GEMEENTEBLAD
Officiële uitgave van de gemeente Velsen
Nr. 136074
28 maart
2025

Privacybeleid gemeente Velsen 2025-2028

1. Inleiding

De gemeente Velsen verzamelt en bewerkt persoonsgegevens in verband met de dienstverlening aan inwoners 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.
De gemeente Velsen hecht veel waarde aan privacy. Dit betekent dat wij ons werk met zorg en respect voor de privacy van zowel inwoners als medewerkers uitvoeren. Om deze reden stellen wij een privacybeleid op. Het gaat hier om informationele privacy. Informationele privacy verwijst naar het recht van individuen om controle te hebben over hun persoonsgegevens en om te beslissen hoe deze informatie wordt gebruikt.
Het doel van dit privacybeleid is om te beschrijven hoe wij aantoonbaar op een juiste wijze omgaan met persoonsgegevens. De Algemene Verordening Gegevensbescherming (hierna: AVG), de Uitvoeringswet AVG (hierna: UAVG) en de Wet politiegegevens (hierna: Wpg) zijn kaders die ons een belangrijk houvast bieden voor de wijze waarop wij omgaan met persoonsgegevens.
Digitalisering en nieuwe technologische ontwikkelingen brengen veranderingen met zich mee in onze samenleving, wat ook resulteert in verschuivingen in de verwachtingen van inwoners met betrekking tot de dienstverlening van de gemeente. Het gebruik van gegevens is essentieel om aan deze verwachtingen te voldoen. Wij besteden veel aandacht aan de zorgvuldige verwerking van deze gegevens, vooral wanneer het gaat om persoonsgegevens. Het beschermen van persoonsgegevens staat hoog in het vaandel en we nemen daarom passende maatregelen op het gebied van informatieveiligheid. De Baseline Informatiebeveiliging Overheid (BIO), die van toepassing is op de gemeente Velsen, stelt normen vast voor informatieveiligheid. Deze normen zijn verder uitgewerkt in ons informatiebeveiligingsbeleid.
Dit privacybeleid beschrijft hoe de gemeente Velsen de kernprincipes van de AVG in de praktijk brengt. Het beleid is verder uitgewerkt in operationeel beleid, zoals een gedragsrichtlijn privacy, werkinstructies en procedures binnen de organisatie voor een juiste implementatie. Deze uitwerkingen worden altijd in samenhang gelezen met dit privacybeleid. In dit stuk is geschreven over “de gemeente”, “ons”, of “wij”. Dit refereert altijd aan de gemeente Velsen.
Dit privacybeleid vervangt het op 26 oktober 2022 vastgestelde privacybeleid.

1.1 Kernwaarden en ambities

Bij de gemeente Velsen werken we met de inwoner in hoofd en hart. We willen een omgeving creëren waarin mensen zich welkom, gerespecteerd en veilig voelen. We zijn transparant in wat we doen en communiceren daar open en eerlijk over. We zijn betrouwbaar, nemen onze taken serieus en nemen de verantwoordelijkheid voor de gevolgen van onze acties. Daarnaast zijn we proactief en proberen we zo effectief en efficiënt mogelijk te werken.

De gemeente Velsen heeft haar besturingsfilosofie vertaald in een aantal kernwaarden. Onderstaand worden deze kernwaarden gekoppeld aan de privacyuitgangspunten:
- **Uitnodigend**: De gemeente Velsen is uitnodigend richting haar inwoners en medewerkers. Het privacybeleid draagt bij aan het zijn van een veilige en betrouwbare overheid. De inwoners weten waar ze aan toe zijn en waarvoor ze bij ons terecht kunnen. Wij proberen de inwoners op voorhand zoveel mogelijk te informeren over wat wij doen met hun persoonsgegevens. Bij onduidelijkheden of wanneer er behoefte is aan meer informatie, kunnen de inwoners op een makkelijke en toegankelijke manier een verzoek indienen. De gemeente Velsen reageert snel op vragen en opmerkingen van haar inwoners. Doordat de contactgegevens van de functionaris gegevensbescherming en de privacy officers op de website zijn gepubliceerd, weten de inwoners hoe zij ons kunnen bereiken.
- **Transparant**: De gemeente Velsen is transparant. Deze kernwaarde sluit naadloos aan bij de verantwoordingsplicht die volgens de AVG geldt. Het is voor de inwoner en de medewerkers duidelijk bij wie welke verantwoordelijkheid ligt en waar ze terecht kunnen bij vragen. Het uitvoering geven aan de rechten van betrokkenen draagt ook bij aan het zijn van een transparante, veilige en betrouwbare overheid.
- **Doeltreffend**: De gemeente Velsen is doeltreffend. De gemeente Velsen probeert mee te gaan met digitalisering en technologische ontwikkeling. Dit betekent dat we steeds meer digitaal werken, ook wat betreft de verwerking van persoonsgegevens. Alle nieuwe en innovatieve oplossingen worden getoetst aan de beginselen uit de AVG, hiermee waarborgen we dat er een kwalitatieve oplossing wordt aangeschaft. Doeltreffendheid gaat ook om het verbeteren van processen en onze dienstverlening. Én

