GEMEENTEBLAD
Officiële uitgave van de gemeente Velsen
Nr. 546774
9 december
2022

Privacybeleid gemeente Velsen

Versie: 1.0
Datum: 26 oktober 2022

1. Inleiding

De gemeente Velsen vindt privacy belangrijk. Dat betekent dat wij met aandacht en respect voor de privacy van bewoners en medewerkers ons werk doen. Hierom stellen we een Privacybeleid vast. De gemeente Velsen verzamelt en bewerkt persoonsgegevens in verband met de dienstverlening aan burgers en bedrijven. Het gaat bijvoorbeeld om de gegevens in de gemeentelijke basisregistratie personen, de registratie van uitkeringsgerechtigden, het bijhouden van gegevens uit bouwaanvragen, registratie voor personeel en het verwerken van gegevens van mensen die een voorziening hebben aangevraagd.
Deze verwerking van persoonsgegevens leidt er wel toe dat de gemeente van alles over de burger te weten komt, wat inbreuk maakt op de vrijheid - de persoonlijke levenssfeer - van de burger. Dat gevaar speelt een grotere rol, naarmate de gemeente meer soorten gegevens van iemand verzamelt, zeker als het gevoelige gegevens betreft (bv. over gezondheid of strafrechtelijke gegevens). Een zorgvuldige omgang met de gegevens van burgers vormt een essentiële bouwsteen voor het vertrouwen van burgers in de overheid. Wie voor ons werkt, begrijpt dit en neem dit mee in zijn of haar dagelijks werk. De gemeente Velsen heeft als wettelijke verplichting dat zij behoorlijk en zorgvuldig omgaat met (persoons-)gegevens om de persoonlijke levenssfeer, de privacy, van betrokkenen te beschermen. Bescherming van (persoons-)gegevens is een grondrecht.
Het privacybeleid is in zijn formulering van uitgangspunten richtinggevend voor alle organisaties, externe professionals en ambtenaren die bij die uitvoering van gemeentelijke taken binnen de gemeente Velsen actief betrokken zijn. Aldus verschaft het een inhoudelijke basis om te komen tot nadere instructies en autorisaties voor professionals, alsmede reglementering van betrokken organisaties, waarmee de gewenste sturing in de praktijk (governance) verder kan worden vormgegeven. Dit beleid is/wordt nader uitgewerkt in operationeel beleid, werkinstructies en richtlijnen.
In dit stuk wordt geschreven over “de gemeente”, “ons”, of “wij”. Dit refereert altijd aan de gemeente Velsen.

1.1 Scope

Het privacybeleid omvat de gehele datastroom van persoonsgegevens binnen de gemeente. Van het genereren of verzamelen van persoonsgegevens, het dagelijks gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging van persoonsgegevens. Dit geldt voor zowel bedrijfsprocessen als de onderliggende voorzieningen voor informatieverwerking en gegevensopslag. Hierbij wordt geen onderscheid gemaakt tussen papieren of digitale informatieverwerking. Dit privacybeleid is bindend voor de gehele organisatie van (de bestuursorganen van) de gemeente Velsen.
Wanneer sprake is van Verwerkers of samenwerking en gegevensuitwisseling met derden gelden dezelfde uitgangspunten. Diezelfde uitgangspunten vormen het kader bij de selectie van leveranciers c.q. Verwerkers. Hiervoor maken wij contractuele afspraken die we ook kunnen toetsen bij de uitvoering van de werkzaamheden. Het beleid is ook van toepassing in geval van uitwisseling van informatie met andere gemeenten en organisaties bij de uitbesteding van publieke taken aan externe partijen.
Het beleid strekt zich uit over de verwerkingen van persoonsgegevens op grond van de Algemene verordening gegevensbescherming en de Wet politiegegevens. Bij de toepassing van deze algemene wetten dient ook de specifieke wet- en regelgeving in acht te worden genomen. Voor een gemeente zijn vele wetten en regels van toepassing, deze wetten en regels geven een nadere invulling aan de hiervoor genoemde wetten. Hierbij moet in gedachten worden gehouden dat speciale wetsbepalingen voorgaan op algemene wetsbepalingen zoals de AVG. De inzichten van de Autoriteit Persoonsgegevens (AP) en de Vereniging van Nederlandse Gemeenten (VNG) hebben bijgedragen aan de totstandkoming van dit beleid.

1.2 Raakvlakken en overlap met andere beleidsthema’s

Het privacybeleid van de gemeente Velsen heeft raakvlakken met andere beleidsthema’s of vertoont hiermee overlap.
Zo is de privacybeleidsvoering wettelijk gekoppeld aan de beginselen van behoorlijk bestuur en is daarmee ondersteunend aan het gemeentelijk integriteitsbeleid. Ook richt het privacybeleid zich in belangrijke mate op het waarborgen van een kwalitatief goede administratieve organisatie. Een kwalitatief goede administratieve organisatie is randvoorwaardelijk voor klantgerichte en klantvriendelijke gemeentelijke taakuitoefening en goed werkgeverschap.

