Algemeen privacybeleid gemeente Katwijk 2.0

Versie: 2.0
Juni 2017
Vastgesteld in B&W op 11 juli 2017

Inhoud

1.Inleiding

De gemeente Katwijk verwerkt ter uitvoering van de aan haar opgedragen publieke taken persoonsgegevens van haar inwoners, bedrijven en medewerkers in de volgende domeinen:
Dienstverlening;
Samenleving;
Bedrijfsvoering en
Wonen en Fysieke leefomgeving.

In het domein Dienstverlening gaat het bijvoorbeeld om gegevens uit de basisregistratie personen (naam, adres, woonplaats, Burgerservicenummer).
In het Domein Samenleving om medische en strafrechtelijke gegevens. In het domein Bedrijfsvoering om gegevens van medewerkers van de gemeente zoals sollicitatiegegevens (brief, formulier, CV, referenties, getuigschrift), maar ook gegevens over ziekte en arbeidsongeschiktheid. In het domein Wonen en Fysieke leefomgeving gaat het tenslotte om naam, adres, woonplaats gegevens bij verstrekte vergunningen en meldingen openbare ruimte maar ook om medische en strafrechtelijke gegevens bij bijv. het casusoverleg jeugd.

Bij gegevensbescherming gaat het om het zorgvuldig, veilig en doelmatig verwerken van persoonsgegevens. Het verwerken van persoonsgegevens omvat alle handelingen in die met persoonsgegevens uitgevoerd kunnen worden zoals het verzamelen, vastleggen, bewaren, wijzigen, opvragen, gebruiken en inzien[1].
Persoonsgegevens zijn de gegevens over een geïdentificeerde of identificeerbaar persoon. Zoals een naam, adresgegevens of een e-mailadres. Maar ook indirecte gegevens kunnen persoonsgegevens zijn, zoals bijvoorbeeld een kentekenplaat op een voertuig of een Burgerservicenummer (BSN).
Privacy is samenvattend te omschrijven als respect voor de persoonlijke levenssfeer van een individu. Om te voorkomen dat een onnodige of te vergaande inbreuk wordt gemaakt op de persoonlijke levenssfeer, is onder meer bij wet voorzien in waarborgen.

De gemeente Katwijk hecht er veel waarde aan dat de verwerkingen van persoonsgegevens zorgvuldig, rechtmatig en veilig plaatsvinden. Het college van Katwijk heeft daarom besloten algemeen privacybeleid te formuleren hoe om te gaan met de verwerking van persoonsgegevens.

In dit algemeen privacybeleid staan kaders beschreven voor het verwerken van privacygevoelige informatie of te wel persoonsgegevens, de bescherming van deze gegevens en omgang met deze gegevens. De kaders gelden voor de gemeente, samenwerkingsverbanden die zijn of worden aangegaan en derden die zijn of worden ingeschakeld. Dit beleid dient als kapstok waaraan voor een specifiek vakgebied een beheerplan of privacyprotocol[2] gehangen kan worden.

Het beschermen van persoonsgegevens kan niet geborgd worden zonder adequate informatiebeveiliging. Het beleid gegevensbescherming hangt daarom samen met het Informatiebeveiligingsplan Katwijk.

[1] Voor de volledige omschrijving zie artikel 1 Wbp/4 AVG
[2] Dit zijn onder andere het privacyprotocol Jeugd, het beveiliggingsplan Suwinet, het beveilingshandboek BRP, het beveilingshandboek Reisdocumenten

2.Uitgangspunten

2.1. Visie op gegevensbescherming

Het uitgangspunt van het privacybeleid is, dat de gemeente respect heeft voor de persoonlijke levenssfeer van haar inwoners, ondernemers en medewerkers. Informatie wordt niet langer bewaard dan nodig voor het doel waarvoor deze is verzameld en niet gebruikt voor doelen die hier niet mee verenigbaar zijn. Het zal bijdragen aan effectieve en efficiënte dienstverlening zowel intern als extern. Ook zal het een vernieuwende manier van (samen) met andere gemeenten en derde partijen ondersteunen, maar blijft daarbij binnen de wettelijke vereisten.

