



Beleids- begroting

2025 - 2028



Gemeente
Hengelo

www.hengelo.nl

6.7.6 Informatiebeveiliging en privacy

In een digitale wereld zijn informatiebeveiliging en privacy zeer belangrijke onderwerpen. De digitale dreiging voor Nederland en haar inwoners is onverminderd groot en verandert voortdurend. Zowel op landelijk en regionaal niveau wordt dit onderkend. Ook binnen de gemeente Hengelo wordt ervoor gezorgd dat bij de dagelijkse werkzaamheden beveiliging en privacy een prominente plek innemen door onder andere "security-by-design" en "privacy-by-design" als standaard te hanteren en volgen we de ontwikkelingen van de wet- en regelgeving om daar tijdig op te kunnen anticiperen.

Bereiken?	Doen?
Uitvoeren jaarlijkse AVG-compliance toets	In 2020 is het volwassenheidsniveau op gebied van privacy binnen de gemeente gemeten aan de hand van het VNG AVG-borgingsproduct. In 2025 wordt deze meting opnieuw uitgevoerd om te bepalen of de gemeente op koers ligt om de vastgestelde ambitie te behalen en stellen we eventueel noodzakelijke maatregelen op.
Toezicht door de Functionaris Gegevensbescherming	De Functionaris Gegevensbescherming (FG) zal toezicht houden op de interne naleving van de regelgeving op het gebied van gegevensbescherming en zal daarvan jaarlijks verslag doen aan de verwerkingsverantwoordelijke, het college van B en W. Ook in de periode 2025-2028 zal de FG in de uitoefening van zijn taken onafhankelijk zijn en geen instructies ontvangen. De reguliere toezichthoudende activiteiten zullen zich m.n. richten op het verwerkingenregister, DPIA's en de behandeling van datalekken. De FG zal jaarlijks een toezichtplan opstellen, waarin ook per jaar een bijzondere focus voor het toezicht kan worden vermeld.
Middelen informatiebeveiliging	De focus op sterke beveiligingsmaatregelen zal in 2025 onverminderd groot zijn. Naast de investeringen in hardware- en softwarematige oplossingen, is het continu investeren in (externe) kennis onontbeerlijk. In 2025 zetten we actief in om kennis in relatie tot de operationele en specialistische werkzaamheden rondom informatiebeveiliging in onze eigen organisatie te borgen.
Monitoring en Respons (<i>Verzamelen, monitoren en analyseren van informatie i.r.t. informatiebeveiliging</i>)	In 2024 is de tijdelijke basisoplossing voor monitoring en respons in gebruik genomen en wordt gewerkt aan continue verbetering. Er is door Hengelo ingeschreven op de vernieuwde landelijke aanbesteding, in 2025 zal hier opvolging aan gegeven worden om te komen tot selectie van een duurzame oplossing, rekening houdende met bestaande producten en diensten.
Bewustwording en samenwerking informatiebeveiliging en privacy	In 2024 is het huidige bewustwordingsprogramma geëvalueerd. Uitkomsten van de evaluatie zijn gewogen en worden in het programma van 2025 meegenomen. Dit geldt zowel voor bewustwording onder huidige medewerkers als voor bewustwording bij de indiensttreding van nieuwe medewerkers. Ook zal er in 2025 specifiek aandacht worden besteed aan bewustzijn voor bestuurders in het kader van nieuwe wetgeving op gebied van informatiebeveiliging.
Uitvoeren van de jaarlijkse penetratie test	Jaarlijks laten wij door een gecertificeerde partner een penetratie test (pentest) uitvoeren door ethisch hackers, waarbij wij telkens de scope van de opdracht verleggen en aanscherpen. Een pentest is een toets op het kunnen binnendringen in het interne en externe (cloud) netwerk van de gemeente Hengelo. De aanbevelingen worden projectmatig opgepakt en doorgevoerd. In 2025 zal opnieuw een pentest worden uitgevoerd.
Verstevigen samenwerking Twentse gemeenten	Op het onderwerp informatiebeveiliging en privacy wordt intensief met de andere Twentse gemeenten opgetrokken. De vakinhoudelijk betrokken medewerkers (CISO's, FG's en PO's) zorgen voor periodieke overleggen en ondersteunen elkaar rondom vraagstukken en uit te voeren werkzaamheden. Informatiebeveiliging en privacy kan immers niet (meer) alleen op het niveau van een individuele gemeente opgepakt worden. In 2024 is een regionale themabijeenkomst informatiebeveiliging geweest met hoofden bedrijfsvoering en CISO's, daar zijn diverse onderwerpen geselecteerd voor nadere verkenning op samenwerking. Deze regionale samenwerking zal in 2025 worden gecontinueerd en waar mogelijk geïntensiveerd.
Verwerkingsregister	In 2025 wordt vervolg gegeven aan het inrichten van het systeem dat is geselecteerd om het verwerkingsregister van de gemeente in op te nemen. Ook zal in samenwerking met de leverancier worden onderzocht of andere compliancemaatregelen uit de AVG binnen dit systeem kunnen worden ingepast. Te denken valt aan een publieke versie van het verwerkingsregister in het kader van transparantie en de uitvoering van DPIA's.
Cyberbeveiligingswet (NIS2/Cbw)	In 2024 is de aangepaste en uitgebreide Europese richtlijn voor informatiebeveiliging gepubliceerd, de Network and Information Security directive (NIS2). De NIS2 wordt omgezet in nationale wetgeving, de Cyberbeveiligingswet (Cbw), en zal medio 2025 van kracht worden. Gemeenten worden aangemerkt als essentiële entiteiten en hebben te voldoen aan de Zorgplicht, Meldplicht en Toezicht. In 2024 zijn we gestart met de voorbereidingen en inrichting om te kunnen voldoen aan deze wetgeving, in 2025 zal dit geïntensiveerd worden.
Ontwikkelingen Sociaal Domein	In het sociaal domein wordt veel met gevoelige informatie gewerkt. Vanwege de ontwikkelingen, waaronder de uitvoering van het transformatieplan, is vanuit informatiebeveiliging en privacy actief betrokkenheid gezocht en gecreëerd. De informatiekundige vraagstukken met inbegrip van informatiebeveiliging en privacy zullen zich in 2025 niet onverminderd voordoen. Daarom wordt er in 2025 vervolg gegeven aan deze betrokkenheid en wordt gezorgd voor borging van aandacht voor deze thema's binnen de huidige en de toekomstige ontwikkelingen die zich zullen voordoen.