Privacy, het beleid in de gemeente Hellendoorn. 18INT01333

Inleiding

Privacy, privésfeer, persoonlijke levenssfeer of eigenruimte is een recht dat de persoonlijke levenssfeer beschermd. De Van Dale omschrijft het als volgt: de persoonlijke vrijheid, het ongehinderd en alleen, in eigen kring of met een partner ergens kunnen vertoeven; gelegenheid om zich af te zonderen, om storende invloeden van de buitenwereld te ontgaan, een toestand waarin een mens er zeker van is dat zonder zijn toestemming zo weinig mogelijk andere mensen zich op zijn terrein zullen begeven. De afgelopen decennia is dit begrip verder uitgebreid met:

- Zelf bepalen wie welke informatie over ons krijgt
- De wens om onbespied en onbewaakt te leven.

In de informatiemaatschappij die de afgelopen jaren in een sneltreinvaart is ontstaan, staat dat onbewaakte leven - vaak op een subtiele manier- onder druk. Gegevens van een gemiddelde inwoner van ons land zijn op dit moment terug te vinden in ongeveer 2000 verschillende databases. En elke keer als je akkoord gaat met het accepteren van een cookie stem je ermee in dat er informatie over jou wordt verzameld en - vaak ook- in sneltreinvaart wordt verspreid.

Privacy is een lastig en breed begrip. Het gaat over de bescherming van persoonsgegevens, de bescherming van het eigen lichaam, de eigen woning met erf, de bescherming van familie en gezinsleven en het recht om vertrouwelijk te pinnen en te communiceren via brief, telefoon, internet of aan een balie. Privacy betekent dat je dingen kunt doen zonder dat de buitenwereld daar weet van heeft, inbreuk op kan maken of een corrigerende invloed op uitoefent.

Privacy is voor gemeenten niet een nieuw onderwerp. Met name binnen het Sociaal domein en bij Burgerzaken is de afgelopen jaren gewerkt aan de bescherming van persoonsgegevens. Daarbij zijn ook de nodige audits uitgevoerd.

Het onderwerp privacy heeft veel verschillende invalshoeken; ethische, informatiekundige, juridische, praktisch, organisatorische en technische. Al deze elementen komen in deze notitie aan bod.

Hoofdpunten van het Privacy beleid

Voor ons als gemeente gelden de volgende hoofdpunten van beleid:

- Het college van B & W is bestuurlijk eindverantwoordelijk voor privacy en het verwerken van persoonsgegevens;
- Uitvoering en handhaving van de regels met betrekking tot privacy is een integrale verantwoordelijkheid van het lijnmanagement;

- De Functionaris Gegevensbescherming oefent hier toezicht op uit, en rapporteert waar nodig;
- Verantwoord en bewust gedrag van medewerkers is essentieel voor het zorgvuldig verwerken van persoonsgegevens;
- Verwerken van persoonsgegevens vindt alleen plaats op basis van een legitieme grondslag en voor het doel waarvoor de gegevens beschikbaar zijn gesteld;
- We vragen de burgers niet meer gegevens dan strikt noodzakelijk en bewaren ze niet langer dan nodig;
- Wij maken op een transparante manier duidelijk hoe wij denken over privacy, hoe we hiermee omgaan en hoe we dit borgen. Dit staat in ons privacystatement;
- Wij handelen vragen en klachten van inwoners of bedrijven over privacy op een toegankelijke en laagdrempelige manier af;
- Wanneer onze persoonsgegevens door een externe partij worden verwerkt liggen daar afspraken onder: deze liggen vast in een zogenaamde verwerkersovereenkomst;
- Over de uitvoering van het beleid wordt periodiek gerapporteerd aan directie en college en – als onderdeel van de jaarlijkse Planning & Control-cyclus- aan de gemeenteraad.

