

Privacybeleid

Het college van burgemeester en wethouders van de gemeente Gennepe,

- Gelezen het voorstel van 5 november 2024;
- Overwegende dat de gemeente een verantwoordingsplicht heeft om aan te tonen middels het Privacybeleid dat aan de privacyregels voldaan wordt;
- Gelet op de Algemene Verordening Gegevensbescherming en de Uitvoeringswet Algemene verordening gegevensbescherming;

Besluit vast te stellen het:

PRIVACYBELEID

1. het Privacybeleid treedt in werking op de dag nadat deze is bekend gemaakt;
2. het Privacybeleid gemeente Gennepe vastgesteld op 20 november 2018 in te trekken.

Aldus besloten in de vergadering van 5 november 2024.

Burgemeester en wethouders van Gennepe,

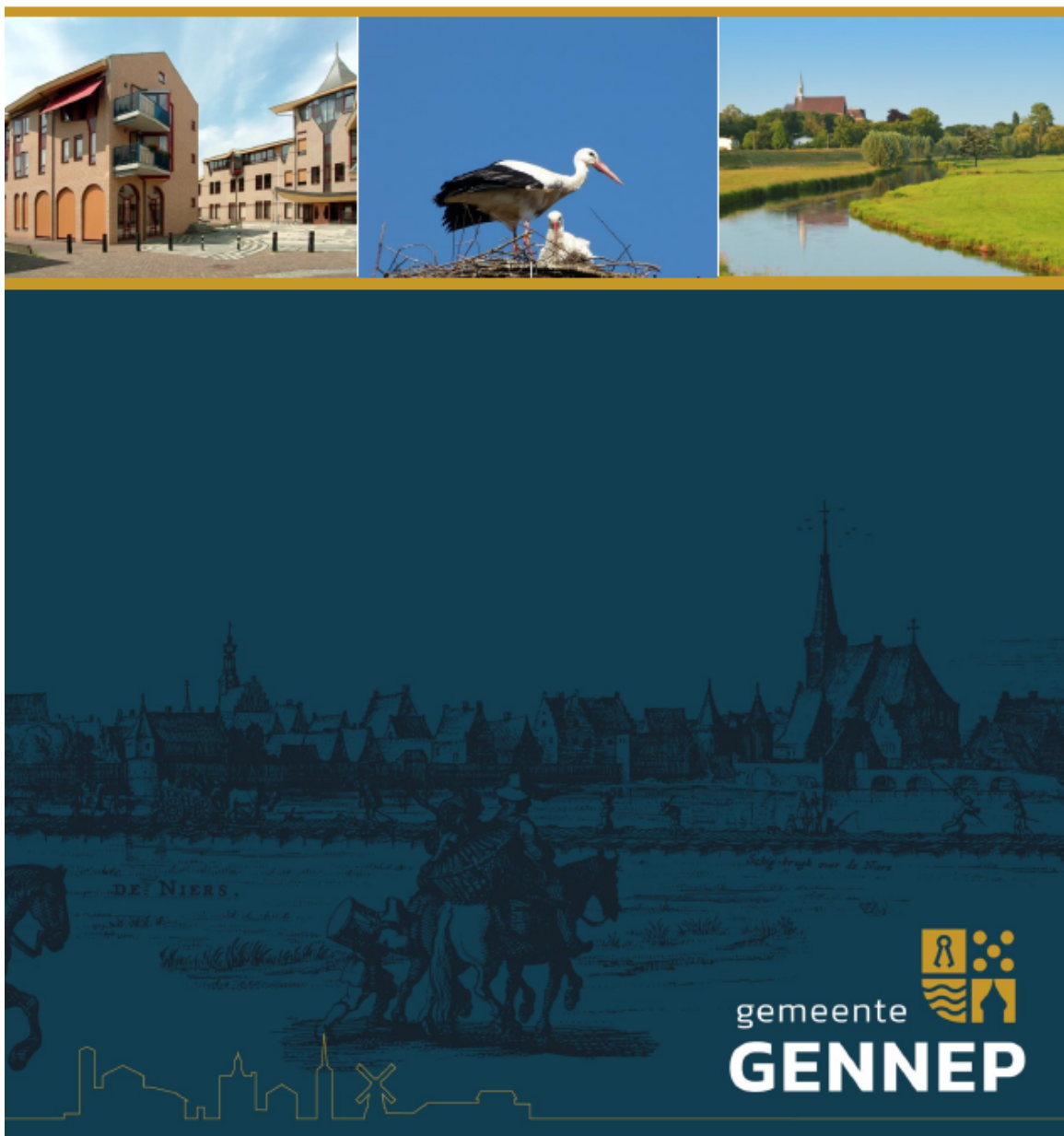
De secretaris, Bart Teunissen

De burgemeester, Hans Teunissen



Privacybeleid

Gemeente Gennepe



Inhoudsopgave

Inhoudsopgave	2
1 Inleiding	3
2 Doel	4
3 Uitgangspunten	4
4 Rollen en verantwoordelijkheden	8
5 Borging en beheersing privacy	11
6 Overige thema's	20
Bijlage 1: Taken en rollen CISO, FG en PO	26
Bijlage 2: Veilig communiceren	Fout! Bladwijzer niet gedefinieerd.

Vastgesteld

Door het college van B&W op 5 november 2024

1 Inleiding

De gemeente Gennep werkt met (persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente om de wettelijke taken goed uit te kunnen voeren. Denk hierbij aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Daarbij kan het gaan om gewone persoonsgegevens, maar ook om bijzondere categorieën van persoonsgegevens. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen en een steeds meer digitale werkomgeving stellen complexere en noodzakelijke eisen aan de bescherming van persoonsgegevens. De gemeente Gennep is zich hiervan bewust en wil daarom met dit privacybeleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy en gegevensbescherming, waaronder de Algemene verordening gegevensbescherming (hierna: AVG), de Uitvoeringswet Algemene verordening gegevensbescherming (hierna: UAVG) en de Wet politiegegevens (hierna: Wpg).

1.1 PRIVACYBELEID

De gemeente Gennep hecht er veel waarde aan dat de verwerkingen van persoonsgegevens zorgvuldig, rechtmatig en veilig plaatsvinden. Binnen de gemeente is hiervoor veel aandacht. Om de positie van het privacyvraagstuk verder te versterken is er een privacybeleid opgesteld. Het College van burgemeester en wethouders (hierna: College) stelt dit beleid dan ook vast. Dit privacybeleid is praktisch ingestoken en vormt een aanvulling op de verplichtingen die voortvloeien uit de AVG en de Wpg. Het privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente Gennep.

In dit beleid staan kaders beschreven voor het verwerken van persoonsgegevens en politiegegevens, de bescherming van deze gegevens en de omgang met deze gegevens. Verder kan het beschermen van persoonsgegevens niet worden geborgd zonder adequate informatiebeveiliging. Het privacybeleid hangt daarom ook samen met het Informatieveiligheidsbeleid van de gemeente Gennep. Aanvullend op dit privacybeleid, kan er voor bepaalde onderwerpen of specifieke domeinen beleid worden opgesteld. Dit geldt bijvoorbeeld voor het verwerken van persoonsgegevens in het sociaal domein, openbare orde en veiligheid en personeelszaken.

1.2 GELDIGHEIDSDUUR

Dit beleid is vastgesteld op 5 november 2024 door het College als eindverantwoordelijke voor de gemeentelijke gegevensverwerking. Het beleid wordt tenminste eens per drie jaar door de Privacy Officer (hierna: PO) beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld bij grote organisatorische veranderingen of wetswijzigingen) kan het College besluiten tot een tussentijdse herziening.

1.3 CONTACT

Vragen over het privacybeleid, gegevensverwerkingen, of wet- en regelgeving op het gebied van privacy en gegevensbescherming kunnen gericht worden aan de PO'ers.

2 Doel

Met dit privacybeleid geeft de gemeente Gennep een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken). Daarnaast beoogt dit privacybeleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen. Met dit privacybeleid wordt tevens een kader voor het verantwoord omgaan met politiegegevens, die de gemeente op grond van de Wet politiegegevens verwerkt, gegeven.

De verdere uitwerking van dit beleid is, voor zover nodig, verder uitgewerkt in operationele documenten binnen de gemeente, zoals werkprocedures. Daarnaast onderkent de gemeente Gennep dat specifiek beleid en procesbeschrijvingen wenselijk zijn voor het verwerken van persoonsgegevens in het sociaal domein.

3 Uitgangspunten

Bij het verwerken van persoonsgegevens gelden een aantal uitgangspunten. De gemeente Gennep onderschrijft deze uitgangspunten en verwerkt persoonsgegevens enkel in overeenstemming met deze uitgangspunten.

3.1 RECHTMATIGHEID EN BEHOORLIJKHEID

Persoonsgegevens worden door de gemeente slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. De gemeente zorgt ervoor dat het verwerken van persoonsgegevens is gebaseerd op één van de grondslagen zoals benoemd in de AVG of Wpg. Daarbij gaat het om de volgende grondslagen:

Grondslagen AVG

1. *Toestemming*
De betrokkene heeft toestemming gegeven om zijn/haar persoonsgegevens te mogen verwerken.
2. *Uitvoering overeenkomst*
Deze grondslag maakt de verwerking van persoonsgegevens mogelijk wanneer dat nodig is voor de uitvoering van een overeenkomst met de betrokkene, bijvoorbeeld om uitvoering te geven aan een arbeidsovereenkomst.
3. *Wettelijke verplichting*
In sommige gevallen komt het voor dat er in een wet is opgenomen dat de gemeente een bepaalde taak heeft. Om deze taak uit te voeren is het noodzakelijk om persoonsgegevens te verwerken.

4. *Vitaal belang*

Er mogen persoonsgegevens worden verwerkt om het vitaal belang van een natuurlijk persoon te kunnen beschermen. Het gaat hierbij om situaties tussen leven en dood.

