

**De afdeling**  
**Inkomen, Zorg & Leerrecht**  
**AVG Proof**

Opdrachtgever: Strategisch Management Team Inkomen, Zorg & Leerrecht  
Stellers: 5.1.2e , 5.1.2e  
Datum: 20 december 2024

# Inhoudsopgave

Inleiding .....	4
Doel .....	4
Achtergrond: grondslagen verwerking persoonsgegevens .....	4
Hoe gaan we vervolgens om met de verwerking van de gegevens? .....	5
Methode .....	5
Verantwoording .....	5
Algemeen .....	6
Organisatiestructuur Inkomen Zorg & Leerrecht (IZL) .....	6
Stand van zaken op het gebied van AVG en privacy, algemeen .....	7
Wat hebben we te doen? Deel I, in vogelvlucht... ..	8
IZ 10 Stafbureau.....	9
Processen en DPIA's.....	9
Informatieveiligheid .....	9
Risico's .....	10
Privacy-bewustzijn en privacy-ambassadeurs .....	10
IZ20 Financiële Ondersteuning .....	11
Processen en DPIA's.....	11
Risico's .....	12
Privacy-bewustzijn en privacy-ambassadeurs .....	12
IZ30 Uitkeringen .....	13
Processen en DPIA's.....	13
Informatieveiligheid .....	13
Risico's .....	14
Privacy-bewustzijn en privacy-ambassadeurs .....	14

IZ40 Bijzondere dienstverlening en Sociale Recherche .....	15
Bijzondere Doelgroepen.....	15
Zelfstandigen en Vorderingen .....	15
Sociale Recherche en Verhaal .....	15
Processen en DPIA's.....	16
Informatieveiligheid .....	16
Risico's .....	16
Privacy-bewustzijn en privacy-ambassadeurs .....	17
IZ50 Wmo en Leerrecht.....	18
Processen en DPIA's.....	18
Informatieveiligheid .....	18
Risico's .....	18
Privacy-bewustzijn en privacy-ambassadeurs .....	18
Audits .....	20
Datalekken .....	21
Wat hebben we te doen? Deel II, een nader ingezoomd beeld.....	22
Samenvatting.....	23
Bijlagen .....	24

# Inleiding

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking. Aan de hand van de AVG zie je als organisatie hoe je moet omgaan met het verzamelen, verwerken, opslaan en verwijderen van persoonsgevoelige informatie.

Juist omdat persoonsgegevens in het dagelijkse werk van onze afdeling veelvuldig voorkomen, is het van het grootste belang om daar zorgvuldig mee om te gaan. We willen als afdeling in beeld hebben hoe we ervoor staan op het gebied van privacy én we willen een gerichte aanpak hebben om, waar nodig, over te gaan tot structurele verbetering van ons AVG-bewustzijn, doen én laten.

Hoe voortvarend we ook willen zijn als afdeling, toch schuilen ongelukken en/of datalekken in een klein hoekje én, bovenal, is het zaak dat we bij het ontwikkelen van nieuwe processen, invoering van nieuw beleid en dat implementeren steeds rekening houden met de AVG. Het vraagt ook bewust daarmee om te gaan en onze weg te vinden in het werken conform de AVG. Vaak vinden we het spannend of blijven we er van weg; er is echter veel mogelijk in het werken conform AVG. De onbekendheid moet eraf én we moeten het vooral een uitdaging gaan vinden om binnen de AVG te werken.

Het SMT van de afdeling heeft naar aanleiding van dit plan al een aantal besluiten genomen; die zijn te vinden in bijlage 3. Dit plan ziet dus niet alleen toe op wat we gaan doen, we zien het juist ook als actief sturingsinstrument dat we ook actueel willen houden én dat bepalend is voor hoe we met AVG willen omgaan.

## Doel

Met dit plan geven we verdere invulling aan sturing op het gebied van AVG binnen I, Z & L. We richten ons op de processen en/of organisatieonderdelen binnen de afdeling. Daar waar ons werk draait om het verwerken, opslaan en omgaan van verschillende persoonsgevoelige en bijzondere gegevens. We gaan na welke kwetsbaarheden en risico's er zijn en we stellen vast hoe we daarmee om willen gaan. De AVG is daarbij de belangrijkste leidraad. Waar strikt volgen geen optie is, zoeken we naar een balans tussen risico's nemen en het beheersen daarvan.

Naast de processen staan we zeker ook stil bij wat er nodig is aan bewustzijnsvergroting en het op de juiste manier omgaan met de AVG van onze medewerkers.

## Achtergrond: grondslagen verwerking persoonsgegevens

We kunnen persoonsgegevens niet zonder meer verwerken. Daar is altijd een grondslag voor nodig.

De volgende grondslagen gelden voor verwerking van persoonsgegevens in de AVG:

Je hebt als organisatie toestemming van de persoon om wie het gaat.

Er is een noodzaak om gegevens te verwerken om een overeenkomst uit te voeren.

Het is noodzakelijk om gegevens te verwerken omdat je dit als organisatie wettelijk verplicht bent.

Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen.

Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang uit te voeren of wel openbaar gezag uit te oefenen.

Het is noodzakelijk om gegevens te verwerken om het gerechtvaardigde belang te behartigen.

Het is van belang om ons er altijd rekenschap van te geven waarom we persoonsgegevens verwerken én

daarbij is het zaak die grondslag te vermelden:

In de privacyverklaring van de organisatie;

In het privacybeleid;

In het verwerkingsregister van de afdeling.

Naast de grondslag dienen wij ook goed te kunnen onderbouwen waarom wij een bepaalde grondslag hebben gekozen.

### Hoe gaan we vervolgens om met de verwerking van de gegevens?

Als we een grondslag hebben én die kunnen beargumenteren, zijn er spelregels waar we ons aan te houden hebben. Die zijn als volgt:

- **Proportionaliteit:** Je checkt of het doel van je verwerking in verhouding staat tot de inbreuk op de privacy van de betrokkenen;
- **Subsidiariteit:** kijk er altijd naar of het doel dat je wilt bereiken, niet op een manier kan worden bereikt die minder ingrijpend is voor de betrokkenen;
- **Transparantie:** de persoon van wie je de gegevens verwerkt, weet hiervan, heeft hiervoor toestemming gegeven en kent zijn rechten;
- **Doelbeperking:** je verwerkt of verzamelt de persoonsgegevens voor één gewettigd doel en gebruikt ze niet voor andere doelen;
- **Gegevensbeperking:** alleen die gegevens die voor het beoogde doel noodzakelijk zijn, mag je vastleggen;
- **Juistheid:** wat je aan persoonsgegevens vastlegt, moet correct zijn en correct blijven;
- **Bewaarbeperking:** de persoonsgegevens mag je niet langer bewaren dan nodig voor het beoogde doel: je moet dus ook tijdig vernietigen;
- **Integriteit en vertrouwelijkheid:** verzamelde persoonsgegevens moet je beschermen tegen toegang door onbevoegden, verlies of vernietiging.
- **Verantwoording:** als verantwoordelijke voor persoonsgegevens moet je kunnen aantonen aan deze regels te voldoen.

### Methode

Per bureau van I, Z & L hebben we de Strategisch Manager en teamleiders geïnterviewd. Daarbij zijn we ingegaan op de onderscheiden hoofdprocessen, hebben we gesproken over de al vastgelegde DPIA's en de processen waar het om gaat. We hebben daarnaast doorgevraagd naar welke andere mogelijke processen nog binnen het bureau uitgevoerd worden.

Voorts hebben we, gegeven het toegenomen belang van logging in elk geval in preventieve zin stilgestaan bij dat onderwerp. Verder stonden we stil bij autorisatiechecks en hebben we AVG-bewustzijn, risico's in de verschillende teams en de beschikbare privacy ambassadeurs besproken. Daarmee hebben we per bureau een beeld gekregen van de stand van zaken van AVG. Op basis van de aangedragen risico's stellen we per team maatregelen voor. Een aantal van deze is bureauspecifiek, andere dienen I, Z & L-breed opgepakt te worden.

### Verantwoording

Dit plan maken we om zowel invulling als versterking te geven aan het in control zijn op AVG-gebied. Door dit plan up-to-date te houden, houden we in beeld waar we als afdeling staan. Het is in feite onze scorekaart om te zien hoe we de grip op AVG zo optimaal mogelijk kunnen realiseren. Het geeft bovendien de Functionaris Gegevensbescherming datzelfde beeld. Zijn bevindingen over de gehele organisatie rapporteert hij aan de Autoriteit Persoonsgegevens (AP).