dit op een zo privacyvriendelijke manier in te richten. Hierbij blijft er ruimte voor maatwerk in situaties die daarom vragen.
- **Verantwoordelijk**: De gemeente Velsen is verantwoordelijk. Dit betekent dat we onze governance op orde hebben, met zorg en respect met de persoonsgegevens van inwoners om gaan, onze verantwoordelijkheid nemen voor ons werk en in ons werk rekening houden met de privacyuitgangspunten uit dit privacybeleid. Ook wanneer we samenwerken met externen nemen we onze verantwoordelijkheid en zorgen we dat we de juiste afspraken hebben gemaakt. Door de verschillende procedures breed kenbaar te maken in de organisatie, zorgen we ervoor dat we adequaat kunnen handelen als er sprake is van een incident, bijvoorbeeld een datalek.

Ambities

De afgelopen jaren heeft de gemeente Velsen hard gewerkt om te voldoen aan de privacywet- en regelgeving. Aan de hand van het borgingsdocument van de Informatiebeveiligingsdienst wordt periodiek het privacyvolwassenheidsniveau binnen de gemeente vastgesteld. Eind 2024 was het volwassenheidsniveau overwegend 3, maar nog niet organisatiebreed.
Ons doel is om te groeien naar een privacyvolwassenheidsniveau 4 op alle privacy thema's in 2028 in de gehele organisatie. Om deze ambitie te realiseren, maken de privacy officers ieder jaar een planning met de te behalen doelstellingen, bijvoorbeeld aantal DPIA's die uitgevoerd moeten worden en de controle van het verwerkingsregister. Dit privacybeleid en de onderliggende procedures vormen de basis voor de gemeente Velsen om deze ambitie waar te maken.

1.2 Scope van dit beleid

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. Hierbij is geen onderscheid gemaakt tussen papieren of digitale informatieverwerking. Dit privacybeleid is bindend voor de gehele organisatie van (de bestuursorganen van) de gemeente Velsen.
Wanneer we samenwerken met andere partijen of gegevens delen met derden, gelden dezelfde uitgangspunten. Deze uitgangspunten helpen ons bij het kiezen van de juiste leveranciers of partners. Wij leggen deze afspraken vast in contracten (bijvoorbeeld een verwerkersovereenkomst) en controleren of ze worden nageleefd tijdens de uitvoering van taken.
Het beleid is van toepassing op de verwerkingen van persoonsgegevens op grond van de AVG en de Wpg. Naast deze algemene wetten moeten we ook specifieke wet- en regelgeving volgen. Als gemeente hebben we te maken met verschillende wetten en regels die de wetgeving verder verduidelijken. Het is belangrijk om te onthouden dat specifieke wetten voorrang hebben boven algemene wetten zoals de AVG.
Een voorbeeld hiervan is de Wet basisregistratie personen (BRP). De BRP richt zich specifiek op het bijhouden van persoonsgegevens in de basisregistratie personen. Het is een verzameling van persoonsgegevens van inwoners van Nederland. Gemeenten zijn wettelijk verplicht om persoonsgegevens van inwoners nauwkeurig en actueel bij te houden in basisregistratie personen. Gemeenten gebruiken de BRP om de identiteit van inwoners te controleren bij het verstrekken van identiteitsdocumenten. De BRP heeft dus in veel gevallen voorrang op de AVG.
De inzichten van de Autoriteit Persoonsgegevens (hierna: AP) en de Vereniging van de Nederlandse Gemeenten (VNG) hebben geholpen bij het opstellen van dit beleid.

1.3 Wettelijk kader, raakvlakken en overlap met andere beleidsthema's

De Algemene Verordening Gegevensbescherming (hierna: AVG), de Uitvoeringswet AVG (hierna: UAVG) en de Wet politiegegevens (hierna: Wpg) vormen het wettelijk kader op basis waarvan dit privacybeleid is opgesteld.
Het privacybeleid van de gemeente Velsen heeft raakvlakken met andere beleidsthema's of vertoont hiermee overlap. Zo is het privacybeleid gekoppeld aan de beginselen van behoorlijk bestuur en is daarmee ondersteunend aan het gemeentelijk integriteitsbeleid. Verder is er samenhang met het informatiebeveiligingsbeleid, de informatievisie en het archiefbeleid. Ook draagt het privacybeleid bij aan het College uitvoeringsprogramma. Het werken met het privacybeleid draagt bij aan het speerpunt bouwen aan vertrouwen uit het College uitvoeringsprogramma. Inwoners van Velsen moeten erop kunnen vertrouwen dat we zorgvuldig omgaan met persoonsgegevens en dat de gemeente Velsen alleen persoonsgegevens vraagt die echt nodig zijn bij uitoefening van haar taken.

