JAARVERSLAG 2012

van de functionaris voor de bescherming van persoonsgegevens van de gemeente

BERGAMBACHT

Index:

.

1. Inleiding.

Het College bescherming persoonsgegevens (CBP) houdt toezicht op de naleving van de wettelijke regels toezien op de bescherming van persoonsgegevens, zo nodig met behulp van sancties. Zonder adequate bescherming en beveiliging van deze gegevens kan het fundamentele recht op bescherming van een ieders persoonlijke levenssfeer niet ten volle worden uitgeoefend.

Door de toenemende digitalisering en globalisering wordt het woud van gegevensverwerking steeds ondoorzichtiger. Het is voor burgers niet meer mogelijk inzicht te hebben in al deze verwerkingen, laat staan daarvan het overzicht te behouden.

Het CBP benadrukt daarom dat bedrijven en overheden nu aan zet zijn. Zij moeten kunnen aantonen dat zij de persoonsgegevens van hun klanten en van de burgers zorgvuldig en volgens de regel van de wet verzamelen en gebruiken.

Als antwoord op deze stelling heeft het College van burgemeester en wethouder van de gemeente Bergambacht destijds besloten om een Functionaris voor de gegevensbescherming (FG) als onafhankelijk toezichthouder te benoemen.

Op deze wijze neemt het College haar verantwoordelijkheid om op een open en transparante wijze, de persoonsgegevens op een juiste wijze te beheren en te verwerken in de betreffende persoonsregistraties.

Het CBP is ervan overtuigd dat deze zelfregulering een effectieve bijdrage zal leveren aan het realiseren van het grondrecht op bescherming van de persoonlijke levenssfeer.

De functionaris voor de gegevensbescherming (FG) moet op grond van artikel 63 lid 5 van de Wet bescherming persoonsgegevens (Wbp) jaarlijks een verslag maken van zijn werkzaamheden en bevindingen.

De werkzaamheden en de bevindingen betreffen de hele gemeentelijke organisatie. Het toezicht op de privacybescherming raakt alle afdelingen.

Deze breedte van het werkveld dwingt de FG tot selectiviteit bij de inzet van de beperkte middelen. De Wbp legt de verantwoordelijkheid voor de privacybescherming bij de verantwoordelijke, de burgemeester of het College van burgemeester en wethouders welke de houder is van de betreffende persoonsregistratie. In de gemeente Bergambacht ligt de verantwoordelijkheid bij de afdelingshoofden van de volgende afdelingen:

- Samenleving;
- Bedrijfsvoering;
- Ruimtelijke Ordening en Beheer.

Ik heb kunnen vaststellen dat ook in 2012 op vele plaatsen binnen de gemeentelijke organisatie met positieve inspanning gehoor is gegeven aan de uitvoering van de Wbp. De leidinggevende van de afdelingen hebben een belangrijke bijdrage geleverd aan de Wbp binnen de gemeentelijke organisatie.

Bij de afdelingen: Samenleving, Bedrijfsvoering en Ruimtelijke Ordening en Beheer moeten nog plannen worden ontwikkeld om te komen tot een Informatiebeveiligingsbeleid en –plan. In het kader van de drie jaarlijkse audit Gemeentelijke basisadministratie persoonsgegevens (GBA) heeft alleen de afdeling Samenleving, burgerzaken dit beleid vorm gegeven. In het RSO is hiervoor aandacht gevraagd om dit onderwerpen in K5 verband te gaan realiseren. Hiervoor is een voorstel gemaakt om binnen de K5 organisatie dit voor de overige gemeentelijke onderdelen te regelen.

Er zijn inmiddels bij diverse bedrijven offertes aangevraagd. Hier uit zal een keuze worden gemaakt door de afdeling ICT K5 namens de K5 gemeenten. Daarna zal er een start worden gemaakt om het Informatiebeveiligingsbeleid en –plan te implementeren in de K5 gemeenten.

2. Bescherming van persoonsgegevens.

Op 1 september 2001 is de Wet bescherming persoonsgegevens (Wbp) in werking getreden. Deze wet geeft regels ter bescherming van de privacy van de burger. De Wbp geeft de burger het recht om te weten wat er met zijn persoonsgegevens gebeurt. Hij kan zijn gegevens inzien en wijzigen en in sommige gevallen bezwaar maken tegen het gebruik van zijn gegevens.

De persoonsgegevens staan, zelfs zonder dat we er van bewust zijn, bij diverse instellingen geregistreerd, zoals verzekeringsmaatschappijen, de bibliotheek, de supermarkten en nog vele honderden andere instellingen.

Ook in de gemeente Bergambacht worden persoonsgegevens geregistreerd, zoals historische- en actuele adressen, geboortegegevens, oudergegevens, huwelijksgegevens, gegevens van kinderen et cetera. Ook in andere bestanden komen persoonsgegevens voor, bijvoorbeeld in het register van bouwvergunningen of in de postregistratie. Met deze gegevens moet de leidinggevende zorgvuldig omgaan. De persoonsgegevens mogen alleen worden gebruikt voor het doel waarvoor ze zijn vastgelegd en worden alleen verstrekt aan derden indien dit voor het doel van de verwerking noodzakelijk is (bijvoorbeeld bij een wettelijke verplichting) of met toestemming van betrokkene.

