

Gezamenlijke FG binnen de Drechtsteden

Gemeente Papendrecht heeft geen eigen Functionaris Gegevensbescherming. Er zijn twee Functionarissen Gegevensbescherming aangesteld die gezamenlijk alle Drechtstedengemeenten bedienen, alsmede de Omgevingsdienst Zuid-Holland Zuid. De Gemeenschappelijke Regeling Sociaal en de GR Dienst Gezondheid en Jeugd hebben ieder een eigen FG. De organisatorische aansturing van de FG's gebeurt door de gemeente Dordrecht. De huidige Functionarissen Gegevensbescherming zijn in 2023 gestart met hun functie. Voordat zij werden aangesteld heeft de bezetting van deze functie enige tijd gewisseld: in 2022 waren er twee andere tijdelijke FG's actief, die de in 2021 vertrokken FG's hebben opgevolgd. In de afgelopen drie jaar heeft de FG-functie dus drie verschillende bezettingen gekend.

Uit de interviews en de verdiepingssessie met de organisatie blijkt bovendien dat de FG's niet allemaal dezelfde taken hadden. In het verleden waren er Adviseurs Gegevensbescherming aangesteld, die oa de wettelijke adviestaken van de FG's uitoefenden. De FG richtte zich toen sec op toezichthoudende taken. Daarna is de capaciteit bij de FG's uitgebreid en zijn de adviestaken weer bij de FG belegd. De huidige FG voor Papendrecht heeft daarom meer tijd om proactief te adviseren. Hij is een traject gestart om te zorgen dat hij meer in het voortraject van besluitvorming en de totstandkoming van stukken wordt betrokken. Ook is de samenwerking met de PC door de huidige FG behoorlijk geïntensiveerd..

CISO

Gemeente Papendrecht heeft geen eigen CISO, deze functie is ondergebracht bij de Servicegemeente Dordrecht. De servicegemeente voert de CISO-taak uit voor alle aangesloten Drechtstedengemeenten. Binnen de gemeente Papendrecht zijn lokale Informatiebeveiligingsmedewerkers aangesteld. Op grond van het informatiebeveiligingsbeleid rapporteert de lokale IB-medewerker rechtstreeks aan de gemeentesecretaris.

Privacy Coördinator

De bezetting van de PC-rol is momenteel in transitie. In de afgelopen periode is de PC-rol bij Papendrecht ingevuld door de eigen concernjurist die hier 1 dag per week capaciteit voor ter beschikking had, aangevuld door externe inhuur. De afgelopen jaren is er sprake geweest van een capaciteitstekort: er was onvoldoende capaciteit beschikbaar om alle privacy-taken goed uit te voeren. Papendrecht heeft daarom recent een fulltime interne PC aangenomen, deze wordt op dit moment ingewerkt door de zittende PC's. Binnen de Drechtsteden wordt er veel samengewerkt en afgestemd tussen de PC's van de verschillende gemeenten, met name via het regionale PC-overleg.

3.4 Uitvoering van taken door samenwerkingspartners

Papendrecht heeft veel gemeentelijke taken belegd bij andere organisaties, doorgaans op regionaal niveau. In het nieuwe privacybeleid wordt aandacht gegeven aan de wijze waarop samenwerkingspartners een veilige omgang met informatie kunnen garanderen. Dit kan door het afsluiten van verwerkersovereenkomsten, of door te regelen dat de samenwerkingspartner zelf verwerkingsverantwoordelijke is.

3.4.1 Gemeenschappelijke regelingen

Papendrecht heeft veel gemeentelijke taken belegd bij gemeenschappelijke regelingen, samenwerkingsverbanden en andere organisaties. Binnen het sociale domein zijn deze belegd bij twee gemeenschappelijke regelingen: de Gemeenschappelijke Regeling Sociaal (GR Sociaal) en de Gemeenschappelijke Regeling Dienst Gezondheid & Jeugd Zuid-Holland Zuid (GR DG&J). Beide gemeenschappelijke regelingen hebben een eigen privacybeleid vastgesteld. Dit in lijn is met het privacybeleid zoals dat door Papendrecht en de andere Drechtsteden op dit moment wordt gehanteerd. Hierin is vastgelegd dat de beide gemeenschappelijke regelingen zelf verwerkingsverantwoordelijke zijn. De taken van de deelnemende gemeenten zijn aan de gemeenschappelijke regelingen gedelegeerd. Dit betekent dat de gemeenschappelijke regeling zelfstandig bevoegd is om de overgedragen bevoegdheden uit te oefenen, en zelf bestuurlijke verantwoordelijkheid draagt. Of de gemeenschappelijke regeling daadwerkelijk zelf verwerkingsverantwoordelijke is, moet uiteindelijk op grond van de feitelijke situatie worden bepaald. De belangrijkste vraag is in hoeverre de deelnemers door middel van instructies, verordeningen of beleidsregels het doel en de middelen van de verwerking van persoonsgegevens vaststellen. Als dit feitelijk door de deelnemers wordt bepaald, dan is de gemeenschappelijke regeling toch een verwerker en niet zelf verwerkingsverantwoordelijke. Op basis van de informatie die tot onze beschikking staat concluderen wij dat beide gemeenschappelijke regelingen zelf verwerkingsverantwoordelijke zijn. Wij hebben namelijk geen instructies of beleidsregels van Papendrecht kunnen terugvinden waarin het doel of de middelen van gegevensverwerking door de gemeenschappelijke regelingen worden bepaald.

Dit betekent dat de gemeenten die bij deze gemeenschappelijke regelingen zijn aangesloten niet tevens een verwerkersovereenkomst met de gemeenschappelijke regeling hoeven te sluiten met betrekking tot het verwerken van de persoonsgegevens van hun inwoners. Het gaat in dit geval namelijk om een samenwerking tussen meerdere verwerkingsverantwoordelijken, en niet om een verwerkersrelatie. Wel moeten het openbare lichaam van een gemeenschappelijke regeling en de deelnemende bestuursorganen een regeling vaststellen waarin zij hun onderlinge verantwoordelijkheid voor de nakoming van de verplichtingen uit de AVG afstemmen. De desbetreffende regeling is vormvrij. Gesteld zou kunnen worden dat het privacybeleid zoals dat door de diverse organisaties is vastgesteld al grotendeels aan deze eis voldoet. De diverse beleidsdocumenten zijn duidelijk inhoudelijk op elkaar geïnspireerd en bevatten een aanzet tot een verantwoordelijkheidsverdeling. Deze aanzet zou nog in meer detail kunnen worden uitgewerkt. Dat hoeft niet noodzakelijkerwijs in het (algemene) privacybeleid, maar kan ook per geval worden vastgesteld. Wel is het zinvol om hier goede (proces)afspraken over te maken, om te zorgen dat de verantwoordelijkheidsverdeling tussen alle partijen duidelijk is zodat in concrete gevallen tijdig kan worden bepaald welke partij aan zet is (verantwoordelijk is) voor het uitvoeren van specifieke activiteiten, zoals een DPIA.

GR Sociaal
De GR Sociaal kent twee uitvoeringsorganisaties:

- Sociale Dienst Drechtsteden, waar de taken van Papendrecht op het gebied van de Participatiewet en aanverwante wetten, de Wet maatschappelijke ondersteuning, de Wet op de schuldhulpverlening, de Wet Kinderopvang en de Wet werk en inkomen zijn ondergebracht.
- Drechtwerk, waar de taken van Papendrecht op het gebied van de Wet sociale werkvoorziening zijn ondergebracht.

De GR Sociaal heeft eigen privacybeleid vastgesteld, en heeft een eigen FG De GR Sociaal wordt bestuurd door een Algemeen Bestuur, waarin alle deelnemende gemeenten door een collegelid vertegenwoordigd zijn. Daarnaast is er een driekoppig dagelijks bestuur. Een gedeelte van de uitvoering van de Wet inburgering is gemandateerd aan de GRS, die de taak uitvoerde als verwerker.

GR DG&J
Bij de GR DG&J zijn de gemeentelijke taken van Papendrecht op het gebied van de Wet publieke gezondheid, de Leerplichtwet, de Jeugdwet, de Regionale Ambulancevoorziening en Veilig Thuis ondergebracht. Per 1 juli 2024 kent deze GR de volgende uitvoeringsorganisaties:

- Leerplicht en Voortijdig Schoolverlaten ZHZ
- Serviceorganisatie Jeugd ZHZ
- Veilig Thuis
- GGD

De GR DG&J heeft eigen privacybeleid vastgesteld, dat in lijn is met dat van de deelnemende gemeenten. De GR DG&J heeft een eigen FG.

