

Privacybeleid gemeente Hof van Twente

Burgemeester en wethouder van de gemeente Hof van Twente;

gelet op gelet op het bepaalde in de Algemene verordening gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg); gelet op titel 4.3 van de Algemene wet bestuursrecht;

besluiten;

vast te stellen het navolgende **privacybeleid gemeente Hof van Twente 2021**.

Inleiding

Binnen de gemeente Hof van Twente (hierna gemeente) wordt gewerkt met persoonsgegevens van burgers, ondernemers, bezoekers, medewerkers van de gemeente en (keten)partners. Deze persoonsgegevens worden verzameld en verder verwerkt voor het goed uitvoeren van de gemeentelijke wettelijke taken, het voldoen aan wettelijke verplichtingen en voor de bedrijfsvoering van de gemeentelijke organisatie.

Privacy speelt een belangrijke rol in de relatie tussen de burger de overheid en staat daarmee hoog op de bestuurlijke agenda. Gemeenten hebben de verantwoordelijkheid over persoonsgegevens 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.

De gemeente toont in dit beleid aan hoe zij de bescherming en beveiliging van persoonsgegevens borgt. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. Dit privacybeleid is in lijn met het informatiebeveiligingsbeleid van de gemeente.

Werkprocessen

De werkprocessen van de diverse afdelingen binnen de gemeente spelen zich vaak af binnen een verplicht wettelijk kader. Dat kader is bepalend voor welke persoonsgegevens op welke manier mogen worden verwerkt. Ambtenaren hebben een geheimhoudingsplicht die bepaalt welke informatie wanneer mag worden verstrekt en aan wie. In het algemeen mogen ambtenaren alleen die persoonsgegevens verwerken die noodzakelijk zijn voor hun taak en het doel dat ze beogen. Werkprocessen zijn opgenomen als verwerkingsactiviteit in het AVG-verwerkingsregister van de gemeente. De afdelingsmanagers en teamcoördinatoren zijn primair verantwoordelijk voor het actueel houden en vastleggen van deze werkprocessen in het verwerkingsregister.

Governance en organisatorische borging privacybescherming binnen de gemeente

Het beschermen en beveiligen van persoonsgegevens vergt inspanningen van het bestuur, management en medewerkers van de gemeente. Het is dus een integrale verplichting voor iedereen die voor de gemeente werkt. De gemeente kent drie bestuursorganen: de gemeenteraad, het college van burgemeester en wethouders en de burgemeester. Kort gezegd hebben we het vaak over de raad, het college en de burgemeester. Deze drie bestuursorganen van de gemeente zijn de verwerkings-verantwoordelijken voor de naleving van de verplichtingen uit de privacywetgeving. Deze drie bestuursorganen hebben het naleven van deze verplichtingen (gedeeltelijk) opgedragen (gemandateerd) aan de ambtelijke organisatie van de gemeente. Het mandaatbesluit waarin dit mandaat is geregeld is gepubliceerd op de website van de gemeente.

De Functionaris Gegevensbescherming (FG) is een wettelijk verplichte functie voor de gemeente. Samen met de CISO, de Privacy Officer, een juridisch medewerker sociaal domein en een beleidsmedewerker informatievoorziening vormt de FG de kerngroep AVG. Dit privacyteam is belast met de monitoring van de kwaliteit van de privacybescherming binnen de gemeentelijke organisatie. Het team is niet zelf verantwoordelijk voor de naleving van de AVG en andere privacyregels. Dat is en blijven de verwerkings-verantwoordelijke bestuursorganen.

In de Privacy Governance staat een beschrijving van de rollen, taken en verantwoordelijkheden ten aanzien van privacy.

Toezicht op de naleving van de privacyregels binnen de gemeente

Het interne toezicht op de naleving van de AVG door de gemeente is belegd bij de FG. Deze FG handelt onafhankelijk en wordt niet aangestuurd door de gemeente. De gemeente oefent geen invloed uit op hetgeen de FG doet. Alle leden en medewerkers van de gemeente werken volledig mee aan alle verzoeken van de FG.