1.4 Definities

De basisbegrippen

- **Algemene Verordening Gegevensbescherming (AVG)**: de AVG is een wet die regelt hoe organisaties in Europa moeten omgaan met persoonsgegevens en hoe zij deze moeten beschermen. De wet zorgt ervoor dat mensen meer controle hebben over hun persoonsgegevens en dat organisaties deze gegevens zorgvuldig en rechtmatig moeten gebruiken.

- **Wet politiegegevens (Wpg):** de Wpg is een wet die regelt hoe organisaties politiegegevens moeten verzamelen, opslaan, gebruiken en beschermen.
- **Persoonsgegevens**: persoonsgegevens zijn 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 (zie definitie hieronder). Gegevens van overleden personen of van organisaties zijn geen persoonsgegevens volgens de AVG en Wpg.
- **Bijzondere persoonsgegevens**: bijzondere persoonsgegevens zijn gevoelige informatie over een persoon. Dit omvat onder andere gegevens over iemands ras, religie, gezondheid of seksuele geaardheid. De wet beschermt deze gegevens extra, omdat ze gevoeliger zijn en meer privacyrisico's met zich meebrengen. Je mag pas bijzondere persoonsgegevens gebruiken als er een uitzondering uit de UAVG van toepassing is of als dit in een specifieke wet staat.
- **Politiegegevens**: politiegegevens zijn persoonsgegevens die worden verwerkt in het kader van uitvoering van taken op het gebied van handhaving van de openbare orde en veiligheid en de opsporing en vervolging van strafbare feiten.
- **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.
- **Betrokkene**: de persoon over wie de persoonsgegevens gaan. De betrokkene is degene van wie de gegevens worden verwerkt.
- **Verwerkingsdoel**: het specifieke doel waarvoor de persoonsgegevens worden verzameld en verwerkt. Een verwerking mag één hoofddoel hebben, maar mag ook meerdere subdoelen hebben zolang ze verenigbaar zijn met het hoofddoel.
- **Grondslag**: een verwerking van persoonsgegevens is rechtmatig (dit begrip is verder uitgelegd in paragraaf 3.2) als de verwerking noodzakelijk is voor één van de vijf wettelijke grondslagen of als er toestemming is gegeven door de betrokkene. Er is altijd één wettelijke grondslag voor één verwerking. Er zijn zes grondslagen voor het verwerken van persoonsgegevens:

1. Het is noodzakelijk om persoonsgegevens te verwerken omdat dit een wettelijke verplichting is.
2. Het is noodzakelijk om persoonsgegevens te verwerken om een taak van algemeen belang uit te voeren/openbaar gezag uit te oefenen.
3. Het is noodzakelijk om persoonsgegevens te verwerken om een overeenkomst uit te voeren
4. Het is noodzakelijk om persoonsgegevens te verwerken om een gerechtvaardigd belang te behartigen
5. Het is noodzakelijk om persoonsgegevens te verwerken om een overeenkomst uit te voeren
6. Er mogen persoonsgegevens worden verwerkt als er toestemming is gevraagd bij betrokkene (toestemming is bij het volgende punt nader toegelicht).
   Het hoeft dus niet zo te zijn dat er in een bepaalde wet moet staan dat je bepaalde persoonsgegevens mag verwerken, als dat wel zo is dan kies je voor grondslag nummer 1. Als er niet in een wet staat dat er bepaalde persoonsgegevens mogen worden verwerkt, maar je hebt als gemeente een taak uit te voeren waarbij bepaalde persoonsgegevens noodzakelijk zijn om te verwerken, dan kies je bijvoorbeeld voor grondslag nummer 2. De meest voorkomende grondslagen bij de gemeente zijn nummer 1 en 2.

- **Toestemming**: als toestemming is gekozen als grondslag voor een verwerking moet er aan de betrokkene vrije, specifieke, geïnformeerde en ondubbelzinnige toestemming worden gevraagd. De betrokkene kan dan door middel van een verklaring of ondubbelzinnige actieve handeling een verwerking aanvaarden. Deze grondslag kan in een veel gevallen niet worden gekozen door een overheid, omdat er sprake is van een machtsverhouding tussen de inwoner en de gemeente. Toestemming moet in alle gevallen goed onderbouwd en uitgelegd kunnen worden.
- **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.
- **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.

<u>Verplichtingen uit de AVG</u>

- **Verwerkingsregister**: een overzicht van verwerkingen die binnen de organisatie plaatsvinden.
- **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.

Een datalek is altijd een beveiligingsincident, maar een beveiligingsincident is niet altijd een datalek. Het verschil tussen een beveiligingsincident en een datalek is dat een beveiligingsincident elke inbreuk op de informatiebeveiliging omvat, terwijl een datalek betrekking heeft op de onbedoelde of ongeautoriseerde toegang tot persoonsgegevens.

