Persoonsinformatie en privacy

Op weg naar adequaat uitvoeringsniveau WBP door gemeente Steenbergen

Rapport inventarisatie persoonsgegevens en toetsing aan privacy kader Gemeente Steenbergen

BMC advies
Datum: juni 2016
Naam adviseur: drs. A.J.M. (Adri) van der Peet
Definitief v1.0

INHOUD

Hoofdstuk 1 Samenvatting

De gemeente Steenbergen heeft BMC verzocht om de gemeente op een adequaat uitvoeringsniveau te brengen van de Wet bescherming persoonsgegevens (Wbp). Naar aanleiding van dit verzoek heeft BMC alle processen in kaart gebracht waarin zij persoonsgegevens verwerkt en deze getoetst aan het wettelijk kader van de Wbp en aanpalende wetgeving.

Hierbij is nadrukkelijk aandacht besteed aan de Wet meldplicht datalekken en in het bijzonder de effecten daarvan voor de verwerking van persoonsgegevens door derden. Daartoe zijn de bewerkersovereenkomsten geïnventariseerd en beoordeeld tegen de achtergrond van de verplichtingen op grond van de Wet meldplicht datalekken.

Dit rapport bevat de resultaten van deze werkzaamheden in de vorm van een register en tevens zijn de bevindingen ten aanzien van het al dan niet voldoen aan de privacyvoorschriften gerapporteerd. Het algemeen beeld is dat de gemeente Steenbergen in administratief/juridisch opzicht op weg is naar een adequaat uitvoeringsniveau van de Wbp c.a., maar dat er ook nog werk ligt om dat niveau te bereiken. Dat werk bestaat uit:

- Uitvoering van een aantal aanbevolen administratieve werkzaamheden, zoals de controle op de inhoud, zo nodig actualisering en naleving van de bewerkers-overeenkomsten, het laten vaststellen van het register gegevensverwerkingen, het bijhouden van de meldingen richting het Autoriteit Persoonsgegevens (AP) en de procedure gegevensuitwisseling met het RIEC.
- Het in kaart brengen van de consequenties van de handhaving van bewaartermijnen en besluiten over de naleving ervan
- De in dit rapport gesignaleerde onrechtmatigheden bij de verwerking van persoonsgegevens te beëindigen.

Daarnaast is het noodzakelijk om de uitvoering van de Wbp te borgen en daarvoor structureel middelen ter beschikking te stellen.

Leeswijzer
Hoofdstuk 2 beschrijft de noodzaak om de uitvoering van de Wbp ter hand te nemen. Daarna komen het toetsingskader en de uitgevoerde werkzaamheden aan de orde in hoofdstuk 3. De bevindingen hebben een plaats gekregen in hoofdstuk 4. Verantwoordelijkheid en borging van de uitvoering komen in hoofdstuk 5 aan de orde. Het rapport sluit af met conclusies en aanbevelingen.

Hoofdstuk 2 De noodzaak te voldoen aan de Wbp

2.1 Aanleiding

De gemeente Steenbergen wil een adequaat uitvoeringsniveau van de Wet bescherming persoonsgegevens (Wbp) bereiken en heeft BMC gevraagd om ondersteuning bij de uitvoering van de werkzaamheden daarvoor. De werkzaamheden hebben bestaan uit het in kaart brengen van processen met persoonsgegevens en het daarop toepassen van het wettelijk kader. Tevens is gewerkt aan de bewustwording rondom de privacy wetgeving in de organisatie en zijn de verschillende bewerkers in kaart gebracht.

2.2 Bestaand wettelijke kader

Wet Bescherming Persoonsgegevens
Sinds 1 september 2001 is de Wbp van kracht. De wet heeft als doel het verwerken van persoonsgegevens transparant te maken voor degenen wiens persoonsgegevens worden verwerkt. Op die manier kan de betrokkene zijn privacyrechten tot gelding brengen, zoals onder meer het recht op inzage en correctie.

De Wbp heeft de eisen van transparantie vorm gegeven door de verantwoordelijke voor de verwerking van persoonsgegevens onder meer een openbaar register te laten aanleggen van gegevensverwerkingen. Een aantal daarvoor in aanmerking komende gegevensverwerkingen dient de verantwoordelijke te melden bij de Autoriteit Persoonsgegevens (het voormalige College bescherming persoonsgegevens), hierna afgekort tot AP. Of een gegevensverwerking voor vrijstelling van de melding in aanmerking komt, is afhankelijk van voorwaarden die daaromtrent zijn gesteld in het zogenaamde Vrijstellingsbesluit. Dat besluit bevat categorieën van gegevensverwerkingen, die onder bepaalde voorwaarden van de melding zijn vrijgesteld.

Naast transparantie stelt de wet voorwaarden op het gebied van rechtmatigheid, waaronder eisen aan doelbinding, kwaliteit van gegevens, bewaartermijnen en beveiliging. Daaraan koppelt artikel 15 van de Wbp een nalevingsplicht.

Wet meldplicht datalekken
Sinds 1 januari 2016 is de Wet meldplicht datalekken van kracht. Deze wet heeft de Wbp uitgebreid met een verplichting om beveiligingsincidenten die gevolgen hebben voor de privacy te melden bij de AP. Met deze wetswijziging loopt Nederland vooruit op de meldplicht die zal worden opgelegd in de toekomstige Europese privacy verordening.