1.3 Doelen privacybeleid

Met het privacybeleid brengen we in kaart welke maatregelen gemeente Velsen heeft genomen om de persoonsgegevens van bijvoorbeeld klanten, burgers en cliënten te beschermen. Daarnaast ondersteunt het beleid de realisatie van de volgende doelen:
het privacybeleid zorgt voor de juiste bescherming van de persoonsgegevens;
Goed privacybeleid draagt bij aan het op orde brengen en houden van de informatiehuishouding van de gemeente. Wanneer de informatiehuishouding van de gemeente op orde is, kan informatie makkelijker en sneller intern en extern worden gedeeld en maakt dat de gemeente efficiënter, transparanter waar dat kan en het vergroot onze dienstverlening;
het privacybeleid schept waarborgen op het gebied van continuïteit en risicomanagement omdat privacybeleid afbreuk- en aansprakelijkheidsrisico's tegengaat;
het privacybeleid voorkomt dat werkprocessen vertraging oplopen omdat de gegevensverwerking een schending van het recht op privacy inhoudt. (onrechtmatige overheidsdaad);
het privacybeleid ondersteunt het informatiebeveiligingsbeleid door nadrukkelijke aandacht te vestigen op het tegengaan van privacyincidenten die de beschikbaarheid, integriteit en vertrouwelijkheid van de gemeentelijke informatievoorzieningen en de opgeslagen persoonsgegevens aantasten. De uitvoering van informatiebeveiliging wordt beschreven in het informatiebeveiligingsbeleid.

2. Definities

AVG: Algemene Verordening Gegevensbescherming.
Wpg: Wet politiegegevens
Autoriteit Persoonsgegevens (AP): is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt.
Betrokkene: de persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.
CISO (Chief Information Security Officer): functionaris met een adviserende, coördinerende en toezichthoudende rol op het gebied van Informatiebeveiliging. Hij ziet er op toe dat de informatieveiligheid in de gemeentelijke organisatie voldoet aan de hiervoor geldende normen.
Datalek : bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens. Maar ook om het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens.
DPIA (Data Protection Impact Assessment): in een vroeg stadium op een gestructureerde en heldere manier in beeld brengen wat de privacyrisico's van een verwerking zijn en welke maatregelen getroffen dienen te worden aan de hand van de geconstateerde risico's. Een DPIA is verplicht als een gegevensverwerking (waarschijnlijk) een hoog privacyrisico oplevert voor de betrokkenen.
FG (Functionaris Gegevensbescherming): een onafhankelijke en deskundige toezichthouder en adviseur met wettelijke taken en bevoegdheden. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van alle privacy wet- en regelgeving waaronder de AVG en Wpg.
Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Denk hierbij aan naam, adres, geboortedatum. Naast deze algemene persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Gegevens van overleden personen of van organisaties zijn geen persoonsgegevens volgens de AVG en Wpg.
Privacyaudit: controles op de naleving van privacybeleid en privacywetgeving.
Privacy by design: houdt in dat bij het ontwerpen van een proces of systeem gegevensbescherming al is meegenomen zodat persoonsgegevens goed worden beschermd en gegevens niet langer worden bewaard dan nodig is voor het doel van de verwerking.
Privacy by default: Instellingen voor een gebruiker worden automatisch zo privacyvriendelijk mogelijk ingesteld. Hieronder valt bijvoorbeeld het niet automatisch aanvinken van toestemming;
PCP: privacy contactpersonen
Procesdoel: een bedrijfsdoelstelling die noodzaakt tot verwerking van persoonsgegevens.
Proceseigenaren: managers die verantwoordelijk zijn voor uitvoering van gemeentelijke taken zoals burgerzaken, uitvoering Jeugdwet, veiligheid.
Procesplan: nadere, schriftelijk geformuleerde beheersmaatregelen voor de bescherming van persoonsgegevens (in de regel de gedocumenteerde follow-up van een DPIA).
Privacy team: de Privacy Officer en de Functionaris Gegevensbescherming.
Toestemming: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de Betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling een hem betreffende verwerking van persoonsgegevens aanvaardt.
Verwerken/Verwerking: Een verwerking is volgens de AVG en Wpg elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens. Veel voorkomende bewerkingen zijn: verzamelen; vastleggen; ordenen; structureren, opslaan; wijzigen; opvragen, beschikbaar stellen, met elkaar in verband brengen; raadplegen; gebruiken; verstrekken; wissen en vernietigen.
Verwerker: de persoon of organisatie die ten behoeve van de verwerkingsverantwoordelijke bepaalde onderdelen van of de gehele verwerking voor zijn rekening neemt.

Verwerkersovereenkomst: een overeenkomst waarin de afspraken staan hoe een verwerker met de persoonsgegevens moet omgaan bij verwerkingen in opdracht en ten behoeve van de verwerkingsverantwoordelijke.
Verwerkingsregister: Het overzicht van verwerkingen die binnen de organisatie plaatsvinden.
Verwerkingsverantwoordelijke: een persoon of instantie die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De bestuursorganen van de gemeente zijn allemaal verwerkingsverantwoordelijken voor de verwerkingen die door of namens de gemeente worden uitgevoerd. De verwerkingsverantwoordelijken zijn onder andere de burgemeester, het college van burgemeester en wethouders en de gemeenteraad.

3. Beginselen van de AVG en Wpg

Nu de AVG en de Wpg inmiddels enkele jaren bestaan, is een nieuwe fase aangebroken, waarin behoefte bestaat de ruimte te nemen die de wet- en regelgeving bieden om onze taken effectief en efficiënt te vervullen en tegelijkertijd burgers met respect, eerlijk en begripvol te behandelen. Daarbij ontstaan (ethische) dilemma's. De (nationale) wet- en regelgeving is namelijk complex en biedt niet altijd voldoende houvast aan lokale beleidsmakers en –uitvoerders bij de uitvoering van hun taken. Verder heeft het recht op bescherming van persoonsgegevens geen absolute gelding en moet worden beschouwd in relatie tot de functie ervan in de samenleving. Dat vraagt soms afweging tegen andere (grond)rechten, bijvoorbeeld in het sociaal domein, waar de Rijksoverheid ons een opdracht heeft gegeven om integraal en domein-overschrijdend te werken. Sommige opdrachten kunnen met elkaar botsen en soms voldoen bestaande (IT-)systemen en werkwijzen nog niet aan de privacy- en informatiebeveiligingseisen.