- **DPIA (Data Protection Impact Assessment):** een DPIA kan gezien worden als een risicoanalyse. Met behulp van deze risicoanalyse breng je in een vroeg stadium op een gestructureerde en heldere manier in beeld wat de privacyrisico's van een verwerking zijn en welke maatregelen getroffen dienen te worden om de risico's te verkleinen. Een DPIA is verplicht als een gegevensverwerking (waarschijnlijk) een hoog privacyrisico oplevert voor de betrokkenen.
- **Privacy audit:** een controle 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 aan de voorkant, 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;

Rollen

- **Autoriteit Persoonsgegevens (AP):** is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt.
- **FG (Functionaris Gegevensbescherming):** een onafhankelijke toezichthouder en adviseur met wettelijke taken en bevoegdheden. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de AVG en Wpg.
- **Privacy Officer (PO):** de Privacy Officer heeft een adviserende en coördinerende rol op het gebied van privacy.
- **CISO (Chief Information Security Officer):** de functionaris met een adviserende, coördinerende en toezichthoudende rol op het gebied van Informatiebeveiliging. Hij ziet erop toe dat de informatieveiligheid in de gemeentelijke organisatie voldoet aan de hiervoor geldende normen.
- **Privacy contactpersonen (PCP):** privacycontactpersonen zijn de ogen en oren van de Privacy Officer binnen de teams.
- **Bevoegd Functionaris (BF):** de bevoegd functionaris is belast met specifieke taken en verantwoordelijkheden met betrekking tot de verwerking van politiegegevens.

Meer informatie over de governance is te vinden in hoofdstuk 2.

2. Governance

Het privacybeleid staat niet op zichzelf en maakt onderdeel uit van een reeks aan maatregelen om de bescherming van de verwerking van persoonsgegevens binnen en door de gemeentelijke organisatie te optimaliseren. Het beschermen van persoonsgegevens is belangrijk en maakt deel uit van ieders werk, maar voor de meeste mensen is het niet het belangrijkste onderdeel van hun werk. Er zijn daarom medewerkers die advies geven over en toezicht houden op de bescherming van persoonsgegevens binnen de organisatie.

2.1 Het bestuur

Het college van B&W stelt het privacybeleid vast en is verantwoordelijk voor het voorzien in passende privacywaarborgen bij alles wat de gemeente doet. Binnen het college valt de bescherming van persoonsgegevens onder de portefeuille privacy. Het college informeert de gemeenteraad door middel van een jaarverslag privacy en legt hiermee verantwoording af over de privacybeleidsvoering. Het college van B&W realiseert beleidstransparantie met behulp van publieksvoorlichting, bijvoorbeeld via de website van Velsen. Er wordt gezorgd voor documentatie van beleid en maatregelen zodat op ieder moment maatschappelijk en juridisch uitleg kan worden gegeven 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 erop toe dat informatiebeveiliging binnen de gemeente Velsen in lijn is met de geldende norm en wordt vastgelegd in het informatiebeveiligingsbeleid.

2.2 Directieteam

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 ervoor dat:

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

2.3 Managers (proceseigenaren)
Managers zijn de proceseigenaren voor de processen die binnen een bepaald team vallen. Managers kennen de processen die onder hun verantwoordelijkheid vallen het beste. Het gaat hier zowel om wet- en regelgeving die specifiek voor een bepaald proces van toepassing is, zoals de Wet maatschappelijke ondersteuning 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. De PO's helpen de manager om dit mogelijk te maken. Dat doen zij door toepasbaar en leesbaar privacybeleid te ontwikkelen, beschikbaar te zijn voor vragen en mee te denken, of als er verdiepende kennis over de AVG gewenst is bij het uitdenken van een nieuw proces. Wat dit betekent in de praktijk:

- Managers geven nieuwe of gewijzigde verwerkingen door aan de PO in verband met het actueel houden van het verwerkingsregister;
- Managers winnen advies in bij een PO voordat gestart wordt met een nieuwe of gewijzigde verwerking/proces;
- Managers betrekken de PO tijdig bij het aanschaffen van nieuwe software;
- Managers zijn verantwoordelijk voor het treffen van mitigerende maatregelen en het nemen van een beslissing over restrisico's bij DPIA's;
- Managers stimuleren het melden van datalekken bij de PO's of CISO;
- Managers blijven zelf verantwoordelijk voor het volgen van het privacybeleid. De PO helpt hen hierbij.

2.4 Functionaris Gegevensbescherming
De gemeente heeft een Functionaris Gegevensbescherming aangesteld. De FG is onafhankelijk. De FG is betrokken bij alles dat te maken heeft met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, controleren, bewustwording creëren, en optreden als contactpersoon van de 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 samen met de Privacy Officers 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. De taken van de FG en de Privacy Officers zijn op elkaar afgestemd, zodat de onafhankelijke positie van de FG wordt gewaarborgd.

