

Jaarverslag 2022 Functionaris Gegevensbescherming Gemeente Groningen

Inhoud

Samenvatting.....	2
1. Inleiding.....	3
2. Algemeen beeld compliance AVG	4
3. Datalekken.....	6
4. Gegeveneffectbeoordelingen (PIA's).....	7
5. Register verwerkingen.....	8
6. Overige onderwerpen	9
7. Aandachtspunten	11

Auteur: Menno van Heumen, Functionaris Gegevensbescherming

Datum: 30 december 2022

Status: definitief

Samenvatting

Als onafhankelijk toezichthouder van de gemeente constateert de Functionaris Gegevensbescherming (FG) dat de Gemeente Groningen vorderingen maakt als het gaat om het voldoen aan de Algemene Verordening Gegevensbescherming (AVG).

Op drie aspecten scoort de gemeente naar het oordeel van de FG nog niet geheel voldoende: het op orde hebben van het register van de verwerkingen (kwalitatief niet publicabel), het uitvoeren van geveenseffectbeoordelingen (Privacy Impact Assessments, of PIA's, worden niet zelfstandig uitgevoerd) en het toepassen van privacy-by-design en -by-default (komt nauwelijks voor).

Na de invoering van de AVG in 2018 is de gemeente stap voor stap zich aan het ontwikkelen tot een organisatie waarbij gesproken kan worden van het 'in control' zijn als het gaat om de gewenste AVG compliance. De stap die in 2022 werd gezet had te maken met meer sturing vanuit de leiding. Afspraken over privacy in de managementcontracten vormen nu een onderdeel van de control-cyclus.

Voor 2023 is een volgende stap mogelijk doordat er meer capaciteit beschikbaar komt voor het aanpakken van de drie hierboven genoemde ontwikkelpunten.

Het aantal meldingen van mogelijke datalekken ligt iets onder de 200 per jaar. Daarvan hoeven er maar minder dan vijf gemeld te worden bij de Autoriteit Persoonsgegevens.

Er worden nu per jaar circa 20 geveenseffectbeoordelingen uitgevoerd. Dat aantal is lager dan op grond van het aantal verwerkingen dat de gemeente (ca 200) heeft uitgevoerd zou moeten worden. Bij alleen een 4-jaarlijkse herijking van een PIA zou het aantal op 50 moeten uitkomen. Omdat er ook nieuwe processen of systemen worden ingevoerd, waarbij een PIA verplicht is, moet dus het aantal PIA's ruim boven de 50 liggen.

De gemeente kent de nodige samenwerkingen, zoals met de stichting WIJ en die in het kader van de Arbeidsmarktregio. Omdat ook daar ontwikkelingen niet stil staan is het goed om ook daar specifiek aandacht te schenken aan waarborgen voor de privacy.

De FG adviseert,

- I. het verwerkingenregister te publiceren als onderdeel van het informeren van de burgers;
- II. te borgen dat de organisatie in staat is zelfstandig geveenseffectbeoordelingen uit te voeren met daarbij een belangrijke uitvoerende rol voor Informatieadviseurs en projectleiders;
- III. beleidsregels vast te stellen voor privacy-by-design en privacy-by-default zodat er betere waarborgen zijn voor de privacy bij het ontwerp en invoering van informatiesystemen;
- IV. de relatie tussen de gemeente en de stichting WIJ vanuit het oogpunt van de privacy te herijken zodat duidelijk wordt welke afspraken gelden bij de verschillende rollen als het gaat over verwerkingsverantwoordelijkheid;
- V. een privacyconvenant op te stellen voor de Arbeidsmarktregio.

1. Inleiding

Het jaarverslag 2022 van de Functionaris Gegevensbescherming (FG) van de gemeente Groningen beoogt verantwoording af te leggen van de taak van de FG zoals die is vastgelegd in de Algemene Verordening Gegevensbescherming (AVG; art 39) en een beeld te geven over waar de gemeente staat als het gaat om het verwerken van persoonsgegevens in relatie tot de AVG.