Privacy vraagt daarmee niet alleen om een heldere bestuurlijke visie op privacy maar ook om duidelijke beleidskaders. Privacywetgeving, waaronder de AVG en de Wpg, biedt niet voor ieder vraagstuk een pasklaar antwoord maar schept juist ruimte door regels in de vorm van principes te formuleren waar aan moet worden getoetst wanneer gegevens verwerkt worden. Deze regels kunnen vaak verschillend worden ingevuld of toegepast. Een belangrijk onderdeel van het beleid is aandacht voor risico oriëntatie en het moreel kompas. De wet is een belangrijke leidraad, maar bij handelen conform de regels of gebruikmaken van de (wettelijke) ruimte, hoort een gewetensvraag: ook al houd ik me aan de regels, is deze oplossing ook in maatschappelijk opzicht wenselijk? Of op de juiste wijze invulling is gegeven aan deze principes en voldoende waarborgen zijn getroffen om de persoonlijke levenssfeer te beschermen is aan de toezichthouder en aan de rechter.

De gemeente Velsen wil met dit beleid de ruimte benutten die er is om haar taken goed uit kunnen voeren en de privacy van betrokkenen beschermen. Waar dit schuurt maken wij dat transparant. Verantwoording afleggen vinden wij horen bij een betrouwbare overheid. Incorporatie van een goede privacybescherming hoort thuis in de werkzaamheden van de organisatie. Uit het voorgaande moge duidelijk zijn dat er onduidelijkheid kan zijn over de eisen die wet- en regelgeving stellen. Dit kan tot onzekerheid leiden en medewerkers kunnen zich gehinderd voelen om hun taken uit te voeren en of privacy ervaren als een vervelende extra check bij reguliere processen. Anderen voeren – vaak ten onrechte – privacyregels juist aan om informatie niet te delen. Iets om je achter te verschuilen. Iedereen is het er echter over eens dat van ons als gemeente verwacht mag worden dat we met aandacht voor de bescherming van privacy ons werk doen. Dit beleid beoogt om de professionals op de werkvloer in staat te stellen afwegingen te maken bij de uitvoering van het werk. We willen dat rechtmatige verwerking van gegevens geen extra belastende handeling vormt maar onderdeel is van de reguliere taken en processen. In de gemeentelijke organisatie zijn de bevoegdheden zo laag mogelijk in de organisatie belegd waarbij iedereen verantwoordelijkheid draagt voor zijn eigen taakveld, op basis van vertrouwen. Dat betekent ook dat afwegingen rond privacy, zeker als deze meer en meer onderdeel worden van de reguliere taken en processen, ook gemaakt (zullen) worden op uitvoerend niveau. Om dit soort afwegingen te kunnen maken en uit te kunnen leggen (transparantie) is een afwegingskader nodig. Onderstaand volgt een opsomming van de diverse belangen/afwegingen.

3.1 Belangenafwegin g

Bij verwerking van persoonsgegevens zijn vaak diverse belangen gemoeid. Dat vraagt om een zorgvuldige afweging. Naast het belang van de individuele burger, is er het publieke (algemeen) belang en zijn er belangen van burgers ten opzichte van elkaar.

3.2 Belang van de burger

Een burger wil dat zijn persoonsgegevens veilig en betrouwbaar worden verwerkt. Daarnaast moeten wij transparant zijn wat wij met die informatie doen. De wensen kunnen wel van verschillend karakter zijn. Aan de ene kant heeft de burger er belang bij dat zo min mogelijk gegevens worden opgeslagen en niet langer worden bewaard dan noodzakelijk. Aan de andere kant verwacht de inwoner efficiënte dienstverlening, waarbij wij niet naar de bekende weg vragen.

3.3 Publiek belang
Wij voeren op diverse gebieden wettelijke en bestuurlijke taken uit. Denk hierbij aan onder andere taken in het sociaal domein, openbare orde en veiligheid of burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat er persoonsgegevens worden verwerkt.

3.4 Belangen van burgers ten opzichte van elkaar
De bescherming van de rechten van de ene burger kan ingrijpende gevolgen hebben voor de belangen en de rechten van de ander. Voordat persoonsgegevens worden verwerkt vindt er een belangenafweging plaats. Daarbij worden de privacy uitgangspunten meegewogen. De gemeente maakt een analyse, zodat de risico's van de verwerking vooraf inzichtelijk zijn. Na een onderbouwde belangenafweging wordt besloten of de gegevensverwerking kan plaatsvinden. Daarbij worden risico's zoveel mogelijk verkleind met de juiste maatregelen.

3.5 Privacy uitgangspunten
De AVG en Wpg omschrijven een aantal uitgangspunten die centraal staan in dit beleid. De gemeente Velsen hanteert hierbij de centrale uitgangspunten van Rechtmatigheid, Behoorlijkheid en Transparantie om invulling te geven aan alle uitgangspunten die de AVG en Wpg stellen. Hieronder worden deze uitgangspunten omschreven en de wijze waarop wij deze concreet invulling geven binnen onze organisatie.