# Algemeen

## Organisatiestructuur Inkomen Zorg & Leerrecht (IZL)

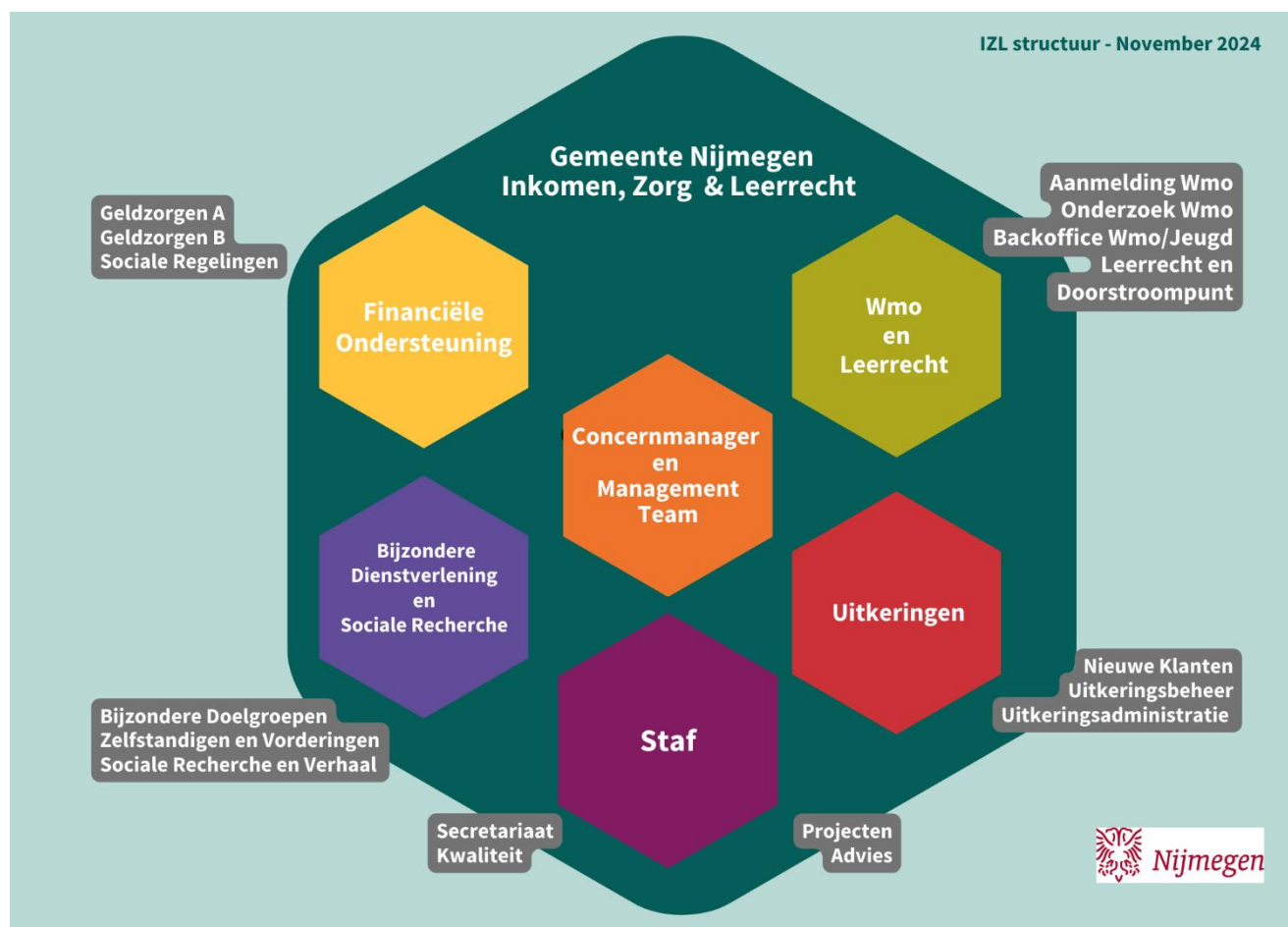
De afdeling IZL valt binnen het Sociaal Domein en heeft vier bureaus en een ondersteunend stafbureau. Per 1 januari 2023 is deze afdeling zoals hierna beschreven gereorganiseerd en gevormd.

De concernmanager en het managementteam (MT) bestaande uit Strategisch Managers zorgen dat de grote lijnen worden gevolgd en ingericht.

De verschillende teams zijn ingedeeld onder de volgende bureaus:

1. Financiële Ondersteuning
2. Wmo en Leerrecht
3. Uitkeringen
4. Bijzondere Dienstverlening en Sociale Recherche
5. Staf

Bureau 1 t/m 4 heeft een strategisch manager boven zich. Binnen de bureaus werkt een aantal teams en elk team heeft een teamleider. Deze staat in direct contact met de uitvoering en collega's. Het Stafbureau heeft als enige bureau een manager die een bureau rechtstreeks aanstuurt.



1

<sup>1</sup> IZL structuur – Mens als Middelpunt IZL

## Stand van zaken op het gebied van AVG en privacy, algemeen

De afgelopen jaren hebben we als I, Z & L nadrukkelijk stil gestaan bij AVG en de betekenis ervan voor ons werkveld en onze cliënten. Dat gebeurde op verschillende momenten en op verschillende manieren. Redelijk recent zijn afdelingsbijeenkomsten waarin twee juristen heldere uitleg gaven over AVG en privacy; deze werden veel bezocht én als erg positief beoordeeld. Het was voor de toenmalige concernmanager aanleiding om te stellen dat deze bijeenkomsten verplichte kost zouden moeten zijn voor nieuwe medewerkers van de afdeling. Deze bijeenkomsten hebben echter na de start van 2023 geen vervolg meer gekregen; het organiserende team erachter werd ontbonden terwijl de activiteit verder niet werd opgepakt. Het is een initiatief waarvan we vinden dat het echter zeker opvolging dient te krijgen: effectief, to the point en helder in uitleg.

De bewustwording op het gebied van AVG en privacy zien we ook gegroeid als we kijken naar hoe snel en gedreven de inzet doorgaans is bij het opstellen van DPIA's, als we kijken naar de uitvoering van het controlplan, als we uitgaan van de toegenomen vragen vanuit medewerkers over AVG, de uitkomsten van de verschillende audits die we kennen en de toename van het gebruik van veilig mailen. Die signalen zijn bemoedigend: met dit plan kijken we echter ook dieper. We willen weten hoe zeer het bewustzijn in de breedte én intrinsiek is toegenomen dan wel of het met name gaat om mensen die vanuit de aard van hun werk hetzij bezig zijn met vragen op het gebied van AVG en privacy of betrokken zijn bij verbetering van AVG en privacy binnen de afdeling, zoals de privacy ambassadeurs, de adviseur AVG en privacy, medewerkers actief betrokken bij de audits en de manager Stafbureau.

Voor een aantal bureaus geldt dat juist deze medewerkers onderwerpen aankaarten op het gebied van AVG en privacy, ook als het gaat om DPIA's en is het nog niet in brede zin zo dat die onderwerpen vanuit procesinvalshoek vanuit alle medewerkers en teamleiders worden aangedragen. We zien daarin wel een onderscheid: voor een aantal teamleiders is dat juist heel nadrukkelijk het geval: zij sturen al geruime tijd op AVG en privacy. Voor anderen geldt dat zij het onderwerp met name oppakken als het op hun pad komt. Ze doen dan wat er verwacht wordt, eventueel met hulp, maar ze onderkennen zeker het belang van AVG.

Een uitvraag van het SMT op bedrijfsvoeringgebied liet ook zien dat niet voor alle teamleiders helder is voor welke DPIA's ze verantwoordelijk zijn. Dat wordt deels verklaard door nieuwigheid en/of tijdelijkheid van contracten van teamleiders. Daar staat tegenover dat je mag verwachten dat de teamleiders een beeld hebben van de processen binnen hun team. En daarbij zich dus ook kunnen afvragen of voor die processen een DPIA nodig is. Dat is nu niet voor iedereen even helder.

Tijdens een audit van de functionaris gegevensbescherming en de privacy officer op 14 november kwam naar voren uit een bespiegeling van de aanwezige privacy ambassadeurs van I, Z & L dat in ieder geval een deel van hen de voortrekkersrol van teamleiders op dit vlak mist. Er was een beperkt aantal privacy ambassadeurs aanwezig maar dit sluit aan op de notie: doen wat nodig is, maar niet per se voorgaan in AVG-vraagstukken. Dat voorgaan kan nadrukkelijker nog kan worden uitgedragen. Het kan ook betekenen dat teamleiders juist meer ondersteuning nodig hebben om zich het onderwerp goed eigen te maken<sup>2</sup>.

Uit diezelfde audit kwam naar voren dat Zivver niet in de volle breedte waar het nodig is, ingezet wordt of kan worden. Juist binnen een afdeling waarin persoonsgegevens zo elementair zijn in onze dienstverlening, is het gebruiken van veilig mailen, zeker als het om persoonsgegevens gaat, essentieel. Optimalisatie van het werken met Zivver of het kunnen bieden van alternatieven staat in elk geval op de planning voor 2025.

---

<sup>2</sup> Bijlage 2: Evaluatie bijeenkomst privacy ambassadeurs datum 14 november 2024.

Het vraagt dus ook om duidelijke keuzes door het SMT van de afdeling. Het SMT kiest nadrukkelijk voor een sturende rol door de teamleiders op het gebied van AVG en privacy. Dat vraagt wel om ondersteuning en facilitering. Facilitering op het gebied van AVG en privacy moet vooral ook dat zijn; ten dienste van de bureaus en de teams.

SMT en de teamleiders nemen hierin expliciet hun voorgangersrol expliciet in; daarbij geruggesteund door de stafadviseur AVG en Informatieveiligheid en privacy ambassadeurs in de verschillende teams.

### **Nota bene**

De gehele afdeling is op dit moment, net als de hele gemeente, momenteel in doorontwikkeling op het gebied van digitalisering. We rollen in deze periode het gebruik van MSOffice365 uit en er zal meer digitaal gewerkt worden in de cloud.

Bijkomend voordeel is dat de autorisaties beter bijgehouden kunnen worden. Zo kunnen alleen bevoegde medewerkers bij dossiers. Het maakt archivering efficiënter, effectiever en dus ook avg-proof.

Door digitalisering in Corsa, voorzien we in logging. Daarnaast worden er momenteel ook stukken via de mail verspreid, bijvoorbeeld wanneer er een bezwaar ligt bij Juridische Zaken. Dit kan uit Corsa worden gehaald, zodra de dossiers gedigitaliseerd zijn. Het digitaliseren van onder andere het archiveringsproces zorgt er dus ook voor dat de data veiliger en beter bewaard worden.

### **Wat hebben we te doen? Deel I, in vogelvlucht...**

We hebben stappen te zetten op het gebied van verankering in de organisatie, verdieping én verbreding van het bewustzijn op AVG-gebied, een voortzetting van de eerdere bijeenkomsten op het gebied van AVG en privacy zou zeer welkom zijn, maar het vraagt ook om beantwoording van een aantal vraagstukken op AVG-gebied en benoemen van risico's en oplossingen binnen de afdeling.

Vóór we dit verder smarter uitenzetten, zoomen we eerst in op de praktijk van de verschillende bureaus van de afdeling. Dat doen we aan de hand van een korte beschrijving van de verschillende bureaus en aan de hand van gesprekken die we in december hadden met de teamleiders en strategisch managers van de verschillende bureaus. We nemen ook de uitkomsten van de audit in november mee in het vaststellen van wat we te doen hebben.



## IZ10 Stafbureau<sup>3</sup>

Dit bureau levert de algehele ondersteuning voor de afdeling. De functies binnen het bureau zijn als volgt:

- Managementondersteuning
- Kwaliteitsmedewerkers (voor de verschillende wet- en regelgevingen)
- Stafadviseur AVG en informatieveiligheid/Wpg-auditor
- Projectleiders
- Juridisch adviseur Wmo en Jeugdwet
- Communicatieadviseur
- Manager Stafbureau

### Processen en DPIA's

De processen waar het bureau zich over ontfermt, zijn alle ondersteunende processen. Opgemerkt moet worden dat er in het werk van de managementondersteuners in voorkomende gevallen gewerkt kan worden met persoonsgegevens.