Het toetsen van de naleving van de privacyregels volgt de structuur van de bestaande informatiebeveiligingscycli waarbinnen getoetst wordt aan de Baseline informatiebeveiliging overheid (BIO). Omdat privacybescherming en informatiebeveiliging verwante werkvelden zijn worden de processen en procedures binnen de twee werkvelden zoveel mogelijk geïntegreerd. Dat kan bijvoorbeeld heel goed bij het voorkomen, verhelpen, registreren en melden van datalekken maar ook bij het uitvoeren van privacy impact assessments (PIA's).

Juridisch kader van het verwerken van persoonsgegevens

Vanaf 25 mei 2018 is in de hele Europese Unie de Algemene verordening gegevens-bescherming (AVG) van toepassing. Daar waar de AVG ruimte laat om op nationaal niveau bepaalde vraagstukken (aanvullend) te regelen, is dit in Nederland gedaan door middel van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG). De UAVG is met ingang van 25 mei 2018 in werking getreden.

Daarnaast zijn er regels voor de verwerking van persoonsgegevens in het kader van de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Deze wetten zijn het gevolg van de implementatie van de EU-Richtlijn 2016/680. Voor zover de gemeente voornemens is een bestraffende sanctie op te leggen, valt de daarmee samenhangende verwerking van persoonsgegevens onder de reikwijdte van de Wpg. Een voorbeeld hiervan is de verwerking van persoonsgegevens door gemeentelijke BOA's.

De AVG legt meer verantwoordelijkheid op organisaties om aan te tonen dat de door hen uitgevoerde verwerkingen aan de regels op het gebied van gegevensbescherming voldoen. De gemeente is gehouden om aan deze verantwoordelijkheidsplicht (accountability) te voldoen. Zo moet de gemeente bijvoorbeeld aantonen dat een verwerking aan de belangrijkste beginselen van gegevensverwerking voldoet, zoals rechtmatigheid, transparantie, noodzaak ten opzichte van het beoogde doel en juistheid. Ook moet de gemeente kunnen laten zien dat de juiste technische en organisatorische maatregelen zijn genomen om de persoonsgegevens te beschermen. Voor zover de gemeente voornemens is een bestuurlijke boete op te leggen, of wanneer de gemeentelijke BOA's hun werk doen dient de daarmee samenhangende gegevensverwerking te voldoen aan de normen van de Wpg.

Verwerken (artikel 4 AVG)

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

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

Beginnelsen uit de AVG (artikel 5 AVG)

De beginselen van de AVG zijn opgesomd in artikel 5 van de AVG. Kort gezegd houden ze in dat persoonsgegevens alleen mogen worden verwerkt als het echt niet anders kan en voor doelen die welbepaald zijn. Wanneer de gemeente wettelijke taken uitvoert is in de wet of in de daarop gebaseerde beleid- en uitvoeringsregels vaak al bepaald wat het doel van de taakuitoefening van de gemeente is. In die gevallen moet ook nog de noodzaak van de verwerking van persoonsgegevens ten opzichte van de beoogde doelen worden aangetoond. Wanneer het doel niet helder is zal dit eerst moeten worden bepaald voordat gestart kan worden met de verwerking van persoonsgegevens.

Op basis van de AVG gelden de volgende beginselen ten aanzien van de verwerking van persoonsgegevens:

- De verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn.
- De verwerking van persoonsgegevens moet een helder doel hebben dat is terug te leiden naar taken, verplichtingen, overeenkomsten of belangen.
- Het verwerken van persoonsgegevens moet noodzakelijk zijn ten opzichte van de beoogde doelen (proportionaliteit en subsidiariteit). Wanneer met geen, of minder (belastende) persoonsgegevens hetzelfde doel bereikt kan worden, moet daar voor gekozen worden.
- De (verwerking van) persoonsgegevens moet(en) juist en van voldoende kwaliteit zijn.
- De (verwerking van) persoonsgegevens moet(en) goed zijn beveiligd en beschermd.
- Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk of verplicht is.