3.6 Rechtmatigheid
Wij gaan uit van de geldende wet- en regelgeving voor gegevensverwerking en hanteren de AVG en Wpg als basis. Voor verwerking van persoonsgegevens moet er altijd een wettelijke grondslag bestaan. Het kan zijn dat wij persoonsgegevens vaker moeten gebruiken. Dit kan alleen als dat doel verenigbaar is met de oorspronkelijke verzameldoeleinden. Mocht blijken dat het niet verenigbaar is dan zal worden gekeken naar een rechtmatige grondslag. Dit wordt getoetst bij het Privacy Team.
Wij leggen alleen persoonsgegevens vast als dit noodzakelijk is voor het specifieke doel van de verwerking. Dit wordt voor de verwerking concreet gemaakt en vastgelegd in het verwerkingsregister.
Diverse gemeentelijke taken vereisen het gebruik van persoonsgegevens. In deze gevallen is het doel in de wet vastgelegd. Tevens wordt in het verwerkingsregister per verwerking bijgehouden op welke grondslag en met welk doel dit gerechtvaardigd is.
Bij de gegevensverwerking wordt rekening gehouden met de beginselen van 'proportionaliteit' en 'subsidiariteit[1]'. Wij vragen slechts die informatie die noodzakelijk is om het beoogde doel te bereiken. Daarbij gebruiken wij altijd de minst ingrijpende methode voor de betrokkenen.

3.7 Behoorlijkheid
Wij hanteren het principe van 'minimale gegevensverwerking'. Dit wilt zeggen dat er geen overbodige gegevens worden gevraagd die niet nodig zijn voor het vastgestelde doel. Hiermee geven wij invulling aan het principe van 'dataminimalisatie'. Zo richten wij onze systemen op een wijze in zodat niet teveel informatie wordt gevraagd. Denk aan online formulieren die geen overbodige invulvakjes hanteren. Verder zijn er werkinstructies en periodieke data "opschoonacties" om het dataminimalisatie principe te waarborgen.
Wij hanteren het beginsel van 'éénmalige vastlegging, meervoudig gebruik': gegevens die bekend zijn worden niet nodeloos opnieuw gevraagd. Dit betekent ook zo veel mogelijk gebruik maken van zogenoemde brongegevens, zoals die zijn opgenomen in het stelsel van basisregistraties. Dit is slechts mogelijk als hier een wettelijke grondslag en verenigbaar doel voor is. De grondslag en verenigbaarheid wordt niet op werknemerniveau bepaald. Dit wordt op afdelingsniveau vastgelegd middels werkinstructies en autorisaties om heldere kaders te schetsen voor onze medewerkers.
Persoonsgegevens worden niet langer bewaard dan noodzakelijk is. De noodzakelijkheid is voor ons altijd gerelateerd aan het doeleinde waarvoor de betreffende persoonsgegevens zijn verzameld. Vaak is dit op basis van wettelijke bewaartermijnen. Wanneer de wet hier niet in voorziet staan de bewaartermijnen beschreven in ons verwerkingsregister. De gemeente Velsen bewaart persoonsgegevens in ieder geval in overeenstemming met de bewaartermijnen die zijn benoemd in de vigerende 'Selectielijst voor gemeenten en intergemeentelijke organen' van de VNG.
De interne organisatie krijgt op termijn toegang tot het verwerkingsregister om de bewaartermijnen te raadplegen. Verder zijn er werkinstructies voor het gebruik van dit register.
Alleen functionarissen (ambtenaren, externen partijen, leveranciers en ketenpartners) waarvoor het voor de directe taakuitoefening noodzakelijk is, hebben inzage in persoonsgegevens. Deze gegevens worden vertrouwelijk behandeld. Verder hebben wij binnen informatiesystemen een autorisatiebeleid, zodat medewerkers alleen toegang hebben tot de gegevens die noodzakelijk zijn voor de uitoefening van hun specifieke taak.

1) Proportionaliteit betekent dat de verwerking in verhouding moet staan tot het te bereiken doel. Daarbij is met name belangrijk om na te gaan of het verwerken van persoonsgegevens een bijdrage levert om dat doel te bereiken. Ook dienen er zo min mogelijk persoonsgegevens te worden verwerkt. Subsidiariteit houdt in dat het doel niet op een andere manier kan worden bereikt die minder ingrijpt in de privacy van werknemers. Er mogen dus geen andere minder zware middelen zijn waarmee het doel kan worden bereikt.

Er wordt gewerkt met geheimhoudingsverklaringen voor externen en leveranciers. Met externe (keten)partners worden overeenkomsten (convenanten) afgesloten.
Persoonsgegevens worden goed beveiligd (conform het basisnormenkader voor informatiebeveiliging ((BIO))) opgeslagen zodat ze adequaat zijn beschermd tegen misbruik, verlies, onbevoegde toegang en bewerking. Door gebruik te maken van 'privacy by design en archiving by design' wordt al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht aan privacyverhogende maatregelen geschonken.
Het is voor zowel ons als de burgers van belang dat persoonsgegevens actueel en correct zijn. Er worden diverse projecten en processen periodiek uitgevoerd om de basisregistratie personen actueel en juist te houden. Dit is tevens een wettelijke verantwoordelijkheid.

3.8 Transparantie

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente Velsen over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Dit gebeurt onder meer door onze privacyverklaring op de website. Verder wordt per team bekeken hoe betrokkenen op een passende wijze worden geïnformeerd. Dit is vastgelegd in werkinstructies om te voldoen aan de informatieplicht onder de AVG en Wpg.
Burgers hebben de mogelijkheid om te vragen waarom en welke persoonsgegevens wij van hen verwerken. In de basis verstrekken wij de gevraagde informatie tenzij de wet anders aangeeft. Verder kunnen burgers om verbetering, aanvulling of verwijdering van persoonsgegevens verzoeken. Dit verzoek wordt gehonoreerd, tenzij ook hier weer de wet anders heeft bepaald (bijvoorbeeld opsporingsbelang).
Om recht te doen aan verzoeken van betrokkenen hebben wij een Procedure rechten van betrokkenen vastgesteld. Hierin is beschreven op welke wijze verzoeken van betrokkenen door ons worden afgehandeld. Hier wordt ook omschreven wie daarbij welke taken en verantwoordelijkheden heeft.
Wij zijn transparant over het type persoonsgegevens dat wij voor een specifiek doel met derden delen. Daarbij kan het zijn dat er een uitzondering is wanneer er belangen zijn, genoemd in wet- of regelgeving, die zich daartegen verzetten. Het soort persoonsgegevens worden bijgehouden in het verwerkingsregister en is opvraagbaar.
Wij zijn open en transparant over hoe wij met persoonsgegevens omgaan. Afwijkingen van dit beleidskader worden beargumenteerd voorgelegd aan het Privacy Team. Indien nodig zal de interne toezichthouder (de FG) escaleren naar het college en/of de burgemeester. Zo wordt maximaal invulling gegeven aan transparantie richting inwoners en de raad.

