gemeente Steenbergen

GEMEENTEBLAD

Officiële uitgave van de gemeente Steenbergen

Nr. 315398

18 juli

2024

Privacy-beleid en daaraan gerelateerde Informatieveiligheid 2022

Steenbergen, augustus 2022

Zo gaat de gemeente Steenbergen om met privacy

In dit beleid laat gemeente Steenbergen zien op welke manier zij omgaat privacybescherming, en wat er wettelijk wel en niet verantwoord is.

Inleiding

Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid. Privacy is een grondrecht (bron:1) en een fundamentele vrijheid; het gaat ook om bescherming van (persoons)gegevens en vertrouwelijke informatie.
Gemeenten zijn de verantwoordelijkheid voor persoons- en politiegegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn. Gemeenten zijn verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Dat geldt voor taken op het gebied van basisadministraties, openbare orde en veiligheid, en het sociaal domein. Data verzamelen en verwerken is geen doel op zich. Informatie is nodig om processen van de gemeente bij producten en diensten tijdens de bedrijfsvoering effectief te laten verlopen. Goed en zorgvuldig omgaan met persoonsgegevens is een dagelijkse bezigheid van gemeenten.
Het beschermen van de privacy is en wordt steeds complexer door technologische ontwikkelingen, explosieve toename van dataverkeer, de decentralisaties, keten-samenwerkings-verbanden, grotere uitdagingen op het terrein van veiligheid en nieuwe (Europese) wetgeving. Aan deze ontwikkelingen kleven dilemma's, risico's en ethische vraagstukken. Privacy en informatieveiligheid staan soms onder druk. Daarom is het belangrijk om transparant te zijn over de manier waarop wordt omgaan met persoons- en politiegegevens en het waarborgen van de privacy.
Wij blijven investeren in veilige digitale ambities, in kennis en kunde.

Scope van de beschrijving van het privacy beleid

Dit privacy beleid beschrijft de bescherming van persoonsgegevens vanuit de Algemene Verordening Gegevensbescherming (AVG).

De Wet Politie Gegevens (WPG) en Bpgboa behoren sinds 2019 ook tot het beschermingsbeleid en gaan over het verwerken van politiegegevens. Buitengewone Opsporingsambtenaren (Boa's) verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten. Het gaat om de WPG domeinen leerplichtwet, werkzaamheden van het team Openbare Orde en Veiligheid en bij de gedelegeerde taak aan de ISD. Politiegegevens over onderzoek en vervolging van strafbare feiten kunnen binnen BIBOB-procedures aan de orde komen. Het zijn alleen Boa's die deze gegevens mogen verwerken.
De bescherming van betrokkenen bij politiegegevens lijkt sterk op die van de AVG, maar wijkt tegelijk af. De toegang tot de WPG rechten zijn te vinden op de website van de gemeente. Dit beschermingsbeleid is beschreven als sectorspecifiek beleid WPG wanneer de gemeente als werkgever is van Boa's. Buitengewone Opsporingsambtenaren verwerken persoonsgegevens vanuit de AVG én politiegegevens op basis van de WPG. Zij dienen te beschikken over grondige kennis van beide wetten.
Het AVG-sectorspecifiek beleid geldt ook voor de bescherming vanuit de Jeugdwet. Deze wet beschrijft eigen procedures voor Jeugdwerkers. Voorbeelden zijn de aantoonbare inschrijving van Jeugdwerkers in een beroepsregister en regels bij inzage door cliënten in hun dossier. De voorwaarde voor de geldigheid van dit beleid is dat jeugdwerkers in dienst zijn van de gemeente.

Wetgeving en definities

Elke lidstaat van de Europese Unie dient vanaf 25 mei 2018 te voldoen aan de Europese Privacy verordening (General Data Protection Regulation – afgekort GDPR). (bron 2)
De Nederlandse versie is de Algemene Verordening Gegevensbescherming (AVG) die samen met de Uitvoeringswet AVG uitkwam, is sindsdien in werking. Voor het telefonisch, al dan niet draadloos, verwerken geldt tegelijk een aanvullende e-privacyrichtlijn. Deze richtlijn zal worden vervangen door een eigen verordening. Deze speelt in op de digitale data-ontwikkelingen, waarbij draadloze informatie-uitwisseling onmiskenbaar een rol speelt. Ook zullen de DGA (Data Governance Act) en technische Eu-Acts nieuwe of aanvullende eisen stellen aan de gemeente bij de omgang met data. Sinds 2019 is de Wet Politie Gegevens (voortaan: WPG) met de BOA functie uitgebreid en van kracht. Deze wet beschermt de politiegegevens die bijzondere opsporingsambtenaren en politie verwerken.
De gemeente voert vaak taken uit op basis van publieke taken en wetten. Indien deze wetten onvoldoende voorzien in de bescherming van de privacy en informatieveiligheid, valt de gemeente terug op de (U)AVG, de e-privacy-richtlijn. Deze wetten borgen de bescherming van inwoners, medewerkers, kortom individuen. Ook kwetsbare groepen in onze samenleving moeten kunnen rekenen op deze bescherming.
Voor de bedrijfsvoering en dienstverlening past de gemeente actuele landelijke normkaders toe, zoals de kaders Baseline Informatiebeveiliging Overheid en AVG borging.

De wijze waarop de gemeente het privacybeleid en de informatieveiligheid onderhoudt in de organisatie, is beschreven in het document Bestuurlijke organisatie Privacybescherming. Dit is als bijlage 1 aan het Privacybeleid toegevoegd.

Reikwijdte
Het privacybeleid is van toepassing op alle verwerkingen van persoons- en politiegegevens door alle bestuursorganen van de gemeente. Oftewel: voor alle verwerkingen die binnen de gemeente plaatsvinden. (bron 3)

Verwerkingsverantwoordelijke
De bestuursorganen van de gemeente zijn allemaal verantwoordelijken voor de verwerkingen die door of namens de gemeente worden uitgevoerd. De bestuursorganen van de gemeente zijn de burgemeester, het college van Burgemeester en Wethouders (het college) en de Gemeenteraad.
De ambtelijke organisatie werkt vanuit teams. Iedere Manager is de verantwoordelijke voor het voldoen aan de AVG richtlijnen binnen het team van medewerkers. (bron 4)

Ons streven in 2023
Het streven van de gemeente Steenbergen is dat de AVG eind 2023 het volwassenheidsniveau 3 wordt toegepast. Het volwassenheidsniveau geeft aan in welke mate de AVG toepassing dagelijks in gebruik is.

Interne beheersing	niveau CMMI	Wijze van managen	Realisatie
Aantoonbaar	5	Sturen op continu verbeteren	2026
	4	Sturen meetbaarheid en op lerend vermogen (bewust bekwaam)	2025
Controleerbaar	3	Sturen op resultaten (onbewust bekwaam)	**2023**
	2	Sturen op processen **(huidig: bewust onbekwaam)**	2022
	1	Sturen op incidenten (onbewust onbekwaam)	2020

Afbeelding: AVG volwassenheidsniveau naar CMMI (bron 5)

Bij het bereiken van volwassenheidsniveau 3 heeft de gemeente werkprocessen, beleid en protocollen beschreven en vastgesteld. Vanaf vertrekpunt ontwikkelt de gemeente haar bedrijfsvoering en dienstverlening naar voorspelbaarheid. Hiervoor is het nodig dat de gehele gemeentelijke organisatie op basis van werkprocessen werkt met structureel gebruik van evaluaties van alle AVG vereisten op activiteiten. De Plan Do Control en Act (PDCA) – cyclus dient standaard toegepast te worden bij de activiteiten van de gemeente.
Vanaf het volwassenheidniveau 4 (CMMI) gaat de gemeente Steenbergen tijdens haar dienstverlening en bedrijfsvoering voldoen aan het drempelniveau van de AVG-integratie -vereiste. Er is sprake van aantoonbaar gebruik van privacybescherming binnen een Plan-Do-Check-Act cyclus (PDCA). De werkwijze van de gemeente wordt voor betrokkenen tastbaar. Binnen de PDCA-cyclus ondervinden beleidvorming, planning, uitvoering en monitoring een evaluatie met bijstelling, als dat nodig is. Dit geldt ook voor nieuwe initiatieven, die de gemeente integreert in de bedrijfsvoering en/of dienstverlening. Het uitvoeren van evaluaties bieden aan burgers, bedrijven en belanghebbenden meer zekerheid en is noodzakelijk bij een veilige digitalisering van de gegevenshuishouding. Digitaliseren van informatie bevordert gemak bij het verwerken. Het kan procedures eenvoudiger maken en versnellen. We hebben de ambitie om te voldoen aan alle wetten en landelijke overheidsnormen, die privacybescherming van betrokkenen en informatie veiligheid regelen.
De gemeente past tijdens de ontwikkeling naar een hoger volwassenheidsniveau steeds meer de PDCA-cyclus toe en handelt naar het beleid "bestuurlijke inrichting privacy-organisatie ". Daarin zijn de verantwoordelijkheden, taken en rollen en overlegvormen vastgelegd.
In maatschappelijke ontwikkelingen staat privacy soms onder druk. De bescherming van privacy staat bevindt zich volop in een maatschappelijke ontwikkeling, waarin het bewustzijn van burgers en bedrijven toeneemt. Er kleven soms privacy dilemma's, -risico's of ethische vraagstukken aan de inzet van bestaande en nieuwe technieken.
Wij willen op een veilige, verantwoorde en ethische manier omgaan met onze data.