3.4.2 Verwerkersovereenkomsten met samenwerkingspartners

Naast de deelname aan gemeenschappelijke regelingen heeft Papendrecht met een aantal samenwerkingspartners een verwerkersovereenkomst gesloten. Hierbij hanteert Papendrecht een model-verwerkersovereenkomst, die is geënt op de model-verwerkersovereenkomst van VNG. Het model van VNG bevat geen bepaling met betrekking tot het periodiek evalueren van de verwerkersovereenkomst. Een evaluatiebepaling is ook geen verplichting op grond van de AVG. Wel is het een best practice om verwerkersrelaties en -overeenkomsten periodiek te evalueren. Tegen deze achtergrond zijn wij ook ingegaan op de (afwezigheid van) evaluatiebepalingen in de verwerkersovereenkomsten.[11]

Bij dit onderzoek zijn zeven geldige verwerkersovereenkomsten aangetroffen. Het is op basis van de beschikbare informatie niet duidelijk of dit alle geldige verwerkersovereenkomsten zijn die gemeente Papendrecht heeft gesloten. Er is een overzicht van gesloten verwerkersovereenkomsten uit 2018, maar deze dient geactualiseerd te worden. In de jaarlijkse FG-adviezen van 2020, 2021 en 2022 wordt steeds aanbevolen om een overzicht van verwerkersovereenkomsten op te stellen. Dit is voor zover wij kunnen vaststellen tot op heden niet gebeurd. Wel zouden de verwerkingen op grond van de verwerkersovereenkomsten inmiddels zijn ondergebracht in het Register van verwerkingen. Dit zien wij inderdaad terug in het register, maar het is op basis van de beschikbare informatie niet mogelijk te constateren of het register op dit punt volledig en actueel is.

[11] De afwezigheid van een evaluatiebepaling in de verwerkersovereenkomsten betekent niet noodzakelijkerwijs dat er geen afspraken zijn gemaakt over evaluatie of dat er niet geëvalueerd wordt. In dit onderzoek hebben wij niet kunnen constateren dat dit gebeurt (is).

Verwerkersovereenkomst Servicegemeente Dordrecht
Servicegemeente Dordrecht voert voor de gemeente Papendrecht een groot aantal taken uit op het gebied van bedrijfsvoering, personeel en organisatie en ICT, waaronder zoals eerder vastgesteld de CISO-taak. Daarnaast voert Servicegemeente Dordrecht taken uit op het gebied van belastingheffing. In de verwerkersovereenkomst zijn alle zaken geregeld die in het kader van de AVG verplicht zijn, zoals het nemen van organisatorische en technische maatregelen ter bescherming van persoonsgegevens en wat er moet gebeuren ingeval van een incident of datalek. Er zijn ten opzichte van de verplichte onderdelen op grond van de AVG geen aanvullende afspreken gemaakt. Ook bevat de verwerkersovereenkomst geen evaluatiebepaling, en ook geen bepaling over reguliere rapportages met betrekking tot de bescherming van persoonsgegevens aan Papendrecht.

Verwerkersovereenkomst behorende bij de uitvoeringsovereenkomst Sterk Papendrecht 2019
Deze verwerkersovereenkomst ziet op de taken die Stichting Sociale Basis uitvoert op grond van de uitvoeringsovereenkomst Sterk Papendrecht 2019. In de verwerkersovereenkomst zijn alle zaken geregeld die in het kader van de AVG verplicht zijn, zoals het nemen van organisatorische en technische maatregelen ter bescherming van persoonsgegevens en wat er moet gebeuren in geval van een incident of datalek. Er zijn ten opzichte van de verplichte onderdelen op grond van de AVG geen aanvullende afspreken gemaakt. Ook bevat de verwerkersovereenkomst geen evaluatiebepaling, en ook geen bepaling over reguliere rapportages met betrekking tot de bescherming van persoonsgegevens aan Papendrecht. Er is een subsidierelatie met de Stichting Sociale Basis en Stichting Jeugdteams. Sterk Papendrecht treed naar buiten voor deze twee stichtingen.

Verwerkersovereenkomst behorende bij de subsidiebeschikking 2021 Coördinator vroegsignalering schulden
Deze verwerkersovereenkomst ziet op het uitvoeren van vroegsignalering van schulden door de Stichting Sociale Basis. Hiervoor ontvangt de stichting subsidie van uit de gemeente. In de verwerkersovereenkomst zijn alle zaken geregeld die in het kader van de AVG verplicht zijn, zoals het nemen van organisatorische en technische maatregelen ter bescherming van persoonsgegevens en wat er moet gebeuren ingeval van een incident of datalek. Er zijn ten opzichte van de verplichte onderdelen op grond van de AVG geen aanvullende afspreken gemaakt. Ook bevat de verwerkersovereenkomst geen evaluatiebepaling, en ook geen bepaling over reguliere rapportages met betrekking tot de bescherming van persoonsgegevens aan Papendrecht.

Verwerkersovereenkomst Signalerend huisbezoek Sociale Basis – Papendrecht
Deze verwerkersovereenkomst ziet op het uitvoeren van signalerende huisbezoeken, waarvoor de Stichting Sociale Basis subsidie ontvangt van de gemeente. In de verwerkersovereenkomst zijn alle zaken geregeld die in het kader van de AVG verplicht zijn, zoals het nemen van organisatorische en technische maatregelen ter bescherming van persoonsgegevens en wat er moet gebeuren ingeval van een incident of datalek. Er zijn ten opzichte van de verplichte onderdelen op grond van de AVG geen aanvullende afspreken gemaakt. Ook bevat de verwerkersovereenkomst geen evaluatiebepaling, en ook geen bepaling over reguliere rapportages met betrekking tot de bescherming van persoonsgegevens aan Papendrecht.

Verwerkersovereenkomst GR Sociaal m.b.t. Inburgering
Papendrecht heeft haar wettelijke taken op het gebied van inburgering aan de GR Sociaal gemandateerd. Deze verwerkersovereenkomst dekt de uitvoering van deze taken. In de

verwerkersovereenkomst zijn alle zaken geregeld die in het kader van de AVG verplicht zijn, zoals het nemen van organisatorische en technische maatregelen ter bescherming van persoonsgegevens en wat er moet gebeuren ingeval van een incident of datalek. Er zijn ten opzichte van de verplichte onderdelen op grond van de AVG geen aanvullende afspreken gemaakt. Ook bevat de verwerkersovereenkomst geen evaluatiebepaling, en ook geen bepaling over reguliere rapportages met betrekking tot de bescherming van persoonsgegevens aan Papendrecht.

Verwerkersovereenkomst uitvoering woonwagenbeleid en woonwagen locatie onderzoek
Deze overeenkomst is gesloten tussen Papendrecht en Companen, een organisatie die het woonwagenbeleid van de gemeente en een woonwagen locatie onderzoek uitvoert. In de verwerkersovereenkomst zijn alle zaken geregeld die in het kader van de AVG verplicht zijn, zoals het nemen van organisatorische en technische maatregelen ter bescherming van persoonsgegevens en wat er moet gebeuren ingeval van een incident of datalek. Er zijn ten opzichte van de verplichte onderdelen op grond van de AVG geen aanvullende afspreken gemaakt. Ook bevat de verwerkersovereenkomst geen evaluatiebepaling, en ook geen bepaling over reguliere rapportages met betrekking tot de bescherming van persoonsgegevens aan Papendrecht.

Convenant jeugdgroepenaanpak Papendrecht
Deze overeenkomst is in maart 2024 gesloten tussen de burgemeester van Papendrecht, de Politie Eenheid Rotterdam, jongerenwerk Suppord (een onderdeel van de gemeentelijke organisatie van Papendrecht) en het Openbaar Ministerie. Incidenteel worden de Raad voor de Kinderbescherming en de jeugdreclassering bij overleggen op grond van deze samenwerking betrokken, maar deze partijen hebben het convenant niet medeondertekend en met hen is ook geen aparte verwerkersovereenkomst gesloten. Het convenant is gebaseerd op de AVG en de Wpg, en ziet zowel op het verwerken van persoonsgegevens als op het verwerken van politiegegevens. Doel is het uitvoeren van een jeugdgroepenaanpak, waarbij signalen en informatie over bestaande en nieuwe problematische jeugdgroepen worden uitgewisseld, om te komen tot groepsgerichte maatregelen, gebiedsgerichte maatregelen. Zo kan waar nodig de beslissing worden genomen om bepaalde personen aan te melden bij een lokaal Zorg- of Veiligheidshuis, of kan ondersteuning vanuit het sociaal domein worden geboden. Hiervoor legt een procesregisseur namens de burgemeester als verwerkingsverantwoordelijke een bestand aan van persoonsgegevens van betrokkenen bij problematische jeugdgroepen en hun ouders of wettelijk vertegenwoordigers. Dit gebeurt op basis van een ‘bruto’ lijst van namen van personen die worden gelinkt aan de jeugdgroep op basis van de beschikbare politiegegevens, aangevuld met informatie over deze personen. Deze bruto-lijst wordt op verzoek van de burgemeester geleverd door de politie. Op basis van deze bruto-lijst wordt door de samenwerkende partijen gezamenlijk een netto-lijst vastgesteld, waarbij onder meer rekening gehouden wordt met verhuizing en detentie. Periodiek voeren de samenwerkende partijen overleg aan de hand van deze netto-lijst. Hier wordt bepaald of en welke maatregelen worden genomen.