4. AVG & Wpg

4.1 Het verwerkingsregister

Binnen de gemeente werken wij met zeer veel processen en dus ook diverse verwerkingen van persoonsgegevens. Middels een verwerkingsregister wordt precies bijgehouden waar welke verwerkingen plaats vinden.

Het privacy team beheert het verwerkingsregister. De PCP leveren de input. Proceseigenaren binnen de domeinen zijn verantwoordelijk voor het opnemen van nieuwe verwerkingen in het verwerkingsregister. Zij worden hierbij ondersteund en geadviseerd door de PCP en de Privacy Officer(s). De FG controleert of het register volledig en up-to-date is. In de procedure Verwerkingsregister gemeente Velsen zijn de rollen en verantwoordelijkheden ten aanzien van het beheer van het register van verwerkingsactiviteiten vastgelegd. Het verwerkingsregister valt onder de verantwoordelijkheid van het college van B&W.

4.2 Data Protection Impact Assessment (DPIA)

De gemeente staat niet stil en is altijd in ontwikkeling. Zo worden processen en systemen periodiek aangepast. Daardoor kan er sprake zijn van een nieuwe verwerking of wijziging van een bestaande verwerking. Om de privacy risico's in kaart te brengen voor een juiste belangenafweging voeren wij vooraf een pre-DPIA uit. De uitvoering van de pre-DPIA valt onder de verantwoordelijkheid van de proceseigenaar. Deze kan een DPIA-verantwoordelijke binnen het proces aanwijzen. Aan de hand van de uitgevoerde
pre-DPIA worden voor zowel informatiebeveiliging als privacy, een risico-inventarisatie uitgevoerd. Op basis van de uitgevoerde pre-DPIA wordt bepaald of voor een afzonderlijke verwerking een hoog risico bestaat. Is dit niet het geval dan kan een privacy advies van het Privacy Team volstaan. Wanneer een verwerking wel een hoog privacy risico voor betrokkenen met zich meebrengt wordt er eerst een DPIA uitgevoerd. Een DPIA geeft inzicht in welke maatregelen getroffen moeten worden om het risico te verkleinen naar een minimaal en acceptabel niveau. Hiermee wordt invulling gegeven aan een juiste belangenafweging.
De gemeente Velsen hanteert een standaard DPIA model. Proceseigenaren zijn verantwoordelijk voor de uitvoering van een DPIA voor een verwerking met een hoog privacy risico. De gemeente hanteert hierbij een instructie ter verduidelijking voor de DPIA verantwoordelijke. Deze informatie is terug te

vinden op de Privacypagina (Sociaal Intranet). Het Privacy Team en de PCP ondersteunen en adviseren bij de uitvoering hiervan. De FG geeft advies over de uitgevoerde DPIA en ondertekent de DPIA.
Het Privacy Team houdt een register bij van uitgevoerde DPIA´s en monitort de voortgang van het DPIA proces. Er wordt gekeken naar de geïmplementeerde beheersmaatregelen en gerapporteerd aan de FG.

4.3 Privacy by Design & Privacy by Default

De gemeente hanteert de principes van 'Privacy by Design' en 'Privacy by Default' op haar verwerkingen.

Privacy by Design: houdt in dat er bij het ontwerpen van producten en diensten voor wordt gezorgd dat persoonsgegevens goed worden beschermd. Bij de inrichting van het proces en/of bouw van het systeem wordt bijvoorbeeld gekeken naar de benodigde technische en organisatorische maatregelen. Medewerkers betrekken het Privacy Team aan het begin van projecten, inkopen en aanbestedingen.
De privacycheck is ook vast onderdeel van het intakeproces[2].

Privacy by Default: houdt in dat de standaardinstellingen van een programma ingesteld dienen te worden op de meest privacy vriendelijke manier. Door deze instellingen wordt de privacy standaard zo goed mogelijk beschermd.
Voor een nieuwe verwerking of een wijziging in een bestaande verwerking wordt een pre-DPIA uitgevoerd. Door deze pre-DPIA wordt aan de voorkant helder of een uitgebreidere DPIA noodzakelijk is. Bij het uitvoeren van een DPIA worden de voor Privacy by Design en Privacy by Default noodzakelijke aspecten (bijvoorbeeld dataminimalisatie en bewaartermijnen) meegenomen in de voorgenomen verwerking. Zo worden in formulieren geen gegevens gevraagd die overbodig zijn. Dit helpt tevens mee aan het principe van dataminimalisatie. Op deze manier wordt geborgd dat nieuwe verwerkingen conform de normen van Privacy by Design en Privacy by Default worden ingericht.

