Gemeente Helmond

Aan de leden van de gemeenteraad

Raadsinformatiebrief 49

Helmond, 11 april 2023	Zaaknummer: 51379829	Telefoon.: 14 0492
Onderwerp: Informatiebeveiliging en privacy	Uw kenmerk:	Uw brief d.d.:

Geachte leden van de gemeenteraad,

Jaarlijks wordt verslag gedaan van de stand van zaken over informatiebeveiliging en privacy. De stand van zaken op het gebied van informatiebeveiliging volgt uit de bestuursrapportage digitale weerbaarheid. Het jaarverslag van de Functionaris voor de Gegevensbescherming (FG) geeft inzicht in de stand van zaken op het gebied van privacy.

In deze raadsinformatiebrief delen we de bevindingen van deze rapportages en geven we aan welke stappen we in 2023 zetten om te versnellen. U vindt een samenvatting van deze bevindingen in de bijlage. Het college en management beschikken over uitgebreidere informatie en acteren hier op. In grote lijnen blijkt dat we weerbaarder worden: we zijn gegroeid van 1,7 naar 2,1 op het gebied van privacy en van 1,8 naar 2,1 voor informatiebeveiliging (op een schaal van 5). In 2022 is de basis gelegd om sneller te kunnen groeien naar het noodzakelijke volwassenheidsniveau 3. Op dat moment beschikt de organisatie over voldoende veerkracht om blijvend te verbeteren, kansen te benutten en om te gaan met risico's.

Digitale weerbaarheid en bescherming van de privacy.
De gemeente Helmond is innovatief en maakt gebruik van de mogelijkheden die digitalisering biedt. De gemeente wil hierbij een betrouwbare partner zijn voor haar inwoners, medewerkers en zakelijke partners en heeft hierbij een maatschappelijke en wettelijke verantwoordelijkheid. Digitalisering biedt hiervoor kansen, maar ook uitdagingen. Naast de uitdagingen die het gevolg zijn van een toegenomen cybercriminaliteit, verandert de digitalisering ook de verhoudingen in onze samenleving. Dit vraagt om actieve sturing door de politiek zodat iedereen kan meedoen en de voordelen ervaart van de digitalisering. De jaarlijkse verantwoording draagt hier aan bij, omdat zij sturing op veilig en verantwoord gebruik van data mogelijk maakt.

In 2022 getroffen maatregelen.
De gemeente neemt privacy en informatiebeveiliging serieus en wil hier zo snel mogelijk in doorgroeien. Er is in 2022 een centraal team van Security en privacy officers (SPO-team) benoemd. Daarmee heeft de organisatie haar slagkracht in potentie vergroot. De kans dat we slachtoffer worden van cybercriminaliteit neemt toe, daarom is een bewustwordingsprogramma aangekocht en uitgevoerd. De mens is immers onze eerste verdedigingslinie. Uit de eind 2022 uitgevoerde meting blijkt dat de medewerkers zich meer bewust zijn van de risico’s. We zijn er nog niet, zoals ook blijkt uit de resultaten van het onlangs gehouden rekenkameronderzoek.

Binnen Parallelweg 44 / tel. 14 0492 / fax: 0492-587400
Correspondentieadres: Postbus 950 / 5700 AZ / www.helmond.nl
e-mail: gemeente@helmond.nl / Bankrelatie: IBANnummer NL 85 BNGH 0285 00 37 39

Met het SPO team is er extra capaciteit en kennis in de organisatie gekomen om de proceseigenaar te ondersteunen bij privacy- en informatiebeveiligingsvraagstukken. Hiermee krijgen de verantwoordelijke managers meer ondersteuning bij:

- het in beeld hebben en houden welke gegevens binnen welke processen worden verwerkt en hoe ze zijn beschermd;
- het uitvoeren van risicoanalyses op informatiebeveiliging en privacy, zodat ze onderdeel kunnen uitmaken van besluitvorming;
- het terugbrengen van het aantal opgetreden incidenten en datalekken;
- het aanscherpen van toegangsrechten.