In het convenant zijn alle zaken geregeld die in het kader van de AVG verplicht zijn, zoals het nemen van organisatorische en technische maatregelen ter bescherming van persoonsgegevens en wat er moet gebeuren ingeval van een incident of datalek. Voor deze onderdelen is aangesloten bij de model-verwerkersovereenkomst van Papendrecht. Daarnaast worden er aanvullende afspraken gemaakt over welke persoonsgegevens van de desbetreffende jongeren de procesregisseur vastlegt in het bestand problematische jeugdgroepen. Hieronder vallen ook gevoelige gegevens als omschrijvingen van het problematische gedrag van de jongeren, en politiegegevens die door de politie zijn verstrekt. Alle jongeren die in dit bestand worden opgenomen en hun wettelijk vertegenwoordigers worden hierover door de procesregisseur per brief geïnformeerd.

In het convenant wordt geen onderscheid gemaakt tussen het verwerken van politiegegevens en het verwerken van persoonsgegevens op grond van de AVG. In principe kunnen alle verwerkingen die op grond van het convenant plaatsvinden om beide soorten gegevens gaan. Verder valt op dat ervoor zover bij ons bekend is geen DPIA is uitgevoerd met betrekking tot het convenant. Dit zou naar ons oordeel wel moeten voordat met de uitvoering van het convenant begonnen wordt, omdat het leidt tot een potentieel groot aantal verwerkingen van persoonsgegevens en politiegegevens, waarbij mogelijk risico's optreden. Op basis van de beschikbare informatie stellen wij verder vast dat er geen advies aan de FG of de privacy coördinator gevraagd is over dit convenant.

3.5 Klachtenprocedure

De Gemeente Papendrecht heeft momenteel geen klachtenprocedure specifiek voor de AVG. Dit is ook geen wettelijk vereiste. Er wordt, ook in regionaal verband, onderzocht of op basis van het model van de VNG 'AVG Klachtenprocedure – IBD-versie 2023'een lokale procedure/werkproces opgesteld kan worden.

Uit de beschikbare informatie blijkt wel dat er een feitelijk werkende (algemene) klachtenprocedure bestaat in Papendrecht. Het klachtenoverzicht van de gemeente Papendrecht met betrekking tot de AVG bevat in totaal twee klachten, beide uit 2023:

- Een klacht met betrekking tot het delen van privégegevens via de gemeente. Deze is ongegrond verklaard, omdat het ging om het delen van gegevens in het kader van vroegsignalering op grond van de Wet gemeentelijke schuldhulpverlening, en hiervoor een afdoende verwerkingsgrondslag bestond.
- Een klacht over het verstrekken van privégegevens door de gemeente aan de kerk. Deze is ongegrond verklaard, omdat de gemeente de desbetreffende gegevens niet bleek te hebben verstrekt.

De privacyverklaring van de gemeente Papendrecht bevat bovendien afdoende informatie voor betrokkenen over het indienen van een klacht bij de PC of bij de Autoriteit Persoonsgegevens.

3.6 Register van verwerkingen en register van incidenten

Papendrecht voert zoals conform de AVG vereist is een register van verwerkingen. Dit is voor dit onderzoek ingezien en hierin zijn geen concrete onregelmatigheden of tekortkomingen geconstateerd. Wel bevatte het FG-advies over het jaar 2022 forse bevindingen met betrekking tot het register van verwerkingen. Op basis van de beschikbare informatie kunnen wij niet vaststellen of deze nu allemaal zijn opgelost.

Ook houdt Papendrecht een register van incidenten en mogelijke datalekken bij. Voor dit onderzoek is het register voor de jaren 2020 t/m 2022 bekeken. Er is in deze periode geen enkel datalek gemeld wat heeft geleid tot een melding bij de Autoriteit Persoonsgegevens. Het ging in alle gevallen om incidenten waarbij er slechts beperkte risico's aan de orde waren, zoals een e-mail die per abuis aan te veel personen was geadresseerd of een formulier wat in een printer was blijven liggen. Verder zijn er twee incidenten gemeld met betrekking tot softwareleveranciers: één koppeling tussen twee programma's die enige tijd voor iedereen open heeft gestaan, maar waarbij geen inbreuk is geconstateerd, en één externe cyberaanval op een leverancier van Papendrecht, waarbij geen persoonsgegevens van Papendrecht zijn buitgemaakt. Bovendien waren er in deze hele periode in

totaal slechts 11 gemelde incidenten. Op basis van de beschikbare informatie kan niet worden vastgesteld of het lage aantal gemelde datalekken en incidenten veroorzaakt wordt doordat er daadwerkelijk weinig datalekken en incidenten plaatsvinden, of doordat deze zich in de praktijk wel vaker voordoen, maar niet worden gemeld.

4. Gegevensbescherming in de praktijk

4.1 De praktijk binnen de organisatie

Een zorgvuldige omgang met persoonlijke gegevens moet een kernwaarde zijn van elke medewerker in een overheidsorganisatie. Daarmee vormen de menselijke factor en de dagelijkse uitvoeringspraktijk een gemeente- en organisatiebreed aandachtspunt. In de interviews en één verdiepende mini-PIA met betrekking tot de uitvoering van de Wpg is inzicht verkregen over de wijze waarop het privacybeleid van de gemeente in de dagelijkse praktijk tot uitdrukking komt. De dagelijkse uitvoeringspraktijk beperkt zich niet tot de gang van zaken in de ambtelijke organisatie van de gemeente. In het kader van het onderzoek is ook aandacht besteed aan de positie van de raad. Bovendien is kort geïnventariseerd wat de rol en betrokkenheid van de OR is met betrekking tot privacy en bescherming van persoonsgegevens.

4.1.1 Algemene bevindingen

Portefeuilleverdeling en verantwoordelijkheden in het college
Hoewel het geen onderdeel is van het privacybeleid *an sich*, gaan we in deze passage ook kort in op de portefeuilleverdeling in het college. Uit de door ons gevoerde gesprekken blijkt dat het college de bestuurlijke verantwoordelijkheid voor het onderwerp privacy ervaart. De burgemeester is portefeuillehouder van privacy in het algemeen en daar waar het openbare orde en veiligheid betreft. Een wethouder heeft de portefeuille digitalisering en informatieveiligheid. In dit onderzoek zijn geen problemen of vraagstukken naar voren gekomen ten aanzien van de huidige portefeuille- en verantwoordelijkheidsverdeling in het college.

Schets organisatiecultuur met betrekking tot privacy
Uit de interviews en de bevindingen naar aanleiding van de documentstudie rijst een beeld op van een cultuur van vrijblijvendheid met betrekking tot veel geldend beleid over privacy en gegevensbescherming. Veel van de afspraken en beleidsvoornemens die door Papendrecht op papier zijn gezet en formeel zijn vastgesteld, worden in de praktijk niet of niet altijd nagekomen. Na afloop van een DPIA wordt niet altijd verslag gedaan aan de FG over de daadwerkelijk genomen maatregelen, zoals op grond van het vastgestelde werkproces voor DPIA’s verplicht is. DPIA’s worden voor zover bij ons bekend ook niet na de hiervoor vastgestelde termijn opnieuw bezien. Het onderwerp privacy komt voor zover bij ons bekend niet periodiek aan de orde bij interne overleggen binnen de gehele gemeentelijke organisatie van Papendrecht (anders dan het reguliere overleg tussen de PC’s en de FG), zoals op grond van het geldende privacybeleid van Papendrecht wel zou moeten gebeuren. Ook het privacybeleid en de werkprocessen rond de AVG en de Wpg zelf worden niet op vaste tijdstippen geëvalueerd en waar nodig herzien. Op basis van de beschikbare informatie kunnen wij niet constateren dat er sprake is van een functionerende PDCA-cyclus. Deelname van nieuw personeel aan activiteiten op het gebied van privacybewustwording is verplicht gesteld. Verder worden in de maand oktober van elk jaar vele bewustwordingsactivitetiten opgezet, waaraan deelname wordt gestimuleerd. Daarnaast is de e-learning betreffende AVG en informatieveiligheid, volgens het informatieveiligheidsbeleid verplicht (10 gouden regels) en is er begin 2024 een nieuwe elearning "Sir Askalot" gestart. Elke medewerker krijgt elke week een paar vragen te beantwoorden. Een uitgebreidere e-learning wordt ontwikkeld en waarschijnlijk verplicht gesteld.

