Beleid Gegevensbescherming

Privacy en veiligheid verwerking persoonsgegevens gemeente Leiden, Leiderdorp, Oegstgeest & Zoeterwoude

Versie 1.1

8-9-2015

Versiebeheer

Datum: 17-9-2015	Tekstuele aanpassingen: Ondertitel, Koptekst, Inleiding, Paragraaf 1.1, 1.3, 3.1.2, 3.1.3, 4 (inleiding)
8-9-2015	Nota b&w portefeuillehouder E.G.E.M. Bloemen
27-10-2015	Beleid gegevensbescherming vastgesteld door college van b&w Zoeterwoude

Inhoudsopgave

1. Inleiding 4
   1.1. Visie op gegevensbescherming 4
   1.2. Reikwijdte 4
   1.3. Juridisch kader 5
   1.4. Ingangsdatum 5
2. Governance en organisatorische borging gegevensverwerking 6
   2.1. Verantwoordelijk vanuit de Wbp 6
   2.2. Verantwoording aan de Gemeenteraad 6
   2.3. Wijze van inrichten gegevensverwerking 6
      2.3.1. Expert ondersteuning: functionaris gegevensbescherming (privacy officer) 6
      2.3.2. Expert ondersteuning: coördinator informatiebeveiliging 7
      2.3.3. Sturing en monitoring 8
   2.4. Bewerkersovereenkomst met derden 8
3. Werkprocessen 9
   3.1. Omgaan met persoonsgegevens 9
      3.1.1. Meldplicht datalekken 9
      3.1.2. Bewust omgaan met persoonsgegevens 10
      3.1.3. Bewaren van gegevens 10
      3.1.4. Toestemming 10
      3.1.5. Open communicatie 11
4. Waarborgen voor gegevensbescherming 11
   4.1. Privacy Impact Assessment 11
   4.2. Dataclassificatie 12
   4.3. Logging van gegevensgebruik 12
   4.4. Statuut informatiebeveiliging 12
   4.5. Melding gegevensverwerking CBP 12
5. Rechten van betrokkene 13
   5.1. Recht tot inzage en correctie van persoonsgegevens 13
   5.2. Recht van verzet 13
   5.3. Indienen bezwaar 14

Bijlage 1: Onderwerpen bewerkersovereenkomst 15

Bijlage 2: Werken met/zonder toestemming 17

1. Inleiding

In de maatschappij is privacy een onderwerp dat veel in de belangstelling staat. Voor het omgaan met persoonsgegevens door overheden, instellingen, bedrijven en burgers is het informatie- en privacy recht volop in ontwikkeling.
Gegevensbescherming en verwerken van privacygevoelige informatie is dan ook een relevant onderwerp voor de gemeenten Leiden, Leiderdorp, Oegstgeest en Zoeterwoude (hierna te noemen gemeenten). Ter uitvoering van beleidstaken en aan haar opgedragen wettelijke taken verwerkt de gemeente persoonsgegevens van haar inwoners, bedrijven en medewerkers.

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 identificeerbare persoon. Zoals een naam, adresgegevens of een e-mailadres. Maar ook indirecte gegevens kunnen persoonsgegevens zijn, 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 gemeenten hechten er veel waarde aan dat de verwerkingen van persoonsgegevens zorgvuldig, rechtmatig en veilig plaatsvinden. De colleges van burgemeester en wethouders hebben daarom besloten beleid te formuleren hoe om te gaan met het verwerken van persoonsgegevens. In dit beleid 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 gemeenten, 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 Statuut informatiebeveiliging Gemeente Leiden, Leiderdorp, Oegstgeest, Zoeterwoude & Servicepunt71.

1.1. Visie op gegevensbescherming

Het uitgangspunt van dat beleid is, dat de gemeente respect heeft voor de persoonlijke levenssfeer van haar inwoners, ondernemers en medewerkers. Het zal bijdragen aan effectieve en efficiënte dienstverlening. Ook zal het een vernieuwende manier van (samen)met andere gemeenten en derde partijen ondersteunen, maar blijft daarbij binnen de wettelijke vereisten.