Rechtsgrond en doel (artikel 6 AVG)

Er zijn zes rechtsgronden in de AVG op basis waarvan persoonsgegevens kunnen worden verwerkt. De rechtsgronden waar de gemeente zich op kan baseren zijn:

Rechtsgrond	Voorbeeld
Uitvoeren of vervullen van een taak van algemeen belang of openbaar gezag (artikel 6, eerste lid letter e AVG)	Uitvoeren van de participatiewet of de wet maatschappelijke ondersteuning
Voldoen aan een wettelijke verplichting (artikel 6, eerste lid letter c AVG)	Voldoen aan een vordering van de officier van justitie.
Gerechtigd belang (artikel 6, eerste lid letter f AVG)	Voeren van een personeelsadministratie
Overeenkomst (artikel 6, eerste lid letter b AVG)	Het inhuren van dienstverleners en adviseurs

De twee rechtsgronden die zich in de praktijk niet of nauwelijks voordoen bij de gemeente zijn:

Rechtsgrond	Voorbeeld
Vitaal belang (artikel 6, eerste lid letter d AVG)	Bij direct en onmiddellijk levensgevaar
Toestemming (artikel 6, eerste lid letter a AVG)	Vrije keuze om wel of niet met de gemeente in zee te gaan.

Doelinden verwerking persoonsgegevens

Het doel waarvoor de gemeente persoonsgegevens verwerkt hangt samen met de rechtsgrond. De gemeente verwerkt de meeste persoonsgegevens voor het uitvoeren van de primaire gemeentelijke overheidstaken. Deze taken staan in wetgeving, daarop gebaseerde regelgeving en beleid. Voor meer informatie over de doelinden van de verwerking van persoonsgegevens door de gemeente wordt verwezen naar het verwerkingsregister.

Er zijn werkprocessen die zodanig samenhangen met de primaire gemeentelijke taken dat ze ook gerekend worden tot de primaire processen, zoals beleidsonderzoek, klachten behandelen, bezwaar en beroep behandelen, voorlichting geven, toezicht houden op de naleving van de gemeentelijke regels en deze regels handhaven.

De secundaire verwerkingen van persoonsgegevens hebben als doel de bedrijfsvoering, het personeelsbeleid en de organisatie en het beheer van de gemeente.

Rechten van betrokkenen

Betrokkenen zijn alle natuurlijke personen van wie de gemeente de persoonsgegevens verwerkt. Persoonsgegevens zijn alle gegevens die direct of indirect herleidbaar zijn naar een natuurlijk persoon; de betrokkene. Persoonsgegevens zijn dus veel meer gegevens dan alleen iemands persoonlijke gegevens zoals bijvoorbeeld naam, adres en woonplaats. Om te kunnen controleren of de gemeente zich wel houdt aan de AVG hebben betrokkenen een controlemiddel. Betrokkenen hebben rechten die ze kunnen uitoefenen en de gemeente is verplicht om daarvoor goede en toegankelijke procedures te hebben. De AVG-rechten van betrokkenen staan in hoofdstuk 3 van de AVG en de Wpg-rechten van betrokkenen staan in § 4 van de Wpg. Deze rechten worden hierna kort toegelicht.

Recht op informatie (artikel 12, 13 en 14 AVG en 24a en 24b Wpg)

Betrokkenen hebben recht op de volgende informatie:

	AVG	WPG
a	de verwerkingsdoelinden;	de doelen en de rechtsgrond van de verwerking;
b	de betrokken categorieën van persoonsgegevens;	de betrokken categorieën van politiegegevens;
c	de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;	de vraag of de deze persoon betreffende politiegegevens gedurende een periode van vier jaar voorafgaande aan het verzoek zijn verstrekt en over de ontvangers of categorieën van ontvangers aan wie de gegevens zijn verstrekt, met name ontvangers in derde landen of internationale organisaties;
d	indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;	de voorziene periode van opslag of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
e	dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;	het recht te verzoeken om rectificatie, vernietiging of afscherming van de verwerking van hem betreffende politiegegevens;
f	dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;	het recht een klacht in te dienen bij de Autoriteit persoonsgegevens, en de contactgegevens van die autoriteit;
g	wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;	de herkomst, voor zover beschikbaar, van de verwerking van hem betreffende politiegegevens.
h	het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige	

informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

i doorgifte aan derde landen

Om tegemoet te komen aan deze informatieverplichtingen heeft de gemeente op haar website een privacyverklaring gepubliceerd. Deze privacyverklaring is een voor het publiek toegankelijke samenvatting van dit privacybeleid en de op het privacybeleid gebaseerde AVG-procedures van de gemeente.