Activiteiten van de FG's

De FG's Drechtsteden voeren jaarlijks een FG-meting uit met betrekking tot de gemeente Papendrecht, waarbij zij de stand van zaken op het gebied van gegevensbescherming en privacy in de gemeente Papendrecht inventariseren en de organisatie adviezen geven over verbeteringen. De FG-adviezen over april 2020- april 2021, april t/m december 2021 en het jaar 2022 zijn bij dit onderzoek betrokken. De rapportage over het jaar 2022 is door de tijdelijke interim-FG's geschreven, de twee eerdere rapporten door de voorgaande vaste functionarissen. De huidige nieuwe FG komt dit jaar met een FG-advies over het jaar 2023.

Een deel van de aanbevelingen die de FG's in de onderzochte adviezen hebben gedaan is inmiddels opgevolgd. Zo is het Register van verwerkingen aangevuld en verbeterd, en is er bij inkoop van ICT meer ingezet op Privacy by Design vanuit de CISO en de Servicegemeente Dordrecht. Ook is de organisatie beter bij gaan houden hoeveel medewerkers aan welke nascholingsactiviteiten en activiteiten rondom bewustwording hebben deelgenomen. De belangrijkste nog openstaande aanbevelingen uit de drie onderzochte FG-adviezen (2020 – 2022) zijn:

- In de FG-adviezen over alle drie getoetste jaren wordt aanbevolen om een actueel en volledig overzicht te maken van benodigde en afgesloten verwerkersovereenkomsten, alsmede van situaties van gezamenlijke verwerkingsverantwoordelijkheid (zoals bij de gemeenschappelijke regelingen). Ook wordt het advies gegeven om waar nodig aanvullende verwerkersovereenkomsten te sluiten. Deze aanbevelingen zijn tot op heden voor zover bij ons bekend niet opgevolgd. In het register van verwerkingen is weliswaar informatie toegevoegd over verwerkingen die op grond van verwerkersovereenkomsten plaatsvinden, maar op basis hiervan kan niet worden vastgesteld of hiermee alle verwerkersovereenkomsten afgedekt zijn. Mogelijk bestaan er overeenkomsten die niet zijn verwerkt in het Register. Bovendien kan uit het Register niet worden afgeleid hoe lang de desbetreffende overeenkomst al loopt en of er evaluatie c.q. herziening heeft plaatsgevonden. Er staat een actualisatie van het register op de planning voor de tweede helft van 2024, waarbij alle verwerkingen worden doorgelopen met proceseigenaren.
- In 2020 heeft de FG geconstateerd dat er een achterstand ingehaald moest worden op gebied van het uitvoeren van DPIA's. Deze achterstand bestond blijkens de FG-adviezen over 2021 en 2022 in deze jaren nog steeds. De FG-adviezen refereren aan een plan voor het prioriteren van de nog uit te voeren DPIA's op basis van risicoanalyse, met daarbij een planning, waarvan de haalbaarheid wordt betwijfeld. De gemeente werkt op dit moment aan het programma 'Processen op orde', waarin een afweging wordt gemaakt over het uitvoeren van een DPIA voor kritieke processen. In paragraaf 4.1.2 gaan we verder in op dit programma. Op basis van de beschikbare informatie kan worden vastgesteld dat er nog steeds sprake is van achterstanden en vertragingen met betrekking tot het uitvoeren van DPIA's. Ook een aantal specifiek door de FG aanbevolen DPIA's, zoals met betrekking tot het thuiswerken, AFAS en de wijkteams binnen het sociaal domein, zijn nog niet uitgevoerd. Aan een DPIA voor MS Teams wordt in regionaal verband gewerkt. De uitkomsten hiervan zijn ten tijde van de onderzoeksperiode nog niet bekend. Capaciteitsgebrek bij het privacy-office van Papendrecht is hier mede de aanleiding toe geweest. Na constatering door de FG in 2021 zijn er verbeteringen doorgevoerd in het DPIA provces. De processenstappen na advies van de FG op een DPIA zijn aangescherpt. Zo wordt er terug gerapporteerd aan de FG over de genomen maatregelen en wordt er een besluit tot risico-acceptatie genomen. De nauwere banden met de FG hebben daar een positieve invloed op. Wel wordt een DPIA nog zeker niet in alle gevallen adequaat opgevolgd (in termen van te nemen maatregelen), en voor zover wij kunnen vaststellen zijn deze nog niet periodiek herbezien.
- Alle drie de FG-adviezen bevatten aanbevelingen met betrekking tot het regelmatig uitnodigen van de FG bij vergaderingen van het midden- en hogere management en het vroegtijdig betrekken van

de FG wanneer beslissingen met gevolgen voor gegevensbescherming zullen worden genomen. Met betrekking tot het vroegtijdig betrekken van de FG kan in het recente verleden zeker een verbetering worden geconstateerd. De huidige FG geeft aan steeds vaker vroegtijdig te worden betrokken door de ambtelijke organisatie (bijvoorbeeld door middel van een pre-DPIA).

- De FG heeft aangegeven in het algemeen minder betrokkenheid te hebben op hoger managementniveau (managementniveau boven teamleiders). Dit contrasteert in negatieve zin met zijn steeds betere betrokkenheid op het niveau van de medewerkers en de teamleiders.
- De FG heeft in alle drie getoetste jaren geadviseerd het Register van verwerkingen op de website van de gemeente te publiceren. Dit is niet verplicht op grond van de AVG, maar heeft wel een positief effect op de positie van betrokkenen. Deze aanbeveling wordt bij de actualisering in 2024 opgevolgd.
- In 2022 is een externe audit uitgevoerd op grond van de Wpg. Deze bevatte een grote hoeveelheid verbeterpunten. Daarom meldde de FG in zijn advies over 2022 dat een herstelplan en plan van aanpak moesten worden opgesteld. Er is een verbeterplan met maatregelen opgesteld en er zijn diverse acties uitgevoerd naar aanleiding van deze audit. In paragraaf 4.1.2 wordt hier nader op ingegaan.
- De FG heeft in 2022 aanbevolen om het trainingsprogramma dat wordt uitgevoerd ter verhoging van het privacy bewustzijn onder de medewerkers van Papendrecht te evalueren. Dit programma is meerdere keren aangepast en verbeterd.

Het FG verslag over 2023 was tijdens de onderzoeksperiode nog niet beschikbaar.

Uit de interviews blijkt dat met de aanstelling van de huidige FG's een positieve ontwikkeling op het gebied van de betrokkenheid van en samenwerking met de FG's in gang is gezet, met name op het niveau van de medewerkers en de teamleiders. De huidige FG's worden gewaardeerd om hun proactieve houding en benaderbaarheid. Uit de interviews blijkt ook dat de betrokkenheid van de FG's bij initiatieven waarbij er iets speelt op het gebied van privacy en gegevensbescherming niet altijd is gegarandeerd. De FG voor Papendrecht is wel agendalid van portefeuillehoudersoverleg, zodat hij is aangehaakt bij de stukkenstroom richting het college van B&W. Dit geeft hem de gelegenheid om stukken te beoordelen op privacy en de bescherming van persoonsgegevens en indien nodig te handelen op basis daarvan. Dit laatste is een aantal keer voorgekomen. De FG geeft aan in de toekomst toe te willen werken naar een situatie waarin hij zich iets meer terug kan trekken en er binnen de organisatie geborgd is dat hij tijdig betrokken wordt wanneer dit nodig is.

Met betrekking tot de betrokkenheid van de FG in verschillende overleggen, hebben we bevonden dat de FG regulier overleg heeft met de gemeentesecretaris naar aanleiding van de jaarstukken en het FG verslag. Ook is er periodiek overleg tussen de FG en de privacy coördinatoren. Ten tijde van de onderzoeksperiode was de FG (nog) niet aanwezig geweest bij het MT van de gemeente en was er (nog) geen overleg geweest met de concerncontroller, hoewel de aanwezigheid van de FG bij dergelijke overleggen wel een meerwaarde kan hebben.