Anders dan casuïstiek (waarin persoonlijke gegevens aan bod komen) waar de medewerkers hun ondersteuning bij geven (uit hoofde van hun functie) én waarvoor de DPIA's van de betreffende processen van toepassing zijn, hebben de medewerkers van het Stafbureau geen directe zelfstandige caseload waar persoonlijke gegevens in betrokken zijn.

Binnen het bureau vindt de toetsing plaats op het zorgvuldig en correct gebruik van Suwinet. Eventuele onrechtmatigheden worden door een daarvoor aangewezen kwaliteitsmedewerker bij een halfjaarlijkse check in beeld gebracht en gerapporteerd.

Het bureau is daarnaast in de functie van zowel de stafadviseur AVG en informatieveiligheid als in de huidige taak van de manager Stafbureau actief op het gebied van AVG en informatieveiligheid. De manager treedt ook op als privacy ambassadeur voor het bureau; er is op dit moment geen achtervang.

De DPIA's die momenteel geoormerkt zijn als vallende onder de verantwoordelijkheid van de manager van het Stafbureau zijn, raken aan de twee meest essentiële applicaties van I, Z & L. De applicaties worden vrijwel afdelingsbreed ingezet en hoewel de proceseigenaar de concernmanager is, draagt de manager Stafbureau gedelegeerd de verantwoordelijkheid voor de DPIA's en voor de naleving ervan. Het gaat daarbij om:

- DPIA Suite (DPIA-nummer 62)
- DPIA Suwinet (DPIA-nummer 79)

### Informatieveiligheid

Voor zowel Suite als voor Suwinet vindt er logging plaats. Voor Suwinet is de logging een van de pijlers voor de halfjaarlijkse controle op het gebruik van Suwinet. Voor Suite geldt dat de logging zich richt op de verwerking.

Voor beide processen vinden autorisatiechecks plaats. Die is bij Suwinet essentieel: aanpassingen dienen tijdig doorgegeven te worden en onregelmatigheden worden direct nader onderzocht en zo nodig volgen ingrijpende maatregelen tot aan ontslag op staande voet toe. Misbruik van Suwinet is in het geheel niet toegestaan en het werken met Suwinet is dus met strikte borgingen compleet.

De autorisatiechecks voor Suite vinden eveneens halfjaarlijks plaats en worden uitgevoerd door de

---

<sup>3</sup> IZ10 5.1.2e – Stafbureau

verschillende teamleiders van I, Z & L op voorzet van iRvN. In 2024 is er op ingezet om teamleiders bewuster te maken van het tijdig doorlopen van aanmeldingen, wijzigingen en/of afmeldingen in Suite. Binnen de afdeling bestaat breed een behoefte om het proces tot aanvragen en wijzigen van autorisaties te verbeteren: nu zijn er nog veel losse stappen in verschillende processen om aanmeldingen, afmeldingen en wijzigingen door te geven. Dat komt de informatieveiligheid uiteindelijk niet ten goede.

### **Risico's**

De risico's die gesignaleerd worden binnen het bureau worden, zijn voor het bureau grosso modo beperkt, gegeven de zeer beperkte mate waarin eventueel met vertrouwelijke gegevens gewerd wordt.

Binnen het bureau is wel gesignaleerd dat het huidige gebruik van Cognos, een applicatie die veelvuldig door I, Z & L gebruikt wordt voor managementinformatie, voor een deel gekoppeld is aan persoonsgegevens in dat systeem. Inmiddels wordt er een DPIA voor het gebruik van Cognos gemaakt.

*Maatregelen om de risico's tegen te gaan:*

- DPIA Cognos uitvoeren om de verschillende risico's te duiden (hetgeen mogelijk gaat inhouden dat persoonlijke gegevens uit Cognos verwijderd dienen te worden)

### **Privacy-bewustzijn en privacy-ambassadeurs**

Het bureau heeft in de huidige situatie slechts één privacy ambassadeur. Dat is de manager van het Stafbureau. Het bureau heeft het afgelopen jaar met name de focus gehad op de ontwikkeling van het bureau. In dat traject is er weinig plaats geweest voor inhoudelijke onderwerpen.

De medewerkers binnen het bureau weten de stafadviseur AVG en informatieveiligheid te vinden of komen met vragen bij de manager. Het is nog niet gekomen van actief uitdragen van AVG-bewustzijn. Hier is zeker ook verbetering mogelijk.

De kennis op het gebied van datalekken en hoe dan te handelen, is volgens de manager voldoende aanwezig bij de medewerkers.

## IZ20 Financiële Ondersteuning<sup>4</sup>

Het bureau bestaat uit 4 onderdelen: twee teams Geldzorgen die zich richten op schuldhulpverlening, een team Bijzondere Bijstand en een team Sociale Regelingen. De teams Geldzorgen A en B ondersteunen samen inwoners met geldzorgen of (dreigende) schulden door het geven van voorlichting, inzicht in financiën, budgetcursussen, budgetcoaching, budgetbeheer of het treffen van een schuldregeling.

Team A bestaat uit de Financieel Experts in de Wijk en de klantmanagers schuldhulpverlening. Team B bestaat uit de medewerkers van Preventie, Budgetbeheer, Schuldregeling, Hercontrole en Kredietbewaking.

De Bijzondere bijstand is bedoeld voor bijzondere noodzakelijke kosten die niet via andere regelingen vergoed worden. Deze noodzakelijke kosten kan men niet betalen uit eigen inkomen of vermogen. Bijzondere bijstand is voor inwoners uit de gemeente Nijmegen met een uitkering of een andere laag inkomen.

Bij team Sociale Regelingen kun je o.a. een aanvraag doen voor Collectieve Aanvullende Ziektekosten (CAZ), kinderopvang, het bus-voordeelabonnement of de meedoen-regeling.

### Processen en DPIA's

Het bureau gebruikt naast de standaardapplicaties Corsa, Suite en Suwinet applicaties voor de specifieke bureau-functies. Voor de teams Geldzorgen zijn dat Allegro, Gidso (gebruikt door de Financieel Experts in de Wijk) en VPS (gebruikt voor vroegsignalering). Voor de aanvragen van de bijzondere bijstand en de sociale regelingen gebruikt het bureau Forus en Decos.

De DPIA's die voor het bureau al gemaakt zijn of in de maak zijn als volgt:

- Financieel Expert in de Wijk (DPIA-nummer 28)
- Vroegsignalering (DPIA-nummer 17)
- Mijn Geldzaken (Allegro) (DPIA-nummer 72)
- Schuldenknooppunt (Allegro) (DPIA-nummer 60)
- Allegro (DPIA-nummer 83)
- Doorontwikkeling Individuele Inkomenstoelage (DPIA-nummer 73)
- Collectieve Aanvullende Zorgverzekering (DPIA-nummer 100)
- Leerlingenvervoer –in de maak-
- Kinderopvang –in de maak-

In de bespreking met het bureau kwam naar voren dat er nog DPIA's ontbreken voor de volgende processen:

- Budgetbeheer (proces)
- Schuldhulpverlening (proces)
- Kredietverstrekking (proces)

Voor de algemene processen van bijzondere bijstand en sociale regelingen de adviseren wij aan de hand van een korte procesbeschrijving een analyse te laten maken door de FG van de eventuele noodzakelijkheid van een DPIA voor het proces. Daarbij kan dan de vraag meegenomen worden in hoeverre de uitwerking hiervan een addendum kan zijn voor de DPIA inzake de Participatiewet.

---

<sup>4</sup> IZ20 5.1.2e – Bureau Financiële Ondersteuning  
IZ21 5.1.2e - Geldzorgen A, IZ22 5.1.2e - Geldzorgen B,  
IZ23 5.1.2e - Sociale Regelingen, IZ24 5.1.2e - Bijzondere Bijstand

## **Informatieveiligheid**

In het gesprek heeft de stafadviseur AVG en informatieveiligheid logging en het belang ervan -en het checken van logging- uitgelegd. Het belang ervan werd onderkend, ook om het als middel in te zetten tegen misbruik van applicaties.

Voor wat betreft autorisatiechecks op applicaties liep de praktijk van de teamleiders uiteen. Er zijn teamleiders die dat heel consciëntieus op zich nemen, er zijn er ook voor wie het geen herkenning oproept. De teamleiders geven aan dat ze behoefte hebben aan een duidelijk beeld van wat er van hen verwacht wordt zodat ze de taken op het gebied van AVG en informatieveiligheid juist in hun jaarprogramma kunnen opnemen. Hier ligt een concrete actie voor 2025 in besloten die bij zal dragen aan een toename van de beheersing op AVG-gebied.

## **Risico's**

In het gesprek met het bureau werd een aantal uiteenlopende risico's benoemd. Veel van deze hangen samen met gelegenheid geven/krijgen om persoonlijke gegevens in te zien, waar je als medewerker niet altijd toe gerechtigd bent:

- Er zijn meerdere mailboxen waar meerdere mensen voor geautoriseerd zijn;
- Wanneer een informatievraag binnenkomt bijvoorbeeld over een specifieke klacht, bestaat er een kans dat een medewerker dieper –dan nodig- in de gegevens van een cliënt duikt;
- Caseloads worden bij ziekte overgenomen;
- Er wordt voor een deel nog gewerkt met Excellijsten met persoonlijke gegevens én die worden ook nog eens geprint
- Een deel van het werk is (nog) gebaseerd op inhoud van mailboxen en gezamenlijke schijven: de transformatie naar Teams vraagt dat er géén persoonlijke gegevens in worden opgeslagen

## **Privacy-bewustzijn en privacy-ambassadeurs**

De medewerkers volgen verplicht alle trainingen via Studytube. Het bureau neemt ook nieuwe medewerkers hier direct in mee. Wanneer er schermen open staan en niet vergrendeld zijn, spreken medewerkers elkaar er direct op aan. Dat bewustzijn is breed én actief. Ook als er medewerkers zijn die stukken mee naar huis wil nemen, is dat aanleiding voor een gesprek: het bureau is daar heel duidelijk in. Datzelfde geldt voor documenten die bij printers bleven liggen: medewerkers spreken elkaar daar nu ook over aan. De teamleiders hebben actief gestuurd op de signalen.