Het doel van deze wetswijziging is om beveiliging van persoonsgegevens te verbeteren en zo beveiligingsincidenten tegen te gaan waardoor de privacy van de burger beter wordt beschermd. Mocht zich ondanks alle getroffen beveiligingsmaat-regelen toch een beveiligingsincident voordoen, dan dient beoordeeld te worden of

de privacy van degenen wiens gegevens in het incident zijn betrokken is of kan worden geschaad. In bevestigend geval is er sprake van een datalek en dient de verantwoordelijke dit te melden bij de AP. Bij ernstige aantasting van de privacy dient de verantwoordelijke ook degenen wiens gegevens zijn gelekt daarvan in kennis te stellen. Voorbeelden van beveiligingsincidenten zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker. Direct bij het ontdekken van een beveiligingsincident dient de verantwoordelijke uiteraard alle maatregelen te treffen om de schade te beperken en voor de toekomst nieuwe incidenten te voorkomen.

2.3 Cbp heet voortaan AP en heeft boetebevoegdheid gekregen

Zoals hiervoor reeds aangegeven is de naam van het College bescherming persoonsgegevens (Cbp) sinds 1 januari 2016 veranderd in Autoriteit Persoonsgegeven (AP).

Naast deze naamswijziging heeft de AP ook boetebevoegdheden gekregen. Waar het Cbp voorheen enkel kon rapporteren, waarschuwen en een last onder bestuursdwang kon opleggen, kan de AP boetes uitdelen tot maximaal € 820.000. Deze boetebevoegdheid is van toepassing op overtreding van de gehele Wbp en niet enkel op de meldplicht datalekken zoals soms aangenomen wordt.

2.4 Toekomstige Europese privacyregels

Op 14 april heeft het Europees Parlement ingestemd met de Algemene verordening gegevensverwerking (kortweg Avg). De Avg zal de de huidige Europese richtlijn en vervangen en naar verwachting in mei 2018 van kracht worden. De Avg heeft rechtstreekse werking voor de lidstaten, hetgeen betekent dat ze overal in Europa gaat gelden.

Belangrijke elementen de Avg zijn:

- De Europese burger moet meer controle over en keuze in de verwerking van persoonsgegevens krijgen. De nieuwe verordening sluit beter aan op de nieuwe technologieën waarmee deze gegevens worden verzameld;
- De verordening introduceert een zogenaamd recht om vergeten te worden. Een organisatie zal dan ook gegevens moeten wissen als iemand hierom vraagt. Dit sluit overigens aan op de huidige bepalingen die betrekking hebben op de bewaartermijnen. Gegevens mogen niet langer worden bewaard, dan noodzakelijk is voor het doel waarvoor ze zijn verzameld. Voor een aantal gegevensverwerkingen zijn thans concrete termijnen vastgesteld (zie hierover verder onder 4.2);
- De verordening brengt grote administratieve lasten met zich mee. Organisaties moeten onder de nieuwe regels
    - investeren in het aanpassen van alle systemen die niet voldoen aan de normen. Zo moeten ze bijvoorbeeld een kopie van (persoons)gegevens in een elektronisch en bruikbaar formaat kunnen opleveren en moet het mogelijk zijn om gegevens te verwijderen.
    - hun verwerkingsprocessen beschrijven en zodanig inrichten dat ze in staat zijn aan te tonen dat ze voldoen aan de wet;

    - uitgebreide documentatie bijhouden over alle verwerkingen van persoonsgegevens die zij doen en alle verwerkingen die zij uitbesteden aan bewerkers;
- Op processen met een waarschijnlijk hoog risico voor rechten en vrijheden van betrokkenen, dient een privacy impact assessment te worden uitgevoerd en het resultaat dient gedocumenteerd en bewaard te worden;
- Overheidsorganisaties en organisaties die het verwerken van persoonsgegevens als kernactiviteit hebben moeten een Data Protection Officer, ofwel functionaris voor de gegevensbescherming (FG) aanstellen;
- Organisaties moeten nadrukkelijk kunnen aantonen dat ze compliant handelen op privacygebied (accountabilityverplichting).

2.5 Drie decentralisaties en privacy

De taken die gemeenten in het sociaal domein sinds 1 januari 2015 uitvoeren gaan gepaard met de verwerking van persoonsgegevens van nieuwe klantgroepen en nieuwe gegevens. Veel van die gegevens betreffen zogenaamde bijzondere gegevens, bijvoorbeeld betreffende de gezondheid of strafrechtelijke gegevens. De verwerking van dergelijke gegevens is aan strengere eisen gebonden, dan bijvoorbeeld de NAW-gegevens. Naast de algemene voorschriften van de Wbp, dient de gemeente ook rekening te houden met de privacybepalingen in de Jeugdwet, Wet maatschappelijke ondersteuning 2015 en de Participatiewet. Deze bepalingen geven nadere invulling aan de algemene voorschriften.

Nu de taken zijn overgedragen worden in de transformatiefase bestaande processen opnieuw ingericht en nieuwe processen doorontwikkeld. Bij zowel enkelvoudige als meervoudige complexe problemen van burgers worden (bijzondere) gegevens gedeeld met de partners. Afhankelijk van de procesinrichting, structuur en eventuele samenwerkingsvorm zijn bewerkersovereenkomsten en convenanten noodzakelijk om de gegevensverwerking binnen de kaders van de privacyregelgeving uit te voeren.