Activiteiten van de Privacy Coördinatoren

Uit de gehouden interviews en de FG-adviezen van de afgelopen jaren blijkt duidelijk dat de achterstand die Papendrecht heeft opgelopen op het gebied van gegevensbescherming en privacy mede te wijten is aan capaciteitsgebrek bij de Privacy Coördinatoren. Papendrecht heeft er daarom voor gekozen om in 2023 een fulltime Privacy Coördinator in vaste dienst aan te stellen. De effecten hiervan blijken nog niet uit dit onderzoek, waarschijnlijk omdat deze persoon op dit moment nog wordt ingewerkt door de huidige coördinatoren. Uit de interviews blijkt dat de Privacy Coördinatoren de

nodige plannen hebben om verbeterpunten aan te pakken, zoals het periodiek en gestructureerd aan de orde laten komen van privacy bij diverse overleggen binnen de organisatie. Verder willen ze de achterstanden op het gebied van DPIA's inlopen, maar door het voormelde capaciteitsgebrek is het nog niet tot daadwerkelijke uitvoering van deze plannen gekomen. Per juli 2024 is een tijdelijke projectleider voor het project "Processen op orde" gestart, die de meest relevante processen in beeld zal brengen, waarvan procesbeschrijvingen gemaakt worden. Daarnaast wordt dan per proces ingezoomd op relevante wetgeving, waaronder de AVG en wordt gekeken naar de vereiste DPIA'S en verwerkersovereenkomsten. Op basis van de interviews kan worden geconstateerd dat er met betrekking tot de activiteiten van de Privacy Coördinatoren nog sprake is van een transitiefase. Niet alle medewerkers weten de privacy coördinatoren even goed te vinden, bovendien voelen zij zich ook niet in alle gevallen adequaat ondersteund. Het is naar wij kunnen vaststellen in de onderzochte periode zelfs meerdere keren voorgekomen dat medewerkers van Papendrecht advies en ondersteuning vroegen aan de Privacy Coördinator van een andere Drechtsteden-gemeente in plaats van aan de eigen coördinatoren.

Activiteiten op het gebied van het vergroten van het privacy bewustzijn en (na)scholing
Papendrecht heeft een privacybewustwordingsplan/nascholingsplan voor de medewerkers op het gebied van privacy. Voor nieuwe medewerkers staan de trainingen per jaar ingepland en in de maand oktober vindt altijd de WIPI plaats. De activiteiten op het gebied van het vergroten van het privacy bewustzijn en nascholing van de medewerkers van de gemeente Papendrecht bestaan uit:

- Uitvoeren van een e-learningmodule op het gebied van informatiebeveiliging en privacy (Sir Ask-A-Lot). Dit wordt vanuit het CISO-team geïnitieerd. Ook raadsleden krijgen vragen vanuit deze module op hun Papendrecht-mailaccount.
- Training voor alle nieuwe medewerkers op het gebied van gegevensbescherming en privacy.
- Jaarlijkse weken van de Informatiebeveiliging, privacy en integriteit (WIPI). Deze worden vanuit de Privacy Coördinatoren, informatieveiligheidsadviseurs en het CISO-team georganiseerd. Gedurende deze maand wordt een aantal lunchbijeenkomsten georganiseerd over actuele onderwerpen met betrekking tot onder meer privacy en gegevensbescherming, en wordt er ook op andere manieren aandacht aan deze onderwerpen besteed. Medewerkers worden door de gemeentesecretaris uitgenodigd om hier actief aan deel te nemen en de deelname wordt ook bijgehouden, maar dit is niet verplicht.

Uitvoerende teams
De teamleiders van de uitvoerende teams zijn ervoor verantwoordelijk dat binnen hun team aan de AVG en (voor zover van toepassing) de Wpg wordt voldaan. Uit de interviews blijkt dat deze verantwoordelijkheid ook echt gevoeld wordt, en er sprake is van een hoge mate van betrokkenheid. Door capaciteits- en kennisgebrek binnen de teams is het echter niet altijd gemakkelijk om hier ook daadwerkelijk uitvoering aan te geven. Hierdoor ontstaan achterstanden op het gebied van gegevensbescherming en privacy. DPIA's blijven soms te lang liggen of worden niet tijdig afgerond of opgevolgd. Complicerende factor hierbij is dat veel taken op regionaal niveau zijn belegd, maar hier in de afgelopen jaren ook het nodige in is gewijzigd. Daarom is het niet altijd duidelijk voor alle betrokken organisaties of een DPIA op regionaal of lokaal niveau moet worden opgepakt, of loopt dit proces stroef. Zo is de DPIA met betrekking tot signalerende huisbezoeken ouderen door de welzijnsorganisaties met drie gemeenten gezamenlijk uitgevoerd. Omdat elke gemeente toch weer net een ander proces volgt, kostte dit veel tijd en viel de meerwaarde van de samenwerking grotendeels weg. Iedere gemeente heeft uiteindelijk het concept aangevuld met de couleur locale en de DPIA vastgesteld.

Verder valt op dat er op het gebied van privacy en gegevensbescherming weinig tot geen specifieke kennis- of bewustwordingsactiviteiten binnen de teams plaatsvinden, met uitzondering van Wpg-specifieke training voor de boa's. Er worden bijvoorbeeld geen casussen besproken, en het onderwerp komt ook niet regelmatig aan de orde tijdens teamoverleggen. Bovendien wordt er geen gebruik gemaakt van de mogelijkheid om binnen ieder team een medewerker als privacy-ambassadeur in te zetten, die een aanjaag- en signaleringsfunctie binnen het team vervult.

Binnen de organisatie waargenomen verbeterpunten
In het kader van dit rekenkameronderzoek zijn in de interviews de volgende verbeterpunten genoemd door medewerkers van de gemeente Papendrecht:

- Project 'Processen op Orde' verder uitrollen en afmaken, en hier voldoende capaciteit en prioriteit voor vrijmaken.
- DPIA's uitvoeren voor alle processen waar een risico ligt op het gebied van gegevensbescherming en privacy. Dit is nu nog onvoldoende geborgd, en er is in de afgelopen jaren een flinke achterstand opgelopen op dit gebied. Per 1 juli 2024 is een projectleider aangetrokken om dit project vlot te trekken en structureler in beeld te krijgen bij welke processen er nog DPIA's uitgevoerd moeten worden, en hier een concreet plan van aanpak voor te maken. Het inlopen van de achterstand op het gebied van DPIA's zal echter ook bij de uitvoerende teams capaciteit kosten. Hier is mogelijk extra capaciteit nodig om deze inhaalslag te kunnen maken.
- In de organisatie processen beter borgen dat beperkende maatregelen op grond van DPIA's daadwerkelijk genomen worden, dat hierover aan de FG terug wordt gerapporteerd, en dat eventueel restrisico worden geaccepteerd. Zorgen dat geëscaleerd wordt naar managementniveau wanneer dit niet goed verloopt.
- Vaker raadssessies organiseren over privacy en gegevensbescherming, bijvoorbeeld met een frequentie van twee keer per jaar. De geplande raadsessies worden ook geannuleerd vanwege volle raadsagenda's. Dit heeft te maken met de nieuwe vergadercyclus van de raad.
- Aanscherpen van de PDCA-cyclus op het gebied van de lerende organisatie (leren van gemaakte fouten/casussen in de praktijk). Meer leren van elkaar, meer ruimte voor het bespreken van eventuele fouten en incidenten, en regelmatig casussen onder de medewerkers bespreken, en zorgen dat hier niet alleen binnen de teams maar ook organisatiebreed van geleerd wordt.
- Structurele afspraken met de FG maken over aanhaken bij reguliere overleggen, met name op management/DT-niveau, en betrokkenheid bij de stukkenstroom.
- Privacy-coördinatoren periodiek laten aansluiten bij MT/DT- en teamoverleggen om onderwerpen op het gebied van privacy en gegevensbescherming te bespreken.
- Duidelijkere en concrete afspraken met verwerkers en gemeenschappelijke regelingen over periodieke rapportage en incidentmanagement op het gebied van privacy en regulier overleg voeren met deze organisaties langs de privacy- en informatiebeveiligingslijn. Nu wordt er eigenlijk blind op vertrouwd dat dit wel goed zit, dat is wat de medewerkers betreft niet voldoende.

4.1.2 Beveiligingsmaatregelen in (uitvoerende) processen

De gemeente heeft een algemeen overzicht van de processen die binnen de gemeente worden uitgevoerd en een algemeen beeld welke beveiligingsmaatregelen hiervoor genomen zouden moeten worden. Dit overzicht is gebaseerd op een standaardtemplate die voor Nederlandse gemeenten van toepassing is. Op papier geeft dit inzicht in de beveiligingsmaatregelen in (uitvoerende) processen binnen de gemeente.

In de praktijk is dit beeld echter niet gevalideerd. Dat betekent dat de technische en organisatorische maatregelen die de gemeente ten behoeve van (uitvoerende) processen moet nemen niet daadwerkelijk in de praktijk zijn getoetst en er geen zekerheid is over de risico's die de gemeente op dit vlak loopt. Het risico hiervan is dat er binnen uitvoerende afdelingen gewerkt wordt op een wijze die onbekende, ongewenste en/of niet-geaccepteerde beveiligingsrisico's met zich meebrengt, ook op het vlak van persoonsgegevens.