De teamleiders geven aan dat er veel gespard wordt onder elkaar. Men denkt goed na over wat wel in een dossier mag worden opgenomen en wat niet. Enerzijds zegt dat veel over het bewustzijn, anderzijds komt dat soms voort uit handelingsangst. De teamleiders geven aan dat het bewustzijn nog verder mag worden versterkt: de ervaringen met de AVG-bijeenkomsten van de beide Stijnen was prima. Ze stellen voor die te herhalen. Dat geeft ook meer helderheid en maakt het maken van keuzes wellicht makkelijker.

Het bureau heeft naar aanleiding van een signaal van een privacy ambassadeur de aanvraagformulieren voorzien van een opmerking om vooral geen medische gegevens mee te sturen. Dat betekent dat de inzet van de privacy ambassadeurs het effect niet mist. Ondanks dat konden niet alle teamleiders aangeven wie in hun team de privacy-ambassadeur is.

## IZ30 Uitkeringen<sup>5</sup>

Het bureau bestaat uit drie teams, te weten Nieuwe Klanten, Uitkeringsbeheer en Uitkeringsadministratie. Bij het eerste team komen de aanvragen voor uitkeringen op grond van de Participatiewet en de IOAW binnen; dit team neemt die aanvragen in behandeling en verwerkt ze.

Het team Uitkeringsbeheer zorgt voor het beheer van de lopende administratie en beantwoordt vragen daarover en verwerkt meldingen ten aanzien van de uitkeringen.

De Uitkeringsadministratie is het team dat de uitkeringen daadwerkelijk uitkeert en waar cliënten terecht kunnen met vragen over de hoogte van de uitkering en met vragen over verrekeningen van inkomsten.

### Processen en DPIA's

De processen van het bureau zijn vrijwel alle gelieerd aan de Participatiewet; met uitzondering van de IOAW. Voor een belangrijk deel zijn er echter wel overeenkomsten: het voornaamste verschil is dat er voor de IOAW geen sprake is van een vermogenstoets die er wel is voor de Participatiewet. Met de DPIA die nu in de maak is voor de Participatiewet én de bijzonder grote overeenkomst aan processtappen, stellen we voor de processen voor de IOAW onder dezelfde DPIA te laten vallen, met een toelichting op het onderscheid.

De DPIA's die er voor dit bureau al zijn, zijn als volgt:

- Project Doe Je Mee? (DPIA-nummer 27)
- Regeling Opvang Ontheemden (DPIA-nummer 37)
- Gegevensuitwisseling Inlichtingenbureau en BNK (DPIA-nummer 35)
- DPIA Participatiewet (ook van toepassing voor IZ40) -in de maak-

In het gesprek stonden we stil bij het onderwerp Gegevensuitwisseling met het Werkbedrijf; dit heeft lang als potentiële DPIA op een longlist gestaan. Het gesprek maakte duidelijk dat dit niet meer aan de orde is. De gegevensuitwisseling die er nu plaatsvindt is aanmelding van cliënten bij het Werkbedrijf. De DPIA daarvan valt, zo geven de teamleiders aan, onder auspiciën van het Werkbedrijf. We willen graag nog even voor de volledigheid een check daarop.

### Informatieveiligheid

Logging op processen werd in het gesprek herkend: ook de notie dat de logging op processen zich voor Suite zich richt op mutaties in Suite en raadplegingen dus (nog) niet meeneemt.

De autorisatiechecks op applicaties was voor de drie teamleiders identiek. Die voeren ze alle drie twee keer per jaar uit. Ervaring van een van de teamleiders bij een andere organisatie was dat deze zelfs elk kwartaal werden uitgevoerd. De teamleiders kijken niet alleen naar de persoon maar ook naar welke autorisatie iemand heeft; dat betekent een correcte uitvoering van de autorisatiechecks. Desgevraagd geven de teamleiders aan dat ze de mutaties op het vlak van autorisatiewijzigingen steeds tijdig doorgeven.

---

<sup>5</sup> IZ30 5.1.2e - Bureau Uitkeringen, IZ31 5.1.2e - Nieuwe Klanten, IZ32 5.1.2e - Uitkeringsbeheer, IZ33 5.1.2e - Uitkeringsadministratie

## **Risico's**

In het gesprek met het bureau kwam het meest nadrukkelijk naar voren het feit dat telefoongesprekken, vaak ook met cliënten niet in een geïsoleerde telefooncel gehouden worden, maar op de flexvloer. Dat betekent dat er meegeluisterd kan worden naar gesprekken van persoonlijke aard; weliswaar door collega's die vanuit de aard van de functie op vergelijkbare wijze geautoriseerd zijn voor applicaties; dat geldt echter niet voor informatie die in gesprekken wordt gedeeld dan wel wordt opgevangen door medewerkers of bezoekers op de werkvloer die niet een zelfde autorisatie hebben.

De teamleiders herkenden daarnaast ook de risico's van documenten die op printers achterblijven en vergelijkbare onderwerpen. Op het moment dat een risico wordt opgemerkt, maken zij dat ook bespreekbaar in teamoverleggen.

*Maatregelen om de risico's tegen te gaan:*

Het SMT heeft besloten te onderzoeken welke maatregelen mogelijk zijn om hier het hoofd aan te bieden. Dat onderzoek vindt in 2025 plaats.

## **Privacy-bewustzijn en privacy-ambassadeurs**

De medewerkers volgen verplicht alle trainingen via Studytube. Het bureau neemt ook nieuwe medewerkers hier direct in mee. Wanneer er schermen open staan en niet vergrendeld zijn, spreken medewerkers elkaar er direct op aan. Dat bewustzijn is breed én actief. Ook als er medewerkers zijn die stukken mee naar huis willen nemen, is dat aanleiding voor een gesprek: het bureau is daar heel duidelijk in. De teamleiders sturen actief op de signalen. Ze constateren wel dat medewerkers nog handelingsangst ervaren. In de ogen van de teamleiders is het goed opnieuw de AVG-sessies te herhalen die eerder veel succes hadden bij de medewerkers.

Alle drie de teams hebben privacy ambassadeurs alhoewel de namen niet meteen alle drie genoemd werden. Van één team is dat wel duidelijk. Daarbij merkte de teamleider nadrukkelijk op dat deze privacy ambassadeur juist graag de rol wil neerleggen. De teamleiders vragen zich af op welke wijze de rol van privacy ambassadeur nu het beste geborgd kan zijn in de organisatie. Er is enerzijds behoefte aan duidelijkheid over de rol van privacy ambassadeur, anderzijds geeft men aan dat men twijfels heeft over de inzet van een privacy ambassadeur per team, ervan uitgaande dat de taken van een privacy ambassadeur slechts door enkelen als een toegevoegde waarde worden gezien. In hun ogen zou de rol van de stafadviseur AVG en Informatieveiligheid daarin veel meer coördinerend en ondersteunend voor de teams kunnen zijn.

## IZ40 Bijzondere dienstverlening en Sociale Recherche<sup>6</sup>

Het bureau bestaat uit de volgende onderdelen:

- Bijzondere Doelgroepen
- Zelfstandigen en Vorderingen
- Sociale Recherche en Verhaal

### Bijzondere Doelgroepen

Het team verzorgt ondersteuning, doorgaans middels het verstrekken van een uitkering, voor dak- en thuislozen, statushouders en inburgeraars. Daar waar verbijzonderde wetten aan de orde zijn, zoals voor inburgeraars de wet Inburgering, zijn die wetten dan ook mede de basis voor de doelbinding in relatie tot de persoonsgegevens. Het team is ook verantwoordelijk voor de uitvoering van de taakstelling huisvesting vergunninghouders.

Voor niet-uitkeringsgerechtigden, zogenaamde nuggers, wordt ondersteuning geboden bij het zoeken naar werk.

Daarnaast is dit team verantwoordelijk voor de uitvoering van de Wet op de Lijkbezorging. Dit houdt in dat het team namens de gemeente zorgdraagt voor het regelen van een uitvaart wanneer er voor een overledene geen nabestaanden zijn. Wanneer er wel nabestaanden zijn, dan wordt er eerst nagegaan of deze bereid zijn opdracht te geven voor de lijkbezorging. Als dat niet het geval is, heeft de gemeente de verantwoordelijkheid om daarin te voorzien. De kosten daarvan kunnen rechtens verhaald worden op de nalatenschap.

### Zelfstandigen en Vorderingen

Dit team ondersteunt zelfstandige ondernemers met de uitvoering van het Besluit bijstandsverlening zelfstandigen (Bbz). De Bbz is een sociaal vangnet dat ervoor zorgt dat ondernemers niet in de bijstand terecht komen. Verder voeren zij de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ) uit.

Het team ondersteunt hen met informatie en indien nodig met het verstrekken van de Bbz en IOAZ.

Binnen dit team vindt ook de incasso plaats van vorderingen die we als gemeente hebben op (voormalige) uitkeringsgerechtigden. De grondslag voor de incasso is eveneens gelieerd aan de Participatiewet en de andere uitkeringswetten.

### Sociale Recherche en Verhaal

Het team Sociale Recherche en Verhaal onderzoekt signalen van mogelijke fraude. Signalen komen vooral binnen via burgers, maar ook weleens via collega's of ketenpartners (zoals de politie).

Het doel is een rechtmatige verstrekking van bijstandsgelden of voorzieningen binnen de Pw en Wmo en jeugdwet. De Sociale Recherche zet verschillende middelen bij de rechtmatigheidsonderzoeken zoals waarheidsvinding, huisbezoeken, gesprekken. De sociaal rechercheur kan uitkeringen beëindigen, intrekken en onrechtmatig verstrekte gelden terugvorderen. Indien nodig wordt een boete of maatregel opgelegd.

---

<sup>6</sup> IZ40 5.1.2e – Bijzondere Dienstverlening en Sociale Recherche en Verhaal

IZ41 5.1.2e – Bijzondere Doelgroepen, IZ42 5.1.2e – Zelfstandigen, IZ43 5.1.2e – Sociale Recherche en Verhaal

Verhaal van het team verhaalt, te veel of onterecht betaalde uitkeringen. Dit zijn belastingen, brutoeringen en derdenbeslag. Ook zorgt dit onderdeel voor het verhalen van kosten ingevolge de Wet op de Lijkbezorging.