De WPG volgt een eigen traject naar hetzelfde volwassenheidsniveau van integratie, die de AVG aangaat. Dit traject is begonnen na de eerste audit. De WPG verplicht een jaarlijkse interne audit op een zelf gekozen thema. Een erkende externe auditor dient de uitwerking van de gemeente te beoordelen. Vier jaarlijks vindt een externe audit plaats over het beleid en de uitvoering. De eerste audit betreft

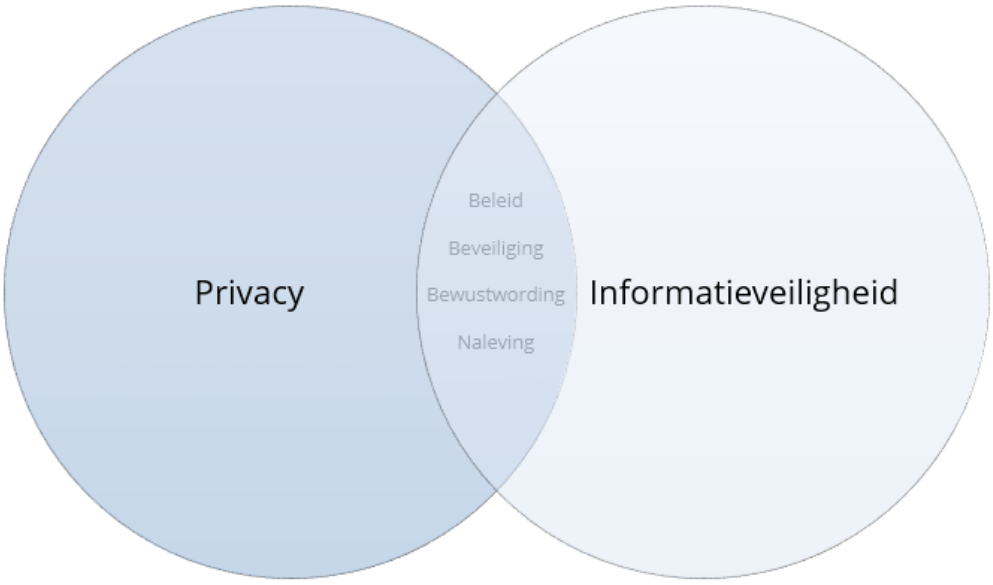
het jaar 2021. De rapportage van de externe audit dient bij de Landelijke Toezichthouder ingebracht te worden en kan aanleiding geven tot een aanwijzing met het verzoek om een verbeterplan binnen een gestelde termijn in te leveren.
De FG is bij de WPG domeinen een onafhankelijke toezichthouder voor de gemeente.

Uitgangspunten

- Bij dataverzamelingen en datagebruik zetten wij het maatschappelijk belang (betrokkenen) voorop;
- Burgers, bedrijven en instellingen kunnen vertrouwen op onze zorgvuldigheid;
- We beschermen onze informatie (bron 6)
- Wij geven toegang tot informatie volgens het "Alleen zien wat voor de functie nodig is"- principe; dit betekent dat iedere medewerker een passende autorisatie ontvangt om informatiespreiding tot het noodzakelijke niveau terug te brengen.
- We werken vanuit Privacy-by-design en Privacy-by-default; Privacy by design (bron 7) houdt in dat al tijdens het (her)ontwerpproces de AVG/WPG erbij wordt betrokken. Dit geldt dus ook bij aanpassingen van processen en systemen. Risico's voor privacybescherming worden zo vroeg mogelijk onderkent en met passende organisatorische en technische maatregelen weggenomen. Privacy by Default voorkomt dat standaard-instellingen in de vorm van digitale aankruisvakjes zijn ingevuld. Uitgangspunt is dat bezoekers van een website de gevraagde informatie zelf invullen!
- Wij nemen passende organisatorische en/of technische maatregelen (bron 8) op basis van risico voor de bescherming van persoonsgegevens. Hoge risico's hebben voorrang op minder grote risico's.
- We vergroten het vertrouwen bij onze burgers, bedrijven en belanghebbenden door aantoonbaar en blijvend te innoveren en investeren in privacy en informatieveiligheid;
- Wij blijven verantwoordelijk voor persoonsgegevens "in huis" en in de regio bij "bronhouderschap". (Bron 9)

Samenhang Privacy en Informatieveiligheid

Medewerkers binnen Privacy en Informatieveiligheid hebben eigen- en gezamenlijke taken.



Afbeelding: Gemeenschappelijke Privacy en Informatieveiligheid

Deze gemeenschappelijkheid blijkt ook uit de AVG (bron 10) waarin staat dat persoonsgegevens op een veilige manier verwerkt moeten worden door het nemen van de juiste technische en organisatorische maatregelen. Maatregelen die ervoor moeten zorgen dat het verwerken van persoonsgegevens op een passende beveiliging kan rekenen. Toetsing vanuit normenkaders vindt plaats op de Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie (BIV).
De bijgevoegde afbeelding geeft aan wat beide vakgebieden bindt en waarmee rekening gehouden moet worden bij het plannen, uitvoeren, evalueren en desgewenst bijstellen (volgens PDCA-cyclus).

Verwerkingen (Bron 11)

Verwerken van persoonsgegevens is elke handeling of elk geheel van handelingen met persoons- en politiegegevens, al dan niet uitgevoerd via geautomatiseerde processen. In de AVG valt onder een verwerking:

- Verzamelen, vastleggen en ordenen
- Bewaren, bijwerken en wijzigen
- Opvragen, raadplegen, gebruiken
- Verstrekken door middel van doorzending
- Verspreiding of enige andere vorm van ter beschikkingstellen
- Samenbrengen, met elkaar in verband brengen
- Afschermen, uitwissen of vernietigen van gegevens

Uit deze opsomming blijkt dat veel wat we veel met een persoonsgebonden gegeven doen. Een verwerking gebeurt op allerlei manier, zoals digitaal, op papier, in gesprek en bij beeldmateriaal.
Een verwerking van de gemeente voldoet aan de AVG als de Beginselen (Bron: 12) worden toegepast. Dit betekent onder meer:

- Dat de gemeente transparant is naar de betrokkene(n) over de wijze van verwerken;
- Dat de gemeente passende maatregelen neemt om de juistheid van de gegevens te behouden.
- Dat dat er sprake is van minimale gegevensverwerking.
- Dat de gemeente bewaartermijnen van gegevens stelt en naleeft.
- Dat de gemeente neemt veiligheidsmaatregelen om ongeoorloofd gebruik, verlies, vernietiging of beschadiging van persoonsgebonden informatie te voorkomen.
- Dat de gemeente gehouden is aan een verantwoordingsplicht.
- Dat verwerkingen doel gebonden zijn en een rechtmatige grondslag hebben.

Doeleinden (Bron 13)
Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten, zoals bijvoorbeeld de Jeugdwet, zijn de doelen voor het verwerken in de wet al vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden

Rechtmatige grondslag (Bron 14)
De wet zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden:

- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel was
- Om een verplichting na te komen die in de wet staat
- Om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden
- Voor de goede vervulling van de gemeentelijke taak om het algemeen belang te dienen
- Voor de bescherming van eigendommen van de gemeente.

De Wet Politie Gegevens kent andere grondslagen. De rechtmatige grondslag voor het verwerken van strafrechtelijke gegevens zijn Art. 8,9,10 en 13 WPG. Deze strafrechtelijke gegevens gaan over de opsporing en vervolging waarmee Boa's te maken hebben.

Categorieën persoonsgegevens (Bron 15)
De (U)AVG onderscheidt Gewone-, Gevoelige- en Bijzondere Persoonsgegevens. Gevoelige en Bijzondere persoonsgegevens zijn in Nederland gelijkwaardig. De gemeente ziet deze persoonsgegeven aan als het hoogste kans risico voor het benadelen van een betrokkene.
Strafrechtelijke gegevens AVG (bron 16) behoren ook tot de persoonsgegevens met een hoog beschermingsniveau. Het is de gemeente -als overheid- toegestaan hiermee om te gaan. Het gebruik van persoonsgegevens is gekoppeld aan verwerkingen, die een medewerker uitvoert op basis van een toegekende autorisatie. (Bron 17) De verantwoording van het gebruik van noodzakelijke persoonsgegevens vindt plaats in het Register van Verwerkingen. (Bron 18) De gemeente gebruikt als overheid het nationale identificatienummer. Het verwerken hiervan is voorzien van passende waarborgen zoals autorisatie bij het uitvoeren van een taak.

De politiegegevens zijn terug te vinden in het WPG-register van verwerkingen.

Categorieën ontvangers

Het verwerken is gebonden aan bevoegdheid en autorisatie. In een beschrijving van een verwerking dient de gemeente aan te geven wie met de verkregen persoonsgebonden informatie omgaat. De gemeente geeft ketenpartners aan. Interne medewerkers zijn aan de functie herkenbaar.

Bewaartermijn
Iedere verwerking heeft eigen bewaartermijnen, die berusten op selectielijsten van de Landelijke overheid. Bij een afgebroken handeling geldt vaak een andere termijn dan een volledig afhandeling. Na de bewaartermijn vernietigt de gemeente de informatie, tenzij de gebruiker noodzakelijke reden heeft om deze persoonsgebonden informatie om zakelijke redenen te bewaren. Er wordt dan een nieuwe bewaartermijn aangehouden, waarna alsnog vernietiging volgt. Bij sommige informatie is de bewaartermijn eeuwigdurend, zoals vergunningen bij pandgegevens.

Passende maatregelen
Om verwerkingen veilig te houden, treft de gemeente passende maatregelen in de organisatie en bij de technieken. In de beschrijving van de verwerking zijn het normenkader van de overheid opgenomen.

Wijze van verwerking
De hoofdregel van de verwerking van persoonsgegevens is dat verwerken alleen toegestaan is in overeenstemming met de wet en op een zorgvuldige wijze. Persoons-/politiegegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt.
De wet spreekt over proportionaliteit. (Bron 19) Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer zonder, of met minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden, moet daar altijd voor worden gekozen.
De gemeente zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn, voordat ze verwerkt worden. (Bron 20) Alleen personen met een geheimhoudingsplicht mogen ze voor de gemeente verwerken. Daarnaast beveiligt de gemeente alle persoonsgegevens. (Bron 21) Dit moet voorkomen dat iemand die daar geen recht toe heeft, de persoonsgegevens niet inziet of kan wijzigen. Hoe de gemeente dit doet, is verwoord in het informatiebeveiligingsbeleid van de gemeente en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie. (Bron 22)

De omgang met politiegegevens is beschreven in het sectorspecifieke beschermingsbeleid.