2.6 Noodzaak

Steenbergen heeft bij de overname van de werkzaamheden in het sociaal domein de eerste stappen gezet richting een adequaat uitvoeringsniveau van de Wbp. Er is privacybeleid voor het sociaal domein vastgesteld, er zijn meldingen gedaan bij de AP voor jeugdhulp en maatschappelijke ondersteuning en voor het delen van gegevens met ketenpartners is een privacyprotocol vastgesteld. Een belangrijk onderdeel van de persoonsinformatiehuishouding voldoet daardoor (in instrumentele zin) aan de privacyvoorschriften. Dat laat onverlet dat ook op andere plaatsen in de organisatie (vaak bijzondere) persoonsgegevens wordt verwerkt en ook daar conform de voorschriften gewerkt zal moeten worden.

Met de komst van de Wet meldplicht datalekken, de nieuwe boetebevoegdheden van het AP en met de verwachte Europese Privacy Verordening komt er steeds meer druk te staan op het inrichten van een adequaat uitvoeringsniveau van de Wbp en het uitvoeren van de administratieve verplichtingen. En naar verwachting gaat dit de komende jaren alleen maar groter worden. De toenemende digitalisering maakt

de bedrijfsvoering steeds afhankelijker van informatiesystemen en de gegevens die daarmee worden opgeslagen. Ook dienen zich nieuwe vormen van digitale criminaliteit aan die ertoe noodzaken informatieveiligheid en privacy een cruciaal onderdeel van de bedrijfsvoering te maken.

Hoofdstuk 3 Toetsingskader en werkzaamheden

3.1 Toetsingskader

Tijdens de inventarisatie is elke gegevensverwerking beoordeeld tegen de achtergrond van de privacywetgeving. De belangrijkste administratief/juridische toetsingscriteria zijn:

- Rechtmatige grondslag: voor het verwerken van persoonsgegevens geeft de Wbp een aantal grondslagen, waaronder de uitvoering van Publiekrechtelijke taken (artikel 8, onder e Wbp);
- Doelbinding: persoonsgegevens mogen alleen worden verwerkt voor een voorafgaand bekend gemaakt doel en alleen die gegevens mogen worden verwerkt die noodzakelijk zijn om het doel te bereiken (artikel 7 Wbp);
- Verenigbaarheid van doelen: gegevens die voor een bepaald doel zijn verzameld, mogen niet voor een ander doel worden gebruikt, tenzij het andere doel verenigbaar is met het oorspronkelijke doel (artikel 9 Wbp);
- Proportionaliteit: niet meer gegevens verwerken dan noodzakelijk is voor een bepaald doel (artikel 11 Wbp);
- Subsidiariteit: is het doel ook te bereiken met minder op de privacy ingrijpende middelen (artikel 11 Wbp);
- Bewaartermijnen: gegevens mogen niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwezenlijking van het doel waarvoor ze zijn verzameld. (artikel 10 Wbp juncto Vrijstellingsbesluit Wbp). Zie hierover paragraaf 4.2.

3.2 Werkzaamheden

In de afgelopen maanden zijn alle processen met persoonsgegevens in kaart gebracht en getoetst aan het thans geldende algemene kader van de Wbp en aan de specifieke privacy bepalingen in de wetgeving die een organisatieonderdeel uitvoert. Voorbeelden van die specifieke bepalingen zijn onder meer terug te vinden in de Participatiewet, de Leerplichtwet, Belastingwetgeving, Wet maatschappelijke ondersteuning 2015 et cetera.

Beveiliging maakt ook deel uit van het toetsingskader, maar het specifieke vakgebied van de beveiliging heeft geen deel uitgemaakt van de werkzaamheden in het kader van deze opdracht. Dat laat onverlet dat de Wbp de verantwoordelijke wel opdraagt om gemeentebreed beveiligingsmaatregelen te treffen tegen diefstal en ander onrechtmatig gebruik van persoonsgegevens. Los van dat feit is het uit oogpunt van continuïteit van de bedrijfsvoering van belang dat de beveiligingsmaatregelen er ook voor zorgen, dat systemen blijven functioneren en de dienstverlening aan de burger gegarandeerd blijft. De problemen met Digid (diginotar) en de cyberaanvallen op de banken tonen aan dat beveiliging meer dan ooit noodzakelijk is.

De werkzaamheden hebben geresulteerd in een totaaloverzicht van alle in de organisatie aanwezige gegevensverwerkingen (bijlage 1).

Van elke gegevensverwerking is in het register vastgelegd waar in de organisatie voor welk doel, over welke personen, welke gegevens worden vastgelegd en aan wie gegevens worden verstrekt. Daarnaast is ook geregistreerd:

- het doel van de verwerking. De Wbp eist dat persoonsgegevens alleen voor het doel waarvoor ze verkregen zijn gebruikt worden. Dit heet ook wel doelbinding;
- de bewaartermijn van de gegevens. De Wbp verbindt namelijk termijnen aan het bewaren van persoonsgegevens;
- de rechtmatige grondslag voor de verwerking. Waarop is de verwerking van persoonsgegevens gebaseerd;
- de applicaties die het bedrijfsproces met persoonsgegevens ondersteunen;
- welke processen zijn uitbesteed aan derden en wie bewerker is van persoonsgegevens;
- van wie de gegevens afkomstig zijn, bijvoorbeeld van de betrokkene of dat geleverd is vanuit de BRP.

Verder zijn met uitzondering van de recente meldingen voor het sociaal domein, alle meldingen van gegevensverwerkingen voor Steenbergen vernieuwd en staan klaar om naar het AP te worden verzonden. Dat laatste geldt ook voor de in te trekken meldingen van eerder gemelde gegevensverwerkingen die zijn komen te vervallen, zoals bijvoorbeeld de verwerking voor de huursubsidies.

