Voorbereiding op de AVG:
Waar staan we en wat moet er nog gebeuren

Een nieuwe privacywet
Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht, die de huidige Wet bescherming persoonsgegevens vervangt. Deze wet leidt niet zozeer tot een ander beschermingsregime maar eist wel met voorgeschreven instrumenten hoe organisaties zich moeten verantwoorden dat ze zich aan de regels houden. Voorheen werden bijvoorbeeld processen waarin persoonsgegevens werden verwerkt aangemeld bij de Autoriteit Persoonsgegevens (de nationale toezichthouder). Onder de AVG worden ze niet meer aangemeld maar moet je wel een register bijhouden waarin alle 'verwerkingen' worden beschreven. De verplichtingen bestaan deels uit zaken die volledig geregeld moeten zijn (het genoemde register moet er bijvoorbeeld zijn, er moet een functionaris voor de gegevensbescherming worden benoemd) en deels uit inspanningsverplichtingen (bijvoorbeeld het bewustzijn van de organisatie versterken, processen en systemen zo inrichten dat privacy maximaal is gewaarborgd). De Autoriteit Persoonsgegevens heeft onder de AVG meer middelen om te handhaven. Ze kan een onderzoek instellen en zonodig een boete opleggen tot maximaal 20 miljoen euro.

Wat zijn persoonsgegevens
Persoonsgegevens zijn alle gegevens die je kunt terugleiden tot een individu. Dat betekent dat élk gegeven waarmee je iemand uit een grotere groep kunt aanwijzen een persoonsgegeven is. Het eerste waar je aan denkt is een naam van iemand, maar ook de combinatie van bijvoorbeeld een geboortedatum en een straatnaam kan betekenen dat je één iemand uit een grotere groep kunt identificeren. Voorbeelden van persoonsgegevens die we binnen de gemeente veel verwerken zijn: namen, adressen, geboortedata, inkomensgegevens, kentekens, gegevens over hulpbehoefte etc.

Er is binnen al die verschillende persoonsgegevens een gradatie in gevoeligheid. Naam, adres, telefoonnummer e.d. zijn 'gewone' persoonsgegevens. Daarnaast zijn er de zogeheten bijzondere persoonsgegevens (gegevens over bijvoorbeeld ras, politieke of religieuze overtuiging, sexuele geaardheid, gezondheid en biometrische gegevens) en gevoelige (financiële) of strafrechtelijke gegevens. Die worden sterker beschermd. Tot slot is er het burgerservicenummer, dat is het allergevoeligst en sterkst beschermd.

Voorbereiding: 10-stappenplan
De Autoriteit Persoonsgegevens heeft een 10-stappenplan gemaakt als hulpmiddel bij de voorbereiding op de AVG. In deze notitie worden aan de hand daarvan de verplichtingen uit de AVG beschreven en wat er nog moet gebeuren om daaraan te kunnen voldoen. In het kader van de verplichtingen van de AVG zal de gemeente intern en extern gegevensbeschermingsbeleid moeten opstellen. De hieronder genoemde 10 stappen vormen daarvan een belangrijk onderdeel.

1. Bewustwording
De gemeente werkt heel veel met persoonsgegevens in allerlei verschillende processen. Denk bijvoorbeeld aan de gegevens ten behoeve van het verstrekken van uitkeringen, de uitvoering van de Jeugdwet, de Basisregistratie Personen, gegevens voor omgevingsvergunningen of gegevens die worden gebruikt bij handhaving. Dat betekent dat de hele organisatie zorgvuldig met die gegevens moet omgaan en zich ervan bewust moet zijn wanneer privacyregels in het geding zijn. Op dit moment verschilt het per afdeling en soms per medewerker hoe sterk dat bewustzijn is. Dat het groeit, blijkt uit de hoeveelheid adviesvragen die worden gesteld. Die neemt hard toe. Er zijn op presentaties gehouden bij sommige vakafdelingen en er is een workshop geweest tijdens de zomerschool. Dit jaar zullen algemene privacycursussen worden aangeboden en voor sommige vakgebieden nog een verdiepende cursus. Het management en bestuurders zullen ook beter moeten worden geïnformeerd. Naast de privacynota die vorig jaar door de raad is vastgesteld, zal bovendien een duidelijker werkinstructie worden gemaakt.

Het doen van DPIA's (zie onder 4) zal ook bijdragen aan een sterker privacybewustzijn van de organisatie.

2. Rechten van betrokkenen
Net zoals nu onder de Wbp kunnen betrokkenen verzoeken om te vragen welke gegevens de gemeente van hen verwerkt, met welk doel, hoe lang de gegevens worden bewaard en aan ze worden verstrekt. Als dat aan de orde is, heeft hij ook recht op rectificatie of aanvulling. Op dit moment komen dit soort verzoeken maar heel zelden binnen en er is geen vaste procedure voor afhandeling. De verwachting is dat het aantal verzoeken zal toenemen, daarom is het verstandig hiervoor een vast proces te hebben. Een actueel register van verwerkingen (overzicht van alle verwerkingen van persoonsgegevens, zie hieronder) is daarvoor onontbeerlijk.