2.5 Privacy Officer
Voor medewerkers én voor bestuurders zijn de Privacy Officers (PO's) het dagelijkse aanspreekpunt bij vragen over de verwerking en bescherming van persoonsgegevens. Zij pakken de regie als het gaat om de privacybewustwording, maar de organisatie blijft zelf verantwoordelijk. Ook ondersteunen de PO's teams bij het invullen van verwerkersovereenkomsten, houden zij samen met de privacycontactpersonen het verwerkingsregister actueel en geven zij gevraagd en ongevraagd advies aan het college, de directie en het lijnmanagement over privacyrisico's en te nemen maatregelen. De PO's handelen datalekken en verzoeken van inwoners af en houden de registers van datalekken en verzoeken bij. De PO's ontwikkelen en onderhouden ook alle privacygerelateerde beleidsstukken en procedures.
De PO's gaan proactief de domeinen in. Zij faciliteren trainingen en informationele bijeenkomsten over privacy en stemmen dit af op het expertise gebied van de collega's. Bij het uitvoeren van DPIA's ondersteunen de PO's de collega's uit de domeinen bij het invullen ervan. Zij monitoren of de acties uit de DPIA's worden opgevolgd. De PO's worden in hun werkzaamheden ondersteunt door de privacycontactpersonen die zich binnen de domeinen bevinden.

2.6 Privacy contactpersonen
Binnen de gemeente Velsen zijn de privacycontactpersonen (PCP) de ogen en oren binnen de teams voor de Privacy Officers. In de eerste instantie zijn de privacycontactpersonen het eerste aanspreekpunt/vraagbaak voor de collega's die te maken krijgen met privacygerelateerde onderwerpen. Als de vraag te complex blijkt te zijn, verwijst de PCP door naar de PO. Daarnaast hebben de PCP een signaleringsfunctie richting de PO's. Ze hebben een belangrijke rol in het actueel houden van het verwerkingsregister, het actueel houden en uitvoeren van DPIA's en zijn nodig voor het verhogen van het privacybewustzijn van medewerkers.

2.7 Chief Information Security Officer (CISO)
De Chief Information Security Officer stelt het informatiebeveiligingsbeleid en de informatiebeveiligingsplanning op. Hij 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 beveiligingsrisico's en te nemen maatregelen. De

CISO stimuleert het bewustzijn van de organisatie over informatiebeveiliging en de CISO vormt samen met de PO het meldpunt datalekken.

2.8 Team Informatiebeveiliging en Privacy (TIP)
De FG, de CISO en de PO's, vormen samen team informatiebeveiliging en privacy (TIP). De PO's en de CISO kunnen elkaar vervangen indien noodzakelijk. Het TIP is ondergebracht binnen de eenheid Concern Control. Het TIP ondersteunt proceseigenaren bij de uitvoering van het gemeentelijk privacybeleid. Dit is ook het contactpunt voor betrokkenen waar zij terecht kunnen voor het uitoefenen van hun privacy-rechten.

2.9 Bevoegd Functionaris
De bevoegd functionaris houdt toezicht op de verwerking van politiegegevens binnen de organisatie en adviseert over de naleving van de Wpg. Deze functionaris beslist wie er toegang mag hebben tot deze gegevens en of ze verstrekt kunnen worden aan een samenwerkingspartner.

2.10 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 persoons-gegevens 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 tot het TIP. Het TIP maakt de afweging of een datalek gemeld moet worden bij de AP.

2.11 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 laten opnemen van nieuwe verwerkingen in het verwerkingsregister en voor de uitvoering van DPIA's. Zij worden hierbij geadviseerd en ondersteund door PO's. Bij processen waaraan privacyrisico's zijn verbonden is het de verantwoordelijkheid van de proceseigenaar om de risico's te accepteren of maatregelen te nemen. Deze maatregelen worden periodiek geëvalueerd met de PO. 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. In veel gevallen behoort het aangaan en ondertekenen van een AVG-overeenkomst ook tot de verant-woordelijkheden van de proceseigenaar.

2.12 Evaluatie
Het privacybeleid is geen statisch document en wordt op termijn geëvalueerd, waarbij veranderde in-zichten, 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 het jaarverslag privacy.