5. *Algemeen belang*

Als er een taak van algemeen belang vervuld moet worden waarvoor de verwerking van persoonsgegevens noodzakelijk is, dan mogen er persoonsgegevens worden verwerkt. Er moet dan wel in de wet staan dat de gemeente deze taak heeft.

6. *Gerechtvaardigd belang*

Bij deze grondslag moet de verwerking noodzakelijk zijn voor de gerechtvaardigde belangen van de gemeente, tenzij de privacybelangen van de betrokkene zwaarder wegen. De gemeente mag deze grondslag niet gebruiken voor haar overheidstaken.

Op basis hiervan mag je persoonsgegevens verzamelen De grondslag



Toestemming
van de gebruiker



Vitale belangen



Wettelijke
verplichting



Overeenkomst



Algemeen belang



Gerechtvaardigd
belang

Grondslagen Wpg

1. *Dagelijkse politietaak*

Hieronder vallen persoonsgegevens die verwerkt worden in het kader van de dagelijkse opsporingstaak.

2. *Handhaving van de rechtsorde in een bepaald geval*

Hiervan is sprake als het gaat om het verwerken van persoonsgegevens die specifiek gericht zijn op bepaalde personen of concrete gebeurtenissen.

3. *Ondersteunende taken*

In sommige gevallen is het mogelijk om de gegevens die zijn verwerkt op basis van de dagelijkse politietaak of handhaving van de rechtsorde in een bepaald geval, verder te verwerken.

3.2 TRANSPARANTIE

Alle communicatie over de verwerking van persoonsgegevens richting de inwoners vindt in duidelijk en begrijpelijke taal plaats. Daarbij wordt het Nederlands taalniveau B1 gehanteerd. Indien er zich complexe situaties voordoen waarbij wordt gecommuniceerd met inwoners, wordt team communicatie betrokken.

3.3 WELBEPAALEN DOELEINDEN

De gemeente verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. In de meeste gevallen worden persoonsgegevens verwerkt om de aan de gemeente opgedragen taken uit te voeren.

voeren. Zonder welbepaald doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen.

3.4 DOELBINDING

Persoonsgegevens en politiegegevens mogen in beginsel niet voor andere doelen worden verwerkt, dan waarvoor zij zijn verzameld. Dit is slechts mogelijk als de twee doelen aan elkaar verwant zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen.

Er vindt geen verwerking plaats van bijzondere politiegegevens tenzij:

- dat onvermijdelijk is voor het doel van de verwerking
- dit in aanvulling is op een verwerking van andere politiegegevens betreffende de persoon
- de gegevens voldoende zijn beveiligd.

3.5 MINIMALE GEGEVENSVERWERKING

Persoonsgegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeente bij voorkeur voor die mogelijkheid.

3.6 PROPORTIONALITEIT EN SUBSIDIARITEIT

De gemeente verwerkt persoonsgegevens enkel als wordt voldaan aan de beginselen van proportionaliteit en subsidiariteit. Het proportionaliteitsvereiste brengt met zich mee dat het doel van de verwerking altijd in verhouding moet staan tot de inbreuk op de privacy van de betrokkene. Op basis van het beginsel van subsidiariteit wordt binnen de gemeente altijd gekeken of het beoogde doel dat voor de verwerking is vastgesteld, ook op een minder ingrijpende manier/ of met minder ingrijpende middelen kan worden bereikt. Daarbij is het van belang dat de privacy van de betrokkene zo min mogelijk wordt geschaad.

3.7 OPSLAGBEPERKING

De gemeente stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijst. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijst op te stellen. Deze selectielijst bepaalt voor een selectie van documenten hoelang deze moeten worden bewaard. De gemeente Gennep is aangesloten bij de 'Selectielijst gemeenten en intergemeentelijke organen 2020' van de VNG.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijst kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid.

Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk is om het doel te bereiken. De gemeente bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een natuurlijk persoon niet meer mogelijk is.

Politiegegevens worden niet langer dan bewaard dan de minimale termijn die noodzakelijk is met een maximum van 5 jaar. Politiegegevens verzameld op grond van artikel 8 Wpg worden één jaar na de datum van eerste verwerking zondanig opgeslagen dat ze alleen nog beschikbaar komen voor hit-no-hit basis.

3.8 JUISTHEID

De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij zijn verzameld of vervolgens worden verwerkt. De gemeente neemt maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

3.9 INTEGRITEIT EN VERTROUWELIJKHEID

De gemeente neemt passende technische en organisatorische maatregelen om de persoonsgegevens te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De gemeente handelt hierbij in overeenstemming met het Informatieveiligheidsbeleid.

3.10 TOEGANG TOT GEGEVENS

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend.

3.11 DOORGIFTE BUITEN DE EER

Het uitgangspunt van de gemeente Gennep is dat er geen persoonsgegevens worden doorgegeven aan landen buiten de Europese Economische Ruimte (hierna: EER). Indien het bij een verwerking niet mogelijk is om persoonsgegevens en/of politiegegevens binnen de EER te verwerken, geschiedt de doorgifte van persoonsgegevens alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid. In het geval dat sprake is van een doorgifte van persoonsgegevens buiten de EER wordt de PO betrokken.

4 Rollen en verantwoordelijkheden

Om aan de verplichtingen uit de AVG en Wpg te voldoen is het van belang om rollen en verantwoordelijkheden duidelijk af te bakenen en te beleggen. De taken en rollen van de CISO, FG en PO zijn concreet beschreven en vastgelegd in het informatieveiligheidsbeleid van de gemeente Gennep. Voor de concrete inhoudelijke taken wordt verwezen naar het informatieveiligheidsbeleid van de gemeente.

4.1 COLLEGE VAN BURGEMEESTER & WETHOUDERS

Het College is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente. Het College is bij de meeste verwerkingen van persoonsgegevens ook de verwerkingsverantwoordelijke in de zin van de AVG. Bij sommige verwerkingen is dat de burgemeester. Het College heeft de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente;
- Stelt het privacybeleid vast;
- Geeft sturing aan privacy beleidsvoering;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Bevordert duurzame privacycultuur.

4.2 AFDELINGSMANAGERS

De eindverantwoordelijkheid voor de ambtelijke uitvoering van het privacybeleid en de naleving van de privacywetgeving binnen de afdeling ligt bij de afdelingsmanagers. De afdelingsmanagers hebben de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de eigen afdeling;
- Verantwoordelijk voor de implementatie en uitvoering van het privacybeleid binnen de eigen afdeling;
- Informeert op verzoek van de FG of PO op welke manier de eigen afdeling compliant is aan de privacywetgeving;
- Bevordert een duurzame privacycultuur;.

4.3 TEAMMANAGERS

Elke teammanager is binnen het eigen team verantwoordelijk voor de naleving van het privacybeleid en een zorgvuldige verwerking van persoonsgegevens. De teammanagers hebben de volgende rollen en verantwoordelijkheden:

- Verantwoordelijk voor het tijdig betrekken van de PO bij nieuwe samenwerkingen met derde partijen, zodat de juiste afspraken gemaakt kunnen worden;
- Verantwoordelijk voor het tijdig betrekken van de PO bij wijzigingen in de verwerking van persoonsgegevens, zodat de PO kan adviseren over maatregelen die vanuit de AVG of Wpg meegenomen moeten worden;

- Verantwoordelijk voor het uitvoeren van Data Protection Impact Assessments (DPIA's) voor hoog risico verwerkingen;
- Verantwoordelijk voor het op peil houden van het kennisniveau van medewerkers op het gebied van privacy, bijvoorbeeld door medewerkers de beschikbare trainingen over privacy en gegevensbescherming te laten volgen;
- Verantwoordelijk voor het registreren van de gegevensverwerkingen in het register van verwerkingen voor zover dit betrekking heeft op het eigen team;
- Verantwoordelijk voor de autorisaties en het intrekken van de autorisaties van medewerkers die persoonsgegevens verwerken;
- Verantwoordelijk voor het tijdig melden van datalekken binnen het team.

Teammanagers kunnen het uitvoeren van DPIA's of het actueel houden van het register van verwerkingen beleggen bij medewerkers uit hun team, maar blijven altijd verantwoordelijk voor het feit dat deze taken worden uitgevoerd.

4.4 FUNCTIONARIS GEGEVENSBESCHERMING

Het aanstellen van een Functionaris Gegevensbescherming (hierna: FG) is voor de gemeente Gennep wettelijk verplicht. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG, Wpg en aanverwante wet- en regelgeving op het gebied van gegevensbescherming. Voor de taken en rollen van de Functionaris Gegevensbescherming (hierna: FG) wordt aangesloten bij de taakbeschrijving uit het Informatieveiligheidsbeleid van de gemeente Gennep. In [bijlage 1](#) is de taakbeschrijving van de FG uit het informatieveiligheidsbeleid opgenomen.

4.5 PRIVACY OFFICERS

De PO'ers hebben een brede functie, waarbij de PO'ers hoofdzakelijk dienen als interne (juridische) ondersteuning van de gehele organisatie voor alle privacygerelateerde vraagstukken en het uitvoeren van het privacybeleid. Ook voor de taakbeschrijving van de PO wordt aangesloten bij de taakbeschrijving uit het Informatieveiligheidsbeleid van de gemeente Gennep. In [bijlage 1](#) is de taakbeschrijving van de PO uit het informatieveiligheidsbeleid opgenomen. In aanvulling op de taken beschreven in bijlage 1 ontwikkelt de PO ook bewustmakingsprogramma's en privacytrainingen voor medewerkers.

4.6 CHIEF INFORMATION SECURITY OFFICER

De Chief Information Security Officer (verder: CISO) draagt zorg voor de informatiebeveiliging binnen de gemeente Gennep. Ook voor de taakbeschrijving van de CISO wordt aangesloten bij de taakbeschrijving uit het Informatieveiligheidsbeleid van de gemeente Gennep. In [bijlage 1](#) is de taakbeschrijving van de CISO uit het informatieveiligheidsbeleid opgenomen.