2.2. Reikwijdte

De kaders die in dit algemeen privacybeleid staan beschreven gelden voor iedereen (zowel intern als externe bewerkers/verwerkers[3]) die gegevens verwerken.

2.3. Juridisch kader

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkene(n) voorop. Er moet voorkomen worden dat er onnodige of te vergaande inbreuken worden gemaakt. De Wet bescherming persoonsgegevens (hierna: Wbp) biedt hiervoor het wettelijk kader. Vanaf 1 januari 2016 is de Wbp uitgebreid met de meldplicht datalekken. Per 25 mei 2016 is de EU Algemene Verordening Gegevensbescherming (AVG) in werking treden. Er geldt een overgangstermijn van twee jaar. De AVG heeft als doel om de privacy van Europese burgers beter te beschermen dat de Wbp nu doet. Wanneer de overgangstermijn van de AVG is verstreken, zal deze boven de Wbp komen te staan.

Als algemene regel geldt dat persoonsgegevens op behoorlijke en zorgvuldige wijze moeten worden verwerkt. De Wbp bepaalt verder dat persoonsgegevens alleen voor een specifiek doel mogen worden verzameld en gebruikt. Maar ook dat deze gegevens niet langer mogen worden bewaard dan noodzakelijk om het doel waarvoor ze zijn verzameld, te realiseren. De betrokkene kan altijd inzage of wijziging van de verwerkte persoonsgegevens vragen.
Om het proces van gegevensverwerking ordelijk te laten verlopen en betrokkenen makkelijk toegang te geven tot de gemeente moet een functionaris gegevensbescherming worden aangesteld.

Gegevensbescherming kan alleen gerealiseerd worden door borging van de informatieveiligheid. Voor de informatieveiligheid werkt de gemeente binnen de kaders van het Strategisch- en Tactisch beleid, het Informatiebeveiligingsplan en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

In aanvulling daarop, of in voorkomende gevallen ter aanvulling van de Wbp, bevat andere wetgeving meer specifieke vereisten voor gegevensverwerking[4].
De gemeente heeft de wettelijk verplichting om gegevensbescherming te borgen. Dit moeten zij doen door technische en organisatorische maatregelen te treffen[5]. Dit beleid geeft formele kaders aan de verplichtingen en bevoegdheden die uit de Wbp en AVG voortvloeien.

[3] Zie artikel 1 Wbp/14 AVG voor uitwerking
[4] Dit zijn onder andere de wet Basisregistratie Personen, de wet Suwi, de Wmo, de Jeugdwet.Wet politiegegevens, Wet Justitiele en strafvordelijke gegevens, Archiefwet (bewaartermijnen) en de Telecomwet.
[5] zie artikel 13 Wbp/15AVG

2.4. Ingangsdatum

Vanaf 1 juli 2017 wordt er begonnen om de beschreven kaders invulling te geven.
Elke twee jaar zal het beleid gegevensbescherming worden geëvalueerd en waar nodig bijgesteld.

3.Governance

3.1. Verantwoordelijke

Het college van burgemeester en wethouders is verantwoordelijk voor gegevensverwerking en informatiebeveiliging. Ook de gemeenteraad of de burgemeester zijn voor specifieke taken verantwoordelijk, zoals het vaststellen van een bestemmingsplan of vergunningprocedures voor activiteiten en evenementen in de openbare ruimte.

3.2. Verantwoording aan de Gemeenteraad

Net zoals het college verantwoording moet afleggen over de gemeentelijk uitgaven, wordt ook verantwoording afgelegd over de realisatie van beleid. Dit geldt ook voor het privacybeleid en de toepassing daarvan. Het privacybeleid wordt om die reden onderdeel van de Planning & Controll cyclus.

Met ingang van 2017 neemt het college in de programmabegroting, een passage op over het privacybeleid. Als voorbereiding op de AVG wordt het privacybeleid elk jaar, geauditeerd.