Steeds meer worden deze persoonsgegevens gekoppeld aan diverse gegevensbestanden. Met de komst van deze koppelingen (Key2Data) c.q. distributie van data-informatie is het noodzakelijk dat het beheer en de zorg hiervoor door een gegevensbeheerder wordt bewaakt. De Wbp geeft ook de verwerker van de persoonsgegevens meer plichten. Zo mogen de gegevens alleen nog worden verwerkt als hier een goede reden voor is, of als de burger zelf hiervoor toestemming heeft gegeven.

Er mogen geen nieuwe persoonsregistraties worden aangelegd, voordat deze is aangemeld en getoetst door de functionaris voor de gegevensbescherming (FG). Bovendien moet een nieuwe persoonsregistratie in de huis-aan-huisbladen worden gepubliceerd voordat men de registratie in gebruik kan nemen. De Wbp schrijft voor dat alle verwerkingen waarin persoonsgegevens staan vermeld, met uitzondering van de in de Wet vrijgestelde verwerkingen, aangemeld dienen te worden bij het College Bescherming Persoonsgegevens (Cbp) of in ons geval bij de FG. In de gemeente Bergambacht heeft het college destijds gekozen voor volledige registratie, waarbij de transparantie van de uitvoering van de Wbp zichtbaar wordt gemaakt voor alle partijen.

Alle verwerkingen, zo ver bekend, van de gemeente Bergambacht waarin persoonsgegevens staan vermeld zijn in een apart register opgenomen, namelijk het register Wbp, welke wordt beheerd door de FG. Het register ligt ter inzage bij de afdeling Samenleving, burgerzaken. In dit register is vermeld:

- naam van de registratie en nummer;
- doel van de registratie;
- de wijze van opslag, handmatig en/of geautomatiseerd;
- de verantwoordelijke afdeling;
- de wijze van beveiliging;
- of de gegevens met een derde worden gedeeld.

Meer informatie over de Wbp kunt u vinden op de website van het College Bescherming Persoonsgegevens (www.cbpweb.nl).

3. Toezicht en beheer.

Toezicht en beheer kunnen worden geborgd door middel van een jaarlijkse zelf evaluatie aan de hand van een vragenformulier. Een zelf evaluatie heeft als hoofddoel de kwaliteit van de registratie en het gebruik van persoonsgegevens te bevorderen. Daarnaast wordt het bewustzijn en het inzicht in de relevante normen bij de registratie en het gebruik van persoonsgegevens bevorderd. De invoering van de Basisregistratie Adressen en Gebouwen (BAG) is hiervan een goed voorbeeld. Op 1 juli 2011 is deze registratie bij de gemeente ingevoerd. Ook hierbij is het uitgangspunt: eenmalig vastlegging en meervoudig gebruik van persoonsgegevens.

Het vragenformulier voor zelfevaluatie.

Kenmerken van de gemeentelijke organisatie	Niet van toepassing	Een beetje van toepassing	Van toepassing
Activiteiten van de organisatie 1. Kernactiviteiten van de organisatie is gericht op het registratie en gebruik van persoonsgegevens			rood
2. De gemeente registreert en gebruikt persoonsgegevens voor derden			rood
3. Er is een hoger dan gemiddeld afbreukrisico of maatschappelijke gevoeligheid gelet op de activiteiten, producten of doelgroep van de organisatie of de regelgeving die van toepassing is			rood
Wijze van verkrijging van de gegevens 4. Gegeven worden geregistreerd en gebruik op grond van eigen waarneming zonder dat betrokkene daarvan op de hoogte is	groen		
5. Gegevens worden geregistreerd omdat betrokkene daartoe verplicht is			rood
Hoeveelheid gegevens 6. Registratie van meer dan 50.000 identificeerbare personen, waaronder worden verstaan zowel personeels- als klantgegevens	groen		
Aard van de gegevens 7. Registratie en gebruik van gevoelige gegevens, zoals gegevens over kinderen, financiële gegevens of zuivere privé gegevens. Gegevens worden gebruikt ter beoordeling van personen			rood

8. Meerdere soorten bijzondere gegevens, waaronder godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod		oranje	
Complexiteit van gebruik en registratie van gegevens 9. Er is bijzondere wetgeving van toepassing op de registratie en het gebruik van persoonsgegevens, die van de gewone privacywet afwijkt			rood
10. Er worden voor veel verschillende doeleinde gegevens geregistreerd en gebruik of er zijn veel verschillende bestanden in de Organisatie aanwezig, veel beheerders of gebruikers, of er vinden veel Uitwisselingen plaats			rood
Verstrekking aan derden 11. Aan meer dan 10 instanties worden gegevens verstrekt			rood
12. Er worden (structureel) gegevens verstrekt aan landen buiten de EU	groen		
Gerezen vragen over gegevensgebruik 13. In uw organisatie rijzen naar uw indruk meer dan gemiddeld vragen over wat er wel of niet mag met persoonsgegevens	groen		
14. Er is behoefte aan 1 aanspreekpunt voor vragen of advies over de registratie en het gebruik van gegevens	groen		
Grootte van de organisatie 15. Veel meer dan 2500 personeelsleden	groen		
Organisatiestructuur 16. Er is sprake van een complexe organisatiestructuur. Bijvoorbeeld een internationaal concern, er zijn meerdere uitvoeringsorganisatie of er is anderszins een complexe verantwoordelijkheidsverdeling	groen		
Ambitie 17. Het is van wezenlijk belang dat de gemeentelijke organisatie zich kan onderscheiden op het gebied van kwaliteit en zorgvuldigheid, in het bijzonder wat betreft de registratie en het gebruik van persoonsgegevens			rood

Groen = geen risico en 0 punten.