Samenwerking (Bron 23)
Met partijen die namens de gemeente diensten uitvoeren, gaat de gemeente een verwerkersovereenkomst aan om een veilig verwerking vast te leggen.
Met partijen met wie de gemeente op aan andere manier binnen de EU samenwerkt, sluit de gemeente een privacy-overeenkomst af, zodat de veilige verwerking van uw persoonsgegevens wordt gegarandeerd. De gemeente houdt een Register van Overeenkomsten.

De gemeente gebruikt voor WPG verwerkingen een apart Register van Overeenkomsten.

Doorgifte (Bron 24)
De gemeente geeft alleen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie op grond van goedgekeurde afspraken door de Europese Commissie. (bron 25)

Transparantie en communicatie

De gemeente, als overheid, speelt voortdurend in op nieuwe ontwikkelingen om transparantie te bevorderen. Drie van die nieuw wetten hebben verstrekkende gevolgen voor de bedrijfsvoering en dienstverlening.

Nieuwe wettelijke ontwikkelingen en transparantie
Wet Open Overheid (WOO)
Na 1 mei 2022 de Wet Open Overheid-WOO kan een persoon (voortaan: betrokkene) een verzoek om informatie indienen bij de gemeente. Deze wet komt verzoekers meer tegemoet dan de Wet WOB. Bij het WOO-verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van andere burgers (naamgenoten of daarop gelijkend). In principe verstrekt de gemeente geen persoonsgegevens als de belangen van anderen worden benadeeld.
De Landelijke Overheid heeft een digitaal platform in voorbereiding waarop burgers hun informatie kunnen vinden. Dit platform “Plooi” bevordert de inzage en verzoek-procedures.

Wet hergebruik van overheidsinformatie (2015)
De Wet hergebruik van overheidsinformatie berust op een Europese richtlijn en is een Nederlandse wet geworden. De voorloper van de WOO bevatte hiervoor richtlijnen (2003, 2013) die op dit moment zijn vervallen. De wet regelt dat de overheid (openbare) informatie over burgers kan hergebruiken. Dit kan toch op gespannen voet staan met de AVG, die uitgaat van doelbinding, een rechtmatige grondslag en bescherming van betrokkenen bij het verwerken van persoonsgebonden informatie. De gemeente maakt bij de behoefte aan hergebruik een zorgvuldige belangenafweging. Het streven bij hergebruik is dat er geen inbreuk op de persoonlijke levenssfeer van betrokkenen ontstaat. In principe verstrekt de gemeente geen persoonsgebonden gegevens, tenzij de wet dat verplicht.
Omgevingswet
De nieuwe wet regelt dat burgers en bedrijven hun aanvraag voor vergunningen beter kunnen volgen en vinden. De gemeente gaat werken met nieuwe digitale systemen om dit mogelijk te maken. Onder bepaalde omstandigheden gebruikt de gemeente de Wet BIBOB om de "integriteit" van de aanvrager van een vergunning vast te stellen. Het onderzoek betreft ook gevoelige en bijzondere persoonsgegevens. Alleen geautoriseerde medewerkers van de gemeente mogen het onderzoek verrichten en hebben toegang tot de resultaten.

Informatieplicht (Bron 26)
De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente geven, ontstaat een informatieplicht over de manier waarop de gemeente met de persoonsgegevens om zal gaan. Dit kan bijvoorbeeld via een E-formulier gebeuren. In de toelichting bij het formulier voorziet de gemeente een toelichting die voldoet aan de AVG.
Een belangrijke bron van informatie over de bescherming van privacy en informatieveiligheid is de privacyverklaring van de gemeentelijke website.
Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

Verwijdering (Bron 27)
De gemeente bewaart de persoonsgegevens niet langer dan nodig is voor het uitvoeren van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel, worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren. De gemeente is gebonden aan een geldende landelijke selectielijst, die beschrijft welke bewaartermijnen gelden.

Rechten van betrokkenen (Bron 28)
De wetten -AVG/WPG- bepaalt niet alleen de plichten van degenen die de persoons-/politiegegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel de 'rechten van betrokkenen' genoemd, en bestaan uit de volgende rechten:

- Recht op informatie: Betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt.
- Recht op inzage: Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.
- Recht op correctie: Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren.
- Recht van verzet/beperking: Betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken.
- Recht om vergeten te worden: In gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.
- Recht op overdraagbaarheid van gegevens: de betrokkene heeft het recht zijn aan de gemeente verstrekte persoonsgegevens te verkrijgen en deze gegevens ongehinderd over te laten dragen.

Recht op bezwaar: Betrokkenen hebben het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.
Indienen van verzoek
Om gebruik te maken van de rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden (lees hier meer over op de pagina rechten van burgers) en betreft persoonsgegevens. De gemeente heeft een maand de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. De wijze waarop de betrokkene de gevraagde informatie ontvangt, verschilt per wet. De informatie hierover valt onder de informatieplicht van de gemeente. Binnen een maand zal de gemeente laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij de gemeente, of een

klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene. (Bron 29)

Een verzoek die strafrechtelijke gegevens betreft vanuit de WPG, kan op dezelfde manier worden ingediend. De wijze waarop de behandeling van het verzoek is geregeld, wijkt procedureel af van de AVG verzoeken. Dit is beschreven in het sectorspecifieke beschermingsbeleid. De termijnen zijn hetzelfde.

Geautomatiseerde verwerkingen

Geautomatiseerde verwerkingen zijn verwerkingen met een door software geregeld besluit. Dit type besluiten zijn gebaseerd op van "ingestelde" kenmerken. Er is geen menselijke tussenkomst geregeld.

Profilering (Bron 30)

De wet geeft aan dat er geen besluit mag worden genomen op basis van profilering.
Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt. Bij profilering wordt aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen. Voorbeelden van persoonlijke aspecten kunnen zijn; financiële situatie, interesses, gedrag of locatie. Logaritmen in software kunnen een profilering inhouden. De gemeente zet zich in om te voorkomen dat deze werking ontstaat en zorgt voor menselijke tussenkomst bij besluiten.
Om profilering wat duidelijker te maken, gebruiken we het volgende voorbeeld: Wanneer een bezoeker op de gemeentelijke website naar een bepaalde dienst kijkt, mag de gemeente geen actie ondernemen om de dienst aan te bieden. Gemeenten mogen wel bekijken hoe vaak een bepaalde dienst bekeken is, maar dus niet specifiek gericht adverteren. Dit doen wij niet.

Big data en tracking

Door middel van Big data onderzoek en tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een levende persoon. Daarnaast worden ze alleen verzameld voor onderzoek dat door, of namens, de gemeente wordt uitgevoerd. De verzamelde gegevens door Big data onderzoek en tracking zijn alleen de gegevens die geautoriseerde personen om noodzakelijke redenen voor hun taak verzamelen. Bij het omzetten in een dataset zal dataminimalisatie worden toegepast. Dit betekent dat de gemeente alleen de data gebruikt, die echt nodig is voor het behalen van het doel. Daarnaast kunnen persoonsgegevens versleuteld of gepseudonimiseerd worden, zodat deze voor lezers niet herleidbaar zijn tot een persoon. (Bron 31) De gemeente verkoopt geen data.
Gemeente Steenbergen maakt geen gebruik van tracking met persoonsgegevens. Het gebruik van Big Data wordt op dit moment niet systematisch toegepast. Wij onderzoeken wel welke voordelen het gebruik van Big Data kan hebben voor onze dienstverlening.
Voor beleidsdoeleinden voert de gemeente regelmatig onderzoeken uit. Persoonsgegevens worden dan geanonimiseerd. Deze persoonsgegevens zijn op geen enkele manier herleidbaar tot een persoon en vallen daarom buiten de bescherming van de AVG. (Bron 32)

Inzet van camera's

De gemeente maakt onder bepaalde omstandigheden gebruik van cameratoezicht, zoals vastgelegd in de Gemeentewet. Het gaat hierbij om bescherming van het bezit en van medewerkers. Ook de bodycam van Boa's hebben deze rechtmatige grondslag. Dit inzet is aan stricte regels gebonden.
De gemeente gebruikt ook cameratoezicht voor het vergroten van de veiligheid op straat en het beschermen van gebouwen van de gemeente. De gemeente plaatst de camera's met het doel de Openbare Veiligheid te dienen met de rechtmatige grondslag: publieke taak. Alleen de politie kan deze beelden volgen en opslaan op grond van de Wet Politiegegevens (voortaan: WPG).
Camera's kunnen een grote inbreuk maken op de privacy van diegene die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen, zetten wij camera's terughoudend in. Bij het plaatsen van camera's stelt de gemeente vooraf een onderzoek in. Dit is een GegevensEffectBeoordeling om de risico's voor de belangen van betrokkenen te onderzoeken.

De politie kan video opnamen opvragen en behandelen vanuit de WPG. Pas na een verzoek van de politie of het Openbaar Ministerie werkt hieraan mee. Deze WPG verwerking voor opsporing en vervolging van strafbare feiten, valt buiten de verwerkingsverantwoordelijkheid van de gemeente.

Plichten van de gemeente

Register van verwerkingen (Bron 33)

De gemeente – als overheid- is wettelijk verplicht een register van alle verwerkingen aan te leggen en te beheren. Ze vervult daarin bijna altijd een verwerkingsverantwoordelijke rol. Elk register bevat wettelijke en aanvullende beschrijvingen van de verwerkingsactiviteiten, zoals:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- De doelen van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen; Een beschrijving van de ontvangers van de persoonsgegevens;
- Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van veiligheidsmaatregelen

De verwerkingen onder de WPG zijn in een WPG-Register van Verwerkingen beschreven. De opbouw van het Register is anders. Een voorbeeld is de grondslag.
Verwerkingen bij de Jeugdzorg vallen onder de AVG en neemt de gemeente op in dat Register van Verwerkingen.