4.7 TECHNISCH INFORMATIE ADVISEUR

De Technisch Informatie Adviseur (TIA) heeft een adviserende en ondersteunende rol bij de technische kant van gegevensbescherming. De TIA adviseert en ondersteunt onder andere bij technische vragen, het veilig delen van persoonsgegevens en bij pentesten.

4.8 STRATEGISCH INFORMATIE ADVISEUR EN ARCHIVARIS

De Strategisch Informatie Adviseur (SIA) en archivaris hebben een adviserende en ondersteunde rol op het gebied van informatievoorziening en –beheer bij gegevensbescherming. De SIO adviseert en ondersteunt onder andere bij vragen over waar gegevens zich bevinden en waar en hoelang deze opgeslagen, bewaard en vernietigd worden.

4.9 MEDEWERKERS

Medewerkers hebben een grote rol in de manier waarop de gemeente Gennep omgaat met persoonsgegevens. Alle medewerkers hebben een eigen verantwoordelijkheid in het omgaan met persoonsgegevens. Van alle medewerkers wordt verwacht dat zij zorgvuldig en integer omgaan met persoonsgegevens en kennisnemen van dit privacybeleid. Ook wordt verwacht dat zij actief hun kennis up to date houden door jaarlijks een (digitale of fysieke) privacy training te volgen.

4.10 INTERNE OVERLEGSTRUCTUREN

Tussen de genoemde stakeholders vinden verschillende periodieke overleggen plaats:

- De PO, FG, TIA en CISO komen driewekelijks bij elkaar om de lopende zaken, ontwikkelingen en innovaties met betrekking tot privacy en informatiebeveiliging te bespreken;
- De PO, FG, CISO en TIA sluiten twee keer per jaar aan bij het teammanagersoverleg.
- In overleg met de teammanager sluit de PO ook tussentijds aan bij teamoverleggen;
- De afdelingsmanager en teammanagers hebben tweewekelijks een bilateraal overleg. In dit overleg is ruimte voor privacy-gerelateerde onderwerpen.
- Strategische Informatie Overleg.

Strategisch Informatie Overleg (SIO)

Het SIO is een overleg over het functioneren en de kwaliteit van de informatiehuishouding van de gemeente Gennep. In het SIO zijn vertegenwoordigd de Gemeentesecretaris en/of Concerncontroller, Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG), Technisch Informatieadviseur (TIA), Strategisch informatieadviseur (SIA) en de Archivaris. In dit overleg worden ook privacy-aspecten en risico's op verschillende onderwerpen integraal besproken. Er wordt actief samengewerkt aan het ontwikkelen van kaders, standaarden, principes en werkwijzen op het gebied van data.

5 Borging en beheersing privacy

De gemeente Gennep moet aantoonbaar voldoen aan de AVG en Wpg. De verantwoordingsplicht brengt verschillende verplichtingen voor de gemeente met zich mee.

5.1 PRIVACY BY DESIGN EN PRIVACY BY DEFAULT

Privacy by design betekent dat in de 'ontwerpfase' van een proces, applicatie of dienst wordt nagedacht over het zo privacyvriendelijk mogelijk inrichten daarvan. Privacy by default betekent dat standaardinstellingen zo privacyvriendelijk mogelijk worden ingesteld. De gemeente houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo optimaal mogelijk persoonsgegevens en politiegegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking. Zo mogen politiegegevens alleen worden verwerkt noodzakelijk voor een specifiek doel. Daarbij wordt rekening gehouden met de uitgangspunten privacy by design en privacy by default.

Binnen de gemeente Gennep zijn er verschillende initiatieven om deze beginselen te waarborgen, zo is dit bijvoorbeeld geborgd in de Samenwerkingswijzer en worden de thema's besproken in de teamoverleggen. Daarbij worden adviseurs op het gebied van privacy, Wpg en gegevensbescherming in een vroeg stadium betrokken bij nieuwe projecten en ideeën. Ook wordt de PO aan de voorkant betrokken bij inkoop- en aanbestedingstrajecten.

5.2 DATA PROTECTION IMPACT ASSESSMENT

Vanuit het oogpunt van een zorgvuldige omgang met persoonsgegevens wordt een Data Protection Impact Assessment (DPIA) uitgevoerd voor verwerkingen die waarschijnlijk een verhoogd risico opleveren voor betrokkenen en/ of processen waarvan de Autoriteit Persoonsgegevens heeft gesteld dat er verplicht een DPIA moet worden uitgevoerd. Deze beoordeling zorgt ervoor dat alle risico's van een verwerking (vroegtijdig) in kaart worden gebracht en maatregelen kunnen worden getroffen. Gelet op de grootte van de gemeente Gennep wordt binnen ieder team jaarlijks gekeken waar wat betreft privacy de hoogste risico's zitten. Ieder team voert minimaal op één proces per jaar een DPIA uit. Bij nieuwe applicaties waar gevoelige persoonsgegevens in worden verwerkt, voert de gemeente Gennep ook een DPIA uit. De processen, waarin politiegegevens worden verwerkt zijn aan te merken als verwerkingen met een hoog risico en moeten worden onderworpen aan een DPIA.

5.3 REGISTER VAN VERWERKINGEN

De gemeente Gennep is verplicht om een overzicht van alle verwerkingen van persoonsgegevens te hebben. De gemeente beschikt over een register van verwerkingen, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt. Ook beschikt de gemeente Gennep over een register van verwerkingen, waarin alle verwerkingen van politiegegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt (Wpg-register). De gemeente Gennep beschikt hierbij over twee varianten: een intern register en een openbaar register. In het kader van transparantie wordt een deel van de informatie uit het interne register openbaar gemaakt.

5.4 INBREUK IN VERBAND MET PERSOONSGEGEVENS

Bij toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is sprake van een inbreuk in verband met persoonsgegevens. Dit wordt ook wel een datalek genoemd. Indien sprake is van een risico voor de betrokkene moet een datalek doorgaans binnen 72 uur worden gemeld bij de toezichthouder, de Autoriteit Persoonsgegevens. Indien er sprake is van een hoog risico, moet het datalek zo spoedig mogelijk bij de betrokkene worden gemeld. Alle datalekken worden intern geregistreerd. Jaarlijks vindt er een evaluatie plaats tussen de PO, FG, TIA en CISO om de voorgevallen beveiligingsincidenten en datalekken te evalueren. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in het Datalekprotocol van de gemeente Gennep.

5.5 SAMENWERKINGEN

Als de gemeente Gennep bij een derde partij een product of dienst afneemt waarbij sprake is van het verwerken van persoonsgegevens door die derde partij in opdracht van de gemeente, wordt een verwerkersovereenkomst gesloten. Hierbij wordt de standaard verwerkersovereenkomst (van de IBD) gehanteerd die door de VNG is vastgesteld. Aangezien de gemeente hierbij altijd verwerkingsverantwoordelijke is dient er een grondslag te zijn voor de gegevensverwerking. De PO wordt betrokken bij het aangaan van een verwerkersovereenkomst.

Samenwerkingsverbanden en ketenpartners

De gemeente werkt in sommige gevallen ook samen met andere partijen die worden aangemerkt als (zelfstandig/gezamenlijk) verwerkingsverantwoordelijke. Deze partijen zijn zelf verantwoordelijk voor het naleven van de privacy wet- en regelgeving, zoals de AVG en Wpg. Om het uitwisselen van deze persoonsgegevens goed te borgen, maakt de gemeente met deze partijen afspraken over privacy, veiligheid, archivering en vernietiging. Er dient altijd een grondslag te zijn voor het uitwisselen van persoonsgegevens met deze partijen en moet er aan het beginsel van doelbinding worden voldaan. In het geval van het uitwisselen van persoonsgegevens in het kader van wetenschappelijk en statistisch onderzoek bepaalt de AVG dat altijd wordt voldaan aan het beginsel van doelbinding.

Uitwisselen persoonsgegevens per mail

Als een medewerker van de gemeente Gennep een e-mail met persoonsgegevens stuurt naar een externe wordt altijd gebruik gemaakt van de optie om beveiligd te mailen via Cryptshare. Hiermee kunnen ook grote bestanden gestuurd worden, waardoor de gemeente geen gebruik maakt van (minder veilige) alternatieven zoals Wettransfer. Daarnaast worden via verschillende applicaties gegevens rechtstreeks gedeeld.

Uitwisselen van data (voor dataproducten/dashboards)

Indien de gemeente Gennep data uitwisselt met externe partijen doet zij dit alleen in overeenstemming met de wetgeving. Er dient een grondslag te zijn, doelbinding en neemt zij beperkende (dataminimalisatie, anonimisering e.d.) - alsmede beveiligingsmaatregelen (versleutelde toegang). Met partijen wordt een data-uitwisselingsovereenkomst gesloten, waarin de afspraken

over de uitwisseling worden vastgelegd, waaronder de verantwoordelijkheid van elke partij. Voorafgaand wordt deze uitwisseling van data c.q. samenwerking beoordeeld in het SIO.