Oranje	= middelhoog risico en 1 punt.
Rood	= hoog risico en 2 punten.

Door het optellen van het aantal punten en het aantal rode vakjes die er zijn aangekruist in de vragenlijst, blijkt dat het privacyprofiel van de gemeentelijke organisatie bepaalt dat de privacy een onmiskenbare risicofactor is binnen de gemeentelijke organisatie. En dat het aanstellen van een functionaris voor de gegevensbescherming (FG) een goede beslissing is geweest. Dat bepaalt immers dat de gemeente Bergambacht vertrouwen heeft in haar organisatie en de kwaliteit van haar dienstverlening.

Algemene normen.
De Wet bescherming persoonsgegevens bevat algemene normen voor het gebruik van persoonsgegevens die door iedere afdeling zelf moeten worden uitgewerkt. De belangrijkste algemene normen zijn de volgende:

- ✓ Doelbinding
- ✓ Rechtmatige grondslag
- ✓ Kwaliteit
- ✓ Transparantie of openheid
- ✓ Rechten en plichten
- ✓ Buitenlands gegevensverkeer

De Wet gaat uit van zelfregulering. De gemeente gaat zelf aan de slag met de uitvoering van de Wet bescherming persoonsgegevens en dat is geen geringe opgave. Het onzorgvuldig omgaan met of onjuist gebruik van persoonsgegevens door de gemeentelijke organisatie kan, in de vorm van imagoschade door het verlies van vertrouwen in de gemeentelijke organisatie en daarmee het vertrouwen van haar burgers kosten. Ook kan het College Bescherming Persoonsgegevens een boete opleggen.

Het is van belang dat de privacywet in de gemeentelijke organisatie goed is geïmplementeerd. Dit betekent concreet dat de gemeente in ieder geval de wettelijke verplichtingen nakomt en maatregelen treft om de rechten van haar burgers te kunnen effectueren. Een evenwichtig privacybeleid, dat ook wordt onderhouden, is noodzakelijk. Zonder draagvlak bij de leidinggevenden van de gemeente zal een privacybeleid niet veel voorstellen. Daarom wordt er ook jaarlijks een quick scan gehouden om te kunnen beoordeling of een registratie van persoonsgegevens wel rechtmatig is. Verder geeft de jaarlijkse rapportage een indruk over de jaarlijks activiteiten op privacygebied.

4. Functionaris voor de gegevensbescherming.

Daar waar een interne toezichthouder, de Functionaris voor de Gegevensbescherming (FG) is benoemd en daardoor de naleving van de bescherming van persoonsgegeven waarborgt, kan het College (College bescherming persoonsgegevens, of ook wel het Cbp genoemd) zich terughoudend opstellen.

De functionaris voor de gegevensbescherming (FG) neemt dan de taken van het College over en is de interne toezichthouder. Wat zijn de taken van een deze functionaris?

De wijze waarop de FG in de praktijk invulling geeft aan zijn toezichthoudende taak op basis van zijn bevoegdheden, hangt sterk af van de aard van de organisatie en de persoonsgegevens die worden verwerkt. Voor de FG zijn een aantal taken wettelijke verplicht en andere taken zijn optioneel.

Het uitoefenen van toezicht door de FG brengt met zich mee, dat de verwerkingsprocessen binnen de gemeentelijke organisatie worden geïnventariseerd. Dit in verband met het oog op

het nakomen van de meldingsverplichtingen van persoonsregistraties. Van de meldingen legt de FG een bestand aan. Klachten die betrekking hebben op het gebruik van persoonsgegevens kunnen door hem worden behandeld.

Jaarlijks dient hij verslag te doen aan het College van zijn werkzaamheden en bevindingen. Binnen de gemeentelijke organisatie waarin hij werkzaam is, functioneert hij als vraagbaak, voor de collega's, de leidinggevende en het College van burgemeester en wethouders kan hij adviseren op het gebied van de toepassing van de Wet bescherming persoonsgegevens (Wbp) of het helpen bij het opstellen van een gedragscode voor het gebruik van persoonsgegevens binnen de gemeentelijke organisatie.

Verder kan hij ook adviseren over het passende niveau van beveiliging van de informatiehuishouding van de gemeentelijke organisatie en over maatregelen die gericht zijn op het beperken van de verwerkingen van persoonsgegevens.