Hoofdstuk 4 Bevindingen

4.1 Algemeen beeld

Bij de gemeente Steenbergen is de ambtelijke verantwoordelijkheid voor de uitvoering van de Wbp bij het management belegd. Steenbergen heeft nog geen privacybeheerder aangewezen.

Er is wel een privacybeheerder voor de Basisregistratie personen (BRP), maar daarvan beperkt de rol/functie zich tot specifiek de BRP. Juist het merendeel van de verwerking van persoonsgegevens bevindt zich buiten het gezichtsveld van de BRP-beheerder en bovendien is de Wbp niet van toepassing op de BRP.

Dat heeft er toe kunnen leiden dat sinds de initiële werkzaamheden in het kader van de inwerkingtreding van de Wbp, de gemeente Steenbergen geen consistent uitvoeringsbeleid Wbp heeft gevoerd. Dat is onder meer af te leiden uit het feit dat er vanuit verschillende onderdelen van de organisatie meldingen zijn gedaan bij de AP, waarvan er ook een aantal ingetrokken hadden moeten zijn. Ook het openbaar register van verwerkingen van persoonsgegevens ontbreekt.

Tijdens de verschillende gesprekken en werksessies werd er vanuit de medewerkers positief en geïnteresseerd gereageerd op het onderwerp. De totale persoonsinformatiehuishouding kon volledig in beeld worden gebracht. In totaal zijn ruim 115 processen met persoonsgegevens geïnventariseerd in deze actualiseringsronde, waarvan er 37 gemeld moeten worden.

In de volgende paragrafen benoemen wij een aantal aandachtspunten, die gedurende de huidige inventarisatieronde zijn geconstateerd.

4.2 Bewaartermijnen

In het algemeen geldt dat identificerende persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor de realisatie van de doeleinden waarvoor ze zijn verzameld en vervolgens verwerkt. Voor van melding vrijgestelde gegevensverwerkingen is de bewaartermijn expliciet in het Vrijstellingsbesluit benoemd. Het betreft hier maximale termijnen waarbij moet worden aangetekend dat dit Besluit een langere bewaartermijn toestaat indien uit een andere wet de noodzaak tot langer bewaren blijkt (bijv. uit de Archiefwet of de Belastingwetgeving).

Wanneer het overzicht van gegevensverwerkingen door de verantwoordelijke bestuursorganen wordt vastgesteld, conformeert het college van burgemeester en wethouders respectievelijk de burgemeester zich aan de genoemde bewaartermijnen. Dit betekent dat de ambtelijk verantwoordelijke proceseigenaren er op moeten toezien dat periodiek opschoning van bestanden met persoonsgegevens plaatsvindt. Dat geldt dan zowel voor de bestanden die zijn opgeslagen in de proces ondersteunende applicaties (bijvoorbeeld de gegevens van oud-medewerkers zijn nog volledig terug te vinden in de personeelsregistratie) als

voor de mappen van de afdelingen en van individuele medewerkers waarin zich schaduwbestanden (fysiek dan wel digitaal) bevinden.

4.3 Openbaar register

Op grond van de Wbp dient de verantwoordelijke een openbaar register bij te houden waaruit aan een ieder kosteloos inlichtingen kunnen worden verstrekt. Dit register ontbrak, maar is nu alsnog opgesteld. Een extractie van het overzicht van gegevensverwerkingen dat is opgesteld kan als openbaar register fungeren.

4.4 Bewerkerscontracten

De organisatie Steenbergen heeft een aantal werkzaamheden uitbesteed aan derden. Voor de verwerking van persoonsgegevens die daarmee gepaard gaat, blijft het gemeentebestuur de verantwoordelijke. Degene die namens de verantwoordelijke, i.c. het college of de burgemeester persoonsgegevens verwerkt, is in termen van de Wbp aan te merken als bewerker.

De beveiligingseisen die de Wbp stelt aan ‘de verantwoordelijke’ gelden onverkort voor deze derden en dienen op grond van artikel 14 Wbp in zogenaamde bewerkerscontracten te worden vastgelegd. Indien een publieke taak van de gemeente is gemandateerd aan een andere partij dan dient een bewerkersovereenkomst opgesteld te worden. Echter, wanneer deze taak is gedelegeerd dan is de volledige verantwoordelijkheid van dit proces, en dus ook de verantwoordelijkheid met betrekking tot privacy, overgeheveld aan deze externe partij.

De gemeente Steenbergen heeft de taken in onderstaande tabel gemandateerd aan externe organisaties. Het is van belang dat met deze partijen een bewerkersover-eenkomst wordt afgesloten of dat de bestaande overeenkomst wordt geactualiseerd in verband met de verplichting op grond van de Wet meldplicht datalekken.

Taak	**Bewerker(s)**
Incidentenregistratie	A&O fonds
Salarisadministratie(s)	RAET en ADP
Terugkeerbegeleiding ex-gedetineerden en Bestuurlijke informatie justitiabelen	Zorg en Veiligheidshuis de Markiezaten
Digitale telefooncentrale	Zetacom
Website en Orderdatabase	Gemeenteoplossingen
Leerplicht en voorkomen voortijdig schoolverlaten	RMC West-Brabant
Taken op het gebied van Werk, Inkomen en Schulden	ISD Brabantse Wal
Heffing en invordering belastingen	TOG Nederland
Administratie kwijtscheldingen	Inlichtingenbureau
Maatschappelijke ondersteuning / Jeugdhulp	Inforing
Burgerzakenmodules	Pink Roccade
Handhaving illegale activiteiten	OMWB
Bijzondere opneming psychiatrische inrichting	Khonraad
Alarmering crisisorganisatie	Halderberge

4.5 Gebruik BRP voor niet-publiekrechtelijke taken

Tot ontvangst van gegevens uit de BRP zijn bevoegd degenen die uitvoering geven aan een publiekrechtelijke taak (art. 1.3 en 1.7 Wet Basisregistratie Personen). Voor elke taak mag een toegesneden set aan gegevens beschikbaar worden gesteld op basis van uitvraag met behulp van bekende identificerende persoonsgegevens. In slechts een beperkt aantal gevallen is uitvraag op adres toegestaan. Alle andere zogenaamde ad-hoc adresvragen zijn in strijd met de wet BRP.