De gemeente heeft deze achterstand geconstateerd en is een programma gestart om dit te herstellen ("Processen op orde"), te beginnen bij de kritieke processen. Hierbij moeten niet alleen informatiebeveiligingsaspecten worden meegenomen, maar wordt er ook meteen gekeken naar de bescherming van persoonsgegevens. Het programma is sinds 2023 in uitvoering maar heeft nog niet de gewenste voortgang. In 2024 is er daarom besloten om externe expertise in te huren en op deze manier een impuls aan de voortgang te geven. Ten tijde van dit onderzoek was deze verbeterslag in gang gezet maar was het nog te vroeg om concrete resultaten te rapporteren.

Ten aanzien van de aansturing van samenwerkingspartners (specifiek de servicegemeente en GR Sociaal (m.b.t. de sociale dienst) valt op dat er voor meerdere jaren ENSIA-bevindingen ten aanzien van Suwinet en DigiD zijn die niet opgelost zijn/worden.

4.2 Wet politiegegevens in de praktijk

In het kader van dit onderzoek is een verdiepende mini-DPIA uitgevoerd met betrekking tot de implementatie van de Wet politiegegevens door het boa-team. De Wpg kent dezelfde basisprincipes met betrekking tot gegevensbescherming en privacy als de AVG, maar wijkt hier op een aantal punten vanaf. Zo zijn de verwerkingsverantwoordelijkheid en de bewaartermijnen wettelijk geregeld, en valt er ook op een aantal andere punten minder te kiezen voor de implementerende organisatie. Daarom is het voldoen aan de Wpg in veel grotere mate te automatiseren dan het voldoen aan de AVG. Een gemeente kan aan een flink deel van de eisen van de Wpg voldoen door een Wpg-conform zaaksysteem voor zijn boa's aan te schaffen en dit correct in te stellen en te gebruiken. Verder kent de Wpg een periodieke auditverplichting voor gemeenten: eens in de vier jaar dient een externe audit te worden uitgevoerd. Eens per jaar moet er een interne audit door de eigen organisatie worden uitgevoerd.

In Papendrecht is in 2022 een externe audit uitgevoerd met betrekking tot de implementatie van de Wpg. Deze bevatte forse bevindingen: de uitkomst hiervan was dat de gemeente Papendrecht op slechts 4 van de 36 getoetste punten geheel of gedeeltelijk aan de Wpg voldeed – op de resterende 32 punten was dit dus niet het geval. De belangrijkste bevindingen uit deze audit waren:

- De gebruikte ICT-systemen (Twyns en Mozaiek) voldoen niet aan de vereisten die op grond van de Wpg gelden voor de systemen waarmee boa's politiegegevens horen te verwerken. Zo waren de bewaartermijnen niet ingesteld en werd hier ook niet op gemonitord. Ook bevatten de systemen geen adequate logging met betrekking tot politiegegevens, en voldeden ze niet aan de geldende technische eisen op het gebied van informatie- en toegangsbeveiliging. Er was bovendien nooit een DPIA uitgevoerd op deze systemen.
- Er was geen register van verwerkingen waarin de doelbinding, rechtmatigheid en noodzakelijkheid van verwerkingen van politiegegevens werd vastgelegd. Ook werden bijzondere politiegegevens niet als zodanig vastgelegd in een register van verwerkingen.

- Ook was er geen bevoegd functionaris aangewezen. Dit moet iemand zijn met kennis van de Wpg, die beslist wie er toegang tot welke gegevens mag hebben en of gegevens verstrekt kunnen worden aan samenwerkingspartners.
- Er werd niet gecontroleerd of verwerkingen wel voldeden aan de eisen van doelbinding, rechtmatigheid en noodzakelijkheid. Ook werd er niet gecontroleerd of de verwerkte gegevens wel juist en volledig waren, en of feiten en subjectieve meningen hierbij wel voldoende gescheiden werden. Het vier-ogen principe zoals de Wpg dit vereist met betrekking tot verwerking van politiegegevens werd dus niet correct toegepast.
- Het in dienst en uit dienst-proces van de boa's was niet helder vastgelegd en er was geen autorisatiematrix. Er werd geen periodieke controle uitgevoerd op de autorisaties van de gebruikers van de systemen. Zo was dus niet geborgd dat alleen huidige bevoegde boa's het systeem konden gebruiken.
- De boa's hadden in de onderzochte periode geen privacy- en securitytraining ontvangen.
- Er was geen procedure ingericht voor het voldoen aan de eisen op het gebied rechten van betrokkenen, zoals het recht op inzage en het recht op correctie van onjuiste gegevens.

De FG heeft Papendrecht naar aanleiding van deze audit in 2022 dringend geadviseerd om een herstel- en verbeterplan op te stellen. Er is een verbeterplan met maatregelen opgesteld en er zijn diverse acties uitgevoerd naar aanleiding van deze audit. Er is voor zover wij kunnen nagaan geen besluit op DT-niveau genomen over het verbeterplan of is de voortgang op het plan op DT-niveau gemonitord.

De gemeentesecretaris is formeel eindverantwoordelijk voor de implementatie van de AVG en de Wpg. De zittende lijndirecteur heeft geen actieve betrokkenheid gehad bij de audit en het opstellen van het verbeterplan met de vereiste maatregelen. De teamleiders van de boa's en privacy coördinatoren zijn verantwoordelijk voor het uitvoeren van de verbetermaatregelen. Zij zijn meermaals betrokken bij de uitvoering van het plan. De aanbevelingen uit de audit zijn op medewerkersniveau in het privacy- en informatieveiligheidsteam tezamen met de boa-coördinator opgepakt.

Veruit de belangrijkste aanbevolen maatregel was het aanschaffen van een Wpg-conform ICT-systeem. Dit is echter verre van soepel verlopen. Er diende eerst een goedgekeurde DPIA te worden gedaan en dit proces duurde om uiteenlopende redenen erg lang, waarbij de complexe convenant structuur met diverse landelijke partijen het extra ingewikkeld maakte. De DPIA is uiteindelijk afgerond en er is overgegaan tot de aanschaf van BRS, een Wpg-conform ICT-systeem. Dit systeem was ten tijde van dit onderzoek nog niet operationeel en de exacte werking/inrichting was nog niet bekend. Verder is er, ook in regionaal verband, gewerkt aan het scholen van de privacy coördinatoren op gebied van de Wpg en is gewerkt aan het opstellen van Wpg beleid.

Daarnaast hebben de boa's in 2023 een Wpg-training gevolgd. Op dit moment wordt druk gewerkt aan de implementatie van het nieuwe BRS-systeem, waaronder het instellen van rollen en rechten voor gebruikers, het trainen van de boa's in het gebruik van het nieuwe systeem, en het aanpassen van de werkinstructies van de boa's aan het nieuwe systeem. De verwachting is dat dit voor het einde van het jaar zal zijn afgerond. Ook is het verwerkingenregister van Papendrecht aangevuld, en zijn de Wpg-verwerkingen hier nu ook in terug te vinden.

Rond de overgang naar BRS bestaat er echter nog wel een risico wat binnen de onderzoeksperiode niet was opgelost, namelijk wat er gebeurt met de politiegegevens die zijn ingevoerd in Twyns en Mozaiek, de huidige systemen. Sinds het contract met de leverancier van deze systemen is opgezegd reageert deze niet meer op verzoeken om de overdracht van gegevens. Bovendien heeft de leverancier eerder uit zichzelf gegevens uit deze systemen verwijderd die eigenlijk bewaard hadden moeten worden. Het risico bestaat dus dat de politiegegevens die zijn opgeslagen in de huidige systemen geheel of gedeeltelijk verloren gaan bij de overgang naar BRS. Bij de oplevering van dit onderzoek was niet duidelijk in hoeverre dit risico is opgelost, dan wel of het nog steeds bestaat.