Ethiek en veiligheid

Bij een discussie over privacy gaat het vaak om een ethische afweging en het spanningsveld tussen privacy en andere belangen, zoals strafvordering (al dan niet preventief) en bestrijding van ongewenst gedrag. Zo zorgden de wetten in het kader van de ‘oorlog tegen terrorisme’ (zoals de Amerikaanse Patriot Act) voor de nodige beroering omdat ze de privacy van de burgers aantast. De voorstanders van deze wetgeving claimen dat het nadeel van het privacy verlies niet opweegt tegen de voordelen, zoals het effectief kunnen bestrijden van terrorisme. Anderen brengen in dat privacy verlies geen nadeel is, dit onder het motto; als je niets fout doet heb je toch niets te verbergen…….. Een andere ontwikkeling is de enorme toename van de opslag van persoonsdata via de computer en het internet. Vaak wordt deze ontwikkeling ‘verkocht’ aan de burger onder het mom van verbetering van computerfunctionaliteit en dienstverlening, terwijl het belang erachter gewoon commercieel is. Data zijn handel en daarmee geld. Er wordt geld voor data betaald omdat er geld mee te verdienen valt. Bedrijven kunnen hun klanten er gerichter mee stimuleren om zaken te kopen en zien daarmee hun omzet toenemen.

Ethiek bindt uiteraard formeel niet. Dat doen wetten wel. Wetten zijn echter mede gebaseerd op ethische overwegingen. Ethiek gaat vaak verder dan de wettelijke normen; wat vinden we onfatsoenlijk of immoreel. En dat we dat vinden betekent nog niet dat het onrechtmatig gedrag is.

Wetgeving algemeen

In verschillende internationale verdragen wordt het recht op privacy gegarandeerd. In artikel 17 van het VN-verdrag voor Burgerlijke en Politieke rechten (uit 1966) staat:

1. Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privéleven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam;

2. Een ieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantastsing.

Ook het handvest van de grondrechten van de Europese unie (artikelen 7 en 8) en het Europees verdrag voor de rechten van de mens (artikel 8 EVRM) garanderen deze rechten. Burgers van Europese landen die de verdragen hebben ondertekend, kunnen zich bij de rechter op deze verdragen beroepen. Maar, het recht op privacy is niet absoluut. Beperking op dit recht zijn mogelijk. Dat staat in artikel 8 lid 2 EVRM. Belangen omtrent nationale veiligheid, openbare veiligheid, economisch welzijn, voorkomen van wanordelijkheden en strafbare feiten, bescherming van gezondheid of goede zeden, of om rechten en vrijheden van andere te beschermen, kunnen reden zijn om de privacy (voor een deel en tijdelijk) te beperken.

De manier waarop deze verdragen worden toegepast kan per EU-lidstaat verschillen.

Concrete regels voor de bescherming van persoonsgegevens zijn opgenomen in een conventie uit 1981 van de Raad van Europa. Deze regels zijn overgenomen in Richtlijn 95/46/EG (databeschermingsrichtlijn) van de Europese Unie en zijn later omgezet in nationale wetgeving.

Sinds 24 mei 2016 geldt in Europa de General Data Protection Regulation (GDPR), in Nederland beter bekend als de Algemene Verordening Gegevensbescherming (AVG). Deze regelgeving hoeft niet door de afzonderlijke lidstaten te worden omgezet in wetgeving, ze geldt nu al in heel Europa. Vanaf 25 mei 2018 moet dit door iedereen worden nageleefd.

Nederlandse wetgeving

In ons land is het recht op privacy vastgelegd in de artikelen 10 tot en met 13 van de grondwet. Een onderdeel van de privacy, de verwerking van persoonsgegevens, wordt sinds 1 september 2001 nader geregeld in de Wet bescherming persoonsgegevens (Wbp). Naast de Wbp zijn er meer specifieke wetten en regels die gaan over persoonsgegevens. Dat zijn:

- De Wet op de Beroepen in de individuele gezondheidszorg (Wet BIG)
- De Wet inzake de geneeskundige behandelingsovereenkomst (Wgbo)
- De Jeugdwet
- De Participatiewet
- De Wet basisregistratie personen (Wet BRP) is de nieuwe grondslag voor de basisregistratie persoonsgegevens en vervangt de Wet gemeentelijke basisadministratie persoonsgegevens (Wet GBA)
- Wet politiegegevens
- Wet justitiële en strafvorderlijke gegevens
- Archiefwet (bewaartermijnen)

De organisatie die landelijk toezicht houdt op de verwerking van persoonsgegevens en zich dus bezig houdt met de bescherming van onze privacy is de Autoriteit Persoonsgegevens (AP). De AVG biedt

de AP betere instrumenten voor een steviger toezicht en het uitdelen van forse boetes. Privé organisaties die zich met privacy bezig houden zijn Bits of Freedom (privacy op het internet) en Buro Jansen &Janssen[1].

Zoals hiervoor al aangegeven is vanaf 25 mei 2018 de AVG van toepassing en vervangt daarmee de Wbp.