1.2. Reikwijdte

De richtlijnen die in dit document staan beschreven gelden voor iedereen (zowel intern als externe bewerkers[3]) die gegevens verwerken.

[1] voor de volledige omschrijving zie artikel 1 Wet bescherming persoonsgegevens
[2] Dit zijn onder andere het privacyprotocol Jeugd, het beveiligingsplan Suwinet, het beveiligingshandboek BRP, het beveiligingshandboek Reisdocumenten ect.
[3] Voor uitleg van de term bewerkers zie artikel 1 Wbp

1.3. 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 wordt de Wbp uitgebreid met de meldplicht datalekken. Binnen enkele jaren zal ook de EU Algemene Verordening Gegevensbescherming (AVG) in werking treden. De AVG heeft als doel om de privacy van Europese burgers beter te beschermen dat de Wbp nu doet. Wanneer de AVG in werking treedt, 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 beschreven doel mogen worden verwerkt. 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 de Strategische en Tactische Baseline Informatievoorziening 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 wettelijke 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.

1.4. Ingangsdatum

Vanaf 1 januari 2016 wordt er begonnen om de beschreven richtlijnen invulling te geven. Elke twee jaar zal het beleid gegevensbescherming worden geëvalueerd en waar nodig bijgesteld.

[4] Dit zijn onder andere de wet Basisregistratie Personen, de wet Suwi, de Wmo, de Jeugdwet.
[5] zie artikel 13 Wbp

2. Governance en organisatorische borging gegevensverwerking

2.1. Verantwoordelijk vanuit de Wbp

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.

2.2. Verantwoording aan de Gemeenteraad

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

Met ingang van 2016 neemt het college in de programmabegroting, een passage op over beleid gegevensbescherming. Als voorbereiding op de AVG wordt het beleid gegevensbescherming elk jaar geauditeerd.

Naast het jaarlijkse verantwoorden, hebben het college en de burgemeester de algemene informatieplicht[6] om de raad te informeren over bijzonderheden (incidenten) ten aanzien van gegevensverwerking.

2.3. Wijze van inrichten gegevensverwerking

De verantwoordelijkheid voor de uitvoering van beleid is belegd bij de afdelingshoofden[7] binnen de gemeente.
Het bevoegdhedenregister (mandaatregeling) van de gemeente zal aangepast worden, zodat elk afdelingshoofd verantwoordelijk wordt voor de zorgvuldige verwerking van persoonsgegevens binnen zijn of haar afdeling[8]. Een afdelingshoofd geeft deze verantwoordelijkheid invulling door taken verder in zijn afdeling te beleggen.

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.

2.3.1. Expert ondersteuning: functionaris gegevensbescherming (privacy officer)

Vanwege het grote belang dat de gemeente hecht aan gegevensbescherming en ter voorkoming van versnippering van het beleid, zal een functionaris gegevensbescherming worden aangesteld[9]. De functionaris gegevensbescherming heeft een onafhankelijke positie in

[6] Artikelen 169 en 180, lid 2 van de Gemeentewet
[7] hier wordt ook een clusterdirecteur en afdelingsmanagers mee bedoeld.
[8] hier wordt ook cluster mee bedoeld
[9] Hiermee wordt gedoeld op de functionaris voor de gegevensbescherming als bedoeld in artikel 62 Wbp. In de nieuwe EU-Algemene verordening gegevensbescherming wordt het aanstellen

de organisatie. De werkzaamheden die een functionaris gegevensbescherming uitvoert hebben een wettelijke grondslag[10].