BRP-gegevens in Melddesk

Voor de vulling van Melddesk, een systeem waarin Publiekszaken de meldingen over de openbare ruimte registreert is een extractie met NAW-gegevens uit de BRP geleverd, die elke 24 uur wordt geactualiseerd.

Dit gebruik is enerzijds in strijd met de wet Brp vanwege het feit dat het hier om bedrijfsvoering gaat en niet om een publiekrechtelijke taak. Anderzijds is de verstrekking buitenproportioneel om meerdere redenen.

1. Er is een volledig BRP-bestandsextractie beschikbaar op een in verhouding zeer beperkt aantal meldingen (gegevens van ruim 23.000 inwoners ten opzichte van enkele honderden meldingen per jaar).
2. Een melding over de openbare ruimte moet in principe niet te leiden tot registratie van persoonsgegevens van de melder, tenzij de melder daar zelf prijs op stelt bijvoorbeeld in verband met een terugkoppeling.
3. De raadpleging van gegevens over de melder geschiedt op adresingang. Langs deze route zijn ook gegevens in te zien van andere personen die op hetzelfde adres zijn ingeschreven.

Gebruik van BRP via DMS

Het documentmanagementsysteem Corsa ondersteunt de bedrijfsprocessen door de ingekomen documenten te registreren en integraal op te nemen. Voor de juiste registratie van naam en adresgegevens wordt gebruik gemaakt van de gegevens uit de BRP. Om dit mogelijk te maken is dit systeem gekoppeld aan de BRP.

Zoals hiervoor reeds gesteld is het gebruik van gegevens uit de BRP slechts toegestaan voor de uitvoering van publiekrechtelijke taken. Alhoewel registratie van documenten gerekend moet worden tot de bedrijfsvoering van de organisatie, wordt er vanuit gegaan dat voor de registratie van documenten voor publiekrechtelijke taken de BRP gebruikt mag worden. De gedachte daarachter is, dat de registratie in feite noodzakelijk is om een publiekrechtelijke taak te starten.

Het gebruik van BRP-gegevens voor de registratie van documenten voor de niet publiekrechtelijke taken is niet toegestaan, zoals bijvoorbeeld voor het registreren van documenten en dossier van medewerkers , grondzaken en financiële administratie. Het feit dat de gemeente vanwege haar wettelijke opdracht in de Wet Brp, beschikt over de persoonsgegevens van haar burgers, is op zichzelf geen rechtmatige grondslag om voor haar eigen bedrijfsvoering van de BRP gebruik te maken.

4.6 Toegankelijkheid Corsa

De gemeente Steenbergen is bezig met het migreren van het documentair systeem naar een zakenmagazijn. Uit oogpunt van efficiency en effectiviteit geldt daarbij als uitgangspunt dat het magazijn breed toegankelijk moet zijn en de dossiers voor elke medewerker beschikbaar moeten zijn. 'Openbaar', tenzij…!

Dit uitgangspunt is in strijd met de doelbindingseis uit de Wbp en met de bepalingen die in de diverse sectorale wetten op dit gebied van toepassing zijn. Zo kent de Participatiewet een geheimhoudingsbepaling voor de medewerkers Werk en Inkomen (art. 65 Participatiewet) en is voor hergebruik van verschillende dossiers in het sociaal domein de expliciete toestemming nodig van de betrokkene (art. 5.1.1. lid 4 WMO 2015). Dit houdt in dat onderlinge raadpleging, ook tussen medewerkers sociaal domein, van dossier van cliënten niet zonder meer is toegestaan.

Voor het documenten- respectievelijk en zakenmagazijn dient een autorisatiestructuur te worden doorgevoerd die in lijn is met de uit te voeren taken van de medewerkers.

4.7 Onrechtmatig gebruik BSN

Het burgerservicenummer (BSN) is een uniek persoonsnummer voor iedereen die ingeschreven staat in de Basisregistratie personen (BRP). Overheidsorganen kunnen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun taak gebruik maken van het BSN-nummer (art. 10 Wet Algemene Bepalingen Burgerservicenummer). In de gemeente Steenbergen wordt het BSN-nummer genoteerd bij iedere zaak die in het zaaksysteem wordt verwerkt. Dat impliceert dat de gemeente ook het BSN registreert voor met name de privaatrechtelijke zaken die zij uitvoert.

Gelet op de ruimhartige openstelling van het zakenmagazijn (zie paragraaf 4.6) kunnen medewerkers inzicht hebben in het leeuwendeel van de zaken in het zaaksysteem en daarmee ook automatisch in het BSN van de betrokkene(n). Hierdoor is er sprake van een onrechtmatige kennisname van het BSN voor die zaken die niet tot het takenpakket van een medewerker kunnen worden gerekend.