5.6 RECHTEN VAN BETROKKENEN

De AVG en Wpg brengen niet alleen verplichtingen mee voor organisaties die persoonsgegevens verwerken, ze geven ook rechten aan de personen van wie persoonsgegevens worden verwerkt. Deze personen worden betrokkenen genoemd. Daarbij gaat het om de volgende rechten:

- **Recht op informatie**
Betrokkenen hebben het recht om geïnformeerd te worden over wat de gemeente met hun gegevens doet en welke rechten zij hebben ten aanzien van de gegevensverwerking.
- **Recht op inzage**
Betrokkenen hebben in bepaalde gevallen het recht om te weten welke persoonsgegevens van hen worden verwerkt of om informatie te ontvangen over een gegevensverwerking.
- **Recht op rectificatie**
Betrokkenen hebben het recht om foutieve persoonsgegevens te laten herstellen of aan te vullen.
- **Recht op gegevenswissing (vergetelheid)**
Betrokkenen hebben in specifieke gevallen het recht om hun persoonsgegevens te laten verwijderen.
- **Recht op beperking van de verwerking**
In specifieke gevallen heeft de betrokkene het recht om zijn persoonsgegevens tijdelijk te laten 'bevroren'. De gemeente mag deze persoonsgegevens dan tijdelijk niet verwerken.
- **Recht op overdraagbaarheid van gegevens (dataportabiliteit)**
Als persoonsgegevens op basis van toestemming of een overeenkomst worden verwerkt, heeft de betrokkene het recht om deze persoonsgegevens over te laten dragen naar een derde partij.
- **Recht op bezwaar**
In specifieke gevallen kan een betrokkene bezwaar maken tegen een gegevensverwerking. Dit is niet hetzelfde als bezwaar in de zin van de algemene wet bestuursrecht (Awb).
- **Recht om niet onderworpen te worden aan geautomatiseerde besluitvorming, waaronder profilering.**
Dit recht houdt in dat er sprake moet zijn van een menselijke tussenkomst bij het verwerken van persoonsgegevens.

Hoe invulling wordt gegeven aan het afhandelen van dergelijke verzoeken is beschreven in de Procedure rechten van betrokkenen van de gemeente Gennep.

Klachten

Betrokkenen kunnen ook een klacht indienen over de omgang met hun persoonsgegevens. Binnen de gemeente Gennep wordt de klacht afgehandeld conform de Werkinstructie Klachtbehandeling.

5.7 BEWUSTWORDING

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de gemeentelijke organisatie voortdurend aan te scherpen, zodat kennis van risico's aantoonbaar wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Daarbij zorgen de teammanagers dat hun (nieuwe) medewerkers de beschikbare privacytrainingen volgen en alle medewerkers jaarlijks een herhaling doen. De PO zorgt er, in samenwerking met de FG en CISO, voor dat het aanbod actueel blijft en er voldoende (ludieke) acties worden georganiseerd om bewustwording te vergroten.

5.8 EVALUATIE

De gemeente streeft ernaar om rondom de verwerking van persoonsgegevens *in control* te zijn en daarover op professionele wijze verantwoording af te leggen. *In control* betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus. Als onderdeel daarvan vindt er ieder jaar op initiatief van de PO een evaluatie plaats over het volwassenheidsniveau van de organisatie op het gebied van privacy en de naleving van het privacybeleid. Hierbij wordt bijvoorbeeld gebruikgemaakt van het borgingsproduct van de VNG. Daarin worden de volgende zeven thema's bekeken:

- Beleid
- Organisatorische inbedding
- Processen
- Rechten van betrokkenen
- Samenwerking
- Gegevensbescherming
- Verantwoording

De PO deelt de bevindingen in ieder geval met de FG, TIA, CISO, afdelingsmanagers en teammanagers en besproken in het SIO.

5.9 AANVULLEND SPECIFIEK VOOR DE VERWERKING VAN POLITIEGEGEVENS (WPG)

De Wpg stelt een aantal nadere eisen, die de gemeente Gennep verwerkt in dit beleid.

Het aanwijzen van de buitengewoon opsporingsambtenaar

De gemeente wijst de buitengewoon opsporingsambtenaar aan, indien de buitengewoon opsporingsambtenaar in het bezit is van een:

- akte van opsporingsbevoegdheid;
- verklaring omtrent het gedrag;

De buitengewoon opsporingsambtenaar voldoet aan de her- en bijscholingsplicht.

De gemeente organiseert ten aanzien van politiegegevens bewustwordingsactiviteiten dan wel cursussen over de omgang met politiegegevens, die door de buitengewoon opsporingsambtenaar (jaarlijks) verplicht worden bijgewoond.

Het verlenen, wijzigen en beëindigen van de toegang tot politiegegevens (artikel 6 van de Wet politiegegevens)

- De gemeente stelt ten aanzien van het verlenen, wijzigen- en beëindigen van toegang tot politiegegevens een autorisatiebeleid vast.
- De gemeente verleent aan de buitengewoon opsporingsambtenaar conform het vastgestelde autorisatiebeleid een autorisatie tot politiegegevens, indien de toegang tot politiegegevens noodzakelijk is voor het uitvoeren van de aan de buitengewoon opsporingsambtenaar opgedragen opsporingstaak.
- De gemeente wijst de buitengewoon opsporingsambtenaar ten aanzien van politiegegevens op de plicht tot geheimhouding en de consequenties bij de schending van deze plicht.
- Indien de buitengewoon opsporingsambtenaar van functie verandert dan wel uit dienst gaat, wordt de autorisatie conform het autorisatiebeleid gewijzigd of beëindigd.

De plicht tot loggen (artikel 32a van de Wet politiegegevens)

- De gemeente dient periodiek de toegekende autorisaties van de buitengewoon opsporingsambtenaar te controleren en evalueren met als doel om de integriteit en de rechtmatigheid van de toegang tot politiegegevens te waarborgen.
- De verwerker heeft ten aanzien van de periodieke controle de plicht om de toegang tot politiegegevens te loggen.
- De verwerker verstrekt op verzoek van de gemeente de logginggegevens zodat deze conform het autorisatiebeleid periodiek gecontroleerd kunnen worden.
- De gemeente gebruikt de logginggegevens uitsluitend voor de controle van de rechtmatigheid van de gegevensverwerking, ter ondersteuning van de verplichte audits en ter waarborging van de integriteit en de rechtmatigheid van de toegang tot politiegegevens.
- De gemeente legt het resultaat van de periodieke controle vast in een verslag van bevindingen, welke wordt gearchiveerd binnen het daartoe bestemde en beveiligde zaaksysteem.
- De gemeente bewaart de logginggegevens alsmede het resultaat van de periodieke controle voor een periode van vijf jaar.

Het verwerken van politiegegevens

- De gemeente voorziet in werkinstructies per boa-domein, die de buitengewoon opsporingsambtenaar bij de uitvoering van de opsporingstaak in acht neemt.
- De buitengewoon opsporingsambtenaar verwerkt politiegegevens ten behoeve van de uitvoering van de politietask als bedoeld in artikel 8 van de Wet politiegegevens.
- De buitengewoon opsporingsambtenaar verwerkt geen politiegegevens, indien het gegevens betreft die niet noodzakelijk zijn voor de uitvoering van de aan hem of haar opgedragen opsporingstaak.

- De buitengewoon opsporingsambtenaar maakt bij het verwerken van politiegegevens onderscheid tussen:
 - de verschillende categorieën van betrokkenen zoals genoemd in artikel 6b van de Wet politiegegevens;
 - gegevens die gebaseerd zijn op feiten en een persoonlijk oordeel zoals genoemd in artikel 4 van de Wet politiegegevens.
- De verwerker dient ervoor te zorgen dat het onderscheid zoals genoemd in het vierde lid en onder a van dit artikel in de applicatie, waartoe de buitengewoon opsporingsambtenaar toegang heeft, mogelijk wordt gemaakt.
- Er vindt geen verwerking plaats van bijzondere politiegegevens tenzij:
 - dat onvermijdelijk is voor het doel van de verwerking;
 - dit in aanvulling is op een verwerking van andere politiegegevens betreffende de persoon;
 - de gegevens voldoende zijn beveiligd.

Let hierbij op; het verwerken van een beeldmateriaal, zoals een foto, kan een bijzonder persoonsgegeven zijn, omdat iemands ras of etniciteit kan worden afgeleid. Bij domein III moet worden opgelet, omdat het noteren van een school voor een bepaalde geloofsovertuiging of beperking (bijvoorbeeld een Christelijke, Joodse, Islamitische school of speciaal onderwijs voor een bepaalde groep) herleidbaar is tot het geloof of gezondheidsgegevens van een leerling.

- De buitengewoon opsporingsambtenaar neemt geen besluiten die uitsluitend gebaseerd zijn op geautomatiseerde verwerking zoals bedoeld in artikel 7a van de Wet politiegegevens, met inbegrip van profilering, dat voor de betrokkene nadelige rechtsgevolgen heeft of hem of haar in aanmerkelijke mate treft.
- Politiegegevens kunnen worden vergeleken met andere politiegegevens met als doel om vast te stellen of verbanden bestaan tussen de betreffende gegevens. De verwerkingsmogelijkheden geautomatiseerd vergelijken en in combinatie zoeken zijn gebonden aan strikte criteria (zie artikel 11 Wpg).

De termijnen van politiegegevens (artikel 14 van de Wet politiegegevens)

- De gemeente voorziet in voldoende waarborgen om te bewerkstelligen dat de politiegegevens conform de wet niet langer worden bewaard dan strikt noodzakelijk is voor de uitvoering van de buitengewoon opsporingsambtenaar opgedragen opsporingstaak.
- De gemeente zorgt ervoor dat de politiegegevens voor de uitvoering van de opsporingstaak zoals bedoeld in artikel 8 van de Wet politiegegevens:
 - gedurende een jaar beschikbaar zijn in het kader van de uitvoering van de opsporingstaak;
 - na een jaar slechts beschikbaar zijn voor het gericht zoeken;
 - na vijf jaar worden verwijderd;
 - na tien jaar worden vernietigd.
- De verwerker zorgt ervoor dat de bewaartermijn conform de wet en het tweede lid van dit artikel geconfigureerd zijn, zodat gewaarborgd is dat de politiegegevens niet langer worden bewaard dan strikt noodzakelijk is voor de uitvoering van de opsporingstaak.

- De buitengewoon opsporingsambtenaar neemt de termijnen conform de wet en het tweede lid van dit artikel in acht.