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,
- informeert en adviseert de verantwoordelijke en bewerkers over hun verplichtingen op grond van de Wbp en in de toekomst de AVG,
- houdt toezicht op de implementatie en toepassing van het beleid gegevensbescherming,
- houdt een register bij van de verschillende meldingsplichtige gegevensverwerkingen, de processen waar persoonsgegevens verwerkt worden en de door de gemeente gesloten bewerkersovereenkomsten, convenanten en vastgestelde privacyprotocollen,
- ziet toe dat inbreuken in verband met persoonsgegevens (incidenten) worden gedocumenteerd, geanalyseerd en wanneer nodig gemeld bij toezichthouder en betrokkene(n),
- adviseert in specifieke kwesties of bij de totstandkoming van nieuw beleid of wet- en regelgeving,
- voert analyses[11] 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 het College Bescherming Persoonsgegevens (CBP).

Om ervoor te zorgen dat de uitvoering van het beleid gegevensbescherming niet stagneert totdat een functionaris gegevensbescherming is aangesteld, zal een andere medewerker de uitvoer van het beleid oppakken.

2.3.2. Expert ondersteuning: coördinator informatiebeveiliging

Gegevensbescherming kan niet geborgd worden zonder adequate informatiebeveiliging. De coördinator informatiebeveiliging draagt zorg voor de informatiebeveiliging. De werkzaamheden die de coördinator informatiebeveiliging uitvoert worden beschreven in het Statuut informatiebeveiliging Gemeente Leiden, Leiderdorp, Oegstgeest, Zoeterwoude & Servicepunt71[12].

---

van een 'functionaris gegevensbescherming (privacy officer)' verplicht gesteld (Europese Commissie 2012/0011). In de verordening wordt van organisaties geëist dat bij het inrichten en het toepassen van bedrijfsprocessen, informatiesystemen en ook producten en diensten, van het begin tot het eind wordt nagedacht over de privacyaspecten en dat passende maatregelen worden genomen. De Verordening treedt naar verwachting in 2018 in werking.

[10] Artikel 18 lid 2 95/46/EG en artikelen 62 t/m 64 Wbp

[11] Bijvoorbeeld een Privacy Impact Analyse (PIA)

[12] http://virtueel.servicepunt71.nl/fileadmin/user_upload/2013_03_13_Statuut_informatiebeveiliging_v1_0.pdf

2.3.3. Sturing en monitoring

Elke 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 4 **Waarborgen voor** .

2.4. Bewerkersovereenkomst met derden

Bij veel gemeentelijke processen worden gegevens verwerkt door derden[13]. Denk hierbij aan werkzaamheden die uitgevoerd worden door Servicepunt71, informatiesystemen die in een Cloudoplossing draaien, 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[14] 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[15]. De Wet meldplicht datalekken, die op 1 januari 2016 in werking treedt, 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. In **Bijlage 1: Onderwerpen bewerkersovereenkomst** is aangegeven welke onderwerpen minimaal opgenomen moeten worden.

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.

[13] Zie voor betekenis artikel 1 Wbp
[14] Zie artikel 14 Wbp
[15] Zie artikel 14 en 77 Wbp

3. Werkprocessen

3.1. 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 doeleind 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[16]. 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[17].

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[18] 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.

3.1.1. Meldplicht datalekken

Vanaf 1 januari 2016 treedt de Wet meldplicht datalekken in werking. 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.

Als deze wet in werking treedt is een gemeente verplicht om datalekken te melden bij het CBP. 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. Het CBP is bevoegd om datalekken te beboeten. Om aan deze wet te kunnen voldoen worden er de volgende maatregelen getroffen:

- er wordt een procedure voor goed incidentbeheer ingericht,

[16] Dit zijn gegevens zoals persoonsgegevens, gezinssamenstelling, adresgegevens, bedrijfsgegevens, inkomen, uitkeringen, onderwijsgegevens, zorgindicaties ect.
[17] Zie artikel 1.7 BRP.
[18] Zie artikel 18 en 21 t/m 23 Wbp

- 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.