3. Beginselen van de AVG en Wpg

Nu de AVG en de Wpg al enkele jaren van kracht zijn, is het tijd voor een nieuwe fase. We moeten de ruimte die de wet- en regelgeving biedt benutten om onze taken effectief en efficiënt uit te voeren, terwijl we inwoners met respect, eerlijkheid en begrip behandelen. Hierbij ontstaan ethische dilemma's. De wet- en regelgeving biedt niet altijd duidelijke richtlijnen voor lokale beleidsmakers en uitvoerders. Bovendien is het recht op bescherming van persoonsgegevens niet absoluut en moet het worden afge-wogen tegen andere rechten.
Privacy vraagt daarmee niet alleen om een heldere bestuurlijke visie op privacy maar ook om duidelijke beleidskaders. Privacywetgeving, waaronder de AVG en de Wet politiegegevens (Wpg), biedt niet voor ieder vraagstuk een pasklaar antwoord maar schept juist ruimte door regels in de vorm van principes te formuleren waaraan moet worden getoetst wanneer gegevens verwerkt worden. Deze regels kunnen vaak verschillend worden ingevuld of toegepast.
Een belangrijk onderdeel van ons beleid is het hebben van aandacht voor risico's en het volgen van ons morele kompas. Hoewel de wet een belangrijke leidraad is, moeten we bij het naleven van de regels of het gebruikmaken van de wettelijke ruimte ook ons geweten raadplegen: zelfs als we ons aan de regels houden, is deze oplossing ook sociaal wenselijk?

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 ook transparant. Verantwoording afleggen vinden wij horen bij een betrouwbare overheid. Het waarborgen van privacybescherming is een integraal onderdeel van al onze organisatiewerkzaamheden.
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.

3.1 Belangenafweging

Bij het verwerken van persoonsgegevens spelen vaak verschillende belangen een rol. Daarom is een zorgvuldige afweging nodig. Naast het belang van de individuele inwoner, is er het publieke (algemeen) belang en zijn er belangen van inwoners ten opzichte van elkaar.
Een inwoner wil dat zijn persoonsgegevens veilig en betrouwbaar worden verwerkt. Aan de ene kant heeft de inwoner 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 telkens om dezelfde informatie vragen.
Daarnaast is er sprake van een publiek belang. De gemeente Velsen voert 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.
Er zijn ook belangen van inwoners ten opzichte van elkaar. De bescherming van de rechten van de ene inwoner kan ingrijpende gevolgen hebben voor de belangen en de rechten van de ander. Bijvoorbeeld waarbij er in een gezin mogelijk sprake is van een onveilige situatie voor het kind. Dit heeft dan gevolgen voor de belangen en rechten van de ouder.
Voordat persoonsgegevens worden verwerkt vindt er een belangenafweging plaats. Daarbij worden de privacyuitgangspunten meegewogen. De gemeente maakt een analyse, een pre-DPIA en waar nodig een DPIA (zie ook paragraaf 4.2), zodat de risico's van de verwerking vooraf inzichtelijk zijn. Daarbij worden risico's zoveel mogelijk verkleind met de juiste maatregelen.

3.2 Welke beginselen vormen het uitgangspunt bij de bescherming van persoonsgegevens?

De AVG en Wpg gaan uit van beginselen waar elke verwerking van persoonsgegevens aan moet doen. Hieronder zijn deze algemene beginselen en de wijze waarop wij deze concreet invulling geven binnen onze organisatie omschreven.
''De verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn'':
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 grondslag bestaan (zie hoofdstuk 1.4 voor definitie van een grondslag uit de AVG).
- 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. Proportionaliteit houdt in dat wij slechts die informatie die noodzakelijk is vragen om het beoogde doel te bereiken. Met subsidiariteit toetsen wij of we de minst ingrijpende methode voor de betrokkenen gebruiken.

Behoorlijkheid

- Wij hanteren het beginsel van 'éénmalige vastlegging, meervoudig gebruik': gegevens die bekend zijn worden niet onnodig 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 grondslag en verenigbaar doel voor is. De grondslag en verenigbaarheid wordt niet op werknemer niveau bepaald. Dit wordt op team- en functieniveau vastgelegd middels werkinstructies en autorisaties om heldere kaders te schetsen voor onze medewerkers.
- 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. Dit noemen we het need to know principe.
- ''Need to know'' betekent dat iemand alleen toegang krijgt tot de informatie die hij of zij echt nodig heeft om zijn of haar werk te doen. Dit beschermt de privacy van inwoners, omdat niet iedereen zomaar alle informatie mag en kan zien. Bijvoorbeeld: een collega van burgerzaken helpt inwoners met het aanvragen van een nieuw paspoort. Deze collega van burgerzaken heeft toegang nodig tot bepaalde persoonsgegevens, zoals hun naam, geboortedatum en adres. Deze persoonsgegevens zijn essentieel om te kunnen raadplegen voor het afronden van deze taak.