Het ter beschikking stellen en verstrekken van politiegegevens (artikel 15 en paragraaf 3 van de Wet politiegegevens)

- De gemeente stelt de politiegegevens conform de wet ter beschikking op basis van het 'Free flow of information' principe, indien het ter beschikking stellen van politiegegevens noodzakelijk is voor de uitoefening van de taken binnen het Wpg-domein.
- De gemeente mag de politiegegevens verstrekken zoals beschreven in de verstrekkingenwijzer aan partijen buiten het Wpg-domein. Daarbij wijst de gemeente de ontvangende partij op de plicht tot geheimhouding die op de verstrekte gegevens van toepassing is.
- De gemeente legt de verstrekking zoals genoemd in het tweede lid van dit artikel vast. (artikel 32, eerste lid aanhef en onder b, van de Wet politiegegevens)
- De verwerker heeft ten aanzien van het tweede lid van dit artikel de plicht om binnen de gebruikte applicaties, technische mogelijkheden te creëren, waarmee verstrekkingen kunnen worden vastgelegd. (artikel 32, eerste lid aanhef en onder b van de Wet politiegegevens)
- De verwerker dient ervoor te zorgen dat de geautomatiseerde verstrekkingen, zoals bijvoorbeeld aan het Centraal Justitieel Incassobureau, conform de wet plaatsvinden en worden gedocumenteerd.
- De gemeente alsmede de verwerker voorzien in de technische mogelijkheden om ervoor te zorgen dat de politiegegevens door middel van een beveiligde wijze worden verstrekt aan de ontvangende partij.
- De gemeente verstrekt geen politiegegevens aan ontvangers in derde landen of internationale organisaties.

De rechten van de betrokkenen (paragraaf 4 van Wet politiegegevens)

Aanvullend op paragraaf 5.6 van dit beleid, draagt de gemeente zorg voor het informeren van de betrokkenen over de verwerking van politiegegevens. Dit vindt plaats conform paragraaf 4 van de Wet politiegegevens. Daarbij heeft de gemeente de plicht tot:

- actieve informatieverstrekking waarbij de informatievoorziening op de website conform de wet plaatsvindt;
- passieve informatieverstrekking; waarbij de informatie op verzoek wordt verstrekt, tenzij het verzoek conform artikel 27 van de Wet politiegegevens geheel of gedeeltelijk kan worden afgewezen, bijvoorbeeld als de informatieverstrekking de opsporing en vervolging belemmert.

De gemeente heeft, conform de wet, een procedure vastgesteld voor de behandeling van verzoeken van betrokkenen.

Het behandelen van datalekken (artikel 33a van de Wet politiegegevens)

De gemeente heeft, conform de wet, een procedure vastgesteld voor het melden van een (vermoedelijke) inbreuk op de beveiliging op politiegegevens, waaronder voor het melden van datalekken.

De gemeente houdt een register bij van gemelde datalekken. Uit dit register blijkt of het een AVG of Wpg melding betreft.

Het register van verwerkingen (artikel 31d van de Wet politiegegevens)

De gemeente houdt een register van verwerkingen bij, waarin per verwerking minimaal de volgende informatie voorkomt:

- de naam en contactgegevens van de gemeente;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën persoonsgegevens die worden verwerkt;
- een beschrijving van de categorieën betrokkenen;
- een beschrijving van de categorieën van ontvangers aan wie de politiegegevens ter beschikking worden gesteld of worden verstrekt;

De gemeente actualiseert jaarlijks het register van verwerkingen.

Het uitvoeren van een audit (artikel 33 van de Wet politiegegevens)

- De gemeente laat conform de wet, eenmaal in de vier jaren een externe audit uitvoeren.
- De gemeente voert ter voorbereiding op de verplichting in het eerste lid van dit artikel, jaarlijks een interne audit uit.
- De gemeente stelt een auditplan vast.
- De betrokken verwerkers dienen ten behoeve van de audit een Third Party Memorandum verklaring te overleggen die conform de 'Nederlandse Orde van EDP Auditors handreiking' wordt uitgevoerd, zodat deze verklaring betrokken kan worden bij de beoordeling van de audit.
- Indien uit de resultaten van de audit, zoals bedoeld in het eerste lid van dit artikel, blijkt dat de verwerking van de politiegegevens op onderdelen niet voldoet aan de wettelijke normen, dient de gemeente binnen een jaar zorg te dragen voor deze tekortkomingen, met als doel dat deze worden verholpen. Daarnaast voert de gemeente binnen één jaar een hercontrole uit, binnen de onderdelen waarvan het resultaat onvoldoende bleek te zijn.
- Indien blijkt dat de beheersmaatregelen ten aanzien van de gebruikte applicatie(s) niet voldoen aan de wettelijke normen, dan draagt de verwerker verantwoordelijkheid voor het verhelpen van de tekortkomingen binnen een periode van één jaar.
- De gemeente zendt een afschrift van de controleresultaten van de externe audit aan de Autoriteit Persoonsgegevens.

De functionaris gegevensbescherming (artikel 36 van de Wet politiegegevens)

De gemeente heeft een functionaris gegevensbescherming aangesteld ten behoeve van de controle en het toezicht op het verwerken van politiegegevens conform de wet en het beleid van de gemeente.

De functionaris gegevensbescherming voert daarbij periodiek controles uit op het naleven van de wettelijke verplichtingen. De functionaris gegevensbescherming stelt periodiek rapportages op en rapporteert zo nodig rechtstreeks aan het college van burgemeester en wethouders.

De verplichtingen van de gemeente

- De gemeente draagt zorg dat de procesinrichting voor de verwerking van politiegegevens in opzet, bestaan en dat de werking voldoet zoals genoemd in de wet, zodat hierop door de auditor en de functionaris gegevensbescherming toezicht kan worden gehouden.
- De gemeente treft daarbij conform de wet passende technische- en organisatorische maatregelen om ongeoorloofde of onrechtmatige verwerkingen, verlies, vernietiging of beschadiging van politiegegevens tegen te gaan, met als doel om de rechtmatigheid en beveiliging van politiegegevens te waarborgen. (artikel 4a en 4b van de Wet politiegegevens)
- Indien er sprake is van een hoog risico op de rechten en vrijheden van betrokkenen, dan voert de gemeente conform artikel 4c van de Wet politiegegevens een risicoanalyse, zoals een Data protection impact assessment (DPIA), uit.
- De gemeente maakt uitsluitend gebruik van een verwerker, indien de verwerker afdoende garandeert dat de passende technische- en organisatorische maatregelen en procedures zodanig worden geïmplementeerd dat voldaan wordt aan het bij of krachtens de wet bepaalde (Artikel 6c, 4a en 4b van de Wet politiegegevens).
- De verwerker verstrekt op verzoek van de gemeente alle informatie die nodig is om de nakoming van de verplichtingen uit artikel 6, 32 en 32a van de Wet politiegegevens aan te tonen.
- De gemeente legt de verplichtingen zoals genoemd in het vijfde lid van dit artikel, vast in een schriftelijke overeenkomst, welke door beide partijen wordt ondertekend. (artikel 6c, tweede lid, van de Wet politiegegevens)
- De gemeente dient te voldoen aan de documentatieplicht zoals genoemd in de wet. (artikel 32, eerste lid, van de wet Politiegegevens)

6 Overige thema's

Het voorliggende privacybeleid moet gezien worden als een algemeen beleid dat schetst hoe de gemeente Gennep om gaat met persoons- en politiegegevens. Het is belangrijk op te merken dat dit een basisbeleid is, waarbij ingezet wordt op algemene en wettelijke vereisten, die voor alle organisatie onderdelen gelden en toegepast kunnen worden. Het privacybeleid is ontworpen om breed toepasbaar te zijn en fundamentele privacyaspecten te bestrijken zonder te zijn afgestemd op de specifieke nuances van een bepaalde afdeling of team.

Binnen de gemeente Gennep worden er binnen de verschillende teams in meer of mindere mate persoonsgegevens verwerkt. Zo wordt bijvoorbeeld in het sociaal domein met veel en kwetsbare informatie gewerkt, terwijl in het ruimtelijk domein het veelal om adresgegevens zal gaan. Zolang er geen specifiek privacybeleid is geformuleerd, geldt het algemene privacybeleid.

Overigens is op sommige thema's binnen de gemeente Gennep wel specifiek beleid geformuleerd, waarin privacy als onderdeel is vertegenwoordigd. Denk bijvoorbeeld aan cookieverklaring, thuiswerkbeleid, wachtwoordbeleid, veilig communiceren en werken met data.

Kort stippen we op hoofdlijnen een aantal specifieke thema's aan, waar verwezen wordt naar beleid of richtlijnen of waar de gemeente in de toekomst specifiek beleid voor kan opstellen.

6.1 GEGEVENSVERWERKING IN HET SOCIAAL DOMEIN

Binnen het sociaal domein worden veel en kwetsbare persoonsgegevens verwerkt in het kader van de uitoefening van de wettelijke taken. In de sectorspecifieke wetgeving is per domein strikt vastgelegd of persoonsgegevens mogen worden uitgewisseld met andere domeinen binnen het sociaal domein. Daarbij gaat het onder andere om de volgende sectorale wetgeving: Jeugdwet, Participatiewet, Wet maatschappelijke ondersteuning, Zorg en Veiligheid, en de Wet gemeentelijke schuldhulpverlening.

Bij bepaalde situaties kan sprake zijn van complexe en domeinoverstijgende problematiek, waarbij het wenselijk is dat gegevens tussen sectoren worden uitgewisseld zonder dat de wet hiervoor een grondslag biedt. Indien er geen grondslag is mogen er geen persoonsgegevens worden uitgewisseld tussen de domeinen.