3.1.2. 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.

3.1.3. Bewaren van gegevens

De Wbp en AVG schrijven voor dat gegevens niet langer bewaard mogen worden dan het doel waar ze voor nodig zijn[19]. 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.

3.1.4. 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.

Het geven van toestemming houdt niet in dat er overal voor getekend moet worden. In **Bijlage 2: Werken met/zonder toestemming** wordt uitgelegd hoe er met toestemming omgegaan moet worden.

[19] zie artikel 10 Wbp

3.1.5. 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 op welke wijze gegevens worden verwerkt en beheerd[20]. Hierbij wordt duidelijk:

- welke gegevens worden verzameld,
- waarom deze gegevens worden verzameld,
- wat vervolgens met deze gegevens gebeurt,
- wie toegang heeft tot deze gegevens,
- welke rechten inwoners en ondernemers hebben.

Dit wordt vastgelegd in privacyprotocollen.

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[21].

Elke aanleiding voor gegevensverwerkingen wordt gedocumenteerd.

4. 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[22]. Er zijn verschillende instrumenten om gegevensbescherming te waarborgen. In dit hoofdstuk worden verschillende instrumenten door de gemeenten ingezet worden.

4.1. 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[23] (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.

[20] Informatie over gegevensverwerking wordt via de website en door middel van folders beschikbaar gesteld.
[21] zie artikel 43 Wbp
[22] zie artikel 13 Wbp
[23] https://cbpweb.nl/nl/zelf-doen/privacycheck/privacy-impact-assessment-pia

4.2. Dataclassificatie

De maatregelen die getroffen moeten worden om de gegevensbescherming te kunnen borgen[24], is 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[25].

4.3. 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.
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.

4.4. Statuut informatiebeveiliging

Het kunnen borgen van de privacy kan niet gerealiseerd worden zonder adequate informatiebeveiliging. Het beleid gegevensbescherming hangt samen met het Statuut informatiebeveiliging Gemeente Leiden, Leiderdorp, Oegstgeest, Zoeterwoude & Servicepunt71. Het Statuut informatiebeveiliging is vastgesteld in maart 2013 en wordt in 2015 geëvalueerd en aangepast naar de richtlijnen van de BIG.

In dit statuut staan beveiligingseisen opgenomen die gelden voor informatiesystemen[26], gedragscodes en richtlijnen hoe de ambtelijke organisatie moet omgaan met privacygevoelige informatie en de fysieke maatregelen die noodzakelijk zijn[27].

De gemeenten Leiden, Leiderdorp, Oegstgeest en Zoeterwoude en het Servicepunt71 hebben gezamenlijk beleidsafspraken gemaakt rondom informatiebeveiliging, het e-mail- en internetgebruik en de privacybescherming daarbij.

4.5. Melding gegevensverwerking CBP

In een aantal gevallen is het wettelijk verplicht om bij het CBP te melden dat er persoonsgegevens verwerkt worden[28]. Een organisatie moet elke verwerking van persoonsgegevens melden, bijvoorbeeld wanneer de organisatie persoonlijke gegevens

[24] Denk hierbij aan encryptie van gegevens, bewaartermijnen, wachtwoord vereisten
[25] https://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-1018-handreiking-dataclassificatie.pdf
[26] denk hierbij aan eisen voor gebruikersnamen, wachtwoorden, doorzoekbaarheidsbeperkingen, autorisatieniveaus ect
[27] denk hierbij aan toegang tot kantoorruimtes, afsluiten van kasten ect
[28] zie artikel 27 t/m 30 Wbp.

opvraagt, gebruikt of verspreidt[29]. De meldingen van de verwerking van persoonlijke gegevens zijn openbaar[30], 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 het CBP gedaan zijn en zal ontbrekende alsnog doen. Dit geldt ook wanneer er bij de invoering van nieuw beleid of regelgeving een nieuwe melding of een wijziging aan het CBP doorgegeven moet worden.
Wanneer de AVG in werking treedt zal de functionaris gegevensbescherming dit niet meer doorgeven aan het CBP, maar zal zelf een register bijhouden.