Het afleggen van jaarlijkse verantwoording doet overigens niet af aan de algemene informatieplicht van het college en de burgemeester afzonderlijk.[6] Het college meldt bijzonderheden ten aanzien van gegevensverwerking, te denken valt aan ernstige inbreuk op of verlies van persoonsgegevens, afzonderlijk en proactief aan de raad. Binnen het college is er ook een wethouder verantwoordelijk gemaakt voor informatiebeveiliging en privacy.

3.3. Wijze van inrichten gegevensverwerking

De verantwoordelijkheid voor de uitvoering van het beleid is bij de afdelingshoofden van de verschillende afdelingen binnen de gemeente Katwijk belegd. Hiervoor is het door de gemeente Katwijk vastgestelde organogram leidend. Elk afdelingshoofd is verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar afdeling plaatsvindt. Zo nodig geeft een afdelingshoofd aan deze verantwoordelijkheid invulling door taken verder in zijn afdeling te beleggen. Indien een verwerking een afdelingsoverstijgend karakter heeft en betrekking heeft op twee of meer afdelingen ligt de verantwoordelijkheid bij de betreffende proceseigenaar.

Het borgen van de privacy is onlosmakelijk verbonden met informatiebeveiliging. Om versnippering van beleid te voorkomen en afdelingen te ondersteunen zullen experts ingezet worden op het gebied van gegevensverwerking en informatiebeveiliging. Deze experts werken nauw met elkaar samen. In de onderstaande alinea's wordt de expert ondersteuning beschreven.

[6] Artikelen 169, lid en 180, lid 2 van de Gemeentewet.

3.3.1. Expert ondersteuning: functionaris gegevensbescherming (privacy officer)

Vanwege het grote belang dat de gemeente Katwijk hecht aan privacybescherming en ter voorkoming van versnippering van het beleid, zal uiterlijk per 1 mei 2018 een functionaris gegevensbescherming worden aangesteld.[7] De functionaris gegevensbescherming heeft een onafhankelijke positie in de organisatie. De werkzaamheden die een functionaris gegevensbescherming uitvoert hebben een wettelijke grondslag[8].

De functionaris gegevensbescherming zal de volgende werkzaamheden uitvoeren:

- houdt toezicht op de naleving van de uit de Wbp, en in de toekomst AVG, voortvloeiende eisen en controleert of de uitgezette acties ook daadwerkelijk worden uitgevoerd;
- informeert en adviseert de verantwoordelijke en bewerkers over hun verplichtingen op grond van de Wbp en in de toekomst de AVG alsmede over technologie en beveiliging van de gegevensverwerking;
- maakt de organisatie en medewerkers bewust van het belang van privacybescherming;
- houdt toezicht op de implementatie en toepassing van het beleid gegevensbescherming en ziet toe op de effectieve werking hiervan;
- ziet erop toe dat de gemeente een privacyboekhouding bijhoud en aan haar documentatieplicht voldoet door o.a:
    - een register bij te houden van de verschillende meldingsplichtige gegevensverwerkingen, de processen waar persoonsgegevens verwerkt worden en de door de gemeente gesloten bewerkersovereenkomsten, convenanten en vastgestelde privacyprotocollen);
    - dat inbreuken in verband met persoonsgegevens (incidenten) worden gedocumenteerd.
- erop toezien dat inbreuken in verband met persoonsgegevens (incidenten) worden geanalyseerd en wanneer nodig gemeld bij toezichthouder en betrokkene(n);
- adviseert gevraagd en ongevraagd in specifieke kwesties of bij de totstandkoming van nieuw beleid of wet- en regelgeving;
- ziet toe op naleving en behandeling van vragen en klachten over persoonsgegevens;
- voert analyses[9] uit en coördineert de nodige vervolgacties;
- treft maatregelen bij calamiteiten of geconstateerde gebreken;
- rapporteert periodiek en bij calamiteiten aan het college van burgemeester en wethouders;
- is contactpersoon voor de Autoriteit Persoonsgegevens (AP).