Voor een goede taakuitoefening dient het college de FG controlebevoegdheid toe te kennen. Deze dienen bij voorkeur in een interne regeling vastgelegd te worden en omvatten:

- de bevoegdheid om ruimtes te betreden;
- de bevoegdheid om inlichtingen en inzage te vragen en;
- om zaken te onderzoeken.

Het College dient er voor zorg te dragen dat de FG voldoende faciliteiten heeft om zijn bevoegdheden goed te kunnen uitoefenen. Een duidelijke positionering van de FG ten opzichte van de leiding van de gemeentelijke organisatie die hem heeft aangesteld, is essentieel.

Deze controlebevoegdheden moeten, volgens de wetgever, overeenkomen met die welke gelden voor het toezicht binnen de overheid. Vergelijk in dit opzicht de bevoegdheden die zijn opgenomen in afdeling 5.2 van de Algemene wet bestuursrecht. Het is de bedoeling van de wetgever geweest om de FG voldoende instrumenten in handen te geven voor het uitoefenen van geloofwaardig en effectief toezicht.

TAKEN.

Toezicht.
Om zowel de belangen van het College als van de betrokkenen, d.w.z. de personen van wie informatie wordt verwerkt, doeltreffend te behartigen kan een FG als intern toezichthouder worden beschouwd. De wijze waarop de FG in de praktijk invulling geeft aan zijn toezichthoudende taak op basis van zijn bevoegdheden, hangt sterk af van de aard van de organisatie en de gegevens die worden verwerkt. In het algemeen zal de FG stelselmatig onderzoek verrichten naar de wijze waarop persoonsgegevens worden verwerkt en beveiligd. Zo nodig kan hij zich hierbij laten ondersteunen door (externe) specialisten. Het goed uitoefenen van toezicht omvat echter meer dan controleren en corrigeren.

Inventarisatie.
Zicht hebben op de verwerking van persoonsgegevens is een belangrijke voorwaarde voor het uitoefenen van effectief toezicht. De FG verkrijgt dit via een inventarisatie van de verwerkingsprocessen binnen de – diverse onderdelen van de – gemeentelijke organisatie. Zo kan de FG onder meer de gegevensstromen in kaart brengen en aangeven of er sprake is van een meldingsverplichting van gegevensverwerking. Deze meldingsverplichting rust overigens bij het college van burgemeester en wethouders en niet bij de FG. Het ligt echter voor de hand dat de FG daarbij een ondersteunde rol vervult. De jaarlijkse scan op de gegevensbestanden van de gemeente speelt hierbij een ondersteunende rol.

Klachtenbehandeling.
De behandeling van klachten over het gebruik van persoonsgegevens maakt deel uit van het takenpakket van de FG. Om klachten van betrokkenen doeltreffend te kunnen afhandelen, is het zaak dat de FG duidelijk herkenbaar en bereikbaar is.

Verslaggeving.
De FG heeft de wettelijke taak een verslag op te stellen van zijn werkzaamheden en bevindingen. Gelet op de positie van de FG brengt hij in de eerste plaats verslag uit aan het college van burgemeester en wethouders. Vervolgens wordt het verslag in een bredere kring bekendgemaakt.

Voorlichting.
Binnen de gemeentelijke organisatie is de FG een vraagbaak voor de medewerkers. Ook is hij betrokken bij de voorlichting over de omgang met persoonsgegevens. Eventuele actuele ontwikkelingen binnen de gemeentelijke organisatie met betrekking tot het gebruik van persoonsgegevens kunnen aanleiding vormen voor extra voorlichting door de FG.

Normontwikkeling.
Effectief toezicht houden, kan het ontwikkelen van normen met zich meebrengen. Binnen de gemeentelijke organisatie kan er ook behoefte ontstaan aan één of meer interne regelingen die zijn toegesneden op de specifieke verwerking binnen de gemeentelijke organisatie, bijvoorbeeld het gebruik van CORSA.

Technologie en beveiliging.
Artikel 13 van de Wbp verplicht het college van burgemeester en wethouders om passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

De beveiligingsmaatregelen moeten er ook op gericht zijn onnodige verzamelingen en verder verwerkingen van persoonsgegevens te voorkomen.

5. Maatschappelijke ontwikkelingen.

De volgende onderwerpen komen aan bod:
- Identiteitsfraude;
- Identiteitsfraude tegengaan in de praktijk;
- Cyberpesten met identiteitsfraude;
- Modernisering van de bevolkingsadministratie.

Identiteitsfraude:
Identiteitsfraude is het gebruik van persoonlijke informatie om met andermans naam toegang te krijgen tot vooral computersystemen, vormen van elektronische dienstverlening en betaal- en creditcardrekeningen. De identiteitsfraude kan langs tal van wegen plaatsvinden, namelijk:
- Bij inbraak in woning of auto;
- Het stelen van post uit brievenbussen of het onderscheppen van post;
- Via het kopiëren van kaartgegevens bij kaartgebruik in winkel of geldautomaat. Het kopiëren van kaartgegevens heet ”Skimmen”. Deze identiteitsfraude gebeurt met gebruikmaking van de pinpas of de creditcard. Met de gekopieerde pinpas kunnen kwaadwillende betalingen doen uit naam van de houder van de pin pas of creditcard. Veel pin automaten zijn inmiddels aangepast, zodat het kopiëren van de magneetstrip van de pinpas niet meer mogelijk is;