Andere Registers

In het kader van aantoonbaar voldoen aan de AVG, houdt de gemeente aanvullend op het Register van Verwerkingen een aantal andere Registers bij. Deze Registers worden in de AVG niet genoemd, maar zijn wel noodzakelijk dienstverlening bij Landelijk Toezicht en het behouden (informatie)veiligheid.

De behandelingen in het kader van de WPG worden in dezelfde soort, maar eigen registers bijgehouden.

Register Gegevens Effect Beoordelingen
Gehouden onderzoeken, de risicotaxaties, worden in een Register vastgelegd. Het gaat om pre-DPIA's en DPIA's.
Register privacy-overeenkomsten
De gemeente houdt bij welke privacy overeenkomsten zijn afgesloten en is alert dat de overeenkomst is getekend voordat het delen van informatie begint. Tot de privacy-overeenkomsten behoren ook de afspraken die gemaakt zijn bij Doorgifte.
Register incidenten
Datalekken, onveilige situaties en veiligheidsincidenten zijn in dit register beschreven.
Register van Rechtsverzoeken
De ontvangen verzoeken worden vastgelegd.
Register van Toestemmingen
Indien verwerkingen een grondslag "Toestemming" hebben, wordt iedere activiteit met een Toestemming vastgelegd. De privacy-wetten willen dat deze wilsuitingen voldoen aan "vrij gegeven, uitdrukkelijk, doelgebonden"-vereisten voldoen. Een toestemming is altijd intrekbaar, maar kan niet altijd met terugwerkende kracht ongedaan worden.

Gegevensbeschermingseffectbeoordeling (Bron 34)

De gemeente beschermt privacy en informatie door een mix van maatregelen op het gebied van Mensen, Processen en Technieken. Onze maatregelen zijn risico gebaseerd. Het grootste risico krijgt voorrang. Het gaat daarbij om de juiste balans tussen informatieveiligheid en gebruiksgemak, waarbij veiligheid het zwaarste weegt.
Met een gegevensbeschermingseffectbeoordeling (voortaan: GEB) worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld voor de bescherming van de privacy van de betrokkene(n). De gemeente voert deze GEB uit bij nieuwe verwerkingen, een geautomatiseerde verwerking, een grootschalige verwerking, of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt. Daarnaast voert de gemeente deze beoordeling planmatig uit op grond van landelijke aanwijzingen van de Autoriteit Persoonsgegevens (voortaan: AP). Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt. De instrument zijn een **pré-DPIA en DPIA**. (bron 35) Een pré-DPIA bevat de toetsingskader van de Europese en Landelijke Autoriteit voor het houden van een verplicht taxatie-onderzoek. Een uitgevoerde GEB is vastgelegd in het Register van Risicotaxaties.

Functionaris voor gegevensbescherming (voortaan: FG) (Bron 36)

De gemeente heeft binnen een regionaal samenwerkingsverband van gemeenten FG's aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoons-/politiegegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de AP. De FG onderhoudt contacten met het bestuurlijk orgaan en rapporteert de voortgang van privacy-ontwikkeling met onafhankelijke adviezen. Het is de bedoeling dat de functionaris de uitvoering op het gebied van bescherming van de privacy aan de organisatie over laat. De teams hebben hun eigen verantwoordelijkheid om te voldoen aan de verplich-

tingen van de AVG. 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 is ook de onafhankelijke toezichthouder van de WPG. De gemeente heeft de aanstelling voor de WPG formeel besloten. Deze en andere vereisten uit de WPG zijn terug te vinden in het sectorspecifieke beleid WPG.

Incidenten (Bron 37)

Formeel heeft de AVG het over "inbreuken" . Er zijn verschillende vormen van "inbreuken". We spreken van een datalek wanneer persoonsgegevens in handen vallen van personen die geen toegang tot die gegevens mogen hebben. Of wanneer er sprake is van verlies van persoonsbonden gegevens. Dit kan ook ontstaan door beschadiging of een verandering van deze gegevens.
Bij een datalek meldt de gemeente dit zonder onredelijke vertraging binnen 72 uur aan de Landelijke Toezichthouder (AP). Als dit later dan 72 uur is, wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval is de gemeente wettelijke gehouden dit aan de betrokkenen in eenvoudige en duidelijke taal te melden. Om toekomstige datalekken te voorkomen worden datalekken, onveilige situaties en veiligheidsincidenten geregistreerd en geëvalueerd. De gemeente handelt een melding volgens een protocol en procedure af en administreert meldingen in een Register Incidenten.

Afsluiting

De wijze waarop de privacy-organisatie binnen de gemeente werkt, is vastgelegd in beleid, protocollen, werkinstructies en planningen. Dit beleid betreft "Bestuurlijke inrichting privacy organisatie".
Als de gemeente een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen. Deze zal via de klachtenregeling van de gemeente worden behandeld. In gevallen waar het reglement niets over zegt, beslist het verantwoordelijke bestuursorgaan van de gemeente.

Wettelijke grondslagen waarop de verwijzing is gebaseerd:
Bron 1 : Grondwet Art 10; GDPR Art 1
Bron 2 : www.ec.europa.eu
Bron 3 : Art 5. lid 1 en 2 AVG
Bron 4 : Art 5. lid 2 AVG; Art 24 – 29 AVG.
Bron 5 : CMMI instituut: Capability Maturity Model Integration is een trainings- en beoordelingsprogramma voor procesverbetering, ontwikkeld aan de Carnegie Mellon University in USA
Bron 6 : Art. 40 AVG (gedragscode); Art. 35 AVG (Gegevenseffectbeoordeling)
Bron 7 : Art. 25 AVG
Bron 8 : Art. 32 AVG
Bron 9 : Art. 24-29 AVG
Bron 10: Art. 5, lid 1, f AVG ; Art 32 AVG
Bron 11: Art. 4 lid 2 AVG
Bron 12: Art. 5 AVG
Brond 13: zie Bron 12
Bron 14: Art. 6, AVG
Bron 15: (Art. 4 lid 1)
Bron 16: Art. 10 AVG
Bron 17: Art. 32 lid 4 AVG; Art 9 2a-b AVG
Bron 18: Art. 30 AVG
Bron 19: Art. 5 lid 1b-c AVG
Bron 20: Art. 5 lid 1d AVG
Bron 21: Art. 32 AVG
Bron 22: Art. 32 lid 1 AVG
Bron 23: Art. 24 t/m 29, AVG
Bron 24: (Art. 44 t/m 50, AVG)
Bron 25: Art 44 en 45 lid 1 AVG; Art 15 lid 2 AVG
Bron 26: Art 13 en 14, AVG
Bron 27: Art 17 lid 1a
Bron 28: Art. 13 t/m 20 AVG
Bron 29: Art 15 lid 4
Bron 30: Art. 22, AVG
Bron 31: Recitals 26, 28, 29; Art 4 lid 5 AVG; Art 32-1a AVG
Bron 32: Art 5 lid 1b; Art 89.
Bron 33: Art 30, AVG
Bron 34: Art. 35, AVG
Bron 35: www.informatiebeveiligingsdienst.nl en wegingskader AP
Bron 36: Art. 37 t/m 39, AVG
Bron 37: Artikel 33,34, AVG

Bijlage 1 Bestuurlijke organisatie privacybescherming

Een compacte beschrijving van rollen, taken en verantwoordelijkheden bij bescherming privacy en daaraan gerelateerde informatieveiligheid
Auteurs : Structuurgroep Privacy en Informatieveiligheid
Datum : Oktober 2022
Vastgesteld : College B&W dd. 13 december 2022

1. Beschrijving van de privacybeschermingsrollen van de gemeente

De Algemene Verordening Gegevensbescherming stelt een organisatie verantwoordelijk voor de verwerking van de persoonsgegevens.
De Verordening is van de hoogste juridische orde binnen de Europese Unie en verplicht iedere verwerkende organisatie een verantwoordelijke rol aan te nemen.
De gemeente neemt verwerkingsverantwoordelijkheid bij het verwerken van persoonsgebonden informatie. Binnen een samenwerking met een andere organisatie, de partner, handelt de gemeente vooraf vanuit een zelfstandig verwerkingsverantwoordelijke rol. Een verwerkingsverantwoordelijke bepaalt bij verwerkingsactiviteiten zelf de doelen en de middelen. (Art. 24 AVG). Verwerkingsverantwoordelijke partners kunnen met elkaar een gezamenlijke nemen en daarover afspraken maken. (Art. 26 AVG) Een andere rol binnen een samenwerking is die van verwerker. Een verwerker volgt de aanwijzingen op en dient te voldoen aan aanwijzingen over het veiligheidsniveau van de verwerkingsverantwoordelijke. (Art. 28 AVG) Een partner kan een andere gemeente zijn, een leverancier of uitvoeringsorganisatie. Wat betekent dit in de praktijk?
De gemeente is zelfstandig verwerkingsverantwoordelijke voor de verwerkingsactiviteiten en legt de rolverdeling in een passende privacy-overeenkomst vast. Iedere partner moet in staat zijn de genomen passende maatregelen en verantwoordelijkheid aan tonen.
Welke rol de gemeente ook uitvoert, in alle gevallen is het noodzakelijk een verdeling van verantwoordelijkheden en taken binnen de organisatie aan te houden. De verordening vereist dat een organisatie aantoonbaar voldoet aan de eisen van de privacybescherming en hierover toegankelijk en transparant is. (Art. 5 AVG)

Bij het toepassen van de Wet Politie Gegevens voorziet de gemeente ook in een verdeling van verantwoordelijkheden en taken. Bij opvallende verschillen, worden deze in de toegevoegde kaders geduid. De gemeente gebruikt een sectorspecifiek beleid voor verwerkingen vanuit de WPG.

Dit beschermingsbeleid is opgedeeld in een beschrijving van :

- interne verantwoordelijkheden, gevolgd door
- Overzicht van overlegvormen
- Overzichten per “instrument” met een taakverdeling.