Om ervoor te zorgen dat de uitvoering van het beleid gegevensbescherming niet stagneert totdat een functionaris gegevensbescherming is aangesteld, wordt de uitvoer van het beleid thans projectmatig opgepakt. Het plan van aanpak is nog in bewerking maar hierin is ook nadrukkelijk aandacht voor bewustwording binnen de organisatie.

3.3.2. Expert ondersteuning: coördinator informatiebeveiliging

Gegevensbescherming kan niet geborgd worden zonder adequate informatiebeveiliging. De coördinator informatiebeveiliging (= de concernadviseur informatiehuishouding) draagt zorg voor de informatiebeveiliging. De werkzaamheden die de coördinator informatiebeveiliging uitvoert worden beschreven in het Informatiebeveiligingsplan Katwijk .

[7] Hiermee wordt gedoeld op de functionaris voor de gegevensverwerking als bedoeld in artikel 37 AVG.

[8] Artikelen 37 t/m 39 AVG

[9] Bijvoorbeeld een Privacy Impact Analyse (PIA), artikel 35 AVG

3.3.3. Sturing en monitoring

Elk afdelingshoofd is verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar afdeling plaatsvindt. Zij zijn daarom ook verantwoordelijk om te monitoren of persoonsgegevens zorgvuldig verwerkt worden, en dit zo nodig bij te sturen.

De functionaris gegevensbescherming en coördinator informatiebeveiliging hebben de verantwoordelijkheid om structureel te toetsen of de wettelijke eisen en de gemeentelijk richtlijnen op het gebied van privacy en informatiebeveiliging zijn geïmplementeerd en worden uitgevoerd. Hoe zij dit doen staat beschreven in hoofdstuk 5 Waarborgen voor gegevensbescherming.

3.4. Bewerkersovereenkomst met derden

Bij veel gemeentelijke processen worden gegevens verwerkt door derden[10] . Denk hierbij aan werkzaamheden die uitgevoerd worden door die in een Cloudleveranciers maar ook aan uitbestede werkzaamheden of samenwerkingsverbanden.

Het delegeren van werkzaamheden aan derden brengt risico's met zich mee op het gebied van gegevensverwerking en informatiebeveiliging. Het college van burgemeester en wethouders blijft verantwoordelijk voor de verwerking van de gegevens. Zij moeten er daarom op toezien dat gegevens juist verwerkt [11]en beveiligd worden.

De Wbp en AVG schrijven voor dat er passende technische en organisatorische beveiligingsmaatregelen getroffen worden om de gegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking[12] . In de Wet meldplicht datalekken wordt van de verantwoordelijke verwacht dat hij overzicht en inzicht heeft in alle gegevensverwerkingen waar hij verantwoordelijk voor is. Naast deze wetten bevat andere wetgeving soms specifieke eisen voor gegevensverwerking door derden. Zo geldt, wanneer er persoonsgegevens verwerkt worden, ook artikel 4.1 van de Wet Basisregistratie Personen (BRP).

Om aan de wettelijke vereisten te voldoen moeten afspraken met derden vastgelegd worden in een contract. Afspraken over gegevensverwerking worden vastgelegd in een bewerkersovereenkomst. De gemeente hanteert in principe de standaard bewerkersovereenkomst van IBD.

Het afdelingshoofd die een dergelijke uitbesteding, samenwerking of uitwisseling aangaat, ziet toe op de totstandkoming van deze afspraken. De functionaris gegevensbescherming wordt bij de totstandkoming betrokken en ziet toe op de naleving daarvan.

3.5. Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag wordt aangemoedigd. Onderdeel van dit privacybeleid zijn daarom ook regelmatig terugkerende bewustwordingscampagnes voor medewerkers van de gemeente Katwijk. Deze campagnes kunnen aansluiten bij andere beveiligingscampagnes.