Wat hierbij relevant is, is dat er partijen zijn die misbruik lijken te maken van dit recht, met als enig doel het innen van dwangsommen. Nu dat in het kader van de Wob niet meer kan, lijkt deze praktijk te verschuiven naar Wbp/AVG. In een enkel geval is misbruik erkend door de rechter. Hierover zal de jurisprudentie zich nog moeten vormen.

Onder de AVG heeft de betrokkene nog meer rechten: recht op beperking van de verwerking, recht op vergetelheid en recht op dataportabiliteit (de gegevens in een handzaam formaat overdragen). Deze zijn voor overheden echter minder relevant, al zal het een enkele keer aan de orde kunnen zijn.

3. Register van verwerkingen
In het hiervoor al genoemde register wordt per proces vermeld welke categorie van persoonsgegevens wordt verwerkt, van welke categorie betrokkenen, voor welk doeleinde, wat de bron is van de gegevens, aan wie eventueel gegevens worden verstrekt, of er een verwerkersovereenkomst is gesloten (als een andere partij voor de gemeente de gegevens verwerkt), zo mogelijk de bewaartermijn en een beschrijving van de beveiliging.

Het register wordt op dit moment aangelegd en is deels gevuld, steeds in overleg met de betrokken vakafdeling. Het vraagt nog een flinke inspanning om het compleet te maken vóór 25 mei a.s. Het register is nu nog een overzicht in excell maar zal worden opgenomen in een ander, zelf ontwikkeld, register genaamd IPA. Hierin wordt van alle informatie die Haarlem verwerkt (ook zonder persoonsgegevens) beschreven in welk proces dat gebeurt en met welke applicatie.

Het register is de basis voor de privacygovernance want het biedt een overzicht van alle verwerkingen van persoonsgegevens. Als het register compleet is, is de volgende stap van alle verwerkingen na te gaan of ze ook zijn toegestaan volgens de wet. Ook moet een proces worden ingericht om het register actueel te houden.

Met het register wordt op verzoek aan de Autoriteit Persoonsgegevens worden verstrekt, die onder andere aan de hand hiervan kan beoordelen of de regels op het gebied van privacy worden nageleefd.

4. Data Protection Impact Assessments
De AVG eist ook dat zogeheten Data Protection Impact Assessments (DPIA)worden gedaan: inventarisatie van privacyrisico's en de benodigde maatregelen. Aan de hand van het register van verwerkingen zal moeten worden beoordeeld waar de grootste privacyrisico's zich kunnen voordoen. Daar zal het eerst een DPIA worden gedaan. Haarlem heeft enige maar niet veel ervaring met het doen van DPIA's. Het is wel een methode die de organisatie goed in de vingers zal moeten krijgen. Het zou daarom goed zijn dit een paar keer te doen onder leiding van een deskundige die hierin ervaren is.

NB een DPIA kan ertoe leiden dat eerder niet voorziene maatregelen moeten worden genomen. Bijvoorbeeld doordat bepaalde persoonsgegevens niet (meer) mogen worden verwerkt of doordat extra beveiligingsmaatregelen nodig zijn.

5. Privacy bij Design & Privacy by Default
Privacy by Design houdt in dat bij het ontwerpen van een nieuw proces meteen wordt geregeld dat dit privacyproof is. Privacy by Default houdt in dat technische en organisatorische maatregelen worden genomen om te zorgen dat standaard alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor het beoogde (en duidelijk bepaalde) doel.

Dit punt houdt verband met de DPIA's. Het gaat in feite om een vergelijkbare toetsing of risicoanalyse en bijbehorende maatregelen, zij het op een eerder moment. Het is belangrijk dat degenen die een nieuw werkproces inrichten of die bijvoorbeeld een aanbesteding begeleiden voor een nieuw systeem van meet af aan rekening houden met privacyeisen.

6. Functionaris voor de gegevensbescherming
Alle overheden moeten een functionaris voor de gegevensbescherming aanwijzen. De FG adviseert en informeert de organisatie en ziet toe op naleving van de regels en is contactpersoon voor de Autoriteit Persoonsgegevens. Over de FG wordt een aparte notitie gemaakt.

7. Meldplicht datalekken
Net als onder de huidige wet moeten ernstige datalekken worden gemeld aan de AP. Wat daarbij komt is de plicht alle datalekken te documenteren, zodat de AP kan controleren of de afweging al dan niet te melden juist is gemaakt.
Voor deze meldingen is een Meldpunt Datalekken ingericht, dat ook nu alle meldingen registreert. Het is goed dit nogmaals onder de aandacht te brengen in de organisatie, als onderdeel van de bewustwordingsactiviteiten. Ook zal het meldpunt jaarlijks een verslag maken van de datalekken die zich hebben voorgedaan.