Overige rechten (15, 16, 17, 18, 19, 21 en 22 AVG en 25 tot en met 31c Wpg)

Op de website van de gemeente is ook gepubliceerd op welke manier er gebruik kan worden gemaakt van de overige AVG-rechten door betrokkenen. Het gaat dan om de volgende rechten op:

- recht op inzage (artikel 15 AVG en 25 Wpg): betrokkenen hebben de mogelijkheid om door middel van een kopie van de persoonsgegevens te controleren of en op welke manier zijn/haar persoonsgegevens worden verwerkt
- recht op rectificatie/correctie (artikel 16 en 19 AVG en 28 Wpg): betrokkenen kunnen een verzoek indienen om persoonsgegevens te corrigeren indien blijkt dat deze niet kloppen
- recht op wissing/recht om vergeten te worden (artikel 17 en 19 AVG en 28 Wpg): betrokkenen hebben het recht om de persoonsgegevens te laten verwijderen. Dit kan niet altijd worden uitgevoerd omdat er in diverse situaties wettelijke bewaartermijnen gelden op basis van bijvoorbeeld de Archiefwet
- recht op beperking van de verwerking (artikel 18 en 19 AVG): betrokkenen kunnen verzoeken om minder gegevens te laten verwerken mits dit mogelijk is gelet op de taken van de gemeente
- recht van bezwaar ook wel verzet (artikel 21 AVG): betrokkenen kunnen bezwaar maken tegen het verwerken van hun persoonsgegevens. De gemeente kan hieraan alleen voldoen als er geen gerechtvaardigde gronden zijn voor de verwerking.
- niet onderworpen worden aan een geautomatiseerd besluit waaronder profiling (artikel 22 AVG)
- indienen van een klacht bij de Autoriteit Persoonsgegevens (artikel 12, 13, 14, 15 AVG en 31a Wpg)

Gebruik maken van deze rechten kan door een mail te sturen naar info@hofvantwente.nl.

Bij een beroep op het recht op inzage is geen motivering nodig. Bij een beroep op één van de andere rechten wel. Het beroep op het recht op wissing zal in het geval van een verwerkingsactiviteit die verband houdt met een overheidstaak vaak niet gehonoreerd kunnen worden vanwege bijvoorbeeld de Archiefwet.

Behandeling AVG- en Wpg-verzoeken

De coördinatie van de behandeling van de AVG-en Wpg-verzoeken gebeurt centraal binnen de gemeente. De verzoeken komen binnen bij info@hofvantwente.nl. Na identificatie van de betrokkene die het verzoek heeft ingediend wordt een ontvangstbevestiging gestuurd en wordt de behandeling van het verzoek gestart. Dit resulteert uiteindelijk in een besluit dat aan de betrokkene wordt gestuurd. Het besluit wordt ondertekend namens de bevoegde verwerkingsverantwoordelijke (raad, college of burgemeester).

Het is belangrijk dat de gemeente de identiteit vaststelt van de betrokkene voordat een verzoek kan worden behandeld. Dat is één van de voorwaarden om aan een AVG-verzoek te kunnen voldoen. Ook moet ervoor worden gewaakt dat er met het voldoen aan het verzoek geen rechten van andere betrokkenen worden geschonden. In sommige gevallen kan een verzoek worden beperkt omdat er redenen zijn met een zwaarwegend algemeen belang die zwaarder wegen dan de privacyrechten van de betrokkene. De gemeente maakt dan een belangenafweging en legt dit uit.

De gemeente streeft naar de behandeling van een verzoek binnen de wettelijke termijn. Wanneer dat nodig is wordt de termijn verdaagd. De beslissing op het verzoek is een bestuursrechtelijk besluit. Dat betekent dat er tegen dit besluit rechtsmiddelen kunnen worden ingesteld. Hoe dat moet staat onder elk besluit (we noemen dat een rechtsmiddelenverwijzing).

Geautomatiseerde verwerkingen

Profiling: Profiling vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt 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. Om profiling 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. Daarnaast geeft de wet aan dat er geen besluit mag worden genomen op basis van profiling.