### **Processen en DPIA's**

Bespreking van de processen en DPIA's van het bureau leverde het inzicht op dat een groot deel van de processen geënt is op de Participatiewet. Daarvoor wordt nu een algemene DPIA gemaakt door de Strategisch Manager van het bureau (5.1.2e).

De processen die we daarnaast binnen het bureau onderscheiden waarvoor al een DPIA bestaat dan wel in de maak is, zijn als volgt:

- Inburgering (DPIA-nummer 33)
- Sociale Recherche anonieme accounts IZL (DPIA-nummer 32)
- Besluit Bijzondere Bijstand Zelfstandigen (DPIA-nummer 77)
- Sociale Recherche –in de maak-
- Participatiewet –in de maak-

In het gesprek constateerden we dat er mogelijk drie of vier DPIA's aanvullend gemaakt zouden moeten worden. Daarbij gaat het om de processen voor verhaal, incasso, de Wet op de lijkbezorging en de taakstelling huisvesting vergunninghouders. Voor incasso geldt dat er in elk geval een DPIA gemaakt dient te worden.

Met de Functionaris Gegevensbescherming is afgesproken dat van de drie overige processen een korte procesbeschrijving zal worden overlegd ter beoordeling of een DPIA vereist is dan wel als addendum kan gelden. Om het beeld van het bureau compleet te hebben: het verdient aanbeveling om ook het proces voor de ondersteuning van de niet-uitkeringsgerechtigden kort te beschrijven; dan kan daar een vergelijkbare check op worden gedaan.

### **Informatieveiligheid**

Logging op processen vindt in een aantal gevallen plaats. Niet iedere teamleider heeft helder voor welke processen dit wel en voor welke processen dit niet plaatsvindt. Daar waar het gebeurt, vindt de logging in elk geval plaats voor het verwerken van mutaties; raadplegingen worden dus niet altijd gelogd. Voor wat betreft het internetrechercheren (Sociale Recherche) is dit ook vastgelegd in de verwerkersovereenkomst van de leverancier.

Voor autorisatiechecks geldt een vergelijkbare situatie. De autorisatiecheck voor Suite wordt herkend. Voor Sociale Recherche geldt dat ook autorisatiechecks plaatsvinden op de zorgfraudeschijven. De teamleiders en strategisch manager spreken uit dat ze heel graag een actievare rol zouden willen invullen op het vlak van autorisatiechecks: alle vier geven ze aan dat ze daar, mits goed gefaciliteerd, meer werk van zouden willen maken.

### **Risico's**

De risico's die gesignaleerd worden binnen het bureau worden met name gezien in contact waarbij identificatie en legitimatie in het geding kan zijn waarbij er gecommuniceerd wordt over vertrouwelijke gegevens; denk aan telefonisch contact of e-mail contact.

De teamleiders geven alle drie aan medewerkers regelmatig te instrueren op dergelijke verzoeken niet in te gaan.



Het bureau gebruikt voor communicatie met derden waar het gaat om vertrouwelijke gegevens Zivver. Dat is de applicatie die binnen Nijmegen als de standaard wordt gezien om zorgvuldige en veilige verzending van e-mail met persoonlijke gegevens te borgen: gebruik van Zivver geeft de grootst mogelijke zekerheid dat de ontvanger ook daadwerkelijk is als beoogd én dat, wanneer uitwisseling van persoonlijke gegevens aan de orde én conform AVG toegestaan is, bij de juiste persoon terecht komt.

Teamleiders en privacy ambassadeurs signaleren beide dat het gebruik van Zivver niet optimaal is. Niet alleen staan de medewerkers soms in contact met instanties die onwillig staan tegenover het gebruik van Zivver; de borgen die nodig zijn om Zivver goed te gebruiken, maken het gebruik ervan soms onmogelijk. De kans is aanwezig dat er, in voorkomende gevallen, vertrouwelijke gegevens niet via Zivver gedeeld worden maar anderszins. Wij geven het dringende advies het gebruik van Zivver te optimaliseren en tegelijkertijd ook te onderzoeken hoe de kans op verzending van persoonsgegevens via andere wegen dan Zivver terug te dringen is dan wel veilige alternatieven te gebruiken naast Zivver. Hier valt te denken aan het gebruiken van Nextcloud, Teams of anderszins.

De kennis op het gebied van datalekken en hoe dan te handelen, is volgens de teamleiders voldoende aanwezig bij de medewerkers.

### **Privacy-bewustzijn en privacy-ambassadeurs**

De drie teamleiders gaan pragmatisch om met het onderwerp AVG. Wanneer het onderwerp zich aandient, in de vorm van vragen, vraagstukken of anderszins, pakken zij het onderwerp op en gaan ze er mee aan de slag. Het belang van de verplichte leerlijnen onderscheiden ze; dat is voor hen een ikinstrument op het gebied van AVG-bewustzijn.

Er wordt niet ingezet op een verdere actieve bewustwording in de teams. De voortrekkersrol lijkt daarvoor in deze teams meer te liggen bij de privacy ambassadeurs. De betreffende ambassadeurs geven wel aan dat een voortrekkersrol van leidinggevend gemist wordt. Gegeven het belang van verdere bewustwording, is het advies meer aandacht te hebben, in reguliere overleggen, door AVG als terugkerend onderwerp op de agenda te zetten. Dit geeft ook de mogelijkheid de samenwerking tussen teamleider en privacy ambassadeur nadrukkelijker neer te zetten.

De drie teams hebben alle een actieve privacy ambassadeur.

## IZ50 Wmo en Leerrecht<sup>7</sup>

Dit is het bureau dat zich voor een groot deel richt op de uitvoering van de Wmo. Daarbij gaat het zowel om dienstverlening aan cliënten die zich aanmelden én voor wie geldt dat er een onderzoek dient plaats te vinden, als om de ondersteunende (back office) activiteiten voor de uitvoering van zorg, de verstrekking van persoonsgebonden budgetten (PGB's) of ondersteuning inzake de uitvoering van de Jeugdwet. In het bureau vinden we ook het team Leerrecht dat zich richt op leerplichtige jongeren, jongeren voor wie een kwalificatieverplichting geldt en voor voortijdig schoolverlaters zonder startkwalificatie. Dat team treedt ook op als Regionaal Meld- en Coördinatiepunt (RMC) voor de voortijdig schoolverlaters zonder startkwalificatie (18-23 jaar).

### Processen en DPIA's

De volgende DPIA's liggen vast voor het bureau:

- Wmo Klassiek (24)
- Gegevensuitwisseling Inlichtingenbureau en WMO/Jeugdwet IZL (39)
- Leerplicht (Excl. Wpg werkzaamheden) IZL (54)
- Leerplicht Wpg activiteiten (59)

Er volgt een nieuw systeem volgend jaar, waar geheel WMO mee zal gaan werken. De verwerkingsovereenkomst en DPIA voor die applicaties worden dan opgepakt door MO en het DEVOPS team /IRVN. Verder is de huidige DPIA niet onderhevig aan grote veranderingen, waardoor deze nu nog optimaal is

Bij de bespreking kwamen geen andere processen naar voren waarvan duidelijk is dat ze nog een DPIA vragen of processen waar dat onduidelijk voor is. Het bureau heeft de verschillende processen dus goed in beeld en kan een goede inschatting maken van de risico's.

### Informatieveiligheid

Logging vindt voor zover het er is, slechts beperkt plaats. Met de vervanging van de huidige applicaties en de komst van nieuwe applicaties gaat dat echter veel meer doelgericht ingericht worden.

Autorisatiechecks vinden met regelmaat plaats. Één teamleider doet dat ook gericht op de algemene mailboxen en groepsschijven. Daarbij wordt opgemerkt dat dat moeilijker is wanneer het gaat om portals. Wanneer mensen uit je team op een ROP zitten, is de controle complexer: als teamleider heb je geen zicht op alle applicaties die mogelijk in een andere rol worden gebruikt.

### Risico's

Er zijn geen noemenswaardige risico's benoemd.

### Privacy-bewustzijn en privacy-ambassadeurs

Het bureau is actief op het gebied van AVG en privacy. De back-office werkt nadrukkelijk met een wekelijkse nieuwsbrief waarin AVG ook een onderwerp is, voor Leerrecht staat het iedere keer op de agenda van het bureau-overleg. Juist omdat Leerrecht zich ook onderwerpt aan de audit Wpg is het belang van zorgvuldig omgaan met de AVG essentieel.

---

<sup>7</sup> IZ50- 5.1.2e , IZ51- 5.1.2e , IZ52 - 5.1.2e , IZ53 - 5.1.2e , 5.1.2e  
IZ52- 5.1.2e en 5.1.2e .

De teams delen ervaringen op het gebied van AVG-vraagstukken met de medewerkers, evenals voorbeelden waaruit blijkt dat er iets mis is gegaan. Er komen veel collega's al met vragen vanuit hun eigen bewustzijn. De teams gaan er heel bewust mee om. Daarnaast nemen de teamleiders onze collega's mee in inwerkprogramma's.

Leerrecht en Wmo hebben beide een gedreven privacyambassadeur, tezamen met de teamleiders. Team Leerrecht heeft een vast onderdeel in hun overleggen, waarbij aandacht besteed wordt aan autorisaties, controles, audit en AVG. Alle medewerkers volgen de studytube trainingen.

Team Backoffice Wmo heeft een kennisplek, nieuwe medewerkers worden goed ingewerkt en meegenomen in de avg en informatieveiligheid. Alle medewerkers volgen de studytube trainingen.

Ook voor de beide teams van beide teams Wmo Klassiek is er een privacy ambassadeur.

## Audits

De afdeling Inkomen Zorg en Leerrecht kent een aantal periodieke audits die niet alleen een formele toetssteen vormen op het snijvlak van informatieveiligheid en AVG en die eenvoudigweg vereisten in zich dragen waar we aan hebben te voldoen; ze geven ons ook waardevolle informatie om onze processen aan te passen waar nodig. Hoewel de voorbereiding van de audits tijd vraagt, is de meerwaarde van de audits groot.