Het is dan ook aan te raden om inzichtelijk te maken welke processen wel gebruik kunnen maken van het BSN en welke niet en dit vervolgens technisch in te regelen in het zaaksysteem. Met het BSN kan namelijk gemakkelijk een koppeling worden gemaakt tussen informatie uit verschillende bestanden. Onzorgvuldig gebruik van het BSN brengt daarom privacyrisico's met zich mee. Bijvoorbeeld misbruik van persoonsgegevens en identiteitsfraude.

4.8 RIEC

De gemeente Steenbergen heeft een convenant gesloten met het Regionaal Informatie- en Expertise Centrum (kortweg RIEC), dat als doel heeft het voorkomen van georganiseerde misdaad en criminaliteit.

Voor de aanpak van georganiseerde misdaad is een intensieve samenwerking tussen gemeenten, justitie, politie, belastingdienst en bijzondere opsporingsdiensten noodzakelijk. Het delen van alle beschikbare relevante informatie en het afstemmen van het overheidshandelen is daarbij cruciaal.

Op basis van deze informatie en nadere analyse worden gemeenten en andere deelnemende partijen geadviseerd over de mogelijke interventiestrategieën om de verwevenheid tussen boven- en onderwereld zowel preventief als repressief tegen te gaan.

De informatie-uitwisseling tussen aan het samenwerkingsverband deelnemende partijen gaat gepaard met het verstrekken van persoonsgegevens aan een RIEC. Op deze vorm van verwerken van persoonsgegevens is de Wet bescherming persoonsgegevens (Wbp) van toepassing.

Een verstrekking van persoonsgegevens aan het RIEC is slechts mogelijk als deze past binnen de kaders van de privacyregelgeving. De gegevensuitwisseling met het RIEC is gaande het inventarisatietraject voor zover als mogelijk privacyproof gemaakt.

Naast de uitwisseling van gegevens met de RIEC-partners, bepleit ‘het RIEC’ het creëren van ondermijningsbeelden door de gemeenten. Het RIEC adviseert gemeenten op basis van signalen en onderbuikgevoelens gegevens te verzamelen uit de verschillende bestanden waarover de gemeenten in het kader van de taakuitvoering zelf beschikken en deze te combineren met gegevens uit andere (‘openbare’) bronnen. Daardoor ontstaan ‘beelden’ c.q. profielen die de gemeenten in staat stellen strafbare feiten te voorkomen of tegen te gaan. Voor een dergelijke heimelijke verwerking van persoonsgegevens door een gemeente is echter geen rechtmatige grondslag aan te wijzen.

4.9 Inzage vergunningaanvragen en behandeldossiers niet geanonimiseerd

De gemeente is verplicht om plannen in het kader van omgevingsvergunningen te publiceren. Ook bij de gemeente Steenbergen liggen deze documenten ter inzage en zijn deze voor een ieder vrij toegankelijk. Voor wat betreft deze publicatie is het noodzakelijk om de volgende gegevens inzichtelijk te maken:

- adres/locatie
- kenmerk
- omschrijving
- datum
- rechtsmiddel (mogelijkheid tot indienen van een zienswijze of bezwaar)

Ondanks de publicatieplicht, is het de gemeente niet toegestaan om persoonsgegevens, waaronder het BSN van de aanvrager openbaar te maken. Datzelfde geldt voor de persoonsgegevens in de behandeldossiers van de omgevingsvergunningen en ook voor andere vergunningen. Aan deze eis vanuit de Wbp voldoet de gemeente Steenbergen thans niet in voldoende mate.

4.10 Openbaarheid van bestuur betekent niet zonder meer openbaarheid van persoonsgegevens

Evenals hiervoor onder 4.9 verwoord betekent de actieve publicatieplicht op grond van de Wet openbaarheid van bestuur niet dat de griffier zonder meer persoonsgegevens in stukken voor de raad en in bijvoorbeeld brieven gericht aan de raad openbaar mag maken.

De voorloper van de AP heeft reeds in 2007 Richtsnoeren voor de publicatie van persoonsgegevens op internet gepubliceerd waaraan de verantwoordelijke, in casu de gemeenteraad zich dient te houden. Het integraal (op de website) publiceren van documenten waarin persoonsgegevens voorkomen is in het algemeen gesproken slechts toegestaan indien dat absoluut functioneel is.

4.11 Toegang gemeentelijke (semi-)statische archieven

Archiefstukken bevatten in de regel ook persoonsgegevens van de personen met wie de gemeente in het (nabije) verleden zaken heeft gedaan. In de stukken kunnen ook persoonsgegevens voorkomen van derden. Op de verwerking van persoonsgegevens in de archieven is zowel de Wbp als de Archiefwet van toepassing. Beide wetten stellen beperking aan de toegankelijkheid van de archieven in verband met de persoonlijke levenssfeer van degenen wiens gegevens in de archiefstukken vastliggen.

Aanvragers van archiefstukken worden in de gelegenheid gesteld om zelfstandig de archieven te raadplegen en stukken op te zoeken. Dat brengt het risico met zich mee dat persoonsgegevens worden ingezien zonder dat vooraf gescreend is kunnen worden of een dergelijke inzage is toegestaan respectievelijk een eventuele toestemming van de betrokkene gevraagd kon worden.