De taak van de FG omvat in het kort het informeren en adviseren van het bestuur, de directie en de werknemers van de gemeente inzake hun verplichtingen, het uitoefenen van toezicht op naleving van de AVG, advisering met betrekking tot de uitvoering van gegevenseffectbeoordelingen (privacy impact assessment ofwel PIA) en het onderhouden van contacten met de Autoriteit Persoonsgegevens (AP). De FG voert zijn dagelijkse werkzaamheden uit samen met de Privacy Officer van Juridische Zaken. De FG van de gemeente is ook de FG van de stichting WIJ en van GGD Groningen, maar dit verslag heeft geen betrekking op die twee organisaties omdat deze een zelfstandig rechtspersoon zijn.

De verantwoording zoals in dit jaarverslag is verwoord gaat in op het algemene beeld van de compliance ten aanzien van de AVG, de bevindingen over het jaar 2021 en 2022 en de aandachtspunten voor 2023. De jaren 2021 en 2022 werden voor iedereen gekenmerkt door de pandemie en de oorlog in Oekraïne met alle gevolgen voor de burgers en daarmee ook de werksituatie binnen de gemeente. Veel aandacht is door het management en de medewerkers geschonken juist aan de burgers.

Een groot deel van die twee jaren heeft de FG zonder de Privacy Officer moeten werken en was de ondersteuning vanuit de organisatie beperkt. Daarom is er in 2022 geen jaarverslag over 2021 uitgebracht.

Het jaarverslag van de FG wordt ter informatie via de Concerndirectie aangeboden aan het college van B&W omdat zij eindverantwoordelijk is voor de verwerking van de persoonsgegevens. Het college dient kennis te nemen van het jaarverslag en kan een uitspraak doen over de vermelde aandachtspunten voor 2023. Daarnaast kan het college het jaarverslag ter informatie aanbieden aan de gemeenteraad en het publiceren op de website van de gemeente.

2. Algemeen beeld compliance AVG

Vier jaar na de invoering van de Algemene Verordening Gegevensbescherming (AVG) in 2018 kan gesteld worden dat ook in 2022 kleine stapjes vooruit worden gezet om te voldoen aan de AVG. Voor het eerst zijn er in de managementcontracten afspraken gemaakt over privacy. Afspraken over de kwaliteit van het verwerkingenregister en de uitvoering van geveenseffectbeoordeling (ook wel PIA; privacy impact assessment). Vanaf 2018 was de aandacht vooral gericht op het dagelijkse werk. 'Mag dit van de AVG?' was een vaak gestelde vraag. Door voorlichting en bewustwordingscampagnes is die onzekerheid verminderd. Maar een verdere voortgang is vooral ook een kwestie van sturing door de leiding. Deze sturing wordt aangebracht via de reguliere, al bestaande planning- en controlcyclus. Omdat privacy een element is van de managementcontracten wordt dit aspect een onderdeel van control. Bijpassend is dan ook dat de functie van de FG in 2022 is ondergebracht bij Concern Control. Verwacht mag worden dat resultaten hiervan de komende jaren zichtbaar zullen worden.

2021 en 2022 zijn voor de Functionaris Gegevensbescherming (FG) jaren geworden van aandacht voor de noodzakelijke dingen: afhandeling datalekken, voorlichting en begeleiding van PIA's daar waar er om gevraagd werd. Maar vooral de noodzakelijke inzet als FG voor GGD Groningen, vanwege vele privacyvraagstukken rondom de Covid pandemie, heeft gemaakt dat er minder ruimte was voor actievere participatie op verschillende thema's zoals bijvoorbeeld het verwerkingenregister.