Audits kunnen een feitelijke impuls betekenen voor verbeteringen binnen de organisatie. Dat geldt zowel voor interne audits als voor externe audits. Naast ook het verplichte karakter van externe audits zijn het mogelijkheden om risico's en kwetsbaarheden tijdig te duiden én met relevante beheersmaatregelen te komen, betekent het daadwerkelijke interesse in de processen waar medewerkers tijd en aandacht in steken én liggen er dus ook mogelijkheden inbegrepen om veranderingen met draagvlak en betrokkenheid te borgen. Zeker wanneer we als organisatie medewerkers betrekken bij voorbereiding en uitvoering van audits, zoals bij I, Z & L ook de lijn is, kunnen de audits krachtige instrumenten zijn.

De audits waar we als I, Z & L aan deelnemen zijn als volgt:

- Accountantscontrole op processen
- NVVK-audit voor schuldhelpverlening
- Wet politiegegevens (Wpg)
- Privacy audit (kleinschalig, onder privacy ambassadeurs)
- DigiD audit
- Suwinet audit

De accountantscontrole leert ons over de rechtmatigheid en doelmatigheid van onze processen en we nemen verbeter suggesties daaruit mee.

De meest recente edities van de audits vonden plaats op het gebied van Suwinet en Wpg. De eerste bevindingen van de Suwinet-audit waren positief: de definitieve bevindingen volgen nog. Verbeteringen daaruit nemen we mee naar 2025. Dat geldt ook voor de bevindingen van de Wpg-audit. Deze viel ook positief uit: de gevraagde verbeteringen nemen we mee voor inbedding in 2025.

## Datalekken

Over de periode 1-1-2023 tot 3-12-2024 zijn er 5 datalekken gemeld bij de Autoriteit Persoonsgegevens (AP). Er waren 10 incidenten binnen de afdeling Inkomen Zorg en Leerrecht (IZL). In die periode vond de reorganisatie en herindeling van bureaus binnen IZ&L plaats, daarom konden resultaten niet worden gefilterd op bureaucodes.

Hierbij is een kanttekening, namelijk de aantallen van datalekken (20 gemelde en 7 niet gemelde datalekken) komen niet overeen met de eerdergenoemde aantallen.

De reden van dit verschil: Het dashboard "PIMS" in Cybermanager toont de datalekken vanaf het moment er gestart is met registreren: 2020. In het begin is niet consequent afdelings- en bureaucode vermeld bij een registratie, het is dus mogelijk dat daardoor één enkel datalek niet als zodanig is geregistreerd.<sup>8</sup>

Datalekken die o.a. binnengekomen zijn:

- Het niet zorgvuldig gebruikmaken van Zivver mail, door e-mails naar externen/klanten niet in de BCC te plaatsen.
- Telefoon kwijtgeraakt of niet kunnen vinden.
- Printjes die bij een netwerkprinter blijven liggen
- Correspondentie (beschikkingen, opvragen gegevens) aan het verkeerde adres gezonden of voormalig huisadres.

---

<sup>8</sup> Bron: Cybermanager datalekkenregister

## **Wat hebben we te doen? Deel II, een nader ingezoomd beeld...**

Per bureau hebben we een beschrijving gegeven van de werkzaamheden, van de nog op te pakken DPIA's, van de stand van zaken op het gebied van logging en hoe daarmee om te gaan, van autorisatiechecks, het bewustzijn op het gebied van AVG, inzet van privacy ambassadeurs en de risico's die in de gesprekken met de verschillende bureaus werden benoemd. We hebben daarnaast de audit van de privacy ambassadeurs in ogenschouw genomen; heel specifiek nemen we daaruit mee dat we bij procesbeschrijvingen expliciet nog het belang duiden van zorgvuldig werken met persoonsgegevens. De bevindingen en de maatregelen die we daaraan gekoppeld hebben, zijn te vinden in bijlage 2: bevindingen interviews en maatregelen.

We hebben daarnaast een concept-jaarplanning opgenomen die de basis kan vormen om meer gestructureerd te gaan werken op het gebied van AVG en informatieveiligheid.

# Samenvatting

Binnen Inkomen, Zorg & Leerrecht draait wat we doen altijd om de mensen aan wie wij voorzieningen bieden, uitkeringen, kredieten verstrekken of andere bijstand verlenen, mensen die te maken hebben met geldzorgen of mensen die op een andere manier in de context van onze dienstverlening. Dat betekent dus ook dat er binnen de afdeling in belangrijke mate gewerkt wordt met persoonsgegevens, ongeacht de vorm. Daarnaast worden ook bijzondere gegevens verwerkt zoals medische en strafrechtelijke gegevens.

Uit dit onderzoek, de interviews en gesprekken is gebleken dat er een basisbewustzijn is op het gebied van AVG en informatieveiligheid. Tegelijkertijd is er nog sprake van handelingsvrees op het gebied van AVG en zien we dat we niet op evenwichtige wijze vormgeven aan onze sturing op dat gebied. Het SMT kiest voor duidelijke sturing op het werken met AVG, enerzijds inzake de verwachtingen ten aanzien van rolverdelingen op het gebied van AVG, anderzijds om de uiteenlopende taken en verantwoordelijkheden op het gebied van AVG en Informatieveiligheid én maatregelen voortvloeiend uit dit plan ook feitelijk uit te laten voeren.

De gesprekken met de verschillende bureaus in december en de korte audit uit november, hebben een aantal kwetsbaarheden naar voren gebracht.

Dit plan is zowel de vastlegging van de stand van zaken zoals deze in 2024 is; het is ook de routekaart voor het vervolg van onze AVG-aanpak binnen de afdeling. We kiezen voor een structurele verankering, bespreking en gedeelde verantwoordelijkheid van het SMT van de afdeling met effectieve ondersteuning waar die aan de orde is.

Het periodiek toetsen van de stand van zaken op AVG-gebied, zeker binnen I, Z & L is daarmee meer dan een verantwoordelijkheid van de stafadviseur AVG en Informatieveiligheid, het is ook een kerntaak en voornaam aandachtspunt van het management.

# Bijlagen

- Bijlage 1: Data Protection Impact Assessment (DPIA) overzicht IZL
- Bijlage 2: Evaluatie Privacyambassadeurs
- Bijlage 3: Bevindingen en maatregelen
- Bijlage 4: Jaarplanning 2025 Informatieveiligheid en privacy



## Bijlage 1

### Data Protection Impact Assessment (DPIA) overzicht IZL

De volgende DPIA's zijn tot nu toe gekoppeld aan de processen van onze afdeling.<sup>9</sup>

Naam DPIA	Verwerker / bijzonderheden	Datum	DPIA nr.
Vroeg signalering	BKR	10-05-21	17
Huishoudboekje	Nvt	17-06-2021	18
WMO klassiek	Geen	20-01-2022	24
Financieel Expert in de Wijk	Topicus, & convenant Bindkracht 10	26-01-2022	28
Sociale Recherche, anonieme accounts IZL	Protocol Gebruik anonieme accounts bij online onderzoek	14-02-2022	32
Wet inburgering	Landelijk niveau: COA, DUO, CBS Lokaal niveau: aanbieders MAP (Module Arbeid en Participatiewet)	24-02-2022	33
Gegevensuitwisseling Inlichtingenbureau en Bureau Nieuwe Klanten (BNK)	Uitvoering controle rechtmatige uitkeringsverstrekking .	02-06-2022	35
Regeling Opvang Ontheemden (Leefgeldregeling Oekraïners)	Uitvoering regeling opvang ontheemden	14-07-2022	37
Gegevens uitwisseling Inlichtingenbureau en WMO/Jeugdwet	Uitwisseling gegevens backoffice WMO/Jeugd en Inlichtingen bureau	06-09-2022	39
Jongeren in beeld	Project gestopt	08-09-2022	40
Leerplicht (Excl. Wpg werkzaamheden)	<ul style="list-style-type: none"><li>• Verwerkersovereenkomst gemeenten.</li><li>• Verwerkersovereenkomst Meta Objects</li><li>• Privacy Protocol VHH Gelderland-Zuid</li><li>• Convenant VHH Gelderland-Zuid</li><li>• Overeenkomst uitwisseling persoonsgegevens thuiszitters SWV – gem Nijmegen</li><li>• Kredit, leverancier van Allegro.</li><li>• Aansluitingsovereenkomst Verwijs Index Schuld Hulpverlening (VISH) met Stichting Netwerk Gerechtsdeurwaarders (SHVI)</li></ul>	20-04-2023	54

<sup>9</sup> Team Privacy – privacy overleg: overzicht FG (Peter Kluver)

Naam DPIA	Verwerker / bijzonderheden	Datum	DPIA nr.
Schuldenknooppunt	<ul style="list-style-type: none"> <li>Kredit, leverancier van Allegro.</li> <li>Aansluitingsovereenkomst Verwijs Index Schuld Hulpverlening (VISH) met Stichting Netwerk Gerechtsdeurwaarders (SHVI)</li> </ul>	19-09-2023	60
GWS / Suite Sociaal Domein	Centric en applicatie IrvN	28-09-2023	62
Mijn Geldzaken	Kred'it voor Allegro Innovadis voor 'Mijn Geldzaken'.	12-01-2024	72
Besluit Bijzondere Bijstand Zelfstandigen (BBZ)	Decos	25-03-2024	77
Suwinet	Bureau Keteninformatisering Werk en Inkomen BKWI. Raadplegen van Suwinet - DIA 20	11-04-2024	79
Allegro	Kred'it B.V.Allegro	29-04-2024	83
Collectieve Aanvullende Zorgverzekering (CAZ)		05-12-2024	100