4.4 Datalekken

Een datalek heeft potentieel een grote impact op betrokkenen en ons als organisatie. Er worden daarom meerdere processen, systemen en acties ingezet om datalekken te voorkomen. Volledig uitsluiten is onmogelijk, maar wij zetten ons in om een cultuur te creëren waarin het snel melden van mogelijke datalekken wordt gestimuleerd. Het kan namelijk zo zijn dat een datalek gemeld moet worden bij de Autoriteit Persoonsgegevens binnen 72 uur en bij betrokkenen. Indien wij niet of niet tijdig melden lopen wij een risico op een boete van de AP. Deze kan oplopen tot een maximum van 20 miljoen euro of 4% van een jaaromzet. Los van een morele verplichting is er dus ook een financieel risico wanneer niet wordt voldaan aan de meldplicht.
Om te voldoen aan bovengenoemde verplichtingen is er een instructie datalekken (zie Privacypagina intranet) opgesteld. In de Procedure beveiligingsincidenten en datalekken (zie Informatiebeveiligingspagina intranet) staat beschreven op welke wijze datalekken worden afgehandeld en wie daarbij welke taken en verantwoordelijkheden heeft. In deze procedure staat ook beschreven hoe en wanneer een datalek dient te worden gemeld bij de AP en/of betrokkenen. Alle datalekken kunnen gemeld worden via het Privacy team of privacy@velsen.nl.
Medewerkers ontvangen meerdere malen per jaar informatie over dit thema om de bewustwording op peil te houden. Alle nieuwe medewerkers krijgen daarnaast bij de indiensttreding tijdens de introductiedag ook een toelichting omtrent privacy in het algemeen en datalekken in het bijzonder. Tevens staat de gemeente Velsen voor een open en veilige cultuur zodat medewerkers zich veilig voelen om datalekken te melden. Dit wordt bevorderd door de bestuurders. Tot slot staan op het Sociaal Intranet van de gemeente Velsen diverse aanvullende bronnen ten aanzien van het melden van datalekken.
Om te blijven anticiperen op mogelijke risico's wordt een intern datalekregister bijgehouden waarin alle geconstateerde beveiligingsincidenten worden geregistreerd. Hierin wordt vastgelegd of het beveiligingsincident heeft geleid tot een datalek en indien dat het geval is, het datalek ook en wanneer dit is gemeld bij de toezichthouder en/of de betrokkenen. Tevens wordt de oorzaak van datalekken onderzocht om zo dringende aanpassingen gelijk door te voeren in de organisatie. Jaarlijks wordt het datalekregister geëvalueerd om trends bij te houden en structurele verbeteringen intern door te voeren. Vastlegging vindt plaats in de jaarrapportage privacy.

4.5 Privacyaudit

Vragen, klachten en het incidentmanagement zijn in wezen steekproefsgewijze toetsing van de uitvoering van het privacybeleid. Om verrassingen te voorkomen, kunnen proceseigenaren zichzelf periodiek controleren in hoeverre beleidsvoering en feitelijke situatie met elkaar overeenstemmen aan de hand

2) Tijdens het intakeproces van het projectportfoliomanagement (PPM) wordt het intakeformulier getoetst op volledigheid en randvoorwaarden. Als onderdelen nog onvolledig zijn omdat het bijv. nog niet geborgd is of omdat er grote risico's aanwezig zijn, zullen de indiener en opdrachtgever het gesprek aangaan met de inhoudelijke adviseurs om ervoor te zorgen dat het projectvoorstel voldoet aan de voorwaarden van Velsen en zo ook P&I. Binnen het PPM toetst de projectentafel of de projectvoorstellen voldoen aan de randvoorwaarden en of het project kan starten. De indiener en/of opdracht zijn hierbij aanwezig. De projectboard binnen PPM is op strategisch niveau en houdt het overzicht op alle projecten en resources. Genomen besluiten over de projectvoorstellen binnen PPM worden op een besluitenlijst vastgelegd die te vinden is op SharePoint. Ook worden alle projecten en de voortgang hiervan bijgehouden in het projectenoverzicht document op SharePoint.

van privacyaudits op de gehanteerde ijkpunten. Daarnaast worden er externe audits uitgevoerd in samenwerking met de FG.

4.6 Rechten van betrokkenen

Betrokkenen zijn alle natuurlijke personen van wie de gemeente de persoonsgegevens verwerkt. Persoonsgegevens zijn alle gegevens die direct of indirect herleidbaar zijn naar een natuurlijk persoon; de betrokkene. Persoonsgegevens zijn dus veel meer gegevens dan alleen iemands persoonlijke gegevens zoals bijvoorbeeld naam, adres en woonplaats. Om te kunnen controleren of de gemeente zich wel houdt aan de AVG en Wpg hebben betrokkenen een controlemiddel. Betrokkenen hebben rechten die ze kunnen uitoefenen en de gemeente is verplicht om daarvoor goede en toegankelijke procedures te hebben. De AVG-rechten van betrokkenen staan in hoofdstuk 3 van de AVG en de Wpg-rechten van betrokkenen staan in paragraaf 4 van de Wpg. Betrokkenen kunnen van hun rechten gebruik maken door een verzoek in te dienen door middel van DigiD via de website of per mail door het verzoek te sturen naar privacy@velsen.nl.