5. 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.

5.1. 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 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.[31] 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.

5.2. Recht van verzet

De gemeente voert publiekrechtelijke taken uit, dit is de grondslag voor gegevensverwerking[32]. 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[33]. 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.

[29] Voor gegevensverwerkingen van overheden en overheidsorganisaties zijn vrijstellingen van de meldplicht opgenomen in het vrijstellingenbesluit op grond van de Wbp.
[30] https://www.collegebeschermingpersoonsgegevens.nl/asp/orsearch.asp
[31] Zie artikel 35 en 36 Wbp
[32] Zie artikel 8 Wbp
[33] zie artikel 40 Wbp

5.3. Indienen 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.

Bijlage 1: Onderwerpen bewerkersovereenkomst

Bij veel gemeentelijke processen worden gegevens verwerkt door derden[34]. Denk hierbij aan informatiesystemen die in een Cloudoplossing draaien, werkzaamheden die worden uitbesteed of samenwerkingsverbanden.
Gegevensverwerking door derden brengt risico's met zich mee. Het college van burgemeester en wethouders blijft verantwoordelijk voor de verwerking van de gegevens. Zij moeten er daarom op toezien dat gegevens juist verwerkt en beveiligd worden. Afspraken over de gegevenswerking worden vastgelegd in een bewerkersovereenkomst.

De onderwerpen die in een bewerkersovereenkomst opgenomen moeten worden zijn:

- Instructies van verantwoordelijke

De bewerking mag alleen uitgevoerd worden in overeenstemming met instructies van de verantwoordelijke.
De bewerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken, maar alleen om uitvoering te geven aan de instructies van de verantwoordelijke.

- Geheimhouding

In deze bepaling wordt aan de bewerker een geheimhoudingsplicht opgelegd, eventueel gecombineerd met een boetebeding. Overigens is opzettelijke niet-naleving van deze geheimhoudingsplicht strafbaar gesteld in het Wetboek van Strafrecht.

- Beveiligingsmaatregelen

De verantwoordelijke draagt zorg dat de bewerker passende technische en organisatorische maatregelen neemt om de persoonsgegevens te beveiligen tegen verlies e.d.
Inschakelen van derden en onderaannemers
In de overeenkomst wordt vastgelegd of, en onder welke voorwaarden, de bewerker subbewerkers mag inschakelen.

- Locatie van de data

De verantwoordelijke moet weten in welke landen zijn data worden opgeslagen. Dit is mede van belang met het oog op de verplichtingen die gelden bij doorgifte van persoonsgegevens naar landen buiten de EU[35].

- Audits/verantwoording

De verantwoordelijke moet kunnen controleren of de bewerker zich houdt aan de gemaakte afspraken. Dit gebeurt vaak in de vorm van een audit (onderzoek) door de verantwoordelijke of door een onafhankelijke derde. In de bewerkersovereenkomst kunnen partijen hier nadere afspraken over maken.

- Aansprakelijkheid

De wet bepaalt dat de verantwoordelijke kan worden aangesproken als iemand schade lijdt doordat de Wet Bescherming Persoonsgegevens niet wordt nageleefd. Dit geldt zelfs als de schade het gevolg is van nalatigheid van de bewerker, die in dat geval ook zelfstandig aansprakelijk is. In de bewerkersovereenkomst worden heldere afspraken gemaakt over deze verdeling.

- Structurele gegevensuitwisseling

[34] Zie voor betekenis artikel 1 Wbp
[35] https://www.cbpweb.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu?qa=EU

Indien er sprake is van structurele uitwisseling of samenwerking met een externe organisatie of andere gemeente(n), dan worden er over de gegevensuitwisselingen afspraken opgenomen in de samenwerkingsovereenkomst.