Interne verantwoordelijkheden.
Dit overzicht geeft in één oogopslag aan, hoe de interne verantwoordelijkheid bij de bescherming van privacy en informatieveiligheid is verdeeld:
Functie Verantwoordelijkheden binnen de Privacy organisatie

- Gemeenteraad
- Griffier
- College van B&W
- Gemeentesecretaris
- Managers
- Proceseigenaar Werkproces(sen)
- Medewerker
- Chief Information Security Officer (CISO)
- Privacy Officer (P.O.)
- Functionaris Gegevensbescherming (FG)
- Wettelijk verwerkingsverantwoordelijke griffie
- (Hoogst)Verantwoordelijke ambtelijke organisatie
- Wettelijke verwerkingsverantwoordelijk
- (Hoogst)Verantwoordelijke ambtelijke organisatie
- Uitvoeringsverantwoordelijke/verantwoordelijke van het team
- Adviserend medewerker werkproces/activiteit
- Verwerkende van informatie
- Adviseur/Beheerder privacy gerelateerde informatieveiligheid
- Ondersteuner implementatie AVG / WPG, adm. beheerder
- Wettelijke AVG adviseur en onafhankelijk toezichthouder

Bij de inrichting van de privacy-organisatie is uitgegaan van het principe van drie verdedigingslinies. De eerste en belangrijkste verdediging is het wordt gevormd door alle medewerkers. Een medewerker kent de eigen omgeving, taken en activiteiten. Afwijkingen in gedrag en informatiehuishouding zijn reden om deze te signaleren naar de tweede verdedigingslinie.

De tweede verdedigingslinie wordt gevormd door de CISO (Informatieveiligheid) en P.O. (Privacy). Zij adviseren passende aanvullende maatregelen aan het lijn-management en na een beslissing voeren zij deze vanuit hun vakgebied uit. Zij informeren de derde verdedigingslinie.
Door onafhankelijk toezicht van de FG wordt de derde verdedigingslinie gevormd. De FG adviseert het bestuurlijke orgaan en indien nodig naar medewerkers van de tweede en/of eerste verdedigingslinie.
De privacybescherming is juridisch opgebouwd en verwoordt juridisch beschreven Bedrijfskundige principes Het integreren van de wetten voor privacybescherming gaat volgens het principe van groeien in volwassenheidsniveau's. Het proces daarnaar toe en het onderhouden van de mate van integratie van deze wetten in de bedrijfsprocessen en dienstverlening, is gebaseerd op normstelsels (BIO en AVG Borging) en het gebruik van Plan-Do-Check-Act.
De mate waarin de gemeente voldoet, wordt door evaluatie per uitgevoerd ontwikkelpunt bepaald en door het afnemen van audits en de FG jaarrapportages.
Hieronder is beschreven vanuit welk organisatieniveau welke organen en functies betrokken zijn bij de uitvoering van bescherming.

Toezichthouder en bestuur

Gemeenteraad

De gemeenteraad heeft een eigen verwerkingsverantwoordelijkheid. Ze vervult een bestuurlijke toezichthoudende rol en verantwoordelijke rol voor de eigen verwerkingen van persoonsgegevens binnen de griffie. Het toezicht op het functioneren van de gemeente bestaat uit een klankbord voor het college B&W en de ambtelijke organisatie. Het gaat om het invoegen van de (U)AVG richtlijnen in beleid, protocollen, procedures en werkzaamheden. De raad laat zich informeren door het college B&W en de adviezen van de Functionaris Gegevensbescherming. Het gaat hierbij tenminste om advies bij bewustwording over privacybescherming en de FG rapportages. Binnen gemeenschappelijke regelingen en in samenwerkingsvormen, die de griffie-organisatie rechtstreeks aangaan, beweegt de griffie zich als zelfstandig verwerkingsverantwoordelijke. Namens college B&W sluit, de Burgemeester deze overeenkomsten af.

Griffier

De griffie is de ambtelijke organisatie-eenheid voor ondersteuning van de Gemeenteraad.
De verantwoordelijkheid voor privacybescherming binnen de griffie-organisatie ligt bij de griffier. Deze functionaris is verantwoordelijk voor alle verwerkingen met persoonsgegevens en voor AVG instrumenten van de Griffie om te voldoen aan de AVG. Beschreven verwerkingen van de griffie zijn te vinden in het AVG register van de gemeente.

College van B&W

Het College van B&W van de gemeente Steenbergen vormt het bestuur van de gemeente en is de 'verwerkingsverantwoordelijk' in de zin van de Algemene Verordening Gegevensbescherming (AVG). Zij is verantwoordelijk voor alles wat te maken heeft met de bescherming van persoonsgegevens binnen de gemeente. Binnen gemeenschappelijke regelingen en samenwerking waarin meerdere partners actief zijn, kan de gemeente optreden als een gedeelde en een zelfstandig verwerkingsverantwoordelijke. Dit komt tot uitdrukking in afspraken binnen een passende privacyovereenkomst. Het college stelt op hoofdlijnen de kaders over de privacybescherming vast. De basis van kaders zijn en Landelijke en Europese privacybeschermingswet- en regelgeving (AVG, UAVG, WPG en Jeugdwet) en Landelijke normen (BIO/AVG borging).
Het college is verantwoordelijk en daarmee aanspreekbaar voor een duidelijk te volgen privacy-beleid en de uitvoering daarvan. Zij stimuleert het management van de ambtelijke organisatie om tijdig maatregelen te nemen, zodat persoonsgegevens van betrokkenen (=inwoners/medewerkers) zijn beschermd. Het college heeft de uitvoerende verantwoordelijkheden voor privacybescherming neergelegd in de ambtelijke organisatie. Bevoegdheden zijn vastgesteld in een mandaatregeling.

De ambtelijke organisatie

Algemeen Directeur / Gemeentesecretaris

De verantwoordelijkheid voor het privacybescherming binnen de ambtelijke organisatie ligt bij de Algemeen Directeur die ook de rol van Gemeentesecretaris vervult. Deze is de hoogst aangestelde ambtenaar is benoemd door het College van Burgemeesters en Wethouders. Hij is belast met de ondersteuning van het college en met de zorg voor het ambtelijke organisatie. Hij is verantwoordelijk voor alle verwerkingsactiviteiten binnen de ambtelijke organisatie, die vallen onder het College B&W. Het Directeur stelt in samenspraak met het managementteam de protocollen, procedures, werkinstructies en acties vast om het gewenste niveau van informatieveiligheid en privacy te bereiken. De Directeur laat zich informeren door de privacy-adviseurs CISO en PO. Hij onderhoudt een regulier overleg met de gemeentelijke onafhankelijke toezichthouder, de functionaris Gegevensbescherming.

Managers

De manager is verantwoordelijk voor het integrale management van het team. Daarmee is de manager verantwoordelijk voor het resultaat van wettelijke privacybescherming en de beschikbare inzet van middelen om hieraan te voldoen. De manager legt verantwoording af aan de Algemeen Directeur/Gemeentesecretaris. Managers hebben te maken met keten- en bedrijfsprocessen van hun team. De manager draagt zorg voor een vereiste beschrijving van verwerkingsprocessen van het team in het Registers van Verwerkingen.De manager coördineert aangemelde incidenten, bewaakt en zorgt dat GEB (Gege-

vensEffectBeoordelingen) op tijd zijn uitgevoerd, neemt beslissingen over passende maatregelen, zorgt dat het wettelijke kennisniveau van medewerkers in het team voldoet, borgt de informatieplicht naar betrokkenen, bereidt met partners privacy-overeenkomsten voor en stimuleert medewerkers om beleid, procedures en werkinstructies te volgen. De manager onderhouden een regelmatig overleg met de CISO en PO over de voortgang van de privacy-ontwikkeling, waartoe het uitvoeren van maatregelen, het leveren van informatie en het beheren van Registers.

Medewerker/proceseigenaar werkproces

Binnen ieder team zijn een of meer medewerkers als proceseigenaren taakverantwoordelijk gesteld. Een proceseigenaar houdt de uitvoering van een of meerdere verwerkingsactiviteiten/werkprocessen in de gaten. Bij wijzigingen van de verwerkingsactiviteit binnen het bedrijfs- en/of werkproces, meldt deze proceseigenaar de verandering aan de manager, aan de CISO en de P.O. De taakeigenaar is betrokken bij het (her)schrijven van de verwerking in het Register van Verwerkingen. De beschrijvingen bevat verschillende AVG-vereisten, zoals gehouden GegevensEffectBeoordelingen, afgesloten Overeenkomsten, applicaties, soort persoonsgegevens, de categorieën betrokkene en ontvangers. Wijzigingen in een verwerking of het vervallen ervan, kunnen verschillen acties veroorzaken. De CISO en P.O. zullen de proceseigenaren bij de uitvoering van deze taken betrekken. Voor collega's zijn de proceseigenaren de kennisdrager van de verwerking en vervullen een voorbeeldtaak bij de bescherming van privacy en informatieveiligheid.

Proceseigenaren borgen de kwaliteit van het werkproces dat een dynamisch karakter heeft.

De WPG is in 2019 aangepast voor het verwerken van politiegegevens door de gemeente. Bijzondere opsporingsambtenaren (BOA's) mogen deze gegevens verwerken vanuit hun "Domein". Bij de wettelijke wijzigingen is rekening gehouden met de AVG richtlijnen voor privacybescherming.
Bij het verwerken van "zwaardere" politiegegevens (Art 9 WPG) is de gemeente verplicht een Bevoegde Functionaris aan te stellen voor het beheer. Deze functionaris beschermt privacy van de betrokkenen en het uitvoeren van onderzoek en opsporing. Vanuit het beheer werkt deze functionaris mee aan rechten van de betrokkene, zoals verzoek om inzage, wissing, rectificatie.
Het beantwoorden van WPG rechtsverzoeken is toebedeeld aan een beslissende functionaris. Bij de politie is dat de Korpschef; bij de gemeente de Burgemeester. Voor het juiste gebruik van de WPG heeft de manager ook proceseigenaren in het team. Dit gebeurt alleen in teams waar Boa's werken.