4.7 Gegevens delen met derden

Wanneer er sprake is van structurele of gevoelige gegevensuitwisseling met derde partijen, worden er afspraken gemaakt over de gegevensuitwisseling. Deze afspraken voldoen tenminste aan de AVG en Wpg en worden vastgelegd in een onderlinge regeling, samenwerkingsovereenkomst (convenant), een gegevensuitwisselings-overeenkomst of een verwerkersovereenkomst.
Er is een model verwerkersovereenkomst aanwezig dat inhoudelijk voldoet aan de eisen die de AVG daaraan stelt. Verwerkers worden bijgehouden in het verwerkingsregister van de gemeente Velsen. De ondertekende versies van de verwerkersovereenkomsten worden gearchiveerd bij het contractdossier. Gemeente Velsen leeft de relevante wet- en regelgeving na door op de juiste wijze in te kopen, aan te besteden en contractuele afspraken vast te leggen met derden. Dit is geborgd in het inkoopbeleid en uitgewerkt in het inkoopproces.
Met betrekking tot doorgifte hanteert de gemeente het uitgangspunt dat persoonsgegevens niet worden doorgegeven aan een bedrijf of vestiging in een land buiten de Europese Economische Ruimte (EER), tenzij deze doorgifte aantoonbaar rechtmatig is. Denk aan doorgiftes aan bekende verwerkers zoals Microsoft of Google. Rechtmatigheid wordt aangetoond in één van de volgende drie gevallen:
Een adequaatheidsbesluit;
Passende waarborgen middels een modelcontract (Standard Contractual Clauses);
Specifieke uitzonderingen.

4.8 Vragen of klachten

Betrokkenen met een vraag, mededeling of klacht over het gebruik van hun persoonsgegevens door de gemeente Velsen kunnen contact opnemen met de gemeente via privacy@velsen.nl. Indien een vraag of klacht niet (voldoende) beantwoord is dan kan men contact opnemen met de FG via fg@velsen.nl. Het is ook mogelijk dat een betrokkene direct contact opneemt met de FG. Tot slot kunnen betrokkenen een klacht indienen bij de AP.
Vragen worden zo snel mogelijk, maar uiterlijk binnen vier weken na ontvangst afgehandeld. Indien een vraag niet tot tevredenheid is afgehandeld, hebben betrokkenen het recht om zich opnieuw te wenden tot het Privacy team. Het Privacy team registreert in dat geval de vraag als een klacht. Klachten worden zo snel mogelijk, maar uiterlijk binnen vier weken afgehandeld. Personen hebben het recht om na afhandeling van een klacht hiertegen verweer te voeren bij de FG voor zover het verweer gericht is op de naleving van privacywetgeving en/of het privacybeleid van Gemeente Velsen.

5. Governance

Het Privacybeleid staat niet op zichzelf en maakt onderdeel uit van een reeks aan maatregelen om de bescherming van c.q. de verwerking van persoonsgegevens binnen en door de gemeentelijke organisatie te optimaliseren. Het is een inherent onderdeel van ieders functie/van ieders dagelijks handelen. Tegelijkertijd is de bescherming van persoonsgegevens niet de core business van de meeste medewerkers. Er zijn daarom medewerkers die advies geven over en toezicht houden op de bescherming van persoonsgegevens binnen de organisatie.

5.1 Het bestuur

Het college van B&W stelt het privacybeleid vast en is verantwoordelijk voor het voorzien in passende privacywaarborgen bij de uitvoering van gemeentelijke taken. De uitvoering van het privacybeleid is gedelegeerd aan het directieteam. Binnen het college valt de bescherming van persoonsgegevens onder de portefeuille privacy. Het college informeert de raad door middel van een jaarrapportage privacy en legt hiermee verantwoording af over de privacybeleidsvoering. Het college betracht beleidstransparantie te bewerkstelligen met behulp van publieksvoorlichting, zoals bijvoorbeeld via de website van Velsen. Er wordt zorggedragen voor documentatie van beleid en maatregelen zodat op ieder moment maatschappelijk en juridisch uitleg gegeven kan worden over de deugdelijkheid van de aanpak.
Het college bevordert samen met proceseigenaren een privacybewuste organisatiecultuur via voorbeeldgedrag en door te voorzien in de middelen voor bewustwording en, zo nodig, training van medewerkers en leidinggevenden. Ook ziet het college er op toe dat informatieveiligheid binnen de gemeente Velsen in lijn is met de geldende norm en wordt vastgelegd in het informatiebeveiligingsbeleid.

5.2 Directie team
De bescherming van persoonsgegevens is een aspect van de bedrijfsvoering, de bescherming van persoonsgegevens valt daarom onder de eindverantwoordelijkheid van de directie. De directie zorgt er voor dat:

- De organisatie in staat is om de eigen verantwoordelijkheden te dragen;
- De controle op de het privacybeleid binnen de organisatie is gewaarborgd.

5.3 Manager s
Managers zijn inhoudelijk verantwoordelijk voor naleving van wet- en regelgeving voor processen die binnen een bepaald team vallen. Het gaat hier zowel om wet- en regelgeving die specifiek voor een bepaald proces van toepassing zijn, zoals de Wmo voor het sociaal domein.
Daarnaast is de betreffende manager ook verantwoordelijk voor naleving van de AVG en Wpg voor de processen die binnen het team vallen. Managers dragen zorg dat hun taken binnen de grenzen van het privacybeleid vallen en rapporteren hierover aan de portefeuillehouder privacy.