De boa-coördinator en de privacy coördinatoren hebben zich in de afgelopen jaren enorm ingespannen om het stroeve proces rond de aanschaf van BRS vlot te trekken. De processen met de Servicegemeente rond de aankoop van het nieuwe ICT-systeem verliepen erg traag, mede omdat het aanvankelijk nog de bedoeling was om de implementatie van de Wpg op regionaal niveau op te pakken en er pas in tweede instantie voor een lokale aanschaf is gekozen. Een zeer belangrijke factor was echter ook capaciteits- en kennisgebrek aan de zijde van Papendrecht. Dit geldt blijkens de interviews zowel voor het uitvoerende team als voor de privacy coördinatoren. In de afgelopen periode is daarom regelmatig de privacy coördinator van een naburige gemeente die hetzelfde ICT-systeem gebruikt en al verder is met de implementatie ervan om advies gevraagd. In de tussentijd heeft Papendrecht in de jaren 2022 en 2023 bewust geen interne Wpg-audits uitgevoerd. Dit zou alleen maar ten koste gaan van de toch al te beperkte capaciteit, en de uitkomst stond bovendien op voorhand vast, want zonder de aanschaf en implementatie van een nieuw ICT-systeem kon Papendrecht onmogelijk aan de eisen vanuit de Wpg voldoen. Al met al heeft Papendrecht dus in de jaren 2021 (het toetsjaar van de audit) tot en met de onderzoeksperiode niet voldaan aan het merendeel van de eisen op het gebied van gegevensbescherming en privacy uit de Wpg.

De problemen rond de aanschaf van BRS en de risico’s die hieruit voortvloeiden voor Papendrecht zijn aangekaart bij de verantwoordelijk teamleider. Dit heeft echter niet geleid tot agendering binnen het DT. De benodigde formatie is wel in het DT geagendeerd. Verder heeft de gemeentesecretaris aangegeven te hebben vernomen dat het traject niet soepel verliep. In dit onderzoek hebben we niet kunnen achterhalen welke afwegingen er zijn gemaakt met betrekking tot agendering in het DT en bij wie er signalen over de risico’s en tekortkomingen zijn neergelegd.

De gemeenteraad van Papendrecht is voor zover achterhaald kon worden nooit inhoudelijk geïnformeerd over de slechte resultaten van de Wpg-audit in 2022, de (voortgang van) het verbeterplan en de problemen rond de aanschaf van BRS. De enige informatie aan de raad die wij konden vinden betreft een korte passage in de jaarrapportage van 2022, waarin slechts wordt vermeld dat de externe Wpg-audit is uitgevoerd en is verzonden aan de Autoriteit Persoonsgegevens. De raad geeft geen vragen gesteld over de Wpg-audit of om aanvullende informatie gevraagd.

4.3 Sturing en informatievoorziening op gemeenschappelijke regelingen en samenwerkingspartners

Zoals eerder toegelicht is de gemeente voor de uitvoering van primaire taken in sterke mate afhankelijk van gemeenschappelijke regelingen en samenwerkingspartners. Dergelijke constructies vragen om sturing op de bescherming van persoonsgegevens bij deze partijen. Afhankelijk van de verhouding tussen de gemeente en de betreffende partij kan het gaan om een verwerkers-relatie of een eigenstandige verwerkingsverantwoordelijkheid. In alle gevallen is het politiek en bestuurlijk van belang om in enige mate inzicht te hebben in de bescherming van de persoonsgegevens in de praktijk.

Op basis van de door ons gevoerde gesprekken blijkt dat er slechts beperkt zicht is op de verwerking van persoonsgegevens door samenwerkingspartners. In het geval van de Servicegemeente Dordrecht (SGD) is dit in het bijzonder door de gesproken functionarissen gesignaleerd. Hierbij gaat het niet alleen om de persoonsgegevens van inwoners, maar ook om de HR-gegevens van het eigen personeel van de gemeente. Er is nauwelijks tot geen inzicht in de risico's, het tactisch en operationeel beleid, relevante beveiligingsincidenten en de genomen beveiligingsmaatregelen. Veelal zijn voortgangsrapportages beperkt in informatie, waar beveiligingsincidenten en –maatregelen door het SGD worden gemeld en frequentie en is het handelingsperspectief van de gemeente beperkt. De capaciteit van de SDG lijkt daarnaast beperkt te zijn en er is een focus op een (intern) verbeterprogramma met weinig aandacht voor aanpalende beleidsterreinen.

Met de andere samenwerkingspartners met wie Papendrecht een verwerkersrelatie heeft zijn voor zover bekend helemaal geen voortgangsrapportages of evaluatiegesprekken afgesproken: na het sluiten van de verwerkersovereenkomst wordt er behoudens incidenten voor zover bekend niet meer over privacy of gegevensbescherming met deze partijen gesproken. In de afgelopen jaren zijn geen incidenten gemeld. Dat betekent dat Papendrecht voor zover bij ons bekend geen actueel beeld heeft van de stand van zaken met betrekking tot gegevensbescherming bij de samenwerkingspartners, en of hierbij risico's ontstaan voor de gemeente als verwerkingsverantwoordelijke.

De beide gemeenschappelijke regelingen zijn zelfstandig verwerkingsverantwoordelijke. Hiermee ligt de relatie daarom ook anders, en hoeft er geen verwerkersovereenkomst te worden gesloten. Echter, in een situatie waarin meerdere verwerkingsverantwoordelijken samenwerken zoals bij de gemeenschappelijke regelingen het geval is, is de *best practice* wel dat er uitdrukkelijke afspraken gemaakt worden over de concrete verantwoordelijkheidsverdeling met betrekking tot de AVG. Zowel bij de GRS als de GR DG&J worden taken in delegatie uitgervoerd en is de verantwoordelijkheidsverdeling duidelijk in de zin dat de gedelegeerde eigenaar concreet als verwerkingsverantwoordelijke optreed. Uitdrukkelijke afspraken zijn voor zover wij kunnen nagaan niet gemaakt.

4.4 Rol van de ondernemingsraad

De gemeente heeft een eigen en lokale ondernemingsraad (OR). Naast de lokale OR is er een regionaal platform van ondernemingsraden, omdat een deel van zaken waar de OR instemmings- of adviesrecht heeft regionaal tot stand (zijn) (ge)komen. Het regionale platform is in het kader van de regionale samenwerking opgezet, met name voor de overgang van lokaal personeel naar de regionale organisatiestructuur Servicecentrum Drechtsteden (SCD).

De OR heeft in het kader van de privacy instemmingsrecht op de verwerking van persoonsgegevens van medewerkers. Ook heeft de OR een adviesrol als het gaat om belangrijke technologische voorzieningen binnen de gemeente. Een voorbeeld van een onderwerp waar de OR een rol heeft is de monitoring- en volgsystemen van bijvoorbeeld bedrijfsauto's.

In de praktijk zijn er in de recente geschiedenis niet veel privacy-gerelateerde onderwerpen waar de OR instemmings- of adviesrecht heeft gehad. Dit komt mede omdat de OR alleen bij de introductie van nieuw personeelsbeleid instemmings- of adviesrecht heeft, en niet bij de actualisatie of (door)ontwikkeling. Voor het gebruik van de elearning "Sir Askalot" is wel geagendeerd in een overleg ter informatie en voor (informele) bespreking..

In grote lijnen ziet een instemmings- of adviestraject bij de OR (ook wanneer het privacy-gerelateerde zaken betreft) er als volgt uit:

- Ter voorbereiding is er sprake van een informeel gesprek tussen OR en de bestuurder, waarbij de bestuurder uitleg geeft over de betreffende kwestie. In de voorbereiding wordt er tekst en uitleg gegeven en worden er (eventueel) al achtergrondstukken ontvangen.
- De OR kan nadere vragen ter beeldvorming stellen voordat er formeel een aanvraag ontvangen wordt.
- Na de voorbereiding ontvangt de OR een aanvraag en wordt er (formeel) gereageerd. Bij de achtergrondstukken van deze aanvraag kan ook sprake zijn van een advies op het gebied van privacy vanuit de ambtelijke organisatie, maar dit is sinds de introductie van de AVG nog niet voorgekomen.
- Naast een individueel instemmings- of adviestraject is er ook twee keer per jaar een artikel 24 overleg waarin gekeken wordt naar de ontwikkelingen van de organisatie.

Naast het formele instemmings- en adviesrecht van de OR zijn er nog twee andere zaken waarbij privacy een rol speelt binnen de OR. Ten eerste kloppen medewerkers aan bij de OR met vraagstukken of problemen die binnen de organisatie spelen. Dit kunnen ook zaken zijn met betrekking tot privacy, de bescherming van persoonsgegevens en/of de (beveiliging van de) informatievoorziening.

Ten tweede heeft de OR een werkwijze waarbij de identiteit en persoonsgegevens van medewerkers die zich bij hen melden verborgen worden gehouden zodat eventuele belangrijke signalen kunnen worden doorgegeven aan de bestuurder zonder dat dit medewerkers potentieel schaadt of blootstelt. Dit kan discussie/gesprek opleveren met de bestuurder, omdat signalen uit de organisatie op deze manier moeilijker te herleiden zijn naar specifieke organisatieonderdelen. Echter, de OR heeft op dit punt een rol in de bescherming van individuele medewerkers. Hoewel er geen formeel protocol is vastgelegd over deze gang van zaken, is er wel een vaste praktijk.