Bijlage 2: Werken met/zonder toestemming

Wat is toestemming precies? Toestemming heeft vooral te maken met goede communicatie tussen de gemeente en de betrokkene(n). Een heel belangrijk element hierbij is open en helder te communiceren met de betrokkene(n).

Voor het werken met toestemming zijn drie stappen van belang:

1. Bepaal de noodzaak

De eerste vraag die elke medewerker zich moet stellen voor hij of zij gegevens uitvraagt, vastlegt of registreert is: welke gegevens zijn noodzakelijk om het doel waarvoor de persoonsgegevens nodig zijn te bereiken?

Het maken van die afweging kan het beste gebeuren aan het begin en eind van elke fase in het werkproces. Dat is een natuurlijk moment om met de betrokkene te concluderen wat de vervolgstappen zullen zijn en welke gegevens daarvoor noodzakelijk zijn om op te vragen. Het is daarbij van belang om gegevens die opgevraagd moeten worden bij professionals met een (medisch) beroepsgeheim, apart te vermelden en te motiveren. In alle gevallen geldt het uitgangspunt, dat als met minder gegevens, of minder diepgaande gegevens kan worden volstaan, dat altijd de voorkeur heeft.

2. Toestemming vragen

Dit houdt in: betrokkene informeren welke gegevens voor welk doeleind wordt verwerkt.
Als helder is welke gegevens noodzakelijk zijn voor de volgende stap in het proces, kan de medewerker dit met de betrokkene bespreken. De waarborgen en rechten van de betrokkene ten aanzien van gegevensverwerking door de gemeente, worden ook besproken. Bijvoorbeeld waar een betrokkene terecht kan om te controleren welke gegevens er werkelijk worden verwerkt, hoe lang ze worden bewaard, en hoe ze eventueel kunnen worden gecorrigeerd[36].

3. Toestemming registreren

Wanneer de bovenstaande stappen zijn doorlopen is schriftelijke toestemming over het algemeen niet nodig. De toestemming moet op enigerlei wijze worden vastgelegd. Dat kan op eenvoudige wijze door bij het verslag van het gesprek met de betrokkene, bij de conclusies en vervolgstappen ook op te nemen welke gegevens voor die vervolgstappen worden opgevraagd en met welk doeleind.

Bij het vragen van toestemming is er altijd de mogelijkheid dat betrokkene geen toestemming verleent, ook nadat hij of zij is geïnformeerd over belang en noodzaak. Het is hierbij belangrijk dat de bezwaren serieus in overweging worden meegenomen. Er zal nu een nieuwe afweging moeten worden genomen. Samengevat zijn er drie mogelijkheden:

1. De dienstverlening stopt, omdat het niet mogelijk is verdere diensten te verlenen,
2. De dienstverlening blijft beperkt tot het deel dat op basis van de beschikbare gegevens verleend kan worden,
3. Naar het professionele oordeel van de medewerker is de situatie dusdanig, dat er toch stappen gezet moeten worden omdat de gezondheid of veiligheid van betrokkene of mensen in de omgeving in het geding zijn. Dan kom je in de onvrijwillige dienstverlening.

Het laatste betekent een zware inperking van de persoonlijke levenssfeer van de betrokkene(n), omdat er een hoger algemeen en wettelijk geregeld belang is dat het persoonlijke belang overstijgt. Een stap die dan ook alleen na zeer zorgvuldige afweging gezet mag worden. Houd daarbij altijd de volgende twee vuistregels in het oog:

1. Is het de betrokkene echt duidelijk waarom de gevraagde dienstverlening nu geen doorgang kan vinden?

[36] Deze informatie wordt verwerkt in een informatiefolder, zodat deze kan worden meegegeven.

2. Bespreek op basis van geanonimiseerde gegevens de situatie met een collega of expert om te beoordelen of onvrijwillige dienstverlening gerechtvaardigd is.