De AVG en de gemeente

In essentie betekent de komst van de AVG voor gemeenten dat nog zorgvuldiger en transparanter moet worden omgegaan met persoonsgegevens. Dat wordt onder meer duidelijk door het volgende:

- De gemeente moet aangegeven voor welk doel, welke persoonsgegevens worden verzameld. Dat moet een gerechtvaardigd doel zijn(wettelijke grondslag en doelbinding, art. 5 lid 1b en art. 6 AVG);
- Er mogen niet meer gegevens worden verzameld dan minimaal nodig zijn voor het doel (dataminimalisatie, art 5 lid 1c AVG);
- Persoonsgegevens mogen niet langer worden bewaard dan nodig (bewaartermijn, art. 5 lid 1e AVG);
- Naast geheimhoudingsplicht voor medewerkers, moet ook de beveiliging van de gemeente goed worden geregeld en vastgelegd in informatieveiligheidsbeleid (Integriteit, beschikbaarheid en vertrouwelijkheid van gegevens art. 5 lid 1 f);
- Als gegevensverwerking vanuit de gemeente door derden plaatsvindt, moeten daar schriftelijke afspraken onder liggen, een zogenaamde verwerkersovereenkomst (delen met derden art. 28 lid 3);
-

De AVG en de rechten van de burgers

De AVG versterkt ook nadrukkelijk de positie van onze inwoners als het gaat om het verwerken van persoonsgegevens. Dat blijkt uit de volgende maatregelen in de AVG:

- Burgers mogen hun gegevens opvragen en inzien (art. 15 AVG) ;
- Burger hebben het recht om hun gegevens te laten wijzigen, als ze niet kloppen (art. 16 AVG);
- Burgers hebben het recht op vergetelheid, of te wel verwijdert te worden uit de bestanden (art. 17 AVG);
- Burgers hebben het recht op dataportabiliteit, of te wel het overdragen van gegevens van de ene profider naar de andere (art. 20 AVG);
- En, ze hebben recht op bezwaar maken tegen de verwerking van hun persoonsgegeven (art. 21 AVG).

[1] Onderzoeksburo dat politie, justitie, inlichtingendiensten en overheden kritisch volgt op het terrein van privacy.

Persoonsgegevens, wat zijn dat

Persoonsgegevens zijn gegevens die herleidbaar zijn tot een natuurlijk persoon. Vaak zijn dat voor de hand liggende gegeven zoals NAW-gegevens, leeftijd, kenteken van de auto en BSN. Maar duidelijk zal zijn dat we voor bepaalde beleidsvelden ook allerlei minder gebruikelijke persoonsgegevens verwerken. Denk maar eens aan inkomen/vermogen, arbeidsverleden, opleiding, gezondheid, opvoeding, huisvestingssituatie, psychische problemen. Dat we zorgvuldig om moeten gaan met de voor de hand liggende persoonsgegevens is essentieel, maar dat geldt nog in versterkte mate voor de persoonsgegevens waar je wat minder snel aan denkt.

Waar het gaat om informatie over ras, uiterlijke kenmerken, seksuele geaardheid/seksuele voorkeur, vakbond lidmaatschap of godsdienst mogen we, zoals de AVG in art 9 lid 1 aangeeft, al helemaal geen gegevens verzamelen, tenzij betrokkene daar uitdrukkelijk toestemming voor geeft.

Wettelijke grondslagen voor verwerking

De wettelijke grondslag voor het verwerken van persoonsgegevens is te vinden in art. 6 van de AVG. Hieronder worden ze beknopt weergegeven;

- Toestemming; betrokkene heeft specifiek toestemming gegeven, die overigens ook weer kan worden ingetrokken;
- Overeenstemming: de verwerking is noodzakelijk in verband met een overeenkomst waarbij betrokkene partij is;
- Wettelijke verplichting; het is wettelijk verplicht om persoonsgegevens te registreren en te verwerken;
- Vitaal belang: de verwerking is noodzakelijk om een persoon te beschermen;
- Algemeen belang: vanwege het openbaar gezag is de verwerking noodzakelijk;
- Gerechtvaardigd belang: de verwerking van persoonsgegevens is noodzakelijk, omdat dat zwaarder weegt dan de fundamentele vrijheid van betrokkene.