8. Verwerkersovereenkomsten
Het komt heel geregeld voor dat de gemeente verwerkingen van gegevens door een andere partij laat verzorgen. Bijvoorbeeld doordat een systeem feitelijk wordt beheerd door een externe partij, zoals gebeurt bij verwerkingen in het hrm-systeem en handhavingssystemen. Met deze externe partijen moet dan een verwerkersovereenkomst worden gesloten.

Haarlem gebruikt een goede, op de APV toegesneden, modelovereenkomst. Uit het register van verwerkingen zal blijken of er meer overeenkomsten nodig zijn. Ook sluiten wij zogenaamde Overeenkomsten van gedeelde verantwoordelijkheid, als beide partijen verantwoordelijk zijn voor de verwerking. In die gevallen is het toch goed om afspraken te maken over welke gegevens met welke doelen worden verwerkt en over beveiligingsmaatregelen.

9. Leidende toezichthouder
Deze stap is alleen relevant voor organisatie met vestigingen in meerdere EU-lidstaten.

10. Toestemming
Voor sommige verwerkingen is toestemming van de betrokkene nodig. Voor overheden is dit echter zelden het geval. Toestemming kan alleen als grondslag (wettelijk toegestane reden) voor verwerking gelden als de betrokkene dat in volledige vrijheid doet. In de relatie tussen een burger en een overheid is dat zelden het geval. Doorgaans zal de grondslag liggen in een wettelijke taak die de gemeente moet uitvoeren.

In die gevallen dat wel op grond van toestemming wordt gewerkt, is het zaak de betrokkene duidelijk te informeren om welke gegevens het gaat en voor welk doel die worden gebruik. De toestemming moet op schrift worden gesteld, om te kunnen aantonen dat de verwerking van de gegevens legitiem is. Toestemming kan overigens altijd weer worden ingetrokken. De verwerking moet dan direct stoppen.

Autorisaties
Een punt dat niet als zodanig wordt genoemd in de tien stappen van de AP is de manier waarop beoordeeld en bepaald wordt wie toegang krijgt tot bepaalde persoonsgegevens. Als dat consequent en goed gebeurt, vermindert dat de risico's op schending van privacy en op datalekken. Op basis van het register van verwerkingen kan worden bepaald wie mag autoriseren. Degenen die dat doen, zullen bewust moeten worden gemaakt van het belang daarvan, hoe te beoordelen

wie autorisatie moet hebben en dat een autorisatie gekoppeld is aan werkzaamheden in plaats van aan personen.

Hoeveel capaciteit is er op dit moment in de organisatie en wat is er nodig?
Op dit moment is er voor de hele organisatie één tactisch privacyadviseur beschikbaar en één strategisch privacyadviseur. Daarnaast is er bij de afdeling Veiligheid een medewerker die geregeld adviesvragen beantwoordt en bij de afdeling interne dienstverlening een medewerker die veel adviesvragen beantwoordt uit m.n. het sociaal domein maar zij moeten dit naast hun andere werkzaamheden doen. Mede door de nieuwe wetgeving groeit binnen en buiten de organisatie de aandacht voor privacy en nemen ook de risico's toe. In de eerste plaats risico's voor degenen om wier gegevens het gaat als die in verkeerde handen zouden komen. Daarnaast ook voor de gemeente zelf: financiële risico's als de Autoriteit Persoonsgegevens boetes of dwangsommen zou opleggen of door schadeclaims. Daarnaast is negatieve publiciteit een risico als zou blijken dat de gemeente in gebreke is gebleven om gegevens goed te beschermen. Om de voorbereiding als hiervoor beschreven goed uit te voeren is op korte termijn meer capaciteit nodig.

Zoals hiervoor gezegd zijn er binnen de organisatie veel vragen om uitleg en advies en moet het register van verwerkingen verder worden gevuld. Dat vraagt een inspanning. Daarnaast moeten op risicovolle nieuwe processen DPIA's worden gedaan. Dit jaar zullen er zeker vier of vijf moeten worden gedaan. Dat vraagt veel tijd en is iets waar Haarlem nog niet heel ervaren in is. Het zou daarom goed zijn dit een paar keer te doen onder leiding van een deskundige die hierin ervaren is. Uit de DPIA's komen risico's naar boven waarop maatregelen zullen moeten worden genomen. Soms organisatorisch, soms technisch. Ook daarvoor is extra inzet nodig.

Voorstel is om nu extra budget vrij te maken om de nodige activiteiten op korte termijn te versnellen in dit cruciale jaar. In de nieuwe bestuursperiode wordt bezien wat structureel nodig is.