- Via het kopiëren van bestanden met persoonsgegevens van klanten (door medewerkers van bedrijven);
- Via het hacken van computersystemen;
- Via informatie in afval- en prullenbakken (dumpsterdiving genaamd);
- Door met een valse identiteit persoonlijke informatie op te vragen via het internet (phishing genaamd). Met phishing proberen kwaadwillende je naar een "verkeerde"website te sturen zonder dat je het merkt. Om vervolgens je gebruiksnaam en wachtwoord van de echte website te ontfutselen;
- Social engineering, dit is door middel van telefoon (of andere manier) proberen te achterhalen wat de gebruikersnaam en wachtwoord zijn van een persoon. Om met de verworven gebruikersnaam en wachtwoord een systeem binnen te komen;
- Het zoeken in registers, bijvoorbeeld Google. Als je goed zoekt kan je door middel van Google achter informatie komen betreffende een persoon. Bij sollicitatiegesprekken wordt er vaak gezocht op naam van de kandidaten om te kijken of er iets bekend is van deze persoon op het internet.

In het Maatschappelijk Overleg Betalingsverkeer (MOB) is identiteitsfraude een belangrijk aandachtspunt. Onderzoek in Amerika heeft uitgewezen dat de schade in 2005 55,7 miljard dollar bedroeg en in 2006 47,3 miljard dollar. Deze bedragen geven aan dat er veel geld in de identiteitsfraudewereld in omloop is. Hoeveel geld er in Nederland omgaat door identiteitsfraude is niet bekend.

Identiteitsfraude tegengaan in de praktijk:
De medewerkers in de front-Office zijn de eerste lijn medewerkers, die met deze problematiek te maken krijgen. Het is zaak om deze fraude in een vroeg stadium te ontdekken. Daarom moeten de medewerkers goed getraind zijn om deze pogingen te herkennen. Door biometrie toe te passen in reisdocumenten wordt het moeilijker om de identiteit van een ander te stelen. Veel moeilijker is het om een iris te kopiëren of een vingerafdruk, maar men wordt steeds vindingrijker op dit gebied. Nu het niet meer mogelijk is om blanco waardedocumenten te stelen bij de gemeenten, proberen de fraudeurs andere middelen toe te passen om de identiteit van een ander te stelen. Het is verstandig om de medewerkers te trainen en te wijzen op de gevaren van identiteitsfraude. In de gemeente Bergambacht volgen de medewerkers van de afdeling Samenleving, burgerzaken jaarlijks trainingen en cursussen op dit terrein.

Er bestaat in Nederland geen algemene "Wet op de privacy" Er zijn diverse wetten, die elke een bepaald aspect van de privacy in Nederland regelen. De belangrijkste en bekendste Wet is de Wet bescherming persoonsgegevens (Wbp).

De minister van Binnenlandse Zaken en Koninkrijksrelaties heeft naar aanleiding van de vragen over de opslag van vingerafdrukken in reisdocumenten de Paspoortwet en de paspoortregeling Nederland 2001 aangepast. De huidige software is in de loop van 2011 aangepast, zodat de vingerafdrukken alleen nog maar in de chip van het reisdocument wordt opgenomen. Bij de gemeenten worden geen vingerafdrukken opgeslagen in de database van het Reisdocumenten Aanvragen en Archief Station (RAAS). Op dit moment wordt onderzocht of de status van de huidige Nederlandse identiteitskaart moet veranderen. Wellicht dat in de toekomst alleen nog maar in het paspoort de vingerafdrukken worden opgenomen.

De vingerafdrukken worden niet aan de grens niet gecontroleerd. Ook is geen automatische controle bij het gemeenteloket. Nederland wilde de vingerafdrukken aanvankelijk centraal opslaan om te voorkomen dat mensen meerdere paspoorten op verschillende namen aanvroegen. Of ook wel de "look-a-like" fraude genoemd. Vanwege problemen met de privacy en beveiliging van de data werd daarvan afgezien. Er wordt geadviseerd om een proef te doen, waarbij de vingerafdrukken standaard worden geverifieerde bij de uitgifte van

reisdocumenten. Tevens moet men rekening houden met de technische en maatschappelijke ontwikkelingen.

Oplichterij met identiteitsfraude:
Op internet worden vaak mensen opgelicht door middel van identiteitsfraude. Zo worden er bijvoorbeeld regelmatig op “Marktplaats.nl” advertenties geplaatst op naam van iemand anders. Vaak betalen de kopers de spullen vooraf, waarna ze tot de conclusie komen dat de beloofde spullen niet zijn opgestuurd.

De modernisering van de bevolkingsadministratie (m-GBA):
De huidige Wet gemeentelijke basisadministratie persoonsgegevens (GBA) zal in de komende periode tot 2016 worden vervangen door de Basis Registratie Personen (BRP). Hierdoor wordt het mogelijk de persoonsgegevens online te kunnen raadplegen door gemeenten en afnemers. Via 14 verschillende modules worden de wijzigingen in de persoonsgegevens direct in een landelijke voorziening, die door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties zal worden beheerd, verwerkt.