Medewerker ("morgenmakers")

Medewerkers kunnen ambtenaren zijn die direct in dienst of indirect voor de gemeente in dienst zijn. Zij werken binnen een of meerdere teams.
Iedere medewerker doet aantoonbare inspanningen om over actuele relevante kennis te hebben over de bescherming van privacy. Binnen het team is iedere medewerker verantwoordelijk voor de uitvoeren van wettelijk beschermingsvereisten. Iedere medewerker houdt zich aan de gedragscode, geheimhoudingsverklaring, het vastgesteld privacy beleid, protocollen en werkinstructies om een privacy- en informatieveilige omgeving te bereiken. De medewerker past aantoonbaar de privacywetten en regels toe in hun werkpraktijk. Een medewerker werkt vooral vanuit voorliggende wetten.
Deze inrichting van privacy-organisatie heeft het uitgangspunt dat de medewerker in de gaten heeft wanneer de voorliggende wetten te weinig privacybescherming biedt voor de betrokkene(n). Het ontbreken van deze kennis is voor de medewerker een directe reden om zich te verdiepen in de geldende richtlijnen en vereisten uit de privacywetten.
Een vereiste is het gebruik van Beginselen uit de AVG (art 5 AVG). Voorbeelden zijn: De medewerker begint niet aan een verwerking van persoonsgebonden informatie als daarvoor geen doel en rechtmatige grondslag is. Verwerken van persoonsgebonden informatie is noodzakelijk, minimaal, niet op een andere manier te doen en gebonden aan een (landelijk bepaalde) opslagtermijn. Het bewaren van persoonlijke informatie op papier, in de eigen zakelijke digitale omgeving, bij chatdiensten valt onder de archiefwet. Voor het beginsel transparantie, heeft de medewerker kennis van de verwerking om de informatieplicht naar betrokkene(n) uit te kunnen verzorgen. Het verwerken van informatie gebeurt ook behoorlijk en aantoonbaar, zodat betrokkenen hun wettelijke recht kunnen gebruiken. De medewerker is bij het delen van persoonlijke informatie buiten de gemeente alert op de aanwezigheid van een getekende privacy-overeenkomst, die in Corsa NXT is geregistreerd. Hij/Zij signaleert onveiligheid en incidenten naar de eigen manager, proceseigenaren van deze werkprocessen en collega's in hun team. De medewerker overtuigt zichzelf dat een nieuwe verwerking is gecontroleerd op het risico voor de betrokkene(n). Een medewerker heeft een verantwoordingsplicht.

Een Buitengewone Opsporings Ambtenaar (Boa) is door de gemeente aangesteld, beschikt over autorisatie en een erkende status om WPG gegevens te mogen verwerken. Een Boa heeft te maken met de AVG en WPG. Persoonsgebonden informatie die de Boa verwerkt, kan van het hoogste risiconiveau zijn. Verkeerd gebruik kan de betrokkene benadelen! Denk hierbij aan het krijgen van een vergunning, behouden van werk, toegang tot een bankrekening e.d. Een Boa dient erg goed op de hoogte te zijn van beleid, protocollen, werkinstructie en eigen bevoegdheden om de taak uit te voeren én de privacybelangen van de betrokkene(n) zo goed mogelijk te beschermen. De WPG is beschreven als specifiek privacybeschermingsbeleid WPG.

Adviseurs

Functionaris Gegevensbescherming

Door de gemeente aangestelde functionaris privacybescherming die de wettelijke onafhankelijke toezichthouder is.

CISO

Functionaris die adviseert over het te voeren beleid over de veiligheid en de informatieveiligheid van de gemeente.

Privacy Officer

Functionaris die ondersteunt bij de implementatie van privacybescherming bij de gemeente. Beheerder van Registers en behandelaar van AVG/WPG rechtsverzoeken en gemelde inbreuken van privacybescherming.

Overlegvormen rond privacybescherming en daaraan gerelateerde informatieveiligheid

Voortgang overleggen

- **De POHO-overleg Privacy**
  De POHO laat zich, als bestuurder namens het College B&W informeren over de privacy-ontwikkeling op hoofdlijnen door de FG en PO
- **Directie overleg**
  De Algemeen Directeur heeft een regulier afzonderlijk overleg met FG, PO en CISO
- **Directie en Management Team (DT/MT)**
  Binnen de ambtelijke organisatie neemt het Directie Team besluiten en deelt deze met het Management Team. Zij nemen de besluiten over prioriteiten bij de ontwikkeling en beheer van privacybescherming
- **Structuurgroep**
  De stuurgroep is een beleidsvoorbereidend en adviserend overleg van een lid van het DT/MT, de FG, PO en CISO.

- **Privacy team**
  Van ieder team zal voorzien in en afgevaardigde aan dit overleg met het doel signalen op te vangen en te bespreken over privacy-issues. Bij het uitbrengen van dit privacy beleid zijn de leden van het Managementteam de privacy-ambassadeur van hun team.
- **Teamoverleg**
  De manager van ieder team initieert team overleggen met eigen medewerkers

2. AVG-instrumenten bij de verwerking

Om te voldoen aan de Beginselen van de AVG (Art 5.AVG) wijst de Verordening verantwoordelijkheden aan bij het verwerken van persoonsgegevens.
De AVG beschrijft ook wettelijke instrumenten, die ieder een eigen rol vervullen om aantoonbare privacybescherming te behouden.
2.1 Matrixen met Verantwoordelijkheden en Taken binnen ambtelijke organisatie
Voor een effectieve ontwikkeling en behoud van de privacy-ontwikkeling is het nodig om verantwoordelijkheden en taken te benoemen. De matrixen geven in een oogopslag de samenhang ervan weer.
De gemeente gebruikt “wettelijke instrumenten” om de privacybescherming aantoonbaar te organiseren.

1. Bewustwording
2. Register van verwerkingen
3. Register van Privacy-overeenkomsten
4. Register van wijze behandelen vermoeden Incidenten (“inbreuken”)
5. Register en afhandelen Gegevens Effect Beoordeling (Data Protection Impact Assessment (DPIA en pre DPIA)
6. Register over afhandelen verzoeken rechten van betrokkenen m.b.t persoonsgegevens
7. Register toestemming

Daarnaast hebben de adviseurs een verantwoordelijkheid en taakverdeling bij het integratie-ontwikkelproces AVG/WPG:

8. Ontwikkelen en beheer van beleid, procedures, handreikingen en formats
9. Deelname overleg Informatieveiligheid en privacy

Bewustwording

Het is een AVG verplichting van de gemeente om aan te voldoen. Dit kan verschillende vormen aannemen en in regionaal samenwerkingsverband plaatsvinden. Bewustwording en prioriteiten komen ook tot stand door audits en verbeterplannen, incidenten en voorbeeldsituaties, wensen van medewerkers/verantwoordelijken en FG rapportage (PDCA). Bewustwording wordt in verschillende vormen herhaald om nieuwe kennis en ervaring in de werkomgeving te laten landen.

1 Bewustwording: ondersteuning van organisatie

- De verantwoordelijken zorgen voor aandacht voor informatieveiligheid en privacy onder alle medewerkers (bewerkers)
- De Algemeen Directeur is de gedelegeerde verantwoordelijke voor de bewustwording binnen de ambtelijke organisatie.
- De Manager heeft een uitvoerende verantwoordelijkheid. De Privacy Officer, Functionaris Gegevensbescherming en CISO geven gevraagd en ongevraagd advies aan de organisatie (medewerkers en management) en bestuur met betrekking tot privacyvraagstukken
- De CISO en Privacy Officer ondersteunen de proceseigenaar en medewerkers bij de keuze van relevante voorlichting op het gebied van privacy en informatieveiligheid. Samenspraak met de verantwoordelijken organiseren zij voorlichting, zoals bij nieuwe medewerkers, informatie op intranet en campagnes.

	Verantwoordelijke. (Directeur | Manager)	Proceseigenaar	Medewerker	Privacy Officer	CISO	FG
• Gevraagd en ongevraagd ondersteunen advies verlenen aan bestuur, management en medewerkers met betrekking tot privacyvraagstukken				X	X	X (Onafh. Advies)
• Voorlichting en communicatie over privacy (bewustwording) aan de organisatie	Besluit	X (verwerking)		X	X	X
• Continue aandacht voor informatieveiligheid en privacy binnen de gemeente	X		X	X	X	
• Delen van leerervaringen met privacy en informatieveiligheid	X	X	X	X	x	X

Registers van Verwerkingen
Het aantonen van een verwerkingen betreft persoons- en politiegegevens. Een beschrijving van een verwerking naar VNG voorbeeld, heeft een gedeeltelijke basis in de wetten (AVG en WPG). Wat niet in de wet is beschreven, heeft zijn nut in de praktijk bewezen. Het gaat om aantonen. Een beschrijving van een verwerking bij de gemeente is mede gebaseerd op applicaties die vanuit de Archiefwet voortkomen. De bron daarbij zijn de selectielijsten van de VNG, die zijn verwerkt in de applicatie I-navigator. De AVG en WPG Register van Verwerkingen hebben ieder een eigen opstelling. Artikel 9 politiegegevens dienen beheerd te worden door een bevoegd functionaris (Boa)

Beheer van het register van verwerkingen

- **De verantwoordelijken delegeren het beheer van de verwerkingen zelf aan de proceseigenaren om de actualiteit en juistheid van de verwerkingen in het register van verwerkingsactiviteiten te borgen. De manager besluit over de verwerking van de persoonsgebonden gegevens. Dit is inclusief het gesignaleerde risico. De manager legt het besluit vast!**
- **De manager stimuleert het gebruik van beschrijvingen van verwerkingsactiviteiten (procesgericht werken) en faciliteert de ontwikkeling daar naar toe. In taakverdeling, kwaliteit, budget en tijd.**
- **De Privacy Officer beheert het overzicht van verwerkingsactiviteiten van het team en (landelijke) format. Hij ondersteunt het team bij het beschrijven van verwerkingen.**
- **De Privacy Officer ondersteunt het naleven van het beleid en beheert het register AVG/WPG en de publieksversies.**
- **De CISO ziet toe op de registratie van passende technische en organisatorische maatregelen , niveau beveiliging (BIO norm), gebruikte software en leveranciers.**
- **De Functionaris Gegevensbescherming ziet toe op kwaliteit van de beschrijving van de verwerkingen in het Register.**