Voor elk product of taak die we als overheid uitvoeren, waarbij gebruik wordt gemaakt van persoonsgegeven, moet duidelijk zijn welke van deze grondslagen van toepassing is. In het Register van Verwerkingen (waarover straks meer) wordt die grondslag vermeld. Overigens geldt voor ons als gemeenten dat voor het overgrote deel de grondslag ‘wettelijke verplichting’ van toepassing is.

Interne privacy beleid uitgewerkt

Het interne privacy beleid wordt voor de gemeentelijke organisatie uitgewerkt op de onderdelen techniek, organisatie en medewerkers. Dit heeft overigens raakvlakken met het Informatieveiligheidsbeleid.

Techniek

Hierbij is het zaak om goede programmatuur te gebruiken, deze goed in te richten en te beveiligen. De werkprocessen die met de programmatuur worden uitgevoerd moeten zodanig zijn ontworpen en ingericht (privacy by design) , dat aan de eisen van privacy worden voldaan. Worden er onjuistheden geconstateerd of is er sprake van nieuwe regelgeving, dat moeten werk processen hierop worden aangepast.

Het Team I en F is verantwoordelijk de technische inrichting van de programmatuur/applicaties. Het vakteam (i.c. het betreffende Teamhoofd) is verantwoordelijk voor de juiste inrichting (of aanpassing) en uitvoering van het werkproces.

Voor informatieveiligheid wordt een geautomatiseerde ISMS[2]-tool gebruikt. Voor privacy wordt een privacy-tool gebruikt. Daarin worden privacy activiteiten (het register van verwerkingen, verwerkersovereenkomsten, datalekken, PIA's en verzoeken van inwoners) in vastgelegd.

Organisatie

Hier gaat het om het treffen van de nodige organisatorische maatregelen;

- Voorop staat dat er privacybeleid moet worden geformuleerd. Met dit stuk wordt hieraan voldaan.
- Voor overheden geldt dat er verplicht (art . 37 AVG) een functionaris gegevensbescherming (FG) moet worden aangesteld. Hierin is per 1-10-2017 voorzien.
- Informatieveiligheidsbeleid: de nota hierover is in maart 2018 vastgesteld. Op basis van de nota worden diverse maatregelen op het terrein van informatieveiligheid verder uitgewerkt en ingevoerd.
- Register van Verwerkingen: in artikel 30 van de AVG is opgenomen dat een register van verwerkingsactiviteiten moet worden ingericht. In dat register komen alle activiteiten en taken te staan waarbij verwerken van persoonsgegeven aan de orde is. En daarin is ook opgenomen wat de wettelijke grondslag is voor de verwerking, welke persoonsgegevens worden verwerkt en wat het doel is. Ook als er sprake is van externe verwerking van persoonsgegeven (en dus een verwerkersovereenkomst moet zijn) staat dat in dit register. Het register is openbaar, dus opvraagbaar door de inwoners. De FG houdt hier toezicht op.
- Autorisaties; het volgens de vastgestelde richtlijnen toekennen, toepassen en intrekken van toegang tot persoonsgegevens. De autorisatie kan onderscheid maken in inzage en bewerking. Per applicatie of organisatieonderdeel is het essentieel dat de autorisaties op orde zijn:
- Van alle persoonsgegevens zijn de bewaartermijnen vastgesteld. Hierna vindt vernietiging plaats. De FG oefent hierop toezicht uit;
- De privacy officer (PO) neemt de verzoeken van burgers (inlichtingen, verwijzingen, vergetelheid) is behandeling en administreert dit in de privacy-tool.
- Volgens de vastgestelde procedure worden datalekken gemeld bij de Ciso. De Ciso behandelt de lekken, meldt deze zonodig bij de AP en administreert ze in de privacy-tool.
- Verwerkingen van persoonsgegevens worden zoveel mogelijk gelogged[3]. De FG ontvangt hiervan periodiek en vertrouwelijk overzichten om mogelijk onregelmatigheden te kunnen

[2] Information Security Management Systeem

constateren. Eventueel passende maatregelen, naar aanleiding hiervan, worden genomen door het management, op basis van adviezen van de FG en unit P en O.
- Wanneer er nieuwe taken komen of bestaande taken opnieuw worden ingericht moeten privacy aspecten worden meegenomen (privacy by design).