6. Doelen in 2012.

In 2012 is het volgende doel nagestreefd:
- Controle activiteiten (quick scan).

Quick scan:
Jaarlijks vindt er een quick scan van de persoonsregistraties plaats. Hierbij wordt gecontroleerd of er wijziging hebben plaats gevonden in het overzicht van de diverse persoonsregistratie van de gemeente Bergambacht.

7. Privacy bij de gemeente Bergambacht 2012.

Er zijn in 2012 geen klachten bij de FG binnen gekomen over schending van de privacy van de burgers van de gemeente Bergambacht.

8. Doelen in 2013.

Quick scan.
In september 2013 zal de jaarlijkse quick scan weer worden gehouden. Het meldingenregister wordt dan weer op actualiteit van de aanwezige registraties gecontroleerd. Omdat een gemeentelijke organisatie een dynamische onderneming is, moet er jaarlijks een quick scan worden uitgevoerd om de gegevensbestanden te controleren of deze nog voorkomen in het meldingregister van de Functionaris voor de bescherming van persoonsgegevens (FG). Medio april 2013 zal de FG een verzoek doen aan de hoofden van de diverse afdelingen om voor 1 september 2013 een quick scan uit te voeren en de resultaten schriftelijk bij de FG te melden.

Privacy van de werknemer.
Registratie van gegevens betreffende de gezondheid vereist voortdurende aandacht en alertheid. Wie hebben toegang tot medische gegevens en met welk doel? Worden de gegevens afdoende beveiligd? Is er helderheid over gegevensstromen bij de uitwisseling tussen verschillende instanties? De ondernemingsraden hebben hier een taak. En kunnen op grond van artikel 27 van de Wet op de ondernemingsraden (WOR) informatie opvragen

om te kunnen beoordelen of de persoonlijke levenssfeer van de medewerkers worden gewaarborgd.

Wat moet en kan een Ondernemingsraden (OR) met de privacy van de zieke werknemer?
Een speerpunt voor 2012 is te onderzoeken de privacy van de zieke werknemer of deze is gewaarborgd, omdat de gemeente niet meer zelfstandig beschikt over een afdeling personeelszaken. Dit uitbesteed aan de gemeenschappelijke regeling van de K5 – gemeenten.

Als een werknemer ziek wordt, wil de werkgever van alles van hem weten. De werkgever heeft bepaalde informatie nodig om het loon van de werknemer door te betalen, om te controleren of de werknemer daadwerkelijk ziek is en om hem spoedig te re-integreren. De behoeft van de werkgever aan informatie raakt direct aan de privacy van de zieke werknemer. Maar wat moet en kan de OR met de privacy van de zieke werknemer?
Met de aanpassing van de Wet op de Ondernemingsraden (WOR) in 1998 heeft de OR een expliciete rol gekregen bij de bescherming van de privacy op de werkplek. Daarnaast houden veel ondernemingsraden zich actief bezig met het ziekteverzuimbeleid in de organisatie. De OR kan hierbij erop toezien dat het verzuimbeleid rekening houdt met de privacy van de ziekte werknemer.

Om de onduidelijkheid hierover weg te nemen heeft het College bescherming persoonsgegevens (Cbp) in 2011 het rapport ": De ziekte werknemer en privacy. Regels voor de verwerking van persoonsgegevens van ziekte werknemers" uitgebracht.

Op basis van wet- en regelgeving zijn vuistregels geformuleerd over het gebruik en de uitwisseling van gegevens van de zieke werknemer door o.a. de werkgever, arbodienst en re-integratiebedrijf. Deze vuistregels zijn overigens niet vrijblijvend.

Voorlichting.
Verder heb ik het voornemen diverse werkoverleggen bezoeken en te onderzoeken hoe de werknemers om gaat met de privacy van de persoonsgegevens, welke zij gebruiken in de diverse werkprocessen.

Toezicht op het gebruik van social media.
Door het gebruik van Ubs-sticks, laptops, iPhone, smartphone, sociale netwerken wordt het noodzakelijk om een verdediging op te werken tegen datalekken en virussen steeds dringender. Informatie lekt vaker uit via social media en er ontstaan tevens security problemen als gevolg van het gebruik van social media. Vertrouwelijk, gevoelige of privé informatie komt beschikbaar en er ontstaan risico voor het lekken van deze informatie. In veel gevallen leidde het onderzoek tot ontslag of andersoortige maatregelen. Waarschijnlijk gebruiken medewerkers deze sociale netwerken al.

De risico's
Wanneer medewerkers tweeten, bloggen of hun email bekijken, weet u niet aan wie ze informatie doorgeven. Veel van de informatie die ze op sociale site plaatsen, is openbaar toegankelijk. Andere informatie verspreidt zich als een virus, zonder dat betrokkene dit weet. De informatie wordt altijd bewaard door de aanbieder van de site, dagen- en mogelijk zelfs jarenlang. Ook wordt de informatie mogelijk bijgehouden door overheidsinstanties. Gegevens kunnen uitlekken en geheimen kunnen openbaar worden gemaakt.