4.12 Gegevensverwerking in het sociaal domein

Per onderdeel van het sociaal domein verwerkt de gemeente sinds 1 januari 2015 persoonsgegevens van nieuwe klantgroepen. Dat betreft

- bij werk en inkomen (Participatiewet), de Wajongers en de Wsw'ers;
- bij maatschappelijke ondersteuning een belangrijk deel van de AWBZ-klanten;
- de jeugdgroepen die ressorteren onder de provinciale (geïndiceerde) jeugdzorg, de geestelijke gezondheidszorg voor jeugdigen (jeugd-ggz) en jeugdigen met een licht verstandelijke beperking (jeugd-lvb), de gesloten jeugdzorg, de forensische zorg en de uitvoering van jeugdbeschermingsmaatregelen en jeugdreclassering.

Voor de individuele gevalsbehandeling per klantgroep is het privacytechnisch gezien noodzakelijk de reguliere Wbp-uitvoeringshandelingen te verrichten, zoals toetsing van de gegevensverwerking aan het kader van de privacywetgeving en het melden of wijzigen van bestaande meldingen.

Meervoudige probleemsituaties vergen een geïntegreerde aanpak en het bij elkaar brengen van gegevens uit de verschillende onderdelen van het sociaal domein in een informatiesysteem en het delen van informatie ook met partners waarmee wordt samengewerkt.

De uitvoering van de Participatiewet is ondergebracht bij ISD Brabantse Wal. De taken op het gebied van Werk en Inkomen zijn in mandaat opgedragen aan de ISD. Daarmee is de verantwoordelijkheid voor de uitvoering met betrekking tot de Steenbergse inwoners bij het college van Burgemeester en wethouders van Steenbergen gebleven, waarmee dit college ook de verantwoordelijke is voor de uitvoering van de Wbp.

De taken die voortvloeien uit de Jeugdwet zijn ondergebracht bij uitvoeringsorgaan Centrum Jeugd en Gezin Steenbergen. Medewerkers CJG verzorgen de intake, 1e lijn hulp, toeleiding en beschikking. Privacyprotocol gegevensverwerking Jeugdhulp voorziet in de nodige privacywaarborgen.

De WMO taken worden uitgevoerd bij Vraagwijzer Steenbergen en ook bij deze taak geldt dat de gemeente het eerste aanspreekpunt is voor de burger en na een intake beslist de gemeente welke organisatie een passende oplossing kan bieden. Bij maatschappelijke ondersteuning zijn de privacywaarborgen vastgelegd in het Privacyprotocol gegevensverwerking maatschappelijke ondersteuning.

De privacyprotocollen voorzien beiden in de mogelijkheid om met toestemming van de betrokkene gegevens te delen met andere partijen die noodzakelijk zijn voor de hulpverlening. Dit biedt de mogelijkheid om bij meervoudige complexe hulpvragen de dienstverlening af te stemmen met andere partners in het sociaal domein. Bij zeer ernstige situaties waarbij de betrokkene geen toestemming wil of kan geven kunnen gegevens gedeeld worden zonder diens toestemming. De professionals hebben hiervoor een afwegingskader.

Hoofdstuk 5 Verantwoordelijkheid en borging

5.1 Verantwoordelijkheid

De ambtelijke verantwoordelijkheid voor de uitvoering van de Wbp ligt logischerwijze bij het management c.q. degenen die verantwoordelijk zijn voor de uitvoering van de processen waarin persoonsgegevens worden verwerkt. Het gaat immers om de wettelijke kaders waarbinnen de procesuitvoering dient plaats te vinden. De handhaving van de privacykaders heeft echter nog geen prioriteit gekregen.

De toenemende digitalisering van de primaire- en bedrijfsvoeringsprocessen en de daarmee gepaard gaande complexiteit van de informatievoorziening veroorzaken tevens een toename van juridische en beveiligingsrisico's. Het is van belang dat managers zich meer dan thans het geval is, bewust zijn van het feit dat zij (mede)verantwoordelijk zijn voor de informatievoorziening die hun processen ondersteunt en daarmee tevens (mede)verantwoordelijkheid dragen voor genoemde risico's.

Om die verantwoordelijkheid te kunnen nemen en te kunnen sturen op privacy is het noodzakelijk om privacy te integreren in de bedrijfsvoering en onderdeel te maken van de planning- en controlcyclus.

5.2 Borging

De uitvoering en handhaving van de privacywetgeving vergt tamelijk specialistische kennis, die normaal gesproken bij het management niet voorhanden is. Om verantwoordelijkheid te kunnen nemen voor de handhaving van de privacykaders, heeft het management van Steenbergen deskundigheid op het gebied van privacywetgeving nodig. De rol van een privacyfunctionaris is nog niet belegd. Wel ligt er het voornemen vanuit de implementatie van de Baseline informatiebeveiliging gemeenten (BIG) om een privacybeheerder te benoemen. Hieronder motiveren wij kort de noodzaak om zowel de rol te beleggen alsook daaraan formatieve capaciteit toe te kennen.

De vrijwel permanente veranderingen in organisatie en processen als gevolg van nieuwe wetgeving, verbetering van de dienstverlening, samenwerkingen met andere gemeenten en met maatschappelijke partners, dienen getoetst te worden aan de kaders van de privacywetgeving. Daarnaast zullen zich de komende tijd naar verwachting nieuwe privacyvraagstukken aandienen, zoals bijvoorbeeld het thuiswerken met BRP-gegevens, cloudcomputing en Bring Your Own Device (BYOD).

Onder de administratieve taken van de privacy beheerders vallen onder meer het beheer van het register van gegevensverwerkingen en het doen van en intrekken van meldingen. De voornoemde veranderingen dienen verwerkt te worden in het openbaar register en bij het AP moeten eventuele meldingen worden gedaan of juist worden ingetrokken.