Medewerkers

Er is veel te regelen in de techniek. Allerlei organisatorische maatregelen kunnen worden genomen, maar de belangrijkste factor blijft de medewerker. De medewerker moet zich ervan bewust zijn dat persoonsgegevens privacygevoelig zijn, dat hij gegevens alleen maar mag gebruiken voor het doel waarvoor de gegevens zijn verzameld, dat hij niet zomaar info aan de balie mag verstrekken en dat soms eerst toestemming moet worden gevraagd voor het verwerken van bepaalde persoonsgegevens. Veel zaken liggen vast in werkprocessen en instructies. Maar het mechanisch uitvoeren hiervan is niet genoeg, kennis van 'het waarom' moet ook aanwezig zijn. Daarom worden voor de medewerkers drie instrumenten gehanteerd:

- Scholing; medewerkers die persoonsgegevens verwerken worden periodiek geschoold. We proberen dat op een moderne en efficiënte manier te doen door het aanbieden van e-learing modules en beknopte workshops;
- DPIA; via een Data Privacy Impact Analyse vinden periodiek toetsen plaats van een dienst/product aan de privacy regels. Een dergelijke analyse verbetert en voorkomt niet alleen fouten, het verbetert werkprocessen maar houdt ook het bewustzijn bij medewerkers levend;
- Interne gedragscode: er komt een beknopte interne gedragscode die voor iedereen beschikbaar is en kan worden gebruikt in werkoverleg of waarderingsgesprek.

Externe beleidskeuzes

Naast intern beleid, dat zich vooral toespitst op onze organisatie en de dienstverlening aan de burger, komen we onder invloed van technische en maatschappelijke ontwikkelingen steeds meer voor keuzes te staan die extern doorwerken. Hierna behandelen we de vier privacy onderwerpen die in dit kader door VNG en KING[4] zijn aangedragen: dat zijn profilering, big data, tracking, doorgifte van informatie buiten de EU en inzet van camera's. Tot slot gaan we ook in op 'open data', de service en stimulering van de bewustwording richting onze inwoners.

PROFILERING

Profilering betreft 'het met behulp van persoonsgegevens maken van persoons profielen van inwoners om specifieke diensten aan te kunnen bieden'. Het gebruik van klantkaarten, het aanklikken van diensten op websites, het boeken van een reis of het bestellen van een boek, wat je kijkt op je smart-TV, alles wat je doet op het internet wordt gevolgd en vastgelegd en gebruikt om je doelgericht aanbiedingen te sturen of je te wijzen op publicaties of bepaalde websites. In de AVG

[3] Logging betekent dat geautomatiseerd wordt vastgelegd wie op welk moment in een systeem een handeling heeft verricht.
[4] Kwaliteits instituut Nederlandse Gemeenten, heet sinds 1-1-18 VNG-realisatie

staat duidelijk dat profilering niet mag (art. 22 lid 2 AVG) tenzij het noodzakelijk is, wettelijk is toegestaan of toestemming heeft van betrokkenen. Als gemeente Hellendoorn maken we nu geen gebruik van persoonsgegevens om profielen op te stellen met als doel om diensten aan te bieden. Ook stellen we geen persoonsgegevens beschikbaar aan derden, met als doel om profielen voor ons op te (laten) stellen.

Kernvraag hierbij is; is profilering voor de gemeente Hellendoorn noodzakelijk en/of in de toekomst zeer wenselijk. Die inschatting is niet zo eenvoudig te maken. Het is een logische verwachting dat het in de toekomst, zeker als je je realiseert welke gegevens we allemaal hebben, wat je er technisch en beleidsmatig mee zou kunnen, het verleidelijker wordt om aan profilering te gaan doen. Denk maar eens aan het gericht benaderen van inwoners die in aanmerking komen voor kwijtschelding.

Het voorstel is om profilering wel als mogelijkheid op te nemen in het privacy beleid, maar onder de volgende strikte voorwaarden;

- Profilering met behulp van persoonsgegevens doen we alleen wanneer de inwoners daar toestemming voor hebben gegeven. Dat kan aan de balie, of bij persoonlijk contacten of op onze website;
- Profilering richting de inwoners die toestemming hebben gegeven kan plaatsvinden als daar door het college vooraf een goed gemotiveerd besluit over is genomen waarin het volgende wordt gewogen;

  1. Zijn de te gebruiken gegevens van behoorlijke kwaliteit

  2. Wordt de privacy voldoende gewaarborgd bij het gebruik van de gegevens

  3. Dient de profilering ook echt een doel (bij de aanpak van een probleem of het verbeteren van een taak die we uitvoeren) en is daarmee goed te motiveren

  4. Wordt er zorgvuldige interne en extern gecommuniceerd over het doel, de aanpak en over wat we doen met de uitkomsten

  5. De Functionaris Gegevensbescherming (FG) oefent hierop toezicht uit en rapporteert zo nodig

Is profilering om de een of andere reden noodzakelijk of wettelijk toegestaan (conform art. 22.2 AVG) dan is het mogelijk om alle inwoners te benaderen, zonder dat daarvoor toestemming is gegeven. Maar, dan nog is het in het kader van een zorgvuldige werkwijze belangrijk om de punten 1 t/m 5 te hanteren.