Big data en tracking: Door middel van Big data onderzoek en tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een natuurlijk 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 door geautoriseerde personen zijn verzameld. Wanneer de gegevens worden omgezet in een dataset zal dataminimalisatie worden toegepast. Dit betekent dat alleen de data die echt nodig is voor het behalen van het doel gebruikt zullen worden. Daarnaast kunnen persoonsgegevens gepseudonimiseerd worden zodat zij niet herleidbaar zijn tot een persoon.

Inzet van camera's: Binnen de gemeente wordt onder bepaalde omstandigheden gebruik gemaakt van cameratoezicht, zoals vastgelegd in de Gemeentewet. Cameratoezicht wordt onder andere gebruikt voor het vergroten van de veiligheid op straat. Camera's kunnen een grote inbreuk maken op de privacy van diegene die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen worden camera's alleen ingezet wanneer er geen andere manieren zijn om het doel te bereiken, en worden er eisen gesteld aan de inzet van camera's.

De BOA's binnen de gemeente Hof van Twente zijn sinds begin 2021 uitgerust met bodycams. De bodycam wordt gebruikt om bij eventuele incidenten een de-escalerend effect te weeg te brengen maar is wel aan strikte regels gebonden. Hiervoor heeft de gemeente Hof van Twente het 'Protocol Bodycams' opgesteld.

AVG-register van verwerkingsactiviteiten

De gemeente houdt een AVG-register van verwerkingsactiviteiten bij, het zogeheten verwerkingsregister. Dit register wordt niet gepubliceerd maar is intern beschikbaar. Het wordt regelmatig geactualiseerd en gecontroleerd op juistheid en volledigheid. Het bijhouden van het verwerkingsregister is een verplichting uit de AVG. In het verwerkingsregister staan in ieder geval de doelen en de rechtsgronden van de verwerkingen van persoonsgegevens evenals een beschrijving van de soort persoonsgegevens die worden verwerkt en de daarbij behorende betrokkenen en eventuele ontvangers.

Informatiebeveiliging

In het kader van de uitvoering van de gemeentelijke taken vertrouwen burgers, bezoekers, ondernemers en derden veel gevoelige persoonsgegevens toe aan de gemeente. Daarom is het belangrijk dat de gemeente deze gegevens goed beschermt en beveiligt binnen haar organisatie en informatiesystemen. Om ervoor te zorgen dat de beveiliging op orde is en blijft worden de getroffen beveiligingsmaatregelen in een continue proces getoetst op werkzaamheid en actualiteit. Bij het beschermen van persoonsgegevens worden extra beveiligingsmaatregelen genomen als er sprake is van grotere risico's voor de persoonlijke levenssfeer. Dat is bijvoorbeeld het geval bij het verwerken van bijzondere persoonsgegevens, de persoonsgegevens van kinderen en bij combinaties van persoonsgegevens die door hun combinatie een grote inbreuk op de persoonlijke levenssfeer kunnen opleveren.

Bijzondere persoonsgegevens

Voor het verwerken van bijzondere persoonsgegevens gelden strengere voorwaarden dan voor het verwerken van gewone persoonsgegevens. Bij bijzondere persoonsgegevens gaat het onder meer om gegevens over de gezondheid van de betrokkene. De hoofdregel is dat bijzondere persoonsgegevens niet verwerkt mogen worden. Op deze hoofdregel bestaan meerdere uitzonderingen. Deze staan in artikel 9, tweede lid, letter g en artikel 23, eerste lid, letter a tot en met j van de AVG. De verwerking van bijzondere persoonsgegevens moet noodzakelijk zijn voor de uitvoering van de aan de gemeente wettelijk opgedragen taken. Voorwaarde is dat bij die uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Bovendien moet het beoogde doel van de verwerkingsactiviteit kunnen worden gekwalificeerd als een doel met een zwaarwegend algemeen belang zoals bedoeld is in artikel 23 AVG, eerste lid, letters a tot en met j.

Strafrechtelijke persoonsgegevens

Voor het verwerken van strafrechtelijke persoonsgegevens gelden ook strengere voorwaarden dan voor het verwerken van gewone persoonsgegevens. De voorwaarden voor het verwerken van strafrechtelijke persoonsgegevens staan in artikel 10 AVG en de UAVG.