- ''Nice to know'' betekent dat sommige informatie misschien interessant of handig is om te hebben, maar je het niet echt nodig hebt voor jouw werk. Bijvoorbeeld: eenzelfde collega van burgerzaken is bezig met het organiseren van een evenement, maar hoeft voor dit geen paspoortaanvragen te verwerken. In dit geval is het misschien interessant om te weten welke inwoners zich recent hebben ingeschreven in de gemeente, maar de persoonsgegevens zijn niet nodig voor het organiseren van het evenement. Die persoonsgegevens mag je niet opvragen of bekijken voor die taak.
- Er wordt gewerkt met geheimhoudingsverklaringen voor externen en leveranciers. Met externe (keten)partners worden overeenkomsten (bijv. convenanten en verwerkersovereenkomsten) afgesloten.
- 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 besteed.
- 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 de Privacy Officers aan het begin van projecten, inkopen en aanbestedingen. De privacycheck is ook vast onderdeel van het intakeproces. De informatie adviseurs coördineren het intakeproces en zorgen dat een intake van een bepaald project of een aanschaf van een systeem langs de integrale adviesronde gaat, waar de Privacy Officers en de CISO meekijken en adviseren.
- Privacy by Default houdt in dat de standaardinstellingen van een programma ingesteld dienen te worden op de meest privacyvriendelijke manier. Door deze instellingen wordt de privacy standaard zo goed mogelijk beschermd.
- 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.

Transparantie

- Iedereen heeft het recht om te weten 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.
- Betrokkenen 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.
- 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 beschrijven wij ook 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. Welke persoonsgegevens we verwerken houden we bij in het verwerkingsregister. Het verwerkingsregister is opvraagbaar.
- Wij zijn open en transparant over hoe wij met persoonsgegevens omgaan. Afwijkingen van dit privacybeleid worden beargumenteerd voorgelegd aan de Privacy Officers. 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.

''De verwerking moet gebonden zijn aan specifieke verzameldoelen (***doelbinding*** *)''*

- 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.
- 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 door de Privacy Officers.

''De gegevens moeten toereikend, ter zake dienend en beperkt tot het noodzakelijke zijn (***minimale gegevensverwerking*** *)''*

- Wij hanteren het principe van minimale gegevensverwerking. Dit wil 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 te veel 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.

*''De gegevens moeten juist zijn (**juistheid**)''*
- Het is voor zowel ons als de inwoners 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.

*'' De gegevens mogen niet langer worden bewaard dan nodig (**opslagbeperking**)''*
- Persoonsgegevens worden niet langer bewaard dan noodzakelijk is. De noodzakelijkheid is voor ons altijd gerelateerd aan het doel waarvoor de betreffende persoonsgegevens zijn verzameld. Vaak is dit op basis van wettelijke bewaartermijnen. De gemeente Velsen bewaart persoonsgegevens in ieder geval in overeenstemming met de bewaartermijnen die zijn benoemd in de ‘Selectielijst voor gemeenten en intergemeentelijke organen’ van de VNG. De (wettelijke) bewaartermijnen leggen wij vast in ons verwerkingsregister.

*''Gegevens moeten goed beveiligd zijn en vertrouwelijk blijven (**integriteit en vertrouwelijkheid**)''*
- Persoonsgegevens worden goed beveiligd (conform het normenkader voor informatiebeveiliging wat geldt voor overheden) en opgeslagen zodat ze goed beschermd zijn tegen misbruik, verlies, onbevoegde toegang en bewerking.

3.3 Aanvullende eisen en principes Wpg
De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt niet alleen onder de AVG maar ook onder de Wpg. De Wpg stelt specifieke bewaartermijnen voor de opslag van politiegegevens, andere eisen bij het delen van politiegegevens tussen verschillende partijen, er is een verplichting tot logging en er zijn in de Wpg aanvullende beperkingen en uitzonderingen op de in de AVG geldende privacyrechten van betrokkenen. Net als in de AVG verplicht de Wpg tot het bijhouden van een verwerkingsregister, maar dient er meer geregistreerd te worden, zoals bijvoorbeeld het gebruik van profilering. In het kader van de Wpg is ook eens per 4 jaar een externe audit verplicht en moeten elk jaar interne audits worden gehouden.
Het normenkader van de Wpg is grotendeels gelijk aan dat van de AVG. Op hoofdlijnen geldt aanvullend nog het volgende:
- De boa's van de gemeente Velsen kunnen naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens te maken met zowel de AVG als de Wpg;
- Duidelijk moet zijn welke gegevens er worden verwerkt onder de AVG en welke onder de Wpg.

De Wpg maakt een onderscheid tussen het ter beschikking stellen van politiegegevens en het verstrekken ervan. Het ter beschikking stellen van politiegegevens houdt in dat deze in principe worden gedeeld met eenieder die de gegevens nodig heeft voor de uitoefening van zijn taak (zogeheten ‘free flow of information’).
Bij het verstrekken van politiegegevens gaat het om het delen van gegevens buiten het Wpg-team. In dat geval moet zijn geborgd dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wpg zijn genoemd. Het gaat dan bijvoorbeeld om verstrekkingen aan de burgemeester, een toezichthouder, een advocaat of een functionaris in het kader van de Wet Bibob.