BIG DATA EN TRACKING

Wat zijn big data en wat is tracking. Allereerst de Big data. We spreken over Big data wanneer we het hebben over heel veel gegevens, waarover we snel kunnen beschikken, uit verschillende databanken, die we zodanig kunnen bewerken en combineren dat er patronen uit zijn te halen. Bij tracking gaat het om verzamelen van locatie gegevens. Bijvoorbeeld via de signalen van de mobiele telefoon kan dan worden nagegaan hoeveel mensen er in een bepaald gebied zijn en hoe ze zich bewegen.

De situatie in Hellendoorn is als volgt: als het gaat om Big data is er binnen het sociaal domein een proef geweest om gecombineerd met externe bestanden en onze eigen gegevens, een sociale kaart te maken van wijken en buurten.

We passen tracking toe bij het meten van verkeersintensiteit op een bepaald weggedeelte. Verder wordt in het centrum van Nijverdal door 'Op naar Nijverdal' tracking toegepast om het aantal bezoekers te meten. Verder hanteren we een 'track en trace' systeem voor onze buitendienstvoertuigen en dienstauto's.

Het is dus helder dat we Big data en tracking gebruiken. Maar de voorwaarden waaronder kunnen worden aangescherpt. En die voorwaarden zijn:

- Big data en tracking gegevens zijn niet herleidbaar tot natuurlijke personen of een kleine groep natuurlijk personen
- Het doel waarvoor de gegevens worden verzameld en onderzocht moet vooraf duidelijk worden gemotiveerd
- De personen die toegang tot deze gegevens en de bewerking ervan zijn daartoe geautoriseerd
- Indien de gegevens aan derden worden verstrekt ligt daaronder een overeenkomst waarin vastligt voor welk doel de gegevens door deze derde mogen worden gebruikt, hoe ze mogen worden gebruikt en wanneer de gegevens door deze derde worden vernietigd
- De FG oefent hierop toezicht uit en rapporteer zo nodig

Ten aanzien van track en trace kan aanvullend nog het volgende worden opgemerkt;

- Bij de plaatsing van apparatuur in onze dienstvoertuigen, zijn adequate afspraken over privacy gemaakt. Deze zijn ook met de OR besproken;
- Dat geldt ook voor het monitoren van een wegvak; aan de voorkant is duidelijk aangegeven (ook in de lokale pers) welke privacy regels hierbij gelden;
- Waar het gaat om het scannen van mobiele telefoon in het centrum, om daar gegevens over koopstromen uit af te leiden, is voor zover bekend niets geregeld over de privacy. Op de site van 'op naar Nijverdal' is in ieder geval niets terug te vinden.

DOORGIFTE VAN GEGEVENS

Het kan voorkomen dat persoonsgegevens specifiek worden gevraagd door buitenlandse overheden of een internationale organisatie. Dan wordt er in de verordening (art. 44 t/m/ art. 50 AVG) onderscheid gemaakt tussen EU-landen en organisatie die alleen binnen de EU opereren en niet EU-landen en organisatie die ook buiten de EU werkzaam zijn.

Volgens de VNG zijn twee opties mogelijk:

- de gemeente geeft geen persoonsgegeven aan niet EU-landen en organisaties die ook buiten de EU-werkzaam zijn;

- de gemeente geeft alleen persoonsgegevens aan niet EU-landen en organisatie die ook buiten de EU werkzaam zijn, als er goedgekeurde afspraken onder liggen met de Europese Commissie.

In verband met toenemende globalisering en toenemende veiligheidseisen bij persoonsverkeer tussen landen (denk aan de visa regels bij het bezoeken van de USA) is het te verwachten dat in de toekomst uitwisselen van persoonsgegeven buiten de EU wel regelmatig voor zal kunnen komen. Het meest praktisch lijkt daarom het kiezen voor optie 2; gegevensuitwisseling kan wereldwijd plaatsvinden, mits dit gebeurt op grond van goedgekeurde afspraken door de Europese Commissie. Het gaat hier dus om specifieke verzoeken tot uitwisselingen en niet om automatische uitwisseling van gegevens. Dat laatste is niet aan de orde.