De gemeente Gennep heeft verschillende documenten opgesteld in het kader van het zorgvuldig verwerken van persoonsgegevens in het sociaal domein. Verwezen wordt naar de DPIA Sociaal domein 2019 en DPIA Zorgned 2023, het Onderzoek 'gegevensdeling in de (digitale) processen van de Wmo 2015' en het bijbehorende werkproces opgesteld in 2021 en het onderzoek 'gegevensverwerking Jeugdhulp' en bijbehorende werkproces opgesteld in 2018. Daarnaast onderkent de gemeente Gennep dat specifiek beleid en procesbeschrijvingen wenselijk zijn voor het verwerken van persoonsgegevens in het sociaal domein.

6.2 GEGEVENSVERWERKING IN HET RUIMTELIJK DOMEIN

De Omgevingswet (Ow) streeft naar vroegtijdige participatie van de omgeving bij de voorbereiding van beleids- en besluitvorming. De gemeente beschikt over veel informatie over verschillende onderdelen van de fysieke leefomgeving die zij in het kader van de eigen taakuitoefening

verzamelen. Nu die taakuitoefening zich heeft uitgebreid naar het organiseren en faciliteren van participatie, worden er door de gemeente gegevens verzameld over de betrokken participanten. Voor zover de Ow niets regelt, gelden de AVG en de UAVG en wordt aangesloten op het voorliggende Privacybeleid van de gemeente Gennep.

Ook onder de Ow worden persoonsgegevens voor een specifiek doel verzameld en mogen vervolgens niet voor andere niet-verenigbare doelen worden gebruikt (doelbinding). Gegevens verzameld voor participatiedoeleinden mogen bijvoorbeeld niet zomaar worden gebruikt voor een nieuwsbrief of andere marketingactiviteiten. Een ontwikkelaar die een participatietraject opzet mag de namen die hij heeft verzameld bijvoorbeeld niet gebruiken voor de potentiële kopers van zijn ontwikkeling.

6.3 PERSONEELSGEGEVENS

De gemeente Gennep verwerkt ook veel persoonsgegevens van haar eigen medewerkers. Deze persoonsgegevens worden enkel opgeslagen in een personeelsdossier. Daarbij gaat het bijvoorbeeld om contactgegevens, kopie van het identiteitsbewijs en het BSN van medewerkers. De gemeente verwerkt in het personeelsdossier geen:

- Gezondheidsgegevens, tenzij er sprake is van een uitzonderingsgeval. Dat is bijvoorbeeld het geval als een medewerker epilepsie heeft en collega's dit moeten weten, zodat zij deze werknemer kunnen helpen als deze een aanval krijgt.
- Strafrechtelijke gegevens, tenzij het gaat om een strafbaar feit op de werkvloer.
- Gegevens over afkomst, religie of andere bijzondere persoonsgegevens.

Inzage en bewaartermijn personeelsdossier

Enkel geautoriseerde personen, zoals een teammanager of een medewerker van P&O, mogen een personeelsdossier inzien. Ook nadat een medewerker uit dienst is kan het noodzakelijk zijn om een personeelsdossier te bewaren. Sommige gegevens uit de salarisadministratie worden 7 jaar bewaard voor de Belastingdienst. Loonbelastingverklaringen en het identiteitsbewijs worden 5 jaar na het einde van het dienstverband bewaard. Als niet in de wet is geregeld hoelang persoonsgegevens uit het personeelsdossier bewaard mogen worden, geldt een bewaartermijn van 2 jaar nadat de medewerker uit dienst is.

Verstrekken persoonsgegevens

In sommige gevallen kan het voorkomen dat de gemeente persoonsgegevens doorgeeft aan derden. Dit wordt alleen gedaan als er een rechtmatige grondslag is en als wordt voldaan aan het beginsel van doelbinding. De PO'er wordt hierbij betrokken.

Digitale leeromgeving

Enkel geautoriseerde personen, zoals een teammanager of een medewerker van P&O, mogen de leeromgeving van een medewerker inzien.

6.4 OPENBAAR MAKEN VAN PERSOONSGEGEVENS (WOO)

Om een transparante overheid te bevorderen moet de gemeente Gennep op basis van de Wet open overheid (Woo) voldoen aan informatieverzoeken van inwoners en (op termijn) informatie actief openbaar maken. In deze documenten kunnen persoonsgegevens staan, bijvoorbeeld namen, functies of uitlatingen van medewerkers van de gemeente Gennep. In die gevallen is er een strijdigheid tussen aan de ene kant het openbaar maken van informatie en aan de andere kant het borgen van de privacy van betrokkenen. In het kader van het openbaar maken van persoonsgegevens geldt binnen de gemeente Gennep het uitgangspunt dat persoonsgegevens niet openbaar worden gemaakt. Hierbij wordt de anonimiseringsrichtlijn van de gemeente Gennep gevolgd. De Gemeente Gennep anonimiseert persoonsgegevens of gegevens die anderszins herleidbaar zijn tot een persoon, voordat deze openbaar worden gemaakt.

De gemeente Gennep maakt hier slechts een uitzondering op indien een strikte belangenafweging tussen het belang van openbaarmaking en de eerbiediging van de persoonlijke levenssfeer van de persoon op wie de gegevens betrekking hebben anders bepaalt. Alleen als het belang van openbaarmaking zwaarder weegt, worden de persoonsgegevens openbaar gemaakt. Dit kan zich bijvoorbeeld voordoen bij omgevingsgerelateerde dossiers. Dan wordt veelal de locatie van bijvoorbeeld een bouwplan openbaar gemaakt. Die locatie is veelal een adres en daarmee herleidbaar naar een persoon.

De Gemeente Gennep maakt bijzondere categorieën persoonsgegevens, persoonsgegevens van strafrechtelijke aard en een Burgerservicenummer (BSN) nooit openbaar. Indien onrechtmatig persoonsgegevens worden gepubliceerd is sprake van een datalek.

Verwezen wordt naar de Procesbeschrijving Woo-verzoek voor de omgang met persoonsgegevens op het moment dat een verzoek wordt ingediend.

6.5 WERKEN MET DATA

Het werken met data wordt steeds belangrijker voor gemeenten om beslissingen te nemen en doelstellingen te realiseren. Dit geldt ook voor de gemeente Gennep. Het gebruik van data biedt kansen bij maatschappelijke opgaven. De gemeente Gennep heeft ook oog voor de risico's bij het werken met data. Een afweging van juridische, ethische en maatschappelijke aspecten is voorafgaand aan de inzet van data vereist.

Privacy in de context van werken met data verwijst naar het recht van individuen om controle te hebben over hun persoonlijke gegevens en hoe deze worden verwerkt door de organisatie. Privacy wordt gewaarborgd door het implementeren van beleid en procedures die ervoor zorgen dat persoonlijke gegevens worden verzameld en verwerkt op een rechtmatige, transparante, veilige en verantwoorde manier, met respect voor de rechten van individuen.

Dit privacybeleid is ook van toepassing op de ontwikkeling van dataproducten. Data producten moeten voldoen aan de wettelijke eisen van de AVG. Dit betekent dat de verwerking rechtmatig moet zijn, er sprake is van doelbinding en er dient een grondslag te zijn. Daarnaast werken we

volgens privacy by design, waarbij we dataminimalisatie toepassen en als basis uitgaan van anonimiseren van data, pseudonimiseren waar het moet en alleen naar herleidbare data met een stevige wettelijke grondslag bij het ontwikkelen van nieuwe data producten.

Daarnaast wordt voorafgaand aan de ontwikkeling van een dataproduct met een hoog privacy risico voor de betrokkenen (afweging door het SIO en FG) een gegevensbeschermingsanalyse (DPIA) uitgevoerd om risico's in beeld te hebben en maatregelen te kunnen treffen. Het is van belang om het werken met data veilig, integer en betrouwbaar te houden. Dit is geborgd in het proces 'dataprodukt'.

We zorgen voor een aanvulling op de bestaande autorisatiematrix, waarin verantwoordelijkheid en rolscheiding in de dataketen vastliggen. Hiermee bedoelen we dat functies niet meer rechten hebben dan noodzakelijk. Rollen die toegang hebben tot de geaggregeerde data hebben niet direct toegang tot onderliggende data. Onderliggende data met persoonsgegevens is alleen toegankelijk voor geautoriseerde medewerkers.

Voor het ontwikkelen van dataproducten is een procesplaat c.q. beschrijving gemaakt, waarin privacy geborgd is. Ook het Strategisch Informatie Overleg (SIO) heeft een belangrijke rol bij de ontwikkeling van dataproducten.

6.6 VEILIG COMMUNICEREN

Binnen de gemeente Gennep zijn kaders en richtlijnen ontwikkeld om veilig, toegankelijk en transparant met informatie en persoonsgegevens om te gaan. Hiervoor zijn verschillende communicatiemiddelen beoordeeld op verschillende aspecten waaronder privacy en informatieveiligheid. In bijlage 2 is een overzicht te vinden.

6.7 ARTIFICIËLE INTELLIGENTIE (AI)

AI

De AI-verordening, ook wel bekend als de AI Act, is aangenomen en bestaat uit regels voor het gebruik van Artificiële Intelligentie (AI) in de Europese Unie (EU). AI biedt veel kansen en voordelen, maar tegelijkertijd brengt AI ook risico's met zich mee. De AI-verordening is onderdeel van de Europese AI-strategie en is de allereerste uitgebreide AI-wet ter wereld.

De AI-verordening omvat eisen en kaders voor de ontwikkeling en het gebruik van AI-systemen door overheden en marktpartijen. Het is bedoeld om innovatie en economische ontwikkelingen de ruimte te geven terwijl publieke waarden worden beschermd. De prioriteit van het Europees Parlement is om ervoor te zorgen dat AI-systemen die in de EU worden gebruikt veilig, transparant, traceerbaar, niet-discriminerend en milieuvriendelijk zijn. Daarnaast vindt het Parlement dat AI-systemen nooit volledig geautomatiseerd mogen zijn en pleit het voor een uniforme definitie van AI die geldt voor alle toekomstige AI-systemen.