4. Verplichtingen uit de AVG

4.1 Het verwerkingsregister
Binnen de gemeente werken wij met veel processen. Voor deze processen is het nodig om persoonsgegevens te verwerken. In ons verwerkingsregister registreren we binnen welke teams er verwerkingen van persoonsgegevens plaatsvinden. De Privacy Officers beheren het verwerkingsregister.
Het verwerkingsregister is in samenwerking met de privacycontactpersonen gevuld. De privacycontactpersonen zijn of kennen de persoon met inhoudelijke expertise en weten dus ook welke persoonsgegevens er bij een proces worden verwerkt en met welk doel. Proceseigenaren binnen de domeinen zijn verantwoordelijk voor het laten opnemen van nieuwe verwerkingen in het verwerkingsregister. Zij worden hierbij ondersteund en geadviseerd door de Privacy Officers. 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 privacyrisico'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. De manager is proceseigenaar maar kan een andere DPIA-verantwoordelijke aanwijzen om de DPIA uit te voeren. Dit is vaak iemand binnen zijn/haar team met inhoudelijke expertise over het proces of een privacycontactpersoon binnen zijn/haar team. Aan de hand van de uitgevoerde pre-DPIA worden voor zowel informatiebeveiliging als privacy, een risicoanalyse uitgevoerd. De Privacy Officers ondersteunen de inhoudelijk expert bij het invullen van de DPIA. Er is een bestaand format voor de pre-DPIA gemaakt die moet worden ingevuld.
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 privacyadvies van de Privacy Officer volstaan. Wanneer een verwerking wel een hoog privacyrisico voor de betrokkenen met zich meebrengt moet er aanvullend een DPIA worden uitgevoerd. Een DPIA geeft inzicht in welke maatregelen getroffen moeten worden om het risico te verkleinen naar een minimaal en acceptabel niveau.
De gemeente Velsen hanteert een standaard DPIA-model. Proceseigenaren zijn verantwoordelijk voor de uitvoering van een DPIA voor een verwerking met een hoog privacyrisico. Net als bij de pre-DPIA mag de proceseigenaar hier weer iemand anders vragen om de DPIA in te vullen. De gemeente hanteert een instructie ter verduidelijking voor de DPIA-verantwoordelijke. Deze informatie is terug te vinden op de privacypagina (Sociaal Intranet). De Privacy Officers ondersteunen en adviseren bij de uitvoering hiervan. De FG geeft advies over de uitgevoerde DPIA.
De Privacy Officers houden een register bij van uitgevoerde DPIA´s en monitoren de voortgang van het DPIA-proces. Zij controleren de geïmplementeerde beheersmaatregelen en rapporteren hierover aan de FG. Er is een procedure (pre-)DPIA waarin de rollen en verantwoordelijkheden ten aanzien van de uitvoering van een DPIA zijn vastgelegd.

4.3 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 Informatiebeveiligings-pagina 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 de Privacy Officers of privacy@velsen.nl.
Alle nieuwe medewerkers krijgen bij de indiensttreding tijdens de introductiedag een toelichting omtrent privacy. 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 Intranet van de gemeente Velsen diverse aanvullende bronnen ten aanzien van het melden van data-lekken.
Om te blijven anticiperen op mogelijke risico's wordt een intern datalekregister bijgehouden waarin alle geconstateerde datalekken worden geregistreerd. Hierin wordt o.a. vastgelegd of en wanneer het datalek 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 worden het datalekregister geëvalueerd om trends bij te houden en structurele verbeteringen intern door te voeren. Vastlegging vindt plaats in het jaarverslag privacy.

4.4 Privacyaudit

Vragen, klachten en het incidentmanagement zijn eigenlijk een soort controle om te zien of we ons aan ons privacybeleid houden. Dit doen we door privacy audits/controles uit te voeren op bepaalde punten waar we ons aan moeten houden. Controles kunnen door de PO's worden uitgevoerd, maar ook mensen van buitenaf kunnen zo'n controle doen, zoals een externe auditor samen met de FG.

4.5 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. De vastgestelde procedure rechten van betrokkenen is gepubliceerd op intranet.

4.6 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 zijn verschillende modelovereenkomsten aanwezig die inhoudelijk voldoen aan de eisen die de AVG daaraan stelt. Bijvoorbeeld een standaard verwerkersovereenkomst en een gegevensdelingsovereenkomst. Verwerkers worden bijgehouden in het verwerkingsregister van de gemeente Velsen. De ondertekende versies van de verwerkersovereenkomsten worden gearchiveerd in ons systeem.
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.

4.7 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. De FG beoordeelt of een vraag zijn positie als onafhankelijke FG in gevaar kan brengen. Als dit het geval is dan draagt hij de vraag over aan de Privacy Officers. Het uitgangspunt is dat vragen en klachten zo goed als mogelijk door de Privacy Officers worden afgehandeld. Vragen en klachten worden binnen vier weken na ontvangst afgehandeld.

Aldus vastgesteld in de collegevergadering van 25 maart 2025
Burgemeester en wethouders van Velsen,
De secretaris, De burgemeester,
D. Veurink F.C. Dales