INZET VAN CAMERA'S

De gemeente Hellendoorn maakt gebruik van cameratoezicht. Primair in de openbare ruimte zoals in de omgeving van het NS station in Nijverdal en het Componistenplein. Maar er hangen ook camera's in semi openbare ruimten zoals de hal van het Huis voor Cultuur en Bestuur, de parkeergarage Henri Dunant en ZSZ Het Ravijn. In deze beleidsnotitie gaat het om cameratoezicht in de openbare ruimte.

Gebruik van camera's om toezicht te houden vindt z'n juridische grondslag in artikel 151c van de Gemeentewet. Daarin staat dat de raad bij verordening de burgemeester de bevoegdheid verleent om voor een bepaalde duur in een bepaald gebied cameratoezicht in te zetten. In lid 1 van dit artikel wordt daarvoor de volgende inhoudelijk grondslag genoemd: Belang van handhaving van de openbare orde.

We gebruiken dus camera's in de openbare ruimte. Maar wat zijn dan de voorwaarden waaronder dat plaats vindt? In de diverse stukken zijn de volgende terug te vinden;

- Het doel om cameratoezicht toe te passen moet vooraf helder worden aangegeven door de burgemeester. Dat kunnen (al dan niet gecombineerd)zijn:
    - Effectiever kunnen handhaven in dat deel van de openbare ruimte
    - Vergroten van het veiligheidsgevoel van gebruikers van die ruimte
    - Preventie ten aanzien van overlast door (jeugd) groepen
    - Preventie ten aanzien van (fietsen) diefstal of andere incidenten
- De gegevens (de opnames) mogen alleen voor het aangegeven doel worden gebruikt (zie ook art. 2 Reglement cameratoezicht en art. 5 lid 1 AVG)
- In het bepaalde gebied wordt helder aangegeven (met bordjes) dat cameratoezicht van toepassing is
- Ook via de reguliere communicatiekanalen wordt actief aangegeven waar, waarvoor en voor welke duur cameratoezicht wordt toegepast
- Bij de communicatie over de toepassing van camera's moet ook duidelijk worden aangegeven dat het Reglement cameratoezicht van toepassing is. In dit reglement gaat het onder meer over privacy aspecten, verstrekking van beelden aan derden en de bewaarduur van de beelden.
- De Functionaris Gegevensbescherming (FG) houdt hierop toezicht.

Het Hellendoornse reglement cameratoezicht, dat uit 2011 stamt, is juridisch gedateerd en verdient daarom een actualisatie. Dit wordt opgenomen in de werkplanning.

OPEN DATA

Voor de definiëring van dit begrip is aansluiting gezocht bij de termen die het Platform Open Data hanteert: open data zijn gegevens die vrij gebruikt kunnen worden, hergebruikt kunnen worden en opnieuw door iedereen verspreid kunnen worden. De gegevens zijn geautomatiseerd verkrijgbaar. Ook wij beschikken over veel data, maar die zijn vrijwel nog niet 'open', dat wil zeggen, zo van onze site af te plukken. Maar het is wel een ontwikkeling die eraan zit te komen, de interesse van bedrijven hiervoor neemt toe. Als gemeente hebben we een taak als het gaat om het hergebruik van overheidsgegevens. In de wet hergebruik overheidsgegevens is daarover het nodige geregeld. Het belangrijkste daarbij is dat open data niet herleidbaar zijn naar persoonsgegevens. Daarmee zou de privacy immers kunnen worden geschaad. Verder is het bij open data belangrijk dat aan zekere kwaliteitseisen wordt voldaan; hoewel dit geen wettelijke eis is het zaak 'open data' beschikbaar te stellen als ze betrouwbaar zijn en duidelijk is uit welke periode de gegevens komen.

COOKIES

Op veel sites wordt vooraf de vraag gestemd of de bezoeker ermee instemt dat cookies worden gehanteerd. Dan gaat het om cookies die het gedrag van de bezoeker registreren, zogenaamde tracking cookies. Als gemeente gebruiken we op onze website alleen functionele cookies (zoals google analytics) die slechts geanonimiseerd gegevens verzamelen. We gebruiken dus geen tracking cookies. Daarom hoeven we hiervoor geen toestemming te vragen op onze site.