[10] Zie voor betekenis artikel 1Wbp/4 AVG
[11] Zie artikel 14 Wbp/32 AVG
[12] Zie artikel 14 en 77 Wbp/32 AVG en 49 AVG

4.Werkprocessen

4.1. Omgaan met persoonsgegevens

Persoonsgegevens worden alleen verwerkt voor het uitvoeren van bepaalde wettelijke taken en vastgestelde regelingen. Dit ter uitvoering van de in de Wbp en AVG voorgeschreven doelbinding en proportionaliteit. Dit houdt in dat persoonsgegevens alleen voor specifieke, uitdrukkelijke en legitieme doeleinden mogen worden verzameld en dat er niet meer persoonsgegevens worden verwerkt dan voor het doel nodig is.

In het merendeel van de gevallen worden persoonsgegevens door de betrokkene zelf verstrekt. Veel gebruikte gegevens of al bekende gegevens die zijn opgenomen in basisregistraties of andere authentieke bronnen, worden daaruit opgevraagd[13] . Dit is in overeenstemming met het principe van 'eenmalige uitvraag en meervoudig gebruik' dat door de overheid en de gemeente wordt gepropageerd. Wanneer voor het uitvoeren van bepaalde wettelijke taken en regelingen persoonsgegevens verwerkt moeten worden, dan worden deze gegevens opgevraagd uit de basisregistratie personen[14] .

Wat er precies met de verzamelde gegevens gebeurt, is afhankelijk van het doel waarvoor ze verzameld worden. Meestal worden ze in een informatiesysteem opgenomen waar ze alleen toegankelijk zijn voor de medewerkers die belast zijn met het uitvoeren van de taak. Gegevens worden niet zonder toestemming van de betrokkene of wettelijke grondslag gedeeld. Informatiesystemen moeten voldoen aan de eisen van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Bijzondere gegevens[15] worden niet verwerkt, tenzij dit nodig is voor het uitvoeren van een wettelijke taak of regeling. Zo kunnen op grond van de Jeugdwet of de Wet maatschappelijke ondersteuning medische- en gezondheidsgegevens worden gebruikt bij de behandeling van een hulpvraag of een ondersteuningsverzoek.

4.2. Meldplicht datalekken

Vanaf 1 januari 2016 is de Wet meldplicht datalekken in werking getreden. Dit is een aanvulling op de Wbp. Een datalek is een inbreuk op de beveiliging, waarbij een kans bestaat dat dit ernstige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van de persoonsgegevens. Hierbij kan gedacht worden aan het kwijtraken van een USB stick met persoonsgegevens, inbraak door een hacker, maar ook onbevoegde autorisaties in een informatiesysteem.

De gemeente is verplicht om datalekken te melden bij het AP. Het gaat hier om datalekken waar de gemeente voor verantwoordelijk is. Daaronder vallen ook datalekken die ontstaan bij een derde partij die werkzaamheden uitvoert voor de gemeente. De AP is bevoegd om datalekken te beboeten. Om aan deze wet te kunnen voldoen worden de volgende maatregelen getroffen:

- er wordt een procedure voor goed incidentbeheer ingericht,
- er worden richtlijnen bepaald waaraan informatiesystemen moeten voldoen om gegevensbescherming te borgen. Deze richtlijnen zullen gelden voor nieuwe en bestaande informatiesystemen,
- alle gegevensverwerkingen waar persoonsgegevens worden verwerkt worden in beeld gebracht en vastgelegd. Dit geldt voor zowel interne gegevensverwerking als bij bewerkers,
- er wordt vastgelegd hoe betrokkene(n) worden geïnformeerd bij een datalek,
- er wordt vastgelegd hoe de gemeente omgaat met signalen over mogelijke datalekken
- de afspraken met bewerkers worden geëvalueerd en bijgesteld waar nodig.

[13] Dit zijn gegevens zoals persoonsgegevens, gezinssamenstelling, adresgegevens, bedrijfsgegevens, inkomen, uitkeringen, onderwijsgegevens, zorgindicaties ect.

[14] Zie artikel 1.7 BRP.