4.5 Rol en positie van de gemeenteraad

De gemeenteraad heeft weinig aandacht voor het onderwerp privacy. Privacy is geen onderwerp van gesprek in de gemeenteraad of onderwerp van (raads)vragen. Tijdens de raadsbijeenkomst die in het kader van dit onderzoek is georganiseerd hebben de drie aanwezige raadsleden aangegeven dat het onderwerp naar hun weten in de afgelopen twee jaar niet aan bod is gekomen (met uitzondering van de FG-presentatie, zie hieronder). De raadsleden waren niet op de hoogte van de stand van zaken met betrekking tot het privacybeleid en de implementatie van de AVG en Wpg (waaronder de Wpg-audit resultaten). Als toelichting hierop wordt aangegeven dat er beperkte affiniteit en interesse is. In het algemeen geeft de raad aan meer geïnformeerd te willen worden over het onderwerp privacy en de bescherming van persoonsgegevens van inwoners. Daarnaast geeft de raad aan het onderwerp wel belangrijk te vinden, maar resulteert een gebrek aan kennis in kleine informatiestroom en interesse.

Raadsleden geven ook aan dat ze afhankelijk zijn van de samenwerking met Drechtsteden ten aanzien van privacy. Het is vanuit hun rol moeilijk om zicht en grip te krijgen op de samenwerking en de verwerking van persoonsgegevens buiten de muren van het gemeentehuis. Raadsleden geven aan dat er op dit punt verbeteringen noodzakelijk zijn aangaande hun controlerende rol.

De ambtelijke organisatie onderschrijft dit beeld en geeft aan dat er weinig tot geen inhoudelijke informatieverstrekking aan de gemeenteraad is op het gebied van gegevensbescherming en privacy. Een uitzondering hierop is het privacybeleid uit 2020 en de hieronder genoemde voorbeelden. Raadsleden ontvangen wel de e-learning “Sir Askalot”.

Er zijn een aantal (vaste/ad hoc) momenten waarop het onderwerp privacy en de bescherming van persoonsgegevens toch aan bod komt:

- De FG heeft in 2023 ter kennismaking en introductie een presentatie en toelichting gegeven over zijn rol als onafhankelijk toezichthouder voor het bevoegd gezag.
  De Privacy coördinator heeft eind 2023 aan de hand van dilemma's thema's over privacy en informatieveiligheid met de raadsleden interactief besproken.
- Jaarlijks wordt aan de raad(sagendacommissie) voorgesteld een presentatie te geven over informatiebeveiliging en over privacy. Dit heeft ook vaker plaatsgevonden, maar is ook wel wegens te volle raadsagenda’s afgewezen.
- Jaarlijks wordt er in het jaarverslag gerapporteerd over bedrijfsvoeringsonderwerpen waaronder privacy en informatiebeveiliging. Deze rapportage was in de onderzochte jaren zeer summier, en op het gebied van privacy volledig procesmatig. Zo bevatte het jaarverslag van 2022 wel de informatie dat de Wpg-audit was uitgevoerd, maar werd er niets gemeld over de slechte resultaten en de maatregelen die Papendrecht op grond hiervan moest nemen.
- De jaarlijkse ENSIA-auditrapportage en collegeverklaring op het gebied van informatiebeveiliging worden vertrouwelijk behandeld in de gemeenteraad. Op het gebied van Suwinet zijn er al meerdere jaren tekortkomingen, maar dit heeft niet geresulteerd in vragen vanuit de gemeenteraad.
- Daarentegen heeft een raadsfractie in 2024 wel vragen gesteld over de verwerking van persoonsgegevens (kentekens) in parkeergarages.

Bijlage A Geïnterviewde personen

Datum	Functie
05-04-2024	Functionaris Gegevensbescherming*
27-03-2024	Privacy coördinator/concern jurist*
26-03-2024	Informatiemanager*
26-03-2024	Informatiebeveiligingsadviseur*
27-03-2024	Secretaris Ondernemingsraad*
04-04-2024	Boa coördinator*
04-04-2024	Directielid
05-04-2024	Teamleider financiën*
22-04-2024	Beleidsregisseurs sociaal domein
29-05-2024	Burgemeester
05-06-2024	Gemeentesecretaris
12-07-2024	Wethouder

* Deze personen hebben tevens deelgenomen aan het afrondende verdiepende gesprek.

Bijlage B Bestudeerde documentatie

Visie- en Beleidsdocumenten

Documentnaam	Datum
Privacy Beleid Drechtsteden versie 3.0 (def 2020 PPD)	10-12-2020
Reglement Functionaris voor de Gegevensbescherming Drechtsteden 2022	31-05-2022
Privacy beleid 2024 concept PPD	12-03-2024
Strategisch Informatiebeveiligingsbeleid Drechtsteden 1.00 definitief	20-05-2020
Eisen en wensen privacy	11-2023
Bewustwording privacy	
Concept Wpg privacybeleid	
Gemeenschappelijke Regeling Sociaal	01-01-2023
Privacybeleid Gemeenschappelijke Regeling Sociaal	09-2022
Gemeenschappelijke Regeling Dienst Gezondheid & Jeugd Zuid-Holland Zuid	15-03-2023
Privacybeleid Dienst Gezondheid & Jeugd Zuid-Holland Zuid	24-05-2018

DPIA's

Documentnaam	Datum
GRD huisbezoek ouderen v.23 Papendrecht	15-09-2021
Vroegsignalering schulden v 2.1	19-11-2021
Wet Inburgering 2021 v 2.1	12-2021
Hoe komt een DPIA tot stand binnen de Drechtsteden	
Overzicht DPIA's vanaf 2020	
DPIA BRS v 1.0	04-12-2020

Verwerkers- en dienstverleningsovereenkomsten

Documentnaam	Datum
19022024 Standaard Verwerkersovereenkomst v 2.5	15-02-2024
Ondertek VWO vroegsignalering Sterk Papendrecht	02-02-2021
Woonwagenbeleid en woonwagenlocatie onderzoek	07-11-2023
Convenant jeugdgroepenaanpak Papendrecht	03-2024
Papendrecht en GR Sociaal inzake uitvoering Wet Inburgering	18-01-2022
Gemeente Dordrecht (servicegemeente) – gemeente Papendrecht	01-01-2022
VWO MODEL V2.4.2 2023	
Papendrecht – Sociale Basis	14-09-2021

Registers en Procedures

Documentnaam	Datum
Handleiding Datalekken register	01-09-2023
Procesbeschrijving datalekken gemeente Papendrecht	

Register 2023 november GPD	
AVG klachtenprocedure IBD versie 2023	09-11-2023
Info zaaktype Persoonsgegevens beperking verwerking verzoek	
Info zaaktype Persoonsgegevens correctieverzoek	
Info zaaktype Persoonsgegevens dataportabliteit verzoek	
Info zaaktype Persoonsgegevens verwerking bewaar	
Info zaaktype Persoonsgegevens verwijderingsverzoek doc Isabel	
Werkinstructie correctieverzoek	
Werkinstructie bezwaar verwerking Persoonsgegevens	04-09-2020
Werkinstructie Persoonsgegevens beperkingsverzoek	04-09-2020
Werkinstructie persoonsgegevens inzake verzoek niet	26-05-2020
Werkinstructie Persoonsgegevens verwijderingsverzoek	04-09-2020
Werkinstructie Persoonsgegevens verzoek overdracht	04-09-2020
Werkwijze behandelen beveiligingsincident DATALEKKEN 2023	
Collegeverklaring 2021 t/m 2023 [vertrouwelijk]	
ENSIA rapportage 2021 t/m 2023 [vertrouwelijk] Assurance rapport 2021 [vertrouwelijk]	

Rapportages

Documentnaam	**Datum**
Jaarrapportage Privacy Papendrecht – definitief	01-07-2020
FG rapportage Papendrecht 2021	
Definitieve rapportage FG april – december	
Papendrecht Privacy rapportage versie 1.2	
Presentatie FG’s Drechtsteden bij de Raad	
Jaarstukken 2020 gemeente Papendrecht	
Jaarstukken 2021 gemeente Papendrecht	
Jaarstukken 2022 gemeente Papendrecht	

Bijlage C Afkortingen en terminologie

Afkorting	Betekenis
AVG	Algemene Verordening Gegevensbescherming
BIG	Baseline Informatiebeveiliging Gemeenten
BIO	Baseline Informatiebeveiliging Overheid
BRP	Basis Registratie Personen
CISO	Chief Informatie Security Officer
DPIA	Data Protection Impact Assesment
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris Gegevensbescherming
IBD	Informatiebeveiligingsdienst
PC	Privacy coördinator
PDCA	Plan-Do-Check-Act
Wpg	Wet politiegegevens