In aansluiting op de AI-verordening heeft de gemeente Gennep een AI-beleid ontwikkeld. Gennep omarmt de landelijke ontwikkelingen en richt haar AI-beleid op de invoering van een waardegedreven digitale gemeente. Privacybescherming is een belangrijk thema in AI. Verwezen wordt naar het gemeentelijk AI-beleid voor de kaders en spelregels.

Algoritmes

Algoritmes zijn er in alle soorten en maten. Van simpele 'recepten' tot geavanceerde, zelflerende systemen. Vaak om bepaalde beslissingen (deels) te automatiseren. Het gebruik van geavanceerde algoritmes kan voordelen bieden. Door patronen te halen uit data, kan bijvoorbeeld inzicht verkregen worden in verschillende maatschappelijke aspecten. Er zijn ook risico's. Algoritmes worden vaak gebruikt om geautomatiseerd besluiten te nemen. Een van de risico's hiervan is de kans op een oneerlijk of bevooroordeeld besluit. Of zelfs op discriminatie.

Algoritmes en AI verwerken vaak persoonsgegevens. Dit betekent dat het gebruik van algoritmes moet voldoen aan de Algemene verordening gegevensbescherming (AVG), net als alle andere verwerkingen van persoonsgegevens.

Op het moment dat de gemeente Gennep gebruik gaat maken van algoritmes, geldt dat dit gebeurt binnen de wettelijke kaders van de AVG alsmede het voorliggende privacybeleid (doelbinding, grondslag, dataminimalisatie, anonimisering, DPIA), AI-beleid en het 'Proces dataproduct'. Dit betekent dat een DPIA voorafgaand aan de verwerking wordt uitgevoerd en het SIO beoordeeld of een algoritme rechtmatig, doelmatig, ethisch en transparant is. Algoritmes worden geregistreerd (intern) alsmede in het landelijke register ([Het Algoritmeregister van de Nederlandse overheid](#)).

Chatbots

Een chatbot is een computerprogramma dat gesprekken tussen mensen simuleert en verwerkt zodat mensen met digitale apparaten kunnen communiceren. Een chatbot kan een programma zijn dat een eenvoudige vraag beantwoordt met één regel, of een geavanceerde digitale assistent die leert en evolueert en op basis van de verzamelde en verwerkte informatie steeds persoonlijker wordt, zoals bijvoorbeeld ChatGPT. ChatGPT werkt op basis van kansberekening en doet voorspellingen over wat waarschijnlijk de beste uitkomst is die past bij een opdracht.

De gemeente Gennep ziet de voordelen van het gebruik van Chatbots en ChatGPT, maar is zich ook bewust van de risico's. Daarom heeft de gemeente Gennep richtlijnen opgesteld voor het gebruik van AI-tools in haar AI-beleid. Verwezen wordt naar het AI beleid van de gemeente Gennep.

Het belangrijkste risico op het gebied van privacy is dat ChatGPT niet voldoet aan de Algemene Verordening Gegevensbescherming (AVG). Alles wat je invoert, kan in verkeerde handen terechtkomen.

De hoofdregel is:

Het is niet toegestaan persoonsgegevens en/of privacy- of bedrijfsgevoelige informatie in te voeren in de Chatbots.

Privacycheck bij AI

Om vast te stellen of de inzet van AI wel of niet mogelijk is en wettelijk is toegestaan, dient voorafgaand aan het gebruik een risicoanalyse te worden uitgevoerd. Dit zijn een Data Protection

Impact Assessment (DPIA), een De Ethische Data Assistent (DEDA) en een Algoritme Impact Assessment (AIA), waarin de risico's en risicobeperkende maatregelen worden vastgesteld.

Ook hier heeft het Strategisch Informatie Overleg (SIO) een belangrijke rol en wordt voorafgaand aan nieuwe digitale (AI)processen de risicoanalyse (DPIA) te besproken. Het SIO geeft dwingend advies of het wel of niet mogelijk is gebruik te maken van nieuwe toepassing. Het SIO kan ook beperkende maatregelen opleggen door regels of richtlijnen op te stellen voor het gebruik van de (AI)-toepassing. In dat geval is het van belang dat de gebruikers goed worden geïnformeerd over hoe zij deze technologie op een verantwoorde wijze kunnen inzetten.



Bijlage 1: Taken en rollen CISO, FG en PO

In deze bijlage worden de taken en rollen van de CISO, FG en PO uit het informatieveiligheidsbeleid van de gemeente Gennep d.d. 9-2-2024 weergegeven. De governance is vastgelegd in het Informatieveiligheidsbeleid, dat bij discrepantie leidend is.

CISO

De CISO is de interne adviseur op het gebied van informatieveiligheid binnen de organisatie. Deze rol is op organisatieniveau verantwoordelijk voor het actueel houden van het beleid, het adviseren van het management, het adviseren bij projecten evenals het opstellen van rapportages.

De CISO heeft in ieder geval de volgende taak en verantwoordelijkheid:

- Rapporteert rechtstreeks aan de gemeentesecretaris en het bestuur;
- Coördineert het formuleren van informatieveiligheidsbeleid;
- Coördineert de uitvoering van de informatieveiligheidsanalyse en zorgt voor de actualisatie;
- Coördineert prioritering informatieveiligheidsmaatregelen uit de informatieveiligheidsanalyse en de uitvoering van het actieplan informatieveiligheid;
- Stelt een plan op voor overleg en rapportage met betrekking tot informatieveiligheid;
- Ondersteunt de directie en afdelingsmanagers met kennis over informatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen;
- Is het aanspreekpunt voor medewerkers over het onderwerp informatieveiligheid;
- Volgt de externe invloeden die van invloed zijn op het informatieveiligheid;
- Geeft gevraagd én ongevraagd advies over informatieveiligheid aan de gehele organisatie;
- Bevordert het beveiligingsbewustzijn in de organisatie;
- Houdt de registratie van informatiebeveiligingsincidenten bij in een incidentenregister en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Ondersteunt het college bij het maken van de rapportage over de informatieveiligheid van de gemeente in het jaarverslag;
- Onderhoudt contact met de Informatiebeveiligingsdienst;
- Rapporteert over de informatieveiligheid van de gemeente in de P&C managementrapportages vergezeld van een in control statement. Hierbij bundelt de CISO de deelbijdragen van het afdelingsmanagement.

FG

De Functionaris Gegevensbescherming (FG) is conform de Algemene Verordening Gegevensbescherming (AVG) de interne toezichthouder op de verwerking van persoonsgegevens binnen de gemeente. De FG heeft de volgende (wettelijke) taken (AVG, artikel 39).

Het takenpakket van de FG bestaat uit:

- Informeren en adviseren van het college, de raad, het management, en de medewerkers over hun verplichtingen met betrekking tot gegevensbescherming;
- Toezien op naleving van zowel de AVG en andere wet- en regelgeving met betrekking tot Gegevensbescherming;
- Toezien op naleving van het gemeentelijk beleid met betrekking tot de bescherming van persoonsgegevens van de verwerkingsverantwoordelijke of de verwerker.
- Het toezien op het toewijzing van verantwoordelijkheden, bewustmaking en opleiding van de bij de verwerking betrokken personeel en de betreffende audits;
- Het geven van advies omtrent Data Protection Impact Assessments (DPIA) en het toezien of de uitvoering daarvan in overeenstemming is met de AVG.
- Toezichthouden op de registraties omtrent de afhandeling van datalekken en toezichthouden op het melden van een datalek bij de Autoriteit Persoonsgegevens (AP) en bij de betrokkenen.
- Samenwerken met en als contactpunt optreden voor de AP;
- Rapporteert rechtstreeks aan het college van burgemeester en wethouders.

PO

De Privacy Officer (PO) richt zich op de uitvoering en de naleving van de AVG. Daarnaast adviseert de PO over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.

De PO heeft in ieder geval de volgende taken:

- Beoordelen van verwerkingen van persoonsgegevens tegen de achtergrond van de kaders van privacywetgeving en adviseert het management bij wijzigingen in procesuitvoering, bedrijfsvoering en de toepassing van een Data Protection Impact Assessment (DPIA).
- Als adviserend lid deelnemen aan programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens.
- Uitleggen van de privacyvoorschriften uit de AVG en de sectorale wetgeving;
- Coördineren van de privacywerkzaamheden;
- Coördineren, samenvoegen en openbaar maken van de overzichten van gegevensverwerkingen die worden aangeleverd door de organisatieonderdelen van de gemeente;
- Coördineren van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens en adviseren over de afhandeling;
- Verzorgen van meldingen en intrekkingen van meldingen bij de FG en AP. Richt procedures in voor het afhandelen van datalekken en draagt zorg voor de afhandeling van datalekken;
- Rapporteren aan het managementteam;
- Beheer en onderhoud van de standaarddocumenten voor verwerkersovereenkomsten, convenanten en reglementen;
- Adviseren en ondersteunen bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten en convenanten en de vaststelling van reglementen.

Bijlage 2: Overzicht communicatiemiddelen Gennep

Inwoners en bedrijven verwachten dat wij Veilig, toegankelijk en transparant met informatie omgaan

Communicatiemiddelen: Als medewerker/bestuurder gebruik je:

❖ Graag	❖ Liever niet	❖ Zeker niet
- Microsoft Teams - Gemeentelijke website(s) - Klantportalen - MijnOverheid - OLO - MijnGennep - MijnZorg - Outlook Gennep (Mail) - Veilig mailen Gennep (Cryptshare) - Brief - Bellen - Fysieke ontmoeting	- Whatsapp - SMS - ChatGTP (Wel onder voorwaarden)	- TikTok - Signal - Telegram - WeTransfer - Dropbox - Privé mail - Social Media met naam@gennep.nl - Facebook - Twitter - Instagram - LinkedIn

Wanneer welk communicatiemiddel:

❖ Medewerkers/bestuurders onderling	❖ Algemeen naar inwoners/bedrijven	❖ Privacygevoelig / Vertrouwelijk naar inwoners/bedrijven
- Microsoft Teams - Outlook Gennep (Mail) - Bellen - Fysieke ontmoeting	- Gemeentelijke website(s) - Outlook Gennep (Mail) - Brief - Bellen - Fysieke ontmoeting	- Klantportalen - MijnOverheid - OLO - MijnGennep - MijnZorg - Veilig Mailen Gennep (Cryptshare)

➡ Volg altijd de richtlijn veilig communiceren.