[15] Zie artikel 18 en 21 t/m 23 Wbp (9 t/m 11 AVG)

4.3. Bewust omgaan met persoonsgegevens

Gegevensbescherming wordt niet alleen geborgd door het uitvoeren van analyses, checklists en het maken van maatregelen. Het is ook van belang dat er bewust met persoonsgegevens wordt omgegaan.

De gemeente vindt het heel belangrijk dat haar medewerkers bewust met persoonsgegevens omgegaan. Om bewustwording te realiseren is kennisoverdracht nodig. De functionaris gegevensbescherming en de coördinator informatiebeveiliging zullen ervoor zorgen dat informatie over gegevensbescherming en informatiebeveiliging herhaaldelijk onder de aandacht wordt gebracht van afdelingshoofden en medewerkers.

4.4. Bewaren van gegevens

De Wbp en AVG schrijven voor dat gegevens niet langer bewaard mogen worden dan het doel waar ze voor nodig zijn[16]. Dit doel wordt beschreven in de wet, daarom lopen de bewaartermijnen van persoonsgegevens uiteen. In diverse wetten zijn minimale en maximale bewaartermijnen opgenomen. Daar waar er geen wettelijke regeling is die voorziet in een verplichte bewaartermijn, kan het college een besluit over de bewaartermijn nemen. Daarnaast geldt de Archiefwet voor het bewaren van papieren en elektronische documenten.

Voor vernietiging van gegevens is altijd een getekend proces verbaal van vernietiging van de gemeentearchivaris vereist. Bij het overbrengen van te bewaren gegevens naar de archiefbewaarplaats van de gemeente is het mogelijk om privacygevoelige gegevens van openbaarheid uit te zonderen voor een periode van maximaal 75 jaar.

4.5. Toestemming

Een rechtstreeks gevolg van het uitvoeren van wettelijke taken en regelingen is het verwerken van persoonsgegevens. Een betrokkene moet daarom inzien dat wanneer er een melding of aanvraag gedaan wordt, dit gepaard gaat met verwerking van zijn/haar gegevens. Het is hierom van belang dat de gemeente betrokkene informeert hoe zijn of haar gegevens verwerkt worden.

In sommige situaties kan het nodig zijn dat gegevens gedeeld worden. Het delen van deze gegevens wordt niet uitgevoerd zonder toestemming of wettelijke grondslag.
Hierbij worden de aanbevelingen uit het onderzoeksrapport van de AP over de rol van toestemming[17]meegenomen.

4.6. Open communicatie

Voor de gemeente is het heel belangrijk dat inwoners en ondernemers erop kunnen vertrouwen dat wij zijn of haar persoonsgegevens zorgvuldig verwerken. Dat vertrouwen wordt gecreëerd door inzichtelijk te maken welke wijze gegevens worden verwerkt en beheerd[18]. Hierbij wordt duidelijk:
1. welke gegevens worden verzameld,
2. waarom deze gegevens worden verzameld,
3. wat vervolgens met deze gegevens gebeurt,
4. wie toegang heeft tot deze gegevens,
5. welke rechten inwoners en ondernemers hebben.

Dit wordt vastgelegd in privacyprotocollen.

[16] Zie artikel 10 Wbp/5 AVG
[17] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toestemmingsrapport_definitief_incl_bijlagen.pdf
[18] Informatie over gegevensverwerking wordt via de website en door middel van folders beschikbaar gesteld.

Open communicatie staat dus voorop maar is niet absoluut. In uitzonderingsgevallen kan de gemeente besluiten om vertrouwelijk persoonsgegevens te verwerken. Dit kan bijvoorbeeld het geval zijn bij kwesties van openbare orde en veiligheid, zoals bij het vervolgen, voorkomen en opsporen van een strafbaar feit[19] .

Elke aanleiding voor gegevensverwerkingen wordt gedocumenteerd.

5. Waarborgen voor gegevensbescherming

De Wbp en AVG bevatten geen verplichtingen over de manier hoe de gegevensbescherming geborgd moeten worden. De Wbp geeft aan dat er technische en organisatorische maatregelen getroffen moeten worden[20] . Er zijn verschillende instrumenten om gegevensbescherming te waarborgen. In dit hoofdstuk wordt uitgelegd wat de verschillende instrumenten zijn.