Activiteiten	Verantwoordelijken (directeur|manager)	Bevoegde functionaris (WPG art.9)	Proceseigenaren	Medewerker	Privacy Officer	CISO	FG
• **Nieuwe projecten melden aan P.O. en CISO, aanwijzen proceseigenaren en hen verwijzen naar P.O.**	**X**			**X**	**X**	**X**	
• Actieve aanlevering van nieuwe en veranderde		**X (FG)**	**X**				

	verwerkingen bij de P.O. en de FG						
•	Werken vanuit de werkprocessen (register in digitale bibliotheek)	X	X	x	X	x	X	X
•	Zorgdragen voor actualiteit van verwerkingen(register)		X	X				
•	Check van(beschrijving) beveiligingsmaatregelen		X				X	
•	Coördinatie van de actualisatie van register van verwerkingen			X		X		
•	Beheer van Register van Gegevensverwerkingen (organisatie en publieke versie)			X		X		
•	Toetsing op kwaliteit, actualiteit, juistheid en volledigheid van (register van) Verwerkingen	X		x		X		X
•	Rapporteren over toetsing						X	X

Privacy-overeenkomsten binnen EU/EER en daarbuiten
De gemeente gebruikt verschillende type privacy-overeenkomsten. De gemeente is een verwerkingsverantwoordelijke partner. Buiten de EU/EER gelden andere privacy-overeenkomsten, die meer zekerheid moeten bieden aan privacybescherming van ingezetenen van de EU/EER. De Landelijke toezichthouder heeft een actieve rol bij deze overeenkomsten. Zonder goedgekeurde overeenkomst = niet delen van persoonsgebonden informatie.
WPG politiegegevens worden door de gemeente niet gedeeld buiten het grondgebied EU/EER. **Privacy-overeenkomsten binnen EU/EER en daarbuiten**
De gemeente gebruikt verschillende type privacy-overeenkomsten. De gemeente is een verwerkingsverantwoordelijke partner. Buiten de EU/EER gelden andere privacy-overeenkomsten, die meer zekerheid moeten bieden aan privacybescherming van ingezetenen van de EU/EER. De Landelijke toezichthouder heeft een actieve rol bij deze overeenkomsten. Zonder goedgekeurde overeenkomst = niet delen van persoonsgebonden informatie.
WPG politiegegevens worden door de gemeente niet gedeeld buiten het grondgebied EU/EER.

Registratie, beheer en actualisatie van privacy-overeenkomsten met verwerkers en mede-zelfstandig verwerkingsverantwoordelijken
- De verantwoordelijken sluiten de overeenkomsten af door ze te ondertekenen.
- De Privacy Officer is verantwoordelijk voor de beschikbaarheid van een actuele model privacy overeenkomst (AVG |WPG).
- De Privacy Officer, Functionaris Gegevensbescherming en CISO ondersteunen de proceseigenaar bij het proces van aangaan van de privacy overeenkomst.
- De Functionaris Gegevensbescherming (FG) ziet er op toe dat de werkwijze volgens de (Europese) privacywetgeving verloopt. De FG ziet toe op de beschikbaarheid, integriteit, vertrouwelijkheid van de registratie en wijze van archivering.

Activiteiten	**Verantwoordelijken (directeur|manager)**	**Proceseigenaren**	**Medewerker**	**Privacy Officer**	**CISO**	**FG**
• Aanwijzen proceseigenaren / contactpersoon naar derden partij en hen verwijzen naar P.O.	**X**					
• Afsluiten van verwerkersovereenkomsten	X	X	X (contactpersoon nr. partner)	X		
• Tekenen van privacy-overeenkomst	X (College B&W |DIR)					

•	Actualiseren en beheren van de model privacyovereenkomst				X	X	
•	Ondersteunen van de organisatie bij keuze type. Overeenkomst	X			X	X	
•	Decentrale archivering van verwerkersovereenkomsten (Corsa NXT)		X				
•	Beheer van Register privacy-overeenkomsten				X		
•	Onderzoek bij de ketenpartner op het naleven van de overeenkomst				X	X	
•	Toezicht op registratie van privacy-overeenkomsten						X

VeiligheidsIncidenten

De AVG spreekt over inbreuken en bedoelt daarmee vermoedens datalekken, onveilige situaties en veiligheidsincidenten. Voor de WPG is hiervoor een apart meldingsregister. Deze meldingen kunnen qua grootte en impact voor de betrokkene verschillen. Hierbij wordt rekening gehouden bij het afhandelen en beoordelen van een melding. De Landelijke toezichthouder (AP) hanteert criteria en verwacht bij melding voor medebeoordeling dat de gemeente binnen 72 uur de melding doet op de website van de AP.

Register van wijze afhandelen bij veiligheidsincidenten (“inbreuken”)·

- De medewerker doet de schriftelijke melding aan de PO of CISO en kan ook vooraf daarover bellen.
- De verantwoordelijke besluit over de implementatie van adviezen die voortkomen uit onderzoek en opgenomen in de rapportage.
- De CISO en de P.O. ondersteunen inhoudelijk de procedure die in werking treedt, geven adviezen aan het management en de proceseigenaren van de verwerkingen. De PO beheert het register onder verantwoordelijkheid van de manager, die over de getroffen verwerkingen gaat. bij een veiligheidsincident, het opstellen van een compact verslag gedurende het proces en de centrale registratie van het incident. Zij geven daarnaast advies aan de verantwoordelijken gedurende het doorlopen van de procedure.
- De Functionaris Gegevensbescherming staat zowel de verantwoordelijke(n), CISO als de P.O. bij. Het gaat om het doorlopen van de incidentenprocedure, het uitvoeren van een tweede analyse van feiten en het geven van bestuurlijke advies. Namens de verantwoordelijke voert de FG de melding bij de Landelijke toezichthouder (AP) uit.
- De Functionaris Gegevensbescherming is toetst de implementatie van de adviezen uit de rapportages.

Activiteiten	**Verantwoordelijke (Directeur | Manager)**	**Proceseigenaar**	**Medewerker**	**Privacy Officer**	**CISO**	**FG**
• Intern melden van beveiligingsincident	X	X	X	X	X	X
• Inventariseren van feiten en omstandigheden	X	X		X	X	
• Opstellen verslag				X	X	
• Uitvoeren analyse				X	X	
• Verstrekken advies				X	X	
• In geval van dilemma’s in analyse en / of advies afstemming verzorgen met respectievelijk Privacy Officer, eigenaar, gemeentesecretaris en bestuurder.					X	X
• Opstellen en verstuuren rapportage veiligheidsincident				x	X	

•	Implementeren adviezen uit rapportages	X		X		X					
•	Toetsing op implementatie-adviezen									X	

Gegevens Effect Beoordelingen (pre- en DPIA)
Een beoordeling kan bestaan uit het toetsen van de verwerking en de situatie aan de kaders van de EU en Landelijke Toezichthouder. Deze kaders geven aan wanneer een DPIA verplicht is. Dit onderzoek wordt een pré-DPIA genoemd. Een DPIA is enerzijds het format en anderzijds de aanduiding van een Gegevens Effect Beoordeling. Iedere afgeronde DPIA wordt beoordeeld door de FG. In de DPIA staan verbeteradviezen vermeld om de benodigde informatieveiligheid met passende maatregelen te bereiken.

Register en afhandelen Gegevens Effect Beoordeling (Data Protection Impact Assessment (DPIA en pre DPIA))
- De Verantwoordelijken dragen zorg voor de aanvraag, inbreng van inhoudelijke, functionele kennis, en uitvoer en effectueren van de resultaten van de DPIA en faciliteren het onderzoek naar de risicotaxatie in noodzakelijke tijd en gelegenheid
- De Privacy Officer is verantwoordelijk voor inhoudelijke ondersteuning van de proceseigenaar bij het doorlopen van de procedure die in werking treedt bij uitvoeren van een (pre)DPIA. De Privacy Officer geeft daarnaast, samen met de CISO, advies aan de verantwoordelijke gedurende het doorlopen van de procedure.
- De Functionaris Gegevensbescherming staat zowel de verantwoordelijke als de Privacy Officer bij in raad en daad bij het doorlopen van de DPIA procedure en het geven van inhoudelijk advies.

Activiteiten	**Verantwoordelijke (Directeur | Manager)**	**Bevoegde Functionaris WPG Art 9**	**Proceseigenaar**	**Medewerker**	**Privacy Officer**	**CISO**	**FG**
• Initiëren/aanvragen DPIA	X		X		X	x	X
• Reguliere DPIA's in plan en control cyclus	X				X		
• Uitvoeren DPIA			x		X		
• Inhoudelijke en procedurele ondersteuning van de eigenaar bij doorlopen van de DPIA procedure					X	X	
• Opstellen verslag inclusief aanbevelingen, verwerken en archiveren van de resultaten van de DPIA					X		
• Uitvoeren acties/implementeren maatregelen voortkomend uit DPIA	X				X	x	
• Informatie van de resultaten verwerken in dagelijkse werkpraktijk	X		x	X			
• Toetsen uitgevoerde acties / geïmplementeerde maatregelen							X
• Toetsen op de procedure, de resultaten, de effectuering en de naleving van de resultaten uit de DPIA							X
• Gehouden DPIA (datum en soort risicotaxatie) noteren in Register van Verwerkingsactiviteiten			x				
• Controleren van het Register van Verwerkingsactiviteiten op doorlopende actualiteit DPIA's					x		
• Beheer van Register Risicotaxatie					X		

•	Verzorgen van periodieke managementrapportage risicotaxaties (dashboard)				x		
•	Opnemen van risicotaxaties in jaarrapportage						X

Recht op verzoeken.
Burgers en medewerkers kunnen verzoeken indienen onder verwijzing naar de privacywetten. Ieder verzoek dient binnen 4 weken afgehandeld te zijn.
Dit geldt voor alle persoonsgebonden rechtsverzoeken AVG en WPG. De afhandeling is echter verschillend tussen de AVG en WPG. Dit is zichtbaar in de volgende matrix.
gende matrix.