De FG hanteert tien aspecten voor het beoordelen van de mate van het voldoen aan de AVG, gebaseerd op art.24 over de plichten van de verwerkingsverantwoordelijke. Een korte karakterisering van die eisen geeft het volgende beeld:

aspect	toelichting
Bewustwording	In samenwerking met Juridische Zaken (JUZA), het Informatiebeveiligingsteam (onderdeel van SSC I&S Regie) Informatiebeheer is er binnen de organisatie veel aandacht voor bewustwording. Naast bijzondere acties, zoals phishing mails en thematische bijeenkomsten, zijn er speciale zelfstudiemodules ontwikkeld. De basismodules hebben vervolgens het predikaat 'digitaal rijbewijs' gekregen waarbij het doel is dat iedere werknemer dit behaalt. De continue aandacht voor bewustwording is een goede zaak.
Register verwerkingen	De FG heeft met hulp van de directies een register opgebouwd. De kwaliteit daarvan is nog onvoldoende om dit in- en extern te publiceren. Dit was in 2018 zo, en is niet veranderd.
Rechten van betrokkenen	Deze rechten zijn kenbaar gemaakt op de website van de gemeente, en procedureel geborgd door het onderbrengen van dit proces bij JUZA in analogie van WOO-verzoeken. Uitoefening van rechten door burgers komt zelden voor.
Toestemming betrokkenen	Voor de meest voorkomende, primaire diensten die de gemeente levert bestaat de grondslag voor het verwerken van de gegevens veelal uit de uitvoering van een wettelijke verplichting of het algemeen belang. Toch zijn er situaties waarbij toestemming expliciet gevraagd en aantoonbaar gemaakt moet worden. Denk daarbij aan toestemming voor doeleinden zoals nieuwsbrieven, andere voorzieningen of producten, het doen van tevredenheidsonderzoeken en enquêtes, maar ook het doorbreken van geheimhoudingsplicht. Er is nog niet vastgesteld dat deze toestemming ondubbelzinnig en actief is gegeven.
Informeren van betrokkenen	Wanneer de gemeente gegevens gaat verzamelen moeten betrokkenen hierover worden geïnformeerd (art. 13 en 14 AVG). Naast het ontbreken van

	een gepubliceerd register bestaat bij de FG het beeld dat in een aantal gevallen betrokkenen minder concreet worden geïnformeerd over het verwerken van hun gegevens dan wordt vereist.
Gegevenseffect-beoordelingen (PIA's)	Van dit middel wordt inmiddels tientallen malen per jaar gebruik gemaakt en dat is een goede ontwikkeling. Het is wel zo dat de inbreng van de FG daarbij groot is ('toetst soms wat hij zelf voorstelt'). De organisatie is nog onvoldoende in staat hier zelfstandig invulling aan te geven. Daarnaast is het nog geen automatisme dat genomen maatregelen worden teruggekoppeld aan de FG.
Privacy-by-design en privacy-by-default	Waar PIA's inzicht geven in nodige maatregelen rond verwerkingen zijn deze twee aspecten vooral bedoeld om bij het procesontwerp privacyaspecten als dataminimalisatie en opslagbeperkingen (beginselen AVG art 5) standaard mee te nemen. Dit vindt nog nauwelijks aantoonbaar plaats. Ook bestaat er geen beleidsmatige invulling van art. 25 (lid 1 en overweging 78) waardoor bij het ontwerp en invoering van nieuwe systemen er mogelijk onvoldoende waarborgen zijn.
Functionaris Gegevensbescherming	Deze is aanwezig (bij Concern Control). GGD Groningen heeft vanaf 1-1-2023 een eigen FG. Na jaren van onderbezetting is de verwachting dat het privacyteam (FG, privacy officer en ondersteuning) uit vier mensen zal bestaan en dat is beter passend bij de zesde grote gemeente van Nederland.
Meldplicht datalekken	Er is een vastgestelde procedure voor het onderzoeken en registreren van meldingen van mogelijke datalekken. Informatiebeveiliging houdt hiervan een register bij. Het aantal meldingen ligt op een bescheiden niveau (iets onder de tweehonderd per jaar). Het aantal dat moet worden gemeld bij de AP is laag, minder dan vijf, een welhaast ongeloofwaardig aantal. De oorzaak zal waarschijnlijk liggen in het massale thuiswerken waarbij de meldingsbereidheid lager ligt. Een aantal systemen bevat vanwege gebrekkige controle onnodig veel persoonsgegevens (eSuite, ServiceNow).
Verwerkersovereenkomsten	Er is een standaard ontwikkeld voor het aangaan van verwerkersovereenkomsten, gebaseerd op het format van de VNG dat in toenemende mate wordt gebruikt. Leveranciers komen nog sporadisch wel eens met hun eigen 'standaard'. Er bestaat inmiddels een totaaloverzicht van de aanwezige overeenkomsten.