## DPIA's voorlopige planning voor 2025

Naam DPIA	Aanvrager	Status	Aanmelding / planning
Ondernemerspunt geldzorgen	5.1.2e	Ovb bestuurlijke besluitvorming	Maart 24 Q1 25
IOAZ	5.1.2e	Addendum	Zomer 23 Q1 25
Participatiewet wet IOAW/ IOW	5.1.2e	In ontwikkeling	Zomer 23 Q1 25
Periodieke uitwisseling met Werkbedrijf – nieuwe klanten	5.1.2e 5.1.2e	Uitzoeken of DPIA nodig is	Zomer 23 Q1 25
Wet Kinderopvang	5.1.2e	In ontwikkeling	Zomer 23 Q1 25
Leerlingenvervoer	5.1.2e	In ontwikkeling	Zomer 23 Q1 25
Geldzorgen B: (proces) Preventie Budgetbeheer Schuldregelingen Kredietverstrekkingen	5.1.2e	Informeert bij PO	Q1 25
Archivering en digitalisering Sociale Recherche	5.1.2e 5.1.2e	Addendum is afgerond.	Aug 24 Q1 25
Rechtmatigheidsonderzoek Sociale Recherche	5.1.2e	En nieuwe versie	Aug 24 Q1 25
Dak – en Thuislozen punt (niet bij Bijz. Doelgroepen)	5.1.2e 5.1.2e MO	Start datum onbekend	Jan 24 Q2 25
Corsa (tweede versie) Oude DPIA is uit 2018	5.1.2e 5.1.2e PIF	Tweede versie	April 24 Q1 25
Wet op de Lijkbezorging	5.1.2e	Uitzoeken of DPIA nodig is	Procesbeschrijving aan PO/FG
Verhaal	5.1.2e	Uitzoeken of DPIA nodig is	Procesbeschrijving aan PO/FG
Nuggets	5.1.2e	Uitzoeken of DPIA nodig is	Procesbeschrijving aan PO/FG
Incasso	5.1.2e	Uitzoeken of DPIA nodig is	Procesbeschrijving aan PO/FG
Briefadressen	5.1.2e	Wordt meegenomen in DPIA Publiekzaken	Geen actie

## Bijlage 2

### Evaluatie privacyambassadeurs <sup>10</sup>

Maatregel	Audit instructie	Bevindingen / verklaring
Lijnmanagement verantwoordelijkheden	Zijn de verantwoordelijkheden voor de lijnmanagers belegd en pakken zij hun rol met betrekking tot de bescherming van persoonsgegevens actief op? Zijn verantwoordelijkheden belegd en beschreven?	We zien binnen de afdeling dat er medewerkers dedicated mee bezig zijn, dat zijn tenminste de privacy ambassadeurs, de adviseur AVG en privacy, manager Stafbureau. Daarnaast zien we een aantal medewerkers voor wie het van nature een belangrijk onderwerp is. De leidinggevendenden nemen hun verantwoordelijkheid binnen uitvoering van controlplan en het opstellen van DPIA's. Verankering in verantwoordelijkheden binnen de lijn kan en moet nadrukkelijker uitgewerkt worden en is een belangrijk aandachtspunt voor het SMT.
Werkprocessen vaststellen	Zijn er werkprocessen in de afdeling vastgesteld waarin persoonsgegevens worden verwerkt? Zo ja, welke processen?	Ja, dit geldt voor het overwegende deel van onze processen. Denk aan alle processen aangaande uitkeringen, Wmo, Leerrecht, Jeugdwet, Bijzondere bijstand, Schuldhulpverlening, Inburgering, bijzondere doelgroepen. Dit vertaalt zich ook in een groot aantal DPIA's.

<sup>10</sup> Evaluatie privacy bijeenkomst privacy ambassadeurs 14-11-2024

Maatregel	Audit instructie	Bevindingen / verklaring
Passende instructies omgang persoonsgegevens	<p>Zijn er instructies en protocollen (voor hoge risico verwerkingen) beschikbaar voor medewerkers over de omgang met persoonsgegevens in werkprocessen en worden ze daarop getraind?</p> <p>Zijn er passende instructies en protocollen voor hoog risicoverwerkingen?</p>	<p>Er zijn uiteenlopende werkinstructies en protocollen die op de verschillende werkprocessen ingaan. Daarin wordt niet altijd specifiek ingegaan op privacy-aspecten en AVG. Tegelijkertijd: er wordt veel mondeling gedeeld en toegelicht inzake AVG voor het betreffende bureau. Bovendien, daar waar het gaat om de meest kritische aspecten van het werk (Suwinet als voorbeeld) hebben we doorlopend aandacht voor de ‘gouden regels’ voor de toepassing, kan niet iedereen toegang krijgen tot Suwinet, wordt elk gebruik gelogd en vindt er net als bij een aantal andere processen jaarlijks een audit plaats die ook ingaat op AVG. Daarbij wordt er ook strikt gekeken naar de autorisaties. Die check vindt voor een groter aantal processen plaats. Denk ook aan Wpg, Allegro, Suite en Forus.</p> <p>We constateren dat de aandacht ervoor in geschreven instructies nadrukkelijker kan: voor een aantal bureaus geldt dat ook de mondelinge toelichting soms beter kan. Wat we verder zien, is dat het belang van het werk dat we doen soms zwaarder lijkt te wegen dan de AVG. Belangrijk: dit raakt niet zelden aan gegevensuitwisseling met derden, niet zelden (semi-)overheidsinstellingen. Dat zegt ook iets over AVG-bewustzijn bij die organisaties.</p>
Register van verwerkingen	<p>Heb je als afdeling in beeld welke verwerkingen plaatvinden? Hebben jullie een beeld welke verwerkersovereenkomsten jullie afgesloten hebben? En zijn deze opgenomen in het centrale verwerkersregister?</p> <p><a href="https://www.nijmegen.nl/verwerkersnijmegen.php">https://www.nijmegen.nl/verwerkersnijmegen.php</a></p>	<p>Dit is niet een van de aspecten die leven bij de privacy ambassadeurs. Dit is wel bekend, uit de aard van hun rollen, bij de adviseur AVG en privacy en de manager Stafbureau. Daar is het in beeld en weet men ook dat deze zijn opgenomen in het verwerkersregister; eventuele uitzonderingen daargelaten.</p>

Maatregel	Audit instructie	Bevindingen / verklaring
Uitvoeren DPIA's	<p>Worden DPIA's structureel uitgevoerd en mitigerende (verzachtende) maatregelen doorgevoerd door de proceseigenaren binnen de afdeling?</p> <p>Worden DPIA's structureel uitgevoerd / nageleefd en mitigerende maatregelen doorgevoerd?</p>	<p>Ja, ze worden opgepakt; er kan verschil zijn in het ritme van oppakken. Dat vindt echter uiterlijk plaats bij de check op de naleving van de DPIA. Ook deze vraag kan niet door elke privacy ambassadeur worden beantwoord; hier weer adviseur AVG en privacy en manager Stafbureau.</p>
Bewaartermijnen	<p>Worden persoonsgegevens die niet meer nodig zijn tijdig verwijderd of geanonimiseerd?</p> <p>Worden persoonsgegevens tijdig vernietigd?</p>	<p>In grotere systeemapplicaties wordt vernietiging zoveel mogelijk structureel ingebed. Dat gebeurt ook zoveel mogelijk met lokale gegevensverwerkingen. Echter, dat is niet overal het geval. Op dit moment is het niet gegarandeerd dat maximale bewaartermijnen overal bewaakt worden.</p>

Maatregel	Audit instructie	Bevindingen / verklaring
Juridische kennis Middelen voor privacybescherming	<p>Is er voldoende kennis en kunde aanwezig binnen de afdeling op het gebied van Privacy?</p> <p>Vinden er organisatie brede trainingen plaats voor medewerkers op het gebied van privacy <i>bewustzijn</i>, inclusief het management?</p> <p>Zijn er voldoende middelen beschikbaar op het gebied van privacy?</p>	<p>Enerzijds weten we van de rollen van de AVG adviseur/manager Stafbureau; daar kunnen mensen met vragen terecht. Anderzijds: als er vragen binnen een bureau spelen bij een van de medewerkers, kan het antwoord voor iedereen belangrijk zijn. Dat zou betekenen dat er vanuit het management een nadrukkelijker rol zou kunnen zijn, of juist voor de privacy ambassadeur. De privacy ambassadeur is ook nog niet altijd bij iedereen bekend. Het risico bestaat ook dat de rol van privacy ambassadeur én van de twee andere functies als een soort overloop wordt ervaren én dat actieve bespreking in de teams uitblijft.</p> <p>We staan er verder bij stil dat informatie nog beter gedeeld mag worden, centraler en beter te vinden.</p> <p>Over de trainingen: er zijn de gemeentebrede trainingen. Daarnaast hebben we als I, Z &amp; L vorig jaar bredere uitleg gehad van 5.1.2e en 5.1.2e; een vergelijkbare training willen we hervatten naast bijvoorbeeld het idee van een AVG-café.</p> <p>Middelen zijn wellicht voldoende beschikbaar: het gaat ook om het doen.</p>
Privacy by Design en Privacy By Default	<p>Wordt rekening gehouden met Privacy by Design (bij ontwerp) en Privacy by Default (bij gebruik) bij nieuwe verwerkingen?</p>	<p>Ja.</p>
Inzicht in privacy incidenten	<p>Heeft de afdeling inzicht in (potentiële) privacy-incidenten, zoals datalekken?</p>	<p>Het besef is er. In voorkomende gevallen worden ze ook gemeld.</p>