5.1. Privacy Impact Assessment

Bij de invoering van nieuw beleid of regelgeving wordt de bescherming van de persoonlijke levenssfeer mee gewogen. Eén van de instrumenten om dit te doen, is de uitvoering van een Privacy Impact Assessment[21] (PIA). Waar het bijvoorbeeld om de uitvoering van nieuwe taken of de aanleg van nieuwe informatiesystemen gaat, kan het wenselijk zijn vooraf een PIA uit te voeren. Het college beoordeelt de noodzaak daartoe van geval tot geval.

De volgende indicatoren worden daarbij als toetsingskader gehanteerd:

- een nieuwe of veranderde gemeentelijke taak,
- aanleg van een groot databestand,
- verwerking van bijzondere persoonsgegevens,
- aanschaf van een nieuw informatiesysteem,
- systematische gegevensuitwisseling met een derde.

5.2. Dataclassificatie

De maatregelen die getroffen moeten worden om de gegevensbescherming te kunnen borgen[22], zijn niet voor elk proces en informatiesysteem hetzelfde. Hierom is het nodig dat alle processen en informatiesystemen die gegevens verwerken een dataclassificatie ontvangen. Dataclassificatie heeft als doel om de continuïteit, integriteit en vertrouwelijkheid van het proces en het informatiesysteem te benoemen. Dit maakt inzichtelijk welke maatregelen genomen moeten worden om de gegevens die verwerkt worden te beschermen.

De functionaris gegevensbescherming en coördinator informatiebeveiliging voorzien elk proces en informatiesysteem van dataclassificatie zoals deze is voorgeschreven door de Informatiebeveiligingsdienst [23]

5.3. Logging van gegevensgebruik

Elk geautomatiseerde systeem dat persoonsgegevens verwerkt, moet logging bijhouden van de verwerkingen. In deze logging staat minimaal vermeld welke gebruiker, op welke moment, welke gegevens heeft verwerkt.

---

[19] zie artikel 43 Wbp/23 AVG

[20] Zie artikel 13 Wbp/4 AVG

[21] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacycheck/privacy-impact-assessment-pia

[22] Denk hierbij aan encryptie van gegevens, bewaartermijnen, wachtwoord vereisten

[23] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2016/08/18-0312-handreiking-dataclassificatie-1-7.pdf

Logging houdt in:

- chronologische registratie van gegevens over van belang zijnde gebeurtenissen, die zich gedurende een periode in een verwerking voordoen,
- het vastleggen in een log, bijvoorbeeld een systeem log of een security log, van feitelijk uitgevoerde bewerkingen en/of pogingen daartoe.

5.4. Informatiebeveilingsplan Katwijk

Het kunnen borgen van de privacy kan niet gerealiseerd worden zonder adequate informatiebeveiliging. Het beleid gegevensbescherming hangt samen met het Informatiebeveilingsplan Katwijk. Het Informatiebeveiligingsplan Katwijk is op 9 mei 2017 vastgesteld door het college van burgemeester en wethouders en is gebaseerd op de richtlijnen van de BIG. Het Informatiebeveiligheidsplan Katwijk zal jaarlijks worden geëvalueerd.

In dit het beveiligheidsplan staan beveiligingseisen opgenomen die gelden voor informatiesystemen[24], gedragscodes en richtlijnen hoe de ambtelijke organisatie moet omgaan met privacygevoelige informatie en de fysieke maatregelen die noodzakelijk zijn[25].

5.5. Melding gegevensverwerking AP

In een aantal gevallen is het wettelijk verplicht om bij de AP te melden dat er persoonsgegevens verwerkt worden[26]. Een organisatie moet elke verwerking van persoonsgegevens melden, bijvoorbeeld wanneer de organisatie persoonlijke gegevens opvraagt, gebruikt of verspreidt[27]. De meldingen van de verwerking van persoonlijke gegevens zijn openbaar, dit is geregeld in de Wbp. In de melding staat wat een organisatie met welke gegevens doet en aan wie de gegevens worden verstrekt.