Conclusie:

Samenvattend kan gesteld worden dat ten opzichte van 2018, de start van de AVG, de gemeente goede stappen heeft gezet bij het voldoen aan de AVG, maar dat er op drie aspecten nog een compliance risico bestaat:

- het informeren van betrokkenen;
- het zelfstandig uitvoeren van de gegevenseffectbeoordelingen (PIA's);
- het toepassen van privacy-by-design.

3. Datalekken

Simpel gezegd is er sprake van een datalek wanneer persoonsgegevens op een plaats zijn gekomen waar deze niet thuishoren, waar deze zichtbaar worden voor onbevoegden of wanneer deze verdwijnen door verlies of diefstal. Aan een datalek gaat altijd een beveiligingsincident vooraf. Omdat er niet altijd sprake zal zijn van persoonsgegevens is het aantal datalekken lager dan het aantal beveiligingsincidenten.

Over de afgelopen jaren bestaat het volgende beeld van het aantal meldingen die zijn gedaan:

jaar	2018	2019	2020	2021	2022
meldingen gemeente	34	149	131	194	175
meldingen AP	6	8	0	5	3

Een organisatie waar geen datalekken voorkomen is een utopie; waar mensen werken kunnen zaken misgaan. Daarnaast kunnen software en systeeminstellingen gebreken vertonen. De aantallen meldingen geven op zichzelf geen aanleiding voor het nemen van concrete maatregelen. Gelet op de omvang van de gemeente (qua medewerkers en inwoners) beoordeelt de FG het aantal meldingen als blijkbaar passend bij de organisatie.

Wél is het interessant te kijken naar de meest voorkomende soorten datalekken.

Circa 30 % van de meldingen gaat over het verzenden van stukken naar een ander adres. Dat is in toenemende mate het gevolg van het gebruik van een foutief e-mailadres dan wel het gebruik van het cc:/veld in plaats van de bcc:/. Dit is echt een kwestie van oplettendheid van de medewerker.

In dezelfde orde van grootte, 30% is er sprake van het onterecht plaatsen van persoonsgegevens in een specifieke omgeving. Twee omgevingen behoeven daarom aandacht: Servicenow en de Suites. Servicenow is het registratiesysteem voor meldingen en aanvragen inzake de ict-dienstverlening. Daarbij wordt onnodig vaak persoonsgegevens, ook van inwoners, opgenomen. Om dit te ondervangen zou er een aanpassing moeten komen van de werkinstructie of een periodieke schoning van die omgeving.

De Suites zijn zaaksystemen die opgebouwd zijn uit dossiers van burgers van de gemeente. Verschillende processen binnen de gemeente worden met deze systemen ondersteund. Soms ook hebben inwoners toegang tot hun dossier. Een dossier bevat vaak bijlages die soms door de burger worden geplaatst (met een teveel aan niet noodzakelijke persoonsgegevens) en soms door de medewerker, eventueel na digitalisering van papieren documenten. Het komt te vaak voor dat er bijlages worden opgenomen in een dossier van een andere burger. Dit is een kwestie van het inbouwen van kwaliteitsverhogende activiteiten.