5.4 Functionaris Gegevensbescherming
De gemeente heeft een FG aangesteld. De FG is onafhankelijk. De FG is betrokken bij alle aangelegenheden die verbandhouden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, controleren, bewustwording creëren, en optreden als contactpersoon van het AP. Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de teams overneemt. De teams hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de gemeentelijke richtlijnen op het
gebied van privacy. De FG handelt vragen of klachten van inwoners of medewerkers af.
5.5 Privacy Officer
Voor medewerkers én voor bestuurders is de Privacy Officer (PO) het dagelijkse aanspreekpunt bij vragen over de bescherming van persoonsgegevens. Ook ondersteunt de PO teams bij het opstellen van verwerkersovereenkomsten, het waar nodig implementeren van adviezen van de FG, het opstellen van modellen en voorbeeldbrieven. De PO vormt samen met de FG en de CISO het meldpunt datalekken.
Zoals aangegeven heeft de FG adviserende én toezichthoudende taken. Het gelijktijdig uitoefenen van beide taken kan spanningen geven. Wanneer dergelijke spanningen voorzienbaar én onwenselijk zijn, kan de PO de beantwoording van een concrete adviesvraag van de FG overnemen.
5.6 Privacy contactpersonen
Binnen de gemeente Velsen zijn de privacy contactpersonen(PCP) het eerste aanspreekpunt van de domeinen/teams. De PCP zijn aanspreekpunt/vraagbaak voor collega's en hebben een signaleringsfunctie richting PO en FG. De contactpersonen stimuleren en coördineren, naast de Privacy Officer, het privacyvriendelijk werken van het betreffende domein/team. De PCP zijn voor de managers, die in de eerstelijnsverantwoordelijkheid dragen, daarmee een onmisbare en dus noodzakelijke schakel om namens het College (als interne eindverantwoordelijke), te voldoen aan privacy wet- en regelgeving. De PCP beheren ook het verwerkingsregister.
Deze interne verantwoordelijkheid dragen managers voor de verwerkingsprocessen die binnen hun teams plaatsvinden. Deze interne verantwoordelijkheid ziet vooral toe op de uitvoering van de verplichtingen uit onder andere de AVG en Wpg.
5.7 Chief Information Security Officer (CISO)
De CISO stelt het informatiebeveiligingsbeleid en de informatiebeveiligingsplanning op. Hij initieert/voert risicoanalyses uit en onderzoekt kwetsbaarheden of laat dit doen. Hij handelt informatiebeveiligingsincidenten af en coördineert bij grote beveiligingsincidenten. Alle beveiligingsincidenten worden bijgehouden door de CISO in een register. De CISO adviseert gevraagd en ongevraagd het college, de directie en het lijnmanagement over risico's en te nemen maatregelen.
De CISO stimuleert de bewustwording binnen en het bewustzijn van de organisatie over informatieveiligheid en risico's. De CISO vormt samen met de FG en de PO het meldpunt datalekken.
5.8 Privacy Team
De FG en de PO, vormen samen het Privacy Team. De PO, CISO en FG kunnen elkaar vervangen indien noodzakelijk. Het Privacy Team is ondergebracht binnen de eenheid Concern Control. Het Privacy Team ondersteunt proceseigenaren bij de uitvoering van het gemeentelijk privacybeleid. Dit is ook het contactpunt voor personen waar zij terecht kunnen voor het uitoefenen van hun privacyrechten.

5.9 Medewerkers gemeente
Medewerkers zijn verantwoordelijk voor de goede omgang met persoonsgegevens in hun werkzaamheden binnen de gemeente Velsen. Interne medewerkers leggen de ambtseed af bij indiensttreding. Externe medewerkers hebben bij indiensttreding een integriteitsverklaring moeten ondertekenen waarin is opgenomen hoe wordt omgegaan met privacy. Zo mogen alleen persoonsgegevens worden gebruikt die nodig zijn ter uitvoering van de werkzaamheden, is vertrouwelijke omgang met persoonsgegevens vereist en is vereist dat medewerkers hun computer afsluiten en hun bureau opruimen als

zij hun werkplek verlaten. Dat voorkomt dat persoonsgegevens onbeheerd worden achtergelaten. Bij vragen over privacygerelateerde onderwerpen of bij vermoeden van een datalek richten zij zich eerst tot de PCP. De PCP maken (met behulp van het Privacy team) de afweging of een datalek gemeld moet worden bij de AP.

5.10 Proceseigenaren
Een proceseigenaar voert, als onderdeel van zijn of haar verantwoordelijkheden binnen de domeinen, regie en houdt toezicht op zijn of haar proces(sen) op basis van dit privacybeleid. Proceseigenaren zijn verantwoordelijk voor het opnemen van nieuwe verwerkingen in het verwerkingsregister en voor de uitvoering DPIA's. Ook archiveren zij ondertekende versies van verwerkingsovereenkomsten. Zij worden hierbij geadviseerd en ondersteund door de PCP en de PO. De FG adviseert en controleert hun werkzaamheden.

Bij processen waaraan privacyrisico's zijn verbonden hanteert de proceseigenaar een procesplan, waarin duidelijk en actueel beschreven is wat het procesdoel is. Het advies van de FG is de basis van het procesplan.
Het procesplan stemt overeen met de werkelijkheid en wordt periodiek geëvalueerd. Het procesplan benoemt de waarborgen voor eerlijke, veilige en betrouwbare procesvoering en omvat eventuele opdrachten aan uitvoeringsorganisaties en afspraken over toezicht door de proceseigenaar op goede uitvoering van werkzaamheden. De proceseigenaar spant zich in om geen onrechtmatig verkregen gegevens te verwerken en houdt zich bij uitvoering van zijn werkzaamheden aan de procedure beveiligingsincidenten en datalekken.
5.11 Evaluatie
Het privacybeleid is geen statisch document en zal op termijn geëvalueerd moeten worden, waarbij veranderde inzichten, wettelijke wijzigingen en best practices meegenomen worden. Jaarlijks wordt bekeken of het privacybeleid nog actueel is. Dit is geborgd door middel van de PDCA (plan-do-check-act)-cyclus in de privacymanagementtool. De FG verzorgt, namens het college, een jaarlijkse evaluatie van de risico's en de getroffen beheersmaatregelen binnen de processen waarvoor de gemeente verantwoordelijk is. Hier valt ook een actueel privacybeleid onder. De bevindingen van deze evaluatie worden weergegeven in de jaarrapportage privacy.