6 Register over afhandelen verzoeken rechten van betrokkenen m.b.t persoonsgegevens

- De verantwoordelijken scheppen faciliterende condities voor de afhandeling van verzoeken van de rechten van betrokkenen met betrekking tot de persoonsgegevens die onder zijn verantwoordelijkheid vallen. Zij wijzen proceseigenaren aan die een bijdrage leveren tot een effectieve afhandeling van AVG verzoeken.
- De Privacy Officer coördineert de team overstijgende verzoeken van betrokkenen. Dit betekent dat deze de verzoeken in ontvangst neemt, het verzoek uitzet binnen de organisatie, informatie samenbrengt en een terugkoppeling geeft naar de verantwoordelijken en aan de betrokkene.
- De Functionaris Gegevensbescherming ziet toe op de afhandeling van de verzoeken van betrokkenen.

		Verantwoordelijke (Directeur | Manager)	**Proceseigenaar**	**Medewerker**	**Privacy Officer**	**CISO**	**Functionaris Gegevensbescherming**
•	Verantwoordelijk voor het opstellen en onderhouden van beleid en procedure voor afhandeling verzoeken				X	X	
•	Ontvangen van AVG verzoeken en deze verwijzen naar de P.O. via privacy@gemeente-steenbergen.nl	X		X			
•	Aanwijzen van proceseigenaren per verzoek	X			X		
•	Ontvangen, uitzetten vraag binnen de organisatie, verzamelen informatie en terugkoppeling naar aanvrager bij afdeling overstijgend verzoek				X		
•	Identificatie verzoeker		X		X		
•	Verzoek uitvoeren		X		X		
•	Procedureel en inhoudelijk ondersteunen bij de procedure verzoek rechten van betrokkenen persoonsgegevens				X		
•	Optimalisatie van de procedure, verzorgen van communicatie en voorlichting en verkrijgen van draagkracht binnen de organisatie rond de procedure verzoek rechten van betrokkenen persoonsgegevens.				X	X	
•	Toezicht op doorlopen procedure verzoek rechten van betrokkenen persoonsgegevens						X
•	Ieder verzoek opnemen in register AVG verzoeken				X		
•	Periodiek rapporteren verzoeken in managementinformatie				X		

Toestemming

De gemeente verwerkt in sommige situaties op grond van een toestemming. Deze is binnen de privacybescherming wettelijk aan vormeisen gebonden. Een instemmend knikje telt niet. Een toestemming moet vrij gegeven zijn. Er is dus geen sprake van afhankelijkheid. Een toestemming dient uitdrukkelijk gegeven te zijn. De gemeente moet dit kunnen aantonen. Een toestemming is intrekbaar en eindigt daarna in werking. Voor het verwerken is altijd een doelbinding en grondslag nodig. De Gemeente verwerkt voornamelijk op basis van een wettelijke of publieke taak. Door een Register aan te houden bij de verwerkingen met een toestemming, houdt de medewerker bij wanneer een toestemming is gegeven en met welke doelbinding. Een voorbeeld hiervan betreft: foto- en beeldmateriaal waarop betrokkenen zijn afgebeeld en contactgegevens van burgers voor contactbeheer.

Toestemming (AVG)
- De verantwoordelijke zorgt ervoor dat de medewerker die op basis van Toestemming verwerkt een Register Toestemming gaat bijhouden.
- De medewerker vraagt aan de betrokkene om toestemming voor de verwerking te geven. En deze toestemming wordt vastgelegd in het Register Toestemming de medewerker bijhoudt. De medewerker geeft aan de P.o. door dat er een Register toestemming wordt bijgehouden aan de manager.
- De P.O. ondersteunt met een format van het Register.

	Verantwoordelijke (Directeur | Manager)	Proces eigenaar	Medewerker	Privacy Officer	CISO	FG
Voorlichting aan medewerkers die met toestemming in een verwerking werken	X			X		X
Beschikbaar stellen van format	X	X		X		
Een proceseigenaar is beheerder		X				
Ondersteuning bij gebruik		X		X		
Verantwoording	X (rapportage)	X		X		X

Procesbegeleiding naar een hogere mate van integratie van AVG en WPG in bedrijfsprocessen en dienstverlening

Privacybescherming van betrokkenen (burgers en medewerkers) zou tot het DNA moeten behoren van de bedrijfsvoering en dienstverlening van de gemeente.De gemeente bevordert privacybescherming in beleid en prioriteiten. Iedere prioriteit doorloopt de fasen van Onderzoek – Beleidsvorming – Planvorming – Monitoren. Iedere fase wordt op het niveau van onderwerp (prioriteit) afgesloten met een evaluatie met het doel vast te stel-len waar de ontwikkeling zich bevindt. Indien het beleid is vastgesteld en wordt toegepast, wordt deze uitvoering gemonitord door onderzoek, ondersteuning, rapportages en bijstelling van beleid en/of uitvoering. Deze evaluaties sluit de cirkel PCDA en geven inzicht in het volwassen-heidsniveau van de integratie van de privacywetten in besluitvorming, de bedrijfsvoering en dienstverlening. Van belang is dat het bestuur en management de voortrekker zijn van dit ontwikkelproces en medewerkers AVG/WPG aanwijzingen gebrui-ken.Deze ontwikkeling past in een maatschappelijke ontwikkeling waarin de overheid zichzelf steeds veiliger maakt en tegelijkertijd opener is over wat ze doet voor de burger.

Ontwikkelen en beheer van beleid, procedures, werkinstructies en formats
- De Verantwoordelijken wijzen proceseigenaren aan, zorgen voor het initiatief en naleving van het beleid ten aanzien van de betreffende persoonsgegevens die onder zijn verantwoordelijkheid vallen. De taakverantwoordelijke is de afdelings- of teammanager van het organisatieonderdeel dat de betreffende persoonsgegevens verwerkt.
- De Privacy Officer, CISO en FG zijn verantwoordelijk voor de ontwikkeling, het beheer, de optimalisatie en de interne en externe communicatie rond procedures, formats en beleid met betrekking tot privacy. Zij doen dat in nauwe samenwerking met de proceseigenaren bij dit aandachtsgebied
- De Functionaris Gegevensbescherming is verantwoordelijk voor de toetsing op het uitvoeren van het beleid en rapporteert hierover aan de directie en bestuur.

	Verantwoordelijke (Directeur | Manager)	Proceseigenaar	Medewerker	Privacy-Officer	CISO	FG
Aanwijzen van proceseigenaren (communicatie | webmaster)	X					
De ontwikkeling, het beheer, de optimalisatie en de interne en externe communicatie rond beleid, procedures, handreikingen en formats met betrekking tot privacy	X(vaststellen)			X	X	
Het implementeren van het beleid, procedures, handreikingen en formats	X (coördinatie)	X		X (ondersteuning)	X (ondersteuing)	
Het inrichten en beheren van een digitale bibliotheek				X (beheer)	X beheer)	

Het beheer en de archivering van procedures, formats en beleid met betrekking tot privacy				X	X	
Het naleven van beleid, procedures, handreikingen, gebruik juiste formats voor privacybescherming		X	X			
Rapporteren over stand van zaken privacy ontwikkeling	X (tussentijds)			X (evt. redaktie)	X (informatie-veiligheid)	X (FG rapportage)
Toezicht op de kwaliteit, archivering, communicatie en toepassing van procedures, formats en beleid						X

3 Deelname overleg Informatieveiligheid en privacy

- De verantwoordelijke(n) spreken met betrokkenen af wie deelneemt aan dit overleg en de terugkoppeling verzorgt naar de achterban. De directie neemt deel aan het overstijgende overleg bij Equalit
- De CISO zit zowel het gemeente breed informatieveiligheidsoverleg, zoals bij Equalit.
- De FG's nemen namens de gemeente Steenbergen bij Equalit deel aan het privacy overleg
- De Privacy Officer zit het privacy overleg voor.
- De CISO, Privacy Officer en de Functionaris Gegevensbescherming nemen deel aan organisatie brede- en onderdeel specifieke overleggen die privacy- en informatieveiligheidsvraagstukken behandelen. Daartoe loopt er ook regionaal overleg FG/PO met 5 aangesloten gemeenten.
- De P.O., CISO en de Functionaris Gegevensbescherming nemen -op uitnodiging- deel aan team-, project- en thema- overleggen, indien hierbij privacyvraagstukken aan de orde zijn.

Activiteiten	Verantwoordelijke (Directeur | Manager)	Proceseigenaren	Medewerker	Privacy Officer	CISO	FG
• Deelnemen aan overleg VNG						X
• Deelnemen aan de Deelnemersraad Equalit	X					
• Deelnemen aan het TOD Equalit					X	
• Deelnemen aan privacy overleg (FG expertgroep) Equalit						X
• Deelnemen aan het FG / PO overleg 5 gemeenten				X		X
• Deelnemen informatieveiligheidsoverleg					X	
• Deelnemen structuurgroep P&I	X			X	X	X
• Voortgangsoverleg informatieveiligheidsoverleg en privacyoverleg (individueel met manager)	X			X	X	X
• Aanwijzen privacy ambassadeurs (zijn MT -leden)	X					
• Deelnemen aan privacy team		X (teamlid)		x	X (afroep)	X (toezicht)
• Deelnemen aan teamoverleg	X		X	X (afroep)	X (afroep)	X (eigen initiatief)
• Project, team en thema overleggen m.b.t privacyvraagstukken	X	X	X	X	X	X
• Aanwijzen decentraal contactpersoon Informatiebeveiliging & Privacy (b.v.k. privacyteam)	X					

• Contactpersoon Privacy en Informatieveiligheid voor derden bij calamiteiten	X		X	X	X

Bijlage 2 Privacy-beleid Steenbergen