Tenslotte blijkt ongeveer 20% van de datalekken te relateren aan het verlies van apparatuur, veelal mobiele telefoons en ipads. Nu is apparatuur beveiligd en door het beheer op afstand zijn de gevolgen van datalekken na verlies beperkt en dat is heuglijk. Het verlies van bedrijfsmiddelen is natuurlijk wel een kostenpost.

4. Gegevenseffectbeoordelingen (PIA's)

Gegevenseffectbeoordelingen zijn een uiterst probaat hulpmiddel bij het beoordelen of er sprake is van risico's bij het verwerken van persoonsgegevens en voor het bepalen van daartoe te nemen maatregelen. Een PIA is verplicht wanneer er 'waarschijnlijk sprake is van een hoog risico voor de rechten en vrijheden van natuurlijke personen' (AVG art. 35).

Om dat te kunnen bepalen is er een richtsnoer uitgegeven door het onafhankelijke Europese adviesorgaan WP29. Deze stelt dat 'In gevallen waarin het niet duidelijk is of een PIA vereist is, deze toch uit te voeren omdat het de verwerkingsverantwoordelijke helpt om aan de wetgeving te voldoen.' De FG stelt zich dan ook op het standpunt dat omdat de gemeente tot 2018 geen PIA's heeft uitgevoerd het (meer dan) wenselijk is dat er PIA's uitgevoerd worden van alle bestaande verwerkingen. Daarom zijn hierover afspraken opgenomen in het managementcontract dat de Concerndirectie heeft afgesloten met de afzonderlijke directeuren; per jaar zal ongeveer van een kwart van de bestaande verwerkingen een PIA worden uitgevoerd. Op deze wijze komen alle verwerkingen eens in de vier jaar aan bod.

Daarnaast zullen er PIA's uitgevoerd moeten worden bij het opzetten van nieuwe processen of bij invoering van nieuwe informatiesystemen omdat de gemeente nagenoeg altijd persoonsgegevens verwerkt. Een risicobeoordeling is dan op zijn plaats.

Het uitvoeren van een PIA is de verantwoordelijkheid van de proceseigenaar. De FG brengt over de uitgevoerde PIA een advies uit.

In 2018 heeft de FG de I-adviseurs van het team Regie IA (onderdeel SSC I&S) geïnformeerd over het toepassen van de PIA en het gebruik van het model. De I-adviseurs zijn bij uitstek geschikt qua kennis en positie om PIA's uit te voeren. De FG is vanaf 2018 dus betrokken als procesbegeleider van te houden PIA's om de I-adviseurs in de gelegenheid te stellen ervaring op te doen. Dit is nog niet succesvol gebleken. De uitvoering van de PIA leunt nog steeds teveel op de kennis en ervaring van de FG.

Het beeld van de tot nu toe uitgevoerde PIA's is:

jaar	2018	2019	2020	2021	2022	Totaal
#pia's	4	30	39	19	17	109

Ruim een derde van de PIA's wordt uitgevoerd in het sociale domein (dmo, inkomensdienstverlening, werk & participatie) en een derde binnen de Servicecentra (ict, hrm, financiën, communicatie). Dat is een op zichzelf verklaarbaar beeld omdat daar de meeste persoonsgegevens worden verwerkt.

De PIA's bevat een advies van de FG aan de verantwoordelijke directeur. Er wordt door de FG zelden een (formele) terugkoppeling ontvangen van de geadviseerde maatregelen.

Het aantal uitgevoerde PIA's is bovendien te laag. Van de bestaande processen zou jaarlijks een kwart bekeken moeten worden op mogelijke privacyrisico's; minimaal 50 dus. Zolang dit niet wordt gehaald zijn de risico's voor de verantwoordelijke directeuren onvoldoende bekend.

5. Register verwerkingen

In 2018 is een eerste ruwe versie gemaakt van het register van verwerkingen. Daarin staat opgenomen voor welke verwerkingen de gemeente Groningen eindverantwoordelijk is conform de definitie daarvan in de AVG (art. 4 lid 7). Deze ruwe versie is gebaseerd op een opgaaf van de diverse directies. De versie is niet volledig en op onderdelen onjuist. In de jaren na 2018 is het bij gebrek aan capaciteit niet mogelijk gebleken hier verandering in aan te brengen.