Wat levert medewerkers het gebruik van sociale media op? Soms meer dan de relaties die ze opbouwen op basis van de opmerkingen, foto's of video's die ze delen. Vaak houden ze ook mailware aan over: virussen, phishing, smishing, wormen zoals Koobface, en andere kwaadaardige code. Facebook-gebruikers kunnen het doelwit geworden van hackers, die via het virus 'Koobface' proberen om geheime gegevens van de surfers, zoals

kredietkaartnummers, in handen te krijgen. Koobface valt de surfers aan via de sociale netwerksite Facebook. Gebruikers van Facebook zullen berichten die ze krijgen via hun vrienden namelijk niet snel wantrouwen. De berichten in kwestie hebben titels zoals "Je ziet er geweldig uit in deze nieuwe video". Het bericht leidt de nietsvermoedende lezer naar een site waarop gevraagd wordt de nieuwste update van Adobe Flash Player te installeren. Wie dit installeert, heeft een besmette computer. Telkens de gebruiker naar sites als Google of MSN surft, zal hij naar besmette sites worden geleid.

De websites van sociale netwerken zijn een favoriet doelwit van cybermisdadigers, omdat ze zo lucratief zijn. Ze tonen grote aantallen gebruikers, die bovendien vaak de inhoud vertrouwen en erop reageren - door uitnodigingen te accepteren, account- of andere gegevens op te geven en op koppelingen te klikken. Criminelen maken misbruik van dit vertrouwen door automatisch gegevens, geld of computercapaciteit te stelen.

Bescherming: de basisbeginselen
Net als webbeveiligingen in het algemeen is de beveiliging van sociale media ingewikkeld en altijd in ontwikkeling. Door privacybeleid van social-media sites vast teleggen is dit de eerste stap in de beveiliging.

De tweede stap is het regelmatig de browsers, antivrirussoftware en invoegtoepassingen voor sociale media bij die op laptops, desktops en smartphones van medewerkers zijn geïnstalleerd, en zorg dat alle patches zijn geïnstalleerd. Werk ook webtoepassingen bij zoals Adobe PDF Reader en Flash Player, Apple Quick Timen. Windows Media Player, RealPlayer en JavaScript.

Integreer beveiliging in het netwerk.
Pas beveiliging toe die specifiek is ontworpen voor de manier waarop wij werken zoals:
- Firewall;
- IPS-software voor de bepaalde netwerkverbindingen;
- Gehoste services;
- Routers.

Blokkeer of beperk de toegang van medewerkers tot websites.
De meeste medewerkers verwachten dat de werkplek inter-service biedt. Het gebruik van sociale netwerken voor persoonlijk doeleinde kan echter ten kosten gaan de productiviteit en de beschikbare bandbreedte. Via privacybeleid kan de medewerker een handleiding worden gegeven in het gebruik hiervan. Een meer realistische benadering bestaat eruit dat de verantwoordelijke de controle houdt over welke soorten websites wanneer kunnen worden gebruikt. Via het gebruikersbeleid kunnen de medewerkers gewezen worden op de risico's en verantwoordelijkheden, die zij nemen en waarom de beveiliging noodzakelijk is. We moeten er voor waken dat datalekken en malware de bedrijfsvoering kunnen aantasten.
De belangrijkste boodschappen voor sociale netwerken zijn:
- Altijd aanpassen; nooit de standaardinstellingen laten staan;
- Maak het aanvallers niet te gemakkelijk. Wachtwoord beleid ook van toepassing laptops, desktops en smartphones van medewerkers;
- Denk na voordat voor u de inhoud van het bericht publiceert;
- Klik niet zomaar op banner of pop-ups;
- Open geen berichten van personen die je niet ken;
- Klik niet op attachments bij mails die je niet verwacht;
- Wees erg terughoudend met het verstrekken van persoonlijke informatie;
- Ga zorgvuldig om met je wachtwoord;
- Zorg voor een goede beveiliging bij externe toegang op het netwerk.

De Beveiliging Advies Commissie zal toezicht houden bij de ontwikkeling van de externe toegang op het netwerk en aan de afdeling ICT K5 gemeenten te verzoeken periode hiervan

een verslag uit te brengen op mogelijk aanvallen op de netwerkomgeving van de gemeente Bergambacht.

9. De Beveiliging advies commissie (BAC).

In de BAC zijn de volgende onderwerpen besproken:

- Bliksembeveiliging gemeentehuis;
- Noodstroom voorziening;
- Brandbeveiliging serveruimte Bergambacht;
- Jaarlijkse quick scan 2012;
- Jaarlijkse audit Reisdocumenten 2012;

10. Werkzaamheden.

Code voor informatiebeveiliging (de Code)

Er is niet één wet waar de technische en organisatorische eisen van de beveiliging is vastgelegd. In diverse wetten worden aan de verantwoordelijk verplichtingen opgelegd om op basis van techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau te realiseren.

De Nederlandse versie van de Code voor Informatiebeveiliging is tot stand gekomen onder supervisie van de NEN normencommissie 381 27 – IT Beveiligingstechniek – met de medewerking van andere organisaties en de financiële ondersteuning van het Ministerie van Economische Zaken, het Ministerie van Verkeer en Waterstaat en de Nederlandse Vereniging van Banken.