### **Bijlage 3 Bevindingen en maatregelen**



Bijlage 3: Bevindingen en maatregelen				
Bevindingen Inkomen, Zorg & Leerrecht	Risico en/of belang	Maatregelen	Wie en wat?	Planning
Het gebruik van Zivver stuit op praktisch vragen en soms ook op weerstand.	Persoonsgegevens lopen risico onbedoeld en onjuist gedeeld te worden.	1.1.24 kan uitleg geven over het optimaal gebruikmaken van Zivver.	Teamleiders nemen contact op met 1.1.24 en plannen uitleg in.	Voorstel: 1e kwartaal 2025.
		Daarnaast verdient het aanbeveling alternatieven voor Zivver te benoemen en deze, met instructie, uit te dragen binnen de afdeling. Denk onder andere aan het gebruik van Nextcloud.	Stafadviseur AVG en Informatieveiligheid (of evt. andere stafadviseur) gaat alternatieven uitzoeken en uitleg geven.	Voorstel: 1e kwartaal 2025.
Niet voor elk team is er een privacy ambassadeur.	Privacyvraagstukken binnen een team worden niet makkelijk gedeeld.	Actief sturen op de inzet van privacy ambassadeurs binnen de afdeling; het SMT heeft de keuze gemaakt die op teamniveau in te vullen. Zo zorgen we ervoor dat de privacy ambassadeurs laagdrempelig toegankelijk zijn voor de collega's. De rol van privacy ambassadeur dient gefaciliteerd te worden.	SMT stuurt hierop en ziet toe op werving privacy ambassadeurs per team.	Voorstel: alle posities ingevuld in 2e kwartaal 2025.
Persoonlijke gegevens (bijvoorbeeld voor continuïteitsredenen) bevinden zich in een aantal gevallen op daarvoor niet-bestemde locaties (gezamenlijke mailboxen, bestanden in gezamenlijke mappen).	Persoonsgegevens lopen risico onbedoeld en onjuist gedeeld te worden.	Actieve communicatie over welke opslagmogelijkheden toegestaan zijn en welke niet.	Voorbereiding door stafadviseur AVG en Informatieveiligheid (of evt. andere stafadviseur) en communicatie door SMT.	Voorstel: voorbereiding 1e kwartaal 2025, communicatie 2e kwartaal 2025.
Binnen de afdeling zien we heel erg actief leiderschap van een aantal teamleiders en privacy ambassadeurs terwijl een aantal anderen meer reactief stuurt op AVG-bewustzijn.	We stuurden nog onvoldoende op hoe we willen dat we met AVG omgaan. Dat maakt dat er grote verschillen zijn binnen de teams. Voor wat betreft de bewustzijnsniveau op het gebied van AVG én informatieveiligheid is het voor een afdeling als de onze van belang om daar gericht op te sturen.	AVG is onderdeel van ons primair proces. De eerste verantwoordelijkheid om de teams én daarmee de afdeling AVG-proof te houden ligt bij de teamleider. Het SMT maakt de verwachtingen en verplichtingen duidelijk.	Besluitvorming en uitdragen door SMT, ondersteund door stafadviseur AVG en Informatieveiligheid (of evt. andere stafadviseur).	Voorstel: bespreekbaar maken na cascaderingsbijeenkomst in januari 2025.
Een aantal rapportages binnen Cognos is gebouwd rond cliëntgegevens die tot op individueel niveau herleidbaar zijn.	Persoonsgegevens lopen risico onbedoeld en onjuist gedeeld te worden.	DPIA-proces Cognos doorlopen om exacte risico's uit te zoeken. Vervolgens systematisch de persoonlijke gegevens uit Cognos verwijderen waar aan de orde.	1.1.24 stelt de DPIA op. Daarna gaat deze in gesprek met een stafadviseur zodat de verwijdering van gegevens uit Cognos voorbereid kan worden.	DPIA is al in de maak.
Persoonlijke telefoongesprekken met cliënten vinden op de werkvloer plaats.	Persoonsgegevens lopen risico onbedoeld en onjuist gedeeld te worden.	Wij bevelen nadrukkelijk aan om randvoorwaarden voor veilig telefoongebruik in te zetten. Dit dient nader onderzocht te worden.	Een stafadviseur kan de mogelijkheden en onmogelijkheden van verschillende alternatieven in beeld brengen ter besluitvorming door het SMT. Daarna volgt implementatie.	Voorstel: onderzoeken in 2e kwartaal 2025.
Applicaties en/of processen hebben nog geen DPIA ondergaan.	De risico's verbonden aan een gegevensverwerking zijn nog niet in beeld dus er is een kans dat persoonsgegevens onbedoeld en onjuist gedeeld worden.	Tweestapsaanpak: 1. Onderzoeken (aan de hand van een korte procesbeschrijving) of een aantal processen een DPIA vereisen 2. De DPIA voor de relevante processen opstellen.	Teamleiders leveren een korte procesbeschrijving aan aan de stafadviseur AVG en informatieveiligheid ter beoordeling aan de FG en privacy officer.	Voorstel: procesbeschrijvingen aanleveren in januari/februari 2025. De te plannen DPIA's als volgt: preventie Q2, budgetbeheer Q3, schuldhulpverlening en kredietverstrekking Q4.
AVG-bewustzijnstrainingen opnieuw plannen.	De basiskennis op het gebied van AVG binnen de afdeling op peil houden en actualiseren en voorkomen dat er mensen in handelingsangst blijven hangen.	Herintroductie van de eerdere uitleg over AVG, respectievelijk start van AVG-café waar laagdrempelig periodiek AVG-vraagstukken besproken kunnen worden.	Voorbereiding en uitvoering door privacy ambassadeurs en stafadviseur AVG en Informatieveiligheid.	Voorstel: voorbereiding 1e kwartaal 2025, uitvoering in te plannen daarna.
Het belang van zorgvuldig werken met AVG vastleggen/benoemen bij procesbeschrijvingen en werkinstructies.	Doorlopend aandacht vragen voor het belang van zorgvuldig werken met persoonsgegevens.	Team Kwaliteit verzoeken dit mee te nemen in procesbeschrijvingen en werkinstructies.	Manager Stafbureau legt deze vraag bij team Kwaliteit neer.	Voorstel: voorbereiding 1e kwartaal 2025, uitvoering in te plannen daarna.
De privacy-ambassadeurs van I, Z & L werken nog los van elkaar.	We maken onvoldoende gebruik van de synergie die samenwerking van de privacy ambassadeurs in zich draagt. Daar wel gebruik van maken, vergroot de grip op AVG en privacy.	Privacy ambassadeurs en stafadviseurs komen een keer per kwartaal bij elkaar om actuele vraagstukken te bespreken.	Stafadviseur AVG en Informatieveiligheid plant; uitvoering samen.	Voorstel: voorbereiding 1e kwartaal 2025, uitvoering in te plannen daarna.
Het gebruik maken van loggings en het checken daarvan wordt steeds belangrijker. I, Z & L werkt naar	Hoewel het een controle achteraf is, kunnen de loggings waardevolle bronnen zijn over het gebruik van applicaties. Op dit moment is de inzet ervan beperkt én vindt er dus ook niet altijd een check plaats. Het belang ervan neemt toe naarmate dit meer en meer gevraagd wordt bij audits. In de huidige situatie zien we dat loggings van Suite alleen gecheckt kunnen worden door de privacy officer. Logging van Corsa voorziet nog niet in alle wenselijke opties.	Voorbereiden werkwijze werken met loggings en laten vaststellen in overleg met CISO; stafadviseur AVG en Informatieveiligheid neemt het voortouw.	Stafadviseur AVG en Informatieveiligheid (of evt. andere stafadviseur) onderzoekt en bereidt voor voor bespreking in het SMT.	Voorstel: voorbereiding 1e kwartaal 2025, uitvoering in te plannen daarna.
Teamleiders voeren periodiek autorisatiechecks uit op autorisaties van applicaties.	Van belang om te checken of we de checks al doen bij de meest gevoelige applicaties én daar planning en vastlegging van inrichten. Bij voorkeur op een eenduidige manier.	Voorbereiden werkwijze werken met loggings en laten vaststellen in overleg met CISO; stafadviseur AVG en Informatieveiligheid neemt het voortouw.	Stafadviseur AVG en Informatieveiligheid (of evt. andere stafadviseur) onderzoekt en bereidt voor voor bespreking in het SMT.	Voorstel: periodiek uitvoeren.

## **Bijlage 4 Jaarplanning 2025 Informatieveiligheid en privacy**

LEGENDA

AVG en privacy

Veiligheid van informatie en persoonsgegevens

	Januari	Februari	Maart	April	Mei	Juni	Juli	Augustus	September	Oktober	November	December		Wie	Geschatte uren op jaarbasis
Cyclus														Stafadviseur AVG en Informatieveiligheid	PM
Updaten Mijn afdeling AVG-proof														Teamleiders	PM
DPIA's (updaten + verbeteracties)														Stafadviseur AVG en Informatieveiligheid	PM
Updaten verwerkingsregister														Teamleiders (met ondersteuning)	PM
DPIA's opstellen														Stafadviseur AVG en Informatieveiligheid	PM
Vernietiging in Suite voorbereiden														Stafadviseur AVG en Informatieveiligheid	PM
Vernietiging in Suite uitvoeren														Stafadviseur AVG en Informatieveiligheid	PM
Vragen controlplan uitzetten														Stafadviseur AVG en Informatieveiligheid	PM
Antwoorden uitvraag controlplan														Teamleiders	PM
Uitkomsten controlplan verzamelen														Stafadviseur AVG en Informatieveiligheid	PM
Verzenden input controlplan naar FG														Stafadviseur AVG en Informatieveiligheid	PM
Jaarverslag FG														FG	PM
Oprfrissen gebruikersaccounts-beheer (incl. autorisatiematrix gevoelige applicaties)														Stafadviseur AVG en Informatieveiligheid	PM
Bedrijfscontinuïteitsplan (verdiepen)														Strategisch manager/concernmanager	PM
Bedrijfscontinuïteitsplan (oefenen)														Strategisch manager/concernmanager	PM
Audits voorbereiding, planning en uitvoering														Kwaliteitsmedewerkers, stafadviseur AVG en Informatieveiligheid	PM
Invullen/update Cybermanager, incl. dataclassificatie en i-veiligheid fysieke locaties														Stafadviseur AVG en Informatieveiligheid	PM
Aanleveren data jaarverslag CISO															

Doortlopend

DPIA's (opstellen, updaten, addendum)

Bijeenkomsten privacy-ambassadeurs I, Z & L organiseren

Beantwoording vragen uit afdeling over AVG, informatieveiligheid en privacy

Bijwonen sessies privacyambassadeurs gemeentebreed

Bewustwording: herhaling vanuit management richting werkvloer over afspraken AVG

Sturen op vervolgacties Mijn afdeling AVG-proof

Bijwonen netwerk informatieveiligheid

Bewustwording: herhaling vanuit management richting werkvloer over afspraken infov.

Datalekken melden

Bewustwording: optimaliseren gebruik Zivver

Losse projecten?

Verwerkingsovereenkomsten projectmatig updaten/verbeteren

Auditschema maken en bijhouden

Multi-factor authenticatie systemen ontwikkelen/instellen

Wachtwoordvereisten, scherp houden

Bewustwording: bitwarden promoten

Gedeelde generieke accounts, centraal beheren

Logging in systemen: hoe opvolging te geven?

Aanhaken op cybermaand oktober

# Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 9, 11, 13, 15, 16, 18, 27, 31, 33