De functionaris gegevensbescherming houdt intern toezicht op de verwerking van persoonsgegevens. Hij of zij zal onderzoeken of alle wettelijk verplichte meldingen bij de AP gedaan zijn en zal erop toezien dat ontbrekende alsnog worden verricht. Dit geldt ook wanneer er bij de invoering van nieuw beleid of regelgeving een nieuwe melding of een wijziging aan de AP doorgegeven moet worden.

Wanneer de AVG van toepassing wordt zal de functionaris gegevensbescherming erop toezien dat er een register bijhouden wordt en vervalt de melding aan de AP.

6. Rechten van betrokkene

In hoofdstuk 3 staat beschreven dat transparantie bij de verwerking van privacygevoelige gegevens voorop staat. Hier staat bijvoorbeeld beschreven dat persoonsgegevens alleen gedeeld worden bij het uitvoeren van een wettelijke taak en wanneer de betrokkene hier toestemming voor geeft.

Die openheid geldt ook bij verdere rechten van de betrokkene.

6.1. Recht tot inzage en correctie van persoonsgegevens

Iedere betrokkene heeft het recht om op te vragen welke persoonsgegevens van hem of haar voor welke doeleinde verwerkt worden. Dit wordt het inzagerecht genoemd. Daarnaast heeft de betrokkene ook het

[24] Denk hierbij aan eisen voor gebruikersnamen, wachtwoorden, doorzoekbaarheidsbeperkingen, autorisatieniveaus ect

[25] Denk hierbij aan toegang tot kantoorruimtes, afsluiten van kasten ect

[26] Zie artikel 27 t/m 30 Wbp

[27] Voor gegevensverwerkingen van overheden en overheidsorganisaties zijn vrijstellingen van de meldplicht opgenomen in het vrijstellingenbesluit op grond van de Wbp.

recht om deze gegevens te laten verbeteren, aan te vullen, te verwijderen of af te schermen, als deze feitelijk onjuist, onvolledig of niet ter zake zijn. Dit wordt het correctierecht genoemd[28]. Dit verzoek kan mondeling en schriftelijk worden ingediend.

Het inzagerecht is niet van toepassing op interne notities die de persoonlijke gedachten van medewerkers bevatten en uitsluitend bedoeld zijn voor intern overleg en beraad.

Het kan voorkomen dat persoonsgegevens van meerdere personen in één dossier of document staan; denk hierbij aan een plan van aanpak in het sociaal domein. Er moet dan rekening gehouden worden met de privacy van de andere gezinsleden bij het beschikbaar stellen van de gegevens. Dit wil zeggen dat de informatie over partners en kinderen ouder dan 16 jaar niet zonder toestemming van die personen verstrekt mag worden.

6.2. Recht van verzet

De gemeente voert publiekrechtelijke taken uit, dit is de grondslag voor gegevensverwerking[29]. Ondanks dat heeft iedere betrokkene het recht om, vanwege bijzondere persoonlijke omstandigheden, te vragen zijn of haar persoonsgegevens niet meer te gebruiken. Dit heet het recht van verzet[30]. De gemeente zal bij dit verzoek beoordelen of de gegevensverwerking gerechtvaardigd is of dat de bijzondere omstandigheden van de betrokkene dusdanig zijn, dat het verzoek moet worden ingewilligd.

6.3. Indienen van bezwaar

Wanneer er een verzoek voor inzage, correctie, verzet van persoonsgegevens wordt gedaan, zal de gemeente een besluit nemen. Bij een besluit over een verzoek kan de betrokkene schriftelijk bezwaar indienen. Hierbij is de Algemene wet bestuursrecht van toepassing.

[28] Zie artikel 35 en 36 Wpb/15 AVG en 16,17 AVG
[29] Zie artikel 8 Wpb/6 AVG
[30] Zie artikel 40 Wpb/21 AVG