Wat is de code informatiebeveiliging eigenlijk?

Informatie (persoonsgegevens, etc.,) is een bedrijfsmiddel dat, net als andere belangrijke bedrijfsmiddelen, waarde heeft voor een organisatie en voortdurend op een passende manier beveiligd dient te zijn. Informatiebeveiliging beschermt informatie tegen een breed scala aan bedreigingen, om de continuïteit van de bedrijfsvoering te waarborgen, de schade voor de organisatie te minimaliseren en het rendement op investeringen en de kansen van de organisatie te optimaliseren. De Code is een handleiding om te komen tot de informatiebeveiliging binnen een organisatie.

Informatie komt in veel vormen voor. Het kan afgedrukt of geschreven zijn op papier, elektronisch opgeslagen zijn, per post of via elektronische media worden verzonden, getoond worden in films of de gesproken vorm aannemen. Welke vorm de informatie ook heeft, of op welke manier ze ook wordt gedeeld of verzonden, ze dient altijd passend beveiligd te zijn.

Informatiebeveiliging wordt gekarakteriseerd als het waarborgen van:

1. **Vertrouwelijkheid:** waarborgen dat informatie alleen toegankelijk is voor degenen, die hiertoe geautoriseerd zijn;
2. **Integriteit:** het waarborgen van de correctheid en de volledigheid van informatie en verwerking;
3. **Beschikbaarheid:** waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot informatie en aanverwante bedrijfsmiddelen.

Bij de handreiking bij het procesdeel van de GBA audit 2007 wordt in de inleiding gesproken dat de beschikbaarheid van gegevens, de kwaliteit en de rechtmatigheid hiervan vragen om specifieke waarborgen. Hierop wordt in de audit GBA gecontroleerd.

Deze waarborgen moeten volgens de richtlijn van het ministerie meetbaar zijn op jaarbasis welke gesteld is op 96%. Waarom geen 100%? Dit is niet mogelijk, er kunnen altijd fouten worden gemaakt in de gegevensverwerking, daarna in de controle hierop en soms ben je afhankelijke van externe factoren in de gegevensverstrekking.

Het is een continu proces en men moet ook realistisch zijn. De structuur van organisaties verandert constant, maar vraagt wel een inspanningsverplichting van de gemeente. Bij invulling van een nieuwe structuur op het gebied van ICT middelen moet ook het Informatiebeveiligingsbeleid en –plan een onderdeel zijn van de nieuwe werkprocessen binnen een gemeentelijke organisatie.

Dit percentage moet gelden voor meetbare gegevens. Deze gegevens worden periodiek bewaakt door deze gegevens te evalueren met de Beveiliging Advies Commissie (BAC)

11. Conclusie en aanbevelingen.

Uit het jaarverslag kunt u afleiden dat gegevensbescherming een continu proces is. Als overheidsinstelling moet de gemeente een goed voorbeeld geven. Daarom moeten we bewust zijn van onze verantwoordelijkheid en de gegevensbestanden zo goed mogelijk beheren.

Aanbevelingen.

1. Andere afdelingen:

Ik adviseer u voor de overige afdelingen van het secretarie, zodra er meer duidelijkheid is over de verder samenwerking binnen de K5, ook mee te nemen in de reorganisatie, een algemeen informatiebeleid en -beveiligingsplan te laten opstellen, zodat het voor onze burgers helder en transparant is dat de persoonsgegevens in onze gemeente op een correcte wijze beveiligd en worden beheerd.

2. Quick scan:

Ik adviseer u door te gaan met het houden van een jaarlijkse quick scan, omdat hierdoor het mogelijk blijft een overzicht te houden van de aanwezige gegevensbestanden en de genomen beveiligingsmaatregelen.

3. Functionaris bescherming persoonsgegevens:

Verder adviseer ik u om in K5 verband een gezamenlijke functionaris voor de bescherming van de persoonsgegevens (FG) aan te stellen, die de zorg heeft voor het beheren van de diverse registraties of deze aan te melden bij het College voor de bescherming van de persoonsgegevens (Cbp). En die een adviserende en controlerende functie heeft voor de gezamenlijk gegevensbestanden binnen de K5 gemeenten.

Betrokkene kan een onafhankelijk advies uitbrengen aan de colleges van de K5 gemeenten. Deze functie zou ook een onderdeel kunnen zijn van de gezamenlijke kwaliteits- / beveiligingsfunctionaris voor de K5 gemeenten.

Verder wil ik u adviseren om u sterk te maken voor een Beveiliging Advies Commissie K5, waarbij elke gemeente een vertegenwoordiger heeft, zodat de Informatiebeveiligingsbeleid en –plan zo breed mogelijk kan worden gedragen door alle K5 gemeenten.

Bergambacht, 7 juni 2013.
De functionaris voor de gegevensbescherming (FG)
van de gemeente Bergambacht,

J. Blinksma.

cc. aan:
- Beveiliging Advies Commissie Bergambacht;
- College voor de Bescherming van de Persoonsgegevens te ‘s-Gravenhage;
- Website gemeente Bergambacht.