Richtlijn Veilig Communiceren Gennep

Inwoners en bedrijven verwachten dat wij Veilig, toegankelijk en transparant met informatie omgaan

1. **Bepaal vooraf of informatie gedeeld mag/moet worden.**
 - o Gebruik geen/minimaliseer persoonsgegevens indien niet noodzakelijk.
 - o Minimaliseer het gebruik, door woorden als cliënt, aanvrager.
2. **Bepaald vooraf welk communicatiemiddel het meest geschikt is.**
 - o Gebruik overzicht communicatiemiddelen Gennep
 - o Berichtenapps zoals Whatsapp mogen niet gebruikt worden voor het delen van; vertrouwelijke en bestuurlijke informatie, besluiten en bijzondere en /of gevoelige persoonsgegevens
3. **Gebruik duidelijke en heldere taal. (B1 niveau)**
 - o Gebruik de Schrijfwijzer Gennep.
4. **Controleer met wie je communiceert.**
 - o Heb je de juiste persoon voor je? / Legitimatie noodzakelijk?
5. **Let op je omgeving wanneer je informatie deelt.**
 - o Kunnen anderen meekijken/meeluisteren?
6. **Wees je bewust dat gedeelde informatie altijd opgevraagd kan worden.**
 - o In het kader van de WOO of Archiefwet, ook Whatsapp e-mails enz.
7. **Sla gedeelde informatie op de juiste wijze op**
 - o Informatie die relevant is voor de reconstructie van besluitvorming, moet bewaard worden, ook whatsapp, e-mails enz.
 - o Twijfel je over hoe en waar, neem contact op met Informatiebeheer
8. **Maak afspraken over veilig communiceren met externen.**
 - o Gebruik de Samenwerkingswijzer Gennep

COMMUNICATIEMIDDELEN DIE JE MAG GEBRUIKEN:

- **Microsoft Teams**
 - o Chatten: Gebruik dit als alternatief voor Whatsapp of e-mail.
 - o Videobellen: Een vergadering mag je alleen opnemen met vooraf (schriftelijke) toestemming van alle deelnemers. Maak ook afspraken over het bewaren/delen/vernietigen van de opname.
 - o Samenwerken in een team: Ook geschikt om samen te werken met externen.
- **Gemeentelijke website:**
 - o Zorg dat teksten, links, afbeeldingen, video's en andere vormen van content voor iedere bezoeker toegankelijk zijn. (Overheidsinstanties zijn wettelijk verplicht om hun digitale kanalen toegankelijk te maken)
- **Klantportaal MijnOverheid:**
 - o De Berichtenbox is een persoonlijke brievenbus waarin inwoners digitale post van de overheid ontvangen. Mogelijk vanuit Djuma voor aangesloten inwoners. Alleen eenzijdige communicatie mogelijk. Gemeente Gennep > Inwoner
- **Klantportaal OLO:**

- Omgevingsloket online. Het landelijke digitale loket voor de omgevingsvergunning en de watervergunning. Aanvragen komen direct binnen in de applicatie Rx. Mission. Tweezijdige communicatie mogelijk Gemeente Gennepe ↔ Inwoner/Bedrijf
- Klantportaal MijnGennepe:
 - Mogelijk vanuit Djuma voor ingerichte zaaktypes. Tweezijdige communicatie mogelijk. Gemeente Gennepe ↔ Inwoner/Bedrijf
- Klantportaal MijnZorg:
 - (Bruikbaar circa 2^e helft 2024) Mogelijk vanuit ZorgNed voor WMO/Jeugd. Tweezijdige communicatie mogelijk Gemeente Gennepe ↔ Inwoner
- Outlook Gennepe (Mail):
 - Maak als alternatief gebruik van Microsoft Teams. Hier kun je snel chatten met collega's of samenwerken in een team.
- Veilig Mailen Gennepe (Cryptshare):
 - Tweezijdige veilige communicatie mogelijk tussen Gemeente Gennepe en Inwoners en Bedrijven. Ook geschikt voor het delen van grote bestanden.
- Brief:
 - Maak gebruik van standaard sjablonen en de schrijfwijzer.
- Bellen:
 - Gebruik MiCollab. Terugbel verzoeken staan in Djuma.
- Fysieke Ontmoeting:-

COMMUNICATIE DIE JE LIEVER NIET GEBRUIKT/ OF ALLEEN ONDER VOORWAARDEN:

- **Whatsapp:**
 - Het gebruik van berichtenapps zoals Whatsapp voor zakelijke communicatie wordt zoveel mogelijk beperkt. Voor bestuurlijke aangelegenheden wordt het gebruik ontraden.
 - Berichtenapps zoals Whatsapp mogen niet gebruikt worden voor het delen van; vertrouwelijke en bestuurlijke informatie, besluiten en bijzondere en/of gevoelige persoonsgegevens, behalve in specifieke in de wet benoemde situaties.
 - Het wordt dringend geadviseerd om de functie geautomatiseerde verwijdering, die in diverse berichtenapps kan worden ingesteld, niet te activeren.
 - Chatberichten die relevant zijn voor de reconstructie van besluitvorming, moeten worden bewaard. De medewerker of het bestuurslid dat gebruik maakt van die berichtenapp, zorgt voor de archivering van de relevante onderdelen in die communicatie.
- **SMS:**
 - Gebruik dit alleen voor informele communicatie. En bijvoorbeeld in combinatie met Cryptshare. (Alternatieven zijn Microsoft Teams en Outlook Gennepe (Mail)).
- **ChatGPT:**
 - ChatGPT is een AI-chatbot. Het is gebaseerd op de GPT-3-technologie van OpenAI en kan vragen beantwoorden, conversaties voeren en zelfs teksten genereren.
 - ChatGPT werkt op basis van kansberekening en doet voorspellingen over wat waarschijnlijk de beste uitkomst is die past bij een opdracht. (Het begrijpt je niet!)
 - Voor effectief gebruik, zijn heldere instructies cruciaal. Taalvaardigheid en inhoudelijke kennis zijn essentieel, omdat de output niet altijd betrouwbaar is en beoordeling vereist.

- Waar kun je ChatGTP voor inzetten?
 - Voor inspiratie, onderzoek, teksten verbeteren
- Hanteer bij gebruik altijd de volgende principes:
 - Deel nooit privacy gevoelige/vertrouwelijke informatie met ChatGTP
 - Wees zelf de expert
 - Dubbelcheck de antwoorden
 - Wees er open over als je ChatGTP gebruikt
- Aandachtspunten:
 - Niet alle antwoorden van ChatGPT zijn correct.
 - ChatGTP gebruikt geen bronvermelding.
 - ChatGPT loopt achter op de actualiteit.
 - CHATGPT 3.5 is getraind op datasets van het internet tot 2021.
 - CHATGPT 4 is getraind met data tot begin 2022.
 - Hoe weet je of je een goede vraag formuleert?
 - Wat is prompting? Een prompt is een instructie of een vraag die je aan de voorkant aan een goede AI-tool geeft om een specifieke respons of output te genereren. De input dus. Een zo gericht mogelijke prompt levert de gewenste informatie op, terwijl een onduidelijke of onvolledige prompt kan leiden tot minder relevante of ongewenste resultaten.
- (on)Mogelijkheden van AI
 - Accuraatheid
 - Overtuigende teksten maar de inhoud hoeft niet juist te zijn.
 - Ethische aspecten
 - Trainen met bevooroordeelde data en verkeerde veronderstellingen (Bias).
 - Trainen met het inhoudelijke werk van iemand anders.
 - Niet altijd zicht op de wijze waarop AI tot een antwoord komt (Black box)
 - Desinformatie
 - Sneller en beter generen van teksten, audio, video en afbeeldingen. - Detectie is lastig en loopt (steeds) achter
 - Ecologische footprint
 - Gebruikt veel energie om te trainen en te gebruiken
 - Afhankelijkheid van technologiebedrijven
 - Kost veel om generatieve AI te maken, te onderhouden en te gebruiken

COMMUNICATIEMIDDELEN DIE JE NIET MAG GEBRUIKEN:

- **TikTok:**
 - Mag niet gebruik worden.
- **Signal:**
 - Mag niet gebruikt worden. Alternatieven zijn Microsoft Teams of Outlook Gennep (Mail)
- **Telegram:**
 - Mag niet gebruikt worden. Alternatieven zijn Microsoft Teams of Outlook Gennep (Mail)
- **WeTransfer:**

- Mag niet gebruikt worden. Alternatief is Cryptshare.
- **Dropbox:**
 - Mag niet gebruikt worden. Alternatief is Cryptshare.
- **Privé Mail:**
 - Mag niet gebruikt worden. Alternatief is Outlook Gennep (Mail)
- **Social Media met naam@gennep.nl**
 - Facebook, Twitter, Instagram en LinkedIn mogen niet gebruikt worden met een account op basis van je Outlook Gennep Mail (naam@gennep.nl). Uiteraard kun je deze social media wel gebruiken met je privé mail. Denk altijd goed na over het gebruik van social media voor werk gerelateerde onderwerpen. Voor advies kun je terecht bij team Communicatie. Deel nooit privacygevoelige of vertrouwelijke informatie.