Gelet op art. 13 en 14 van de AVG is het aan de gemeente om actief te communiceren over aspecten van de verwerkingen zoals doel, grondslag, bewaartermijn, het delen met derden, etc. En dat reeds bij de verkrijging van de gegevens. Op dit punt heeft de gemeente nog werk te verrichten.

Bijzondere aandacht zou de gemeente moeten schenken aan twee bijzondere vormen van verwerkingen:

- Verwerkingen waarbij gebruik wordt gemaakt van camera's of sensoren. Daarmee kan aan de burgers ook duidelijk gemaakt worden welke van die apparaten onder verantwoordelijkheid van de gemeente vallen. Een grafische weergave op een plattegrond ligt daarbij voor de hand omdat het de openbare ruimte betreft.
- Verwerkingen waarbij gebruik wordt gemaakt van algoritmes voor complexere rekenregels of analyse en onderzoek. Deze ontwikkeling vergt buitengewoon veel aandacht voor helderheid over wat informatiesystemen nu doen met gegevens van en over burgers. De Vereniging van Nederlandse Gemeenten (VNG) heeft daartoe een classificatiemodel ontwikkeld dat bruikbaar kan zijn bij de informatie die de gemeente zou kunnen verschaffen. Het gebruik van een algoritme is geen verwerking op zich maar gekoppeld aan een bestaande verwerking. Toch is het aan te bevelen dat er over algoritmes apart wordt gecommuniceerd om transparantie te verhogen.

6. Overige onderwerpen

- A. Er is een start gemaakt met de noodzakelijke herziening van het 'reglement e-mail en internetgebruik' voor medewerkers. Deze regeling is sterk verouderd en nodig aan herziening toe; de geldigheidstermijn is al enkele jaren overschreden. De nieuwe regeling gaat heten 'gebruik digitale hulpmiddelen' en zal door het SSC MO&C worden geformaliseerd.
- B. De FG adviseert desgevraagd de klachtenfunctionaris(sen) en de ombudsman binnen de gemeente wanneer burgers zich bij hen hebben gemeld met klachten waarbij privacy ook een steeds vaker genoemd aspect is. Veelal is er eerder sprake van klachten over de wijze van handelen van de gemeente dan een daadwerkelijke overtreding van de AVG. Ook zijn er burgers die direct contact opnemen met de FG met de vraag 'of de gemeente zich wel houdt aan de AVG'. Dat aantal is minder dan vijf per jaar.
- C. De gemeente heeft nog geen uitgangspunten vastgesteld voor het ontwikkelen of aanschaffen van informatiesystemen vanuit de optiek van privacy-by-design (art. 25 AVG). Dat is niet alleen een juridisch gemis, maar heeft in de praktijk een bijzondere uitwerking:
- Zo heeft de FG een negatief advies uitgebracht omtrent de invoering van de zogenaamde 'Voorzieningswijzer'. Een systeem waarmee een uitgebreid dossier van de burger wordt opgebouwd ten einde te bewerkstelligen dat van toepassing zijnde voorzieningen (al dan niet aangeboden door de gemeente) zouden kunnen worden geëffectueerd. Proportionaliteit en rechtmatigheid kunnen dan problematisch worden, en andere oplossingen zijn even zo goed denkbaar.
 - Vernieuwing Applicaties Sociaal Domein (VASD). Onder deze noemer is de gemeente een programma in 2019 gestart om de dienstverlening te verbeteren, informatie uit te kunnen wisselen en de hoeveelheid bestaande systemen (en daarmee gepaard gaande beheer inspanning) te verminderen. Dat is een complexe operatie met vele betrokkenen, waaronder de Stichting WIJ.
Na drie jaar is er op onderdelen van de verwerkingen van de persoonsgegevens nog onvoldoende zicht op deze verwerking en de betekenis daarvan voor de burger. Elementen daarbij zijn zeggenschap over met name generieke gegevens (zoals contactgegevens), maar ook rechtmatigheid van een integraal klantbeeld en zoets als functiescheiding; toewijzing van hulp moet gescheiden zijn van aanbieden van hulp. De aanpak is vooral gericht op procesinrichting en samenwerking. Dat is zeker een nobel streven, maar de aandacht voor 'gegevensbescherming door ontwerp' is in ieder geval niet zichtbaar geworden voor de FG. Belangrijke begrippen hierbij zijn dataminimalisatie, het kunnen uitoefenen van controle door betrokkene en transparantie over functies van de verwerkingen (doelstelling, grondslag en verantwoordelijke).
- D. In dat kader is het goed om aandacht te vragen voor de onderlinge relatie tussen de gemeente en de stichting WIJ als het gaat om het verwerken van persoonsgegevens. Deze relatie kent namelijk drie vormen:
- (i). de gemeente als verwerker. Door het leveren van ICT-infrastructuur aan WIJ verwerkt de gemeente in opdracht van WIJ gegevens van werknemers van WIJ;
 - (ii). de gemeente als eindverantwoordelijke van verwerkingen (vanuit WMO en Jeugdwet) en de WIJ in de rol van verwerker (bepaling welke zorg noodzakelijk is, zorg die door de gemeente wordt gefinancierd);
 - (iii). WIJ in de rol van zelfstandig verwerkingsverantwoordelijke voor het aanbieden van zorg (die dan weer wordt vergoed door de gemeente).