Bewaartermijnen

Op grond van de Archiefwet is de gemeente verplicht de onder haar berustende archiefbescheiden in goede, geordende en toegankelijke staat te brengen en te bewaren. Ook moet de gemeente zorgdragen voor de vernietiging van de daarvoor in aanmerking komende archiefbescheiden. In een selectielijst is vastgelegd welke bescheiden worden bewaard. Tevens is aangegeven welke bescheiden voor vernietiging in aanmerking komen en binnen welke termijn vernietiging moet plaatsvinden. Archiefbescheiden die niet voor vernietiging in aanmerking komen en ouder zijn dan twintig jaar worden overgebracht naar een archiefbewaarplaats (artikel 12 van de Archiefwet).

Voor zover in de archiefbescheiden persoonsgegevens voorkomen is daarop de AVG van toepassing. Voor de archiveringstaak zijn diverse uitzonderingen in de AVG opgenomen.

Baseline informatiebeveiliging overheid (BIO)

Voor de gemeente geldt de baseline informatiebeveiliging overheid (BIO) als beleidskader. De naleving van de BIO wordt getoetst in een zogenoemde regelkring of pdca cyclus (plan-do-check-act). Het tijdig, juist en volledig uitvoeren van PIA's, het opvolgen van de maatregelen die voortvloeien uit deze PIA's (comply) of het uitleggen waarom dit niet het geval is (explain) vormen een integraal onderdeel van de BIO. Ook worden er interne en externe audits uitgevoerd op de naleving van het privacy- en securitybeleid en de informatiesystemen.

Binnen de gemeente is een aanvullend informatiebeveiligingsbeleid vastgesteld. Korthedshalve wordt daarnaar verwezen.

Datalekken

Wanneer een (vermoedelijke) inbreuk op de persoonsgegevens (een datalek) wordt geconstateerd, wordt dit via een interne procedure geregistreerd en zo nodig gemeld bij de AP en de betrokkenen. Er is al sprake van een datalek wanneer persoonsgegevens in onbevoegde handen kunnen zijn gekomen. Melden aan de AP is verplicht wanneer betrokkenen een risico hebben gelopen. Alleen als er geen of een verwaarloosbaar risico is voor betrokkenen kan de melding achterwege blijven. Wanneer er een hoog risico is voor betrokkenen moet er ook worden gemeld aan de betrokkenen zelf. Er is een procedure voor het registreren en melden van datalekken vastgesteld.

Informatieuitwisseling met derden

Wanneer dat noodzakelijk is voor de uitvoering van de gemeentelijke taken of wanneer er een wettelijke verplichting is, kan de gemeente persoonsgegevens verstrekken aan derden. Dat gebeurt altijd na een belangenafweging waarbij het belang van de gemeente en de ontvanger wordt afgewogen tegen het belang van de betrokkenen bij het niet verwerken/verstrekken van de persoonsgegevens. Het verwerken en verstrekken van persoonsgegevens wordt tot een minimum beperkt. Belangenafwegingen worden gemaakt door medewerkers en niet door algoritmen of vink-lijstjes. Wanneer de gemeente een geheimhoudingsplicht heeft zal er een geldige reden moeten zijn om deze te doorbreken. Een toets aan de geheimhoudingsverplichtingen zal altijd voorafgaan aan een verstrekking. De beoordeling en het eindoordeel van de belangenafweging worden in het dossier vastgelegd door de primaire behandelaar.

Inwerkingtreding

Dit privacybeleid treedt een dag na bekendmaking in werking. Het Privacybeleid Hof van Twente 2018 en het Privacyreglement gemeente Hof van Twente worden per die datum ingetrokken. Het beleid wordt jaarlijks geëvalueerd en indien nodig herzien. Aanpassingen aan dit beleid worden bekendgemaakt. De meest actuele versie van het beleid is te vinden op de website van de gemeente.

*Aldus vastgesteld in de vergadering van het college van burgemeester en wethouders van de gemeente Hof van Twente d.d. 19 oktober 2021
Burgemeester en wethouders van Hof van Twente,
de secretaris, de burgemeester,
drs. D. Lacroix drs. H.A.M. Nauta-van Moorsel MPM*