5.3 Capaciteit

Kennis, ervaring en capaciteitsinzet op dit vakgebied is noodzakelijk om een adequaat uitvoeringsniveau van de privacywetgeving te borgen. Binnen de organisatie is nog geen capaciteit beschikbaar gesteld voor een privacyfunctionaris. De benodigde capaciteitsinzet voor Steenbergen komt naar schatting, bij een gemiddelde van 8 uur per week, uit op tussen de 300 en 400 uur per jaar. Gelet op de privacyvraagstukken die op de gemeente afkomen de komende jaren, zal de capaciteitsbehoefte eerder op 400 uur en zelfs meer uren uitkomen dan op 300 uren.

Nog enkele voorbeelden van privacyvraagstukken ter onderbouwing van deze veronderstelling. Advisering bij

- Datalekken;
- invoering nieuwe wet- en regelgeving;
- invoering van zaakgericht werken;
- gegevensverzameling in het kader van criminaliteitsbestrijding (ondermijningsbeeld);
- het gebruik van persoonsgegevens in Big data-projecten.

Bovendien zal de gemeente opvolging moeten geven aan adviezen van de AP, zoals bijvoorbeeld naar aanleiding van de publicatie van de AP over toestemmingen in het sociaal domein (21 april 2016) of de publicatie van een adres van een wietkwekerij (6 juni 2016, Renkum).

De ervaring over de komende jaren zal uitmaken hoeveel tijd er uiteindelijk aan privacy besteed zal worden.

Hoofdstuk 6 Conclusies en aanbevelingen

6.1 Conclusies

1. Steenbergen staat de komende tijd veel veranderingen te wachten waaraan privacyissues verbonden zijn. Voorbeelden daarvan noemden wij in de voorgaande paragraaf. Daarnaast moet de gemeente vanaf 2018 op grond van de Avg aantoonbaar aan privacymanagement doen. Gelet op de prioriteitstelling tot op heden, is een vergroting van het privacybewustzijn bij management en medewerkers noodzakelijk.

2. Door de recente uitvoering van de inventarisatie van de processen met persoonsgegevens en de toetsing van de gegevensverwerking aan het wettelijk kader is de gemeente Steenbergen op weg naar een adequaat uitvoeringsniveau Wbp.

3. De gemeente Steenbergen wisselt gegevens uit met het RIEC. De levering van gegevens aan het RIEC vanuit de bronnen binnen de gemeente is niet voor elke bron mogelijk en voor de bronnen waaruit dat wel mogelijk is, dient de melding te worden gedaan. Die meldingen zijn alsnog gedaan. Voor het creëren van ondermijningsbeelden door de gemeente is (nog) geen rechtmatige grondslag aanwezig.

4. Bij Steenbergen ontbreekt het nog aan uitvoeringsbeleid voor de handhaving van de bewaartermijnen.

5. Door de gemeente worden bewerkersovereenkomsten niet op de naleving van de contractvoorwaarden gecontroleerd. Tevens voldoen de bestaande overeenkomsten niet aan de eisen van de Wet meldplicht datalekken.

6. Er is sprake van een onrechtmatige koppeling van de BRP met de melddesk.

7. Er is sprake van onrechtmatig gebruik van het BSN in melddesk en zaaksysteem.

8. De toegang tot het document- respectievelijke zakenmagazijn sluit niet goed aan op de eisen die vanuit de privacywetgeving worden gesteld.

9. Omgevingsvergunningen die bij de gemeente ter inzage liggen zijn niet of niet voldoende geanonimiseerd waardoor in strijd met de privacyvoorschriften persoonsgegevens openbaar worden gemaakt.

10. De wijze van raadpleging van archiefstukken brengt risico's van privacyschendingen met zich mee.

6.2 Aanbevelingen

Om het resultaat van de in hoofdstuk 2 beschreven inspanningen te borgen in de organisatie bevelen wij aan:

1. Besturing op privacy te organiseren en privacy, evenals beveiliging te integreren in de bedrijfsvoering en mee te nemen in de planning- en controlcyclus. Concreet betekent dit het managementinstrumentarium uitbreiden met een handreiking voor het management hoe inhoud te geven aan de verantwoordelijkheid voor privacy en een instructie hoe privacy mee te nemen bij het opstellen van de jaarplannen.

2. Middelen toe te wijzen om te kunnen voorzien in de benodigde capaciteit om de uitvoering van de Wbp uit te voeren en het resultaat van de werkzaamheden zoals beschreven in dit rapport te borgen.

Daarnaast bevelen wij aan

3. Het register van gegevensverwerkingen te laten vaststellen door de verantwoordelijke bestuursorganen, het openbaar register ter inzage te leggen en de ter inzagelegging bekend te maken via de gebruikelijke communicatiekanalen.

4. Om in overleg met de proceseigenaren te komen tot beleid ter zake de handhaving van de bewaartermijnen. Hiervoor dient de bewaartermijn per proces te worden afgesproken en de daadwerkelijk verwijdering van persoonsgegevens te worden geregeld.

5. De geïnventariseerde bewerkerscontracten in de tabel van paragraaf 4.4 aanpassen aan de Wet meldplicht datalekken en periodiek te controleren op de naleving ervan

6. De toegang tot dossiers en zaken in het documentaire en zakensysteem zodanig in te richten dat medewerkers toegang krijgen die aansluit bij het takenpakket.

7. De onrechtmatige verwerking van het BSN te beëindigen door aanpassingen in de bestandskoppelingen.

8. Het onrechtmatig gebruik van gegevens uit de BRP te beëindigen aanpassingen in de bestandskoppelingen.