Deze drie vormen vergen afzonderlijk een goede beschrijving van de afspraken die over de privacy gemaakt moeten worden. Daarbij is het vooral voor de burger van belang te weten wie er verantwoordelijk is en hoe de avg-rechten kunnen worden uitgeoefend. Deze helderheid is nog niet aanwezig.

- E. Met betrekking tot de Arbeidsmarktregio en het RMC (Regionaal Meld- en Coördinatiepunt; leerlingenzaken) heeft de stad een centrale rol in de provincie of regio welke is afgedwongen door de landelijke overheid. Dat brengt met zich mee dat de FG van de gemeente betrokken kan worden bij activiteiten die deze samenwerkingen uitvoeren. Dat gebeurt niet consequent of structureel waardoor het compliance beeld van deze samenwerkingen onvolledig is. Dat geldt zeker wanneer de regio zelf ook weer samenwerkingsverbanden aangaat. Dit speelt ondermeer bij de aandacht die er moet zijn voor schoolgaande jeugd (tot de leeftijd van 27 jaar (..)). Dit brengt veel juridisch getint maatwerk met zich mee en zou gepaard moeten gaan met duidelijke informatievoorziening naar de betrokken burger.

Het is voor de FG niet duidelijk of zijn beeld van deze regionale organisaties volledig en juist is.

7. Aandachtspunten

Gelet op het algemene beeld van de compliance (blz. 5) en de bevindingen (blz. 6 t/m 10) is de FG van oordeel dat op een aantal gebieden verbeteringen wenselijk zijn. De punten zijn:

- VI. Publicatie van het verwerkingenregister als onderdeel van het informeren van de burgers;
- VII. Borgen dat de organisatie in staat is zelfstandig gegevenseffectbeoordelingen uit te voeren met daarbij een belangrijke uitvoerende rol voor Informatieadviseurs en projectleiders;
- VIII. Het vaststellen van beleidsregels voor privacy-by-design en privacy-by-default zodat er betere waarborgen zijn voor de privacy bij het ontwerp en invoering van informatiesystemen.
- IX. De relatie tussen de gemeente en de stichting WIJ vanuit het oogpunt van de privacy te herijken zodat duidelijk wordt welke afspraken gelden bij de verschillende rollen als het gaat over verwerkingsverantwoordelijkheid.
- X. Het opstellen van een privacyconvenant voor de Arbeidsmarktregio.