INFORMATIE EN SERVICE AAN ONZE INWONERS

Als overheid hebben we ook een rol in de bewustwording van onze inwoners als het gaat om privacy. De rijksoverheid doet dat met radio en TV-spotjes. Maar ook voor ons is het mogelijk om op een praktische manier hieraan een bijdrage te leveren. Wij denken daarbij aan het volgende;

- Op onze site staat een helder statement hoe we met persoonsgegevens omgaan (het privacy statement)
- Bij de uitreiking van nieuwe identiteitsdocumenten ontvangt men een aantal tips om identiteitsfraude te voorkomen
- Op onze (web) formulieren staat duidelijk voor welke gegevens vooraf toestemming moet worden gegeven om ze te mogen verwerken
- Zo nodig wordt op de website toestemming gevraagd voor het gebruik van cookies
- Op onze (web) formulieren staat een verwijzing naar het privacy statement
- In de gesprekken met inwoners (telefoon, spreekkamer of balie) wordt gewezen op de privacyregels.

Privacy statement

Op basis van de AVG is het verplicht om een privacy verklaring te hebben wanneer de website persoonsgegevens verwerkt. Bij ons is dat het geval. Bij het invullen van diverse formulieren op het e-loket worden persoonsgegevens gevraagd. Dus, wij moeten een privacy statement vaststellen.

Het privacy statement komt aan het einde in deze nota aan de orde, omdat het het sluitstuk is van de inhoudelijke discussie over hoe je als gemeente met de privacy en persoonsgegevens van je inwoners om wilt gaan. Het statement is als bijlage bijgevoegd.

Training en scholing van medewerkers

Privacy is net als informatieveiligheid en integriteit, je moet er constant alert op zijn, en regelmatig aandacht voor vragen in de organisatie. Eind 2017 en in het eerste kwartaal van 2018 is er veel aandacht geweest voor informatieveiligheid, door een aftrapbijeenkomst en e-learning-modules. Hierbij zijn aspecten van privacy ook aan de orde gekomen. Zoals al eerder aangegeven willen we voor iedereen via e-learning een basismodule over privacy laten volgen. Voor de medewerkers van het KCC en voor medewerkers die heel veel met (bijzondere) persoonsgegevens werken volgt er een verdiepingsslag.

Samen met het unit P en O werken we uit hoe op de langere termijn de kennis over privacy in de organisatie kan worden geborgd. Belangrijk daarbij is het instrueren van tijdelijke en nieuwe medewerkers.

Organisatie en verantwoording

Hieronder worden de formele rollen en verantwoordelijkheden ten aanzien van privacy van de verschillende onderdelen en functies binnen de gemeente op hoofdlijnen beschreven.

Gemeenteraad
De gemeenteraad stelt waar nodig en op hoofdlijnen de kaders vast voor privacy en gegevensverwerking, inclusief de bijhorende middelen. De raad controleert het college van B & W ten aanzien van de uitvoering. Een en ander gebeurt als onderdeel van de jaarlijkse programmabegroting en jaarrekening.

College van B en W
Het college is integraal verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens. Het college komt zonodig met voorstellen richting de raad over beleidskaders en de benodigde middelen (via de begroting). Via de jaarrekening en de bestuursrapportages informeert het college de raad over de voortgang en de resultaten.

Management
Het management is verantwoordelijk voor de inrichting en de uitvoering van de maatregelen inzake privacy. Belangrijke onderdelen daarvan zijn het actueel houden van het register van verwerkingen, het melden van datalekken en aanpassen van werkprocessen.

Functionaris gegevensbescherming
De Functionaris Gegevensbescherming houdt toezicht op de naleving van de privacy regelgeving, de uitvoering van aanbevelingen uit de Privacy Impact Assessments en is contacpersoon voor de Autoriteit persoonsgegevens. Verder rapporteert de FG periodiek aan het college en het Management.

Chief Information security officer
De Ciso houdt toezicht op de informatiebeveiliging en rapporteert hierover aan het management en het college. Hij adviseert over het beleid en bewaakt de voortgang van de uitvoering van voorgestelde verbetermaatregelen uit onderzoeken en audits.

Adviseur Privacy/Privacy officer
Ondersteunt en adviseert het management over privacyvraagstukken, het afsluiten van bewerkersovereenkomsten en vragen van burgers.

Bijlagen

Afkortingen

Privacy statement

Versie 03-05-2018

F. Dijkstra