Ook worden er voortdurend technische maatregelen getroffen, die de organisatie in lijn brengen met de actuele cyberrisico's. U kunt daarbij denken aan:

- Het (continu) up to date houden van hard- en software.
  Dit zorgt ervoor dat de mogelijkheid dat een hacker van buitenaf onze hard- en software benadert, tot een minimum beperkt wordt. Net als in 2021 zijn in 2022 door een externe gecertificeerde auditor een aantal security scans uitgevoerd. Hierbij is onder andere getest of een hacker van buitenaf op ons netwerk kan komen. Uit het onderzoek zijn geen kritieke bevindingen waargenomen.
- Het gebruik van meerfactor authenticatie (MFA).
  Dit is een sterke methode om te waarborgen dat alleen bevoegde gebruikers toegang krijgen tot een applicatie. Naast een gebruikersnaam en wachtwoord wordt dan meestal gebruik gemaakt van een authenticator app, een code per SMS of een andere ‘factor’ waardoor we zeker weten dat het ook echt de gebruiker is die inlogt. In 2022 is MFA ingericht voor toegang tot het Helmond netwerk.
- Het inrichten van Identity en Acces Management.
  Dit moet ervoor zorgen dat medewerkers de juiste toegang hebben tot ons netwerk, applicaties en de benodigde functionaliteiten en dat deze rechten tijdig worden beëindigd. Er is onder andere een koppeling gelegd tussen onze personeelsapplicatie en de applicatie die de toegang tot het netwerk mogelijk maakt. Op die manier worden de rechten van in dienst komende of uit dienst gaande medewerkers direct verleend respectievelijk beëindigd.
- Robuuste back-ups.
  Om de bedrijfscontinuïteit te borgen worden dagelijks back-ups gemaakt. Zij worden bewaard op fysiek gescheiden apparaten op verschillende locaties. Periodiek wordt de integriteit van de data en de veiligheid van de apparaten getoetst.

Met al deze maatregelen is ook een basis gelegd voor een versnelde groei in 2023.

Bijlage:
1. Infographic digitale weerbaarheid en privacy

Hoogachtend,
burgemeester en wethouders van Helmond,

mevr. P.J.M.G. Blanksma-van den Heuvel
burgemeester

H.J. de Ruiter
secretaris

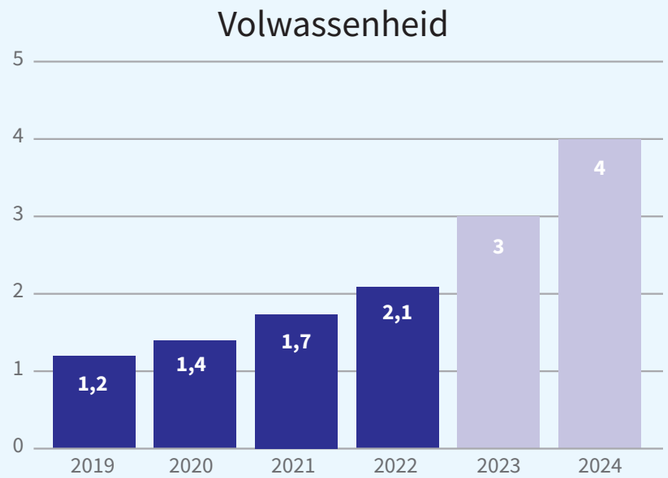
Verantwoording privacy en (digitale) weerbaarheid 2022

De gemeente Helmond heeft de beschikking over gevoelige gegevens, het is haar plicht om te zorgen dat deze informatie onder alle omstandigheden veilig en beschermd is. Gaat er toch iets mis, dan hoort dat snel te worden opgemerkt en direct hersteld. Deze rapportage bevat de stand van zaken op het gebied van informatieveiligheid en privacy. U krijgt daarbij inzicht in de (digitale) weerbaarheid van onze organisatie en in de wijze waarop de persoonsgegevens van onze inwoners, medewerkers en zakelijke partners (betrokkenen) zijn beschermd.

Managementsamenvatting

De gemeente Helmond groeit met kleine stappen. Ze neemt privacy en informatiebeveiliging serieus. Het is de ambitie van de gemeente Helmond om in de loop van 2023 volwassenheidsniveau 3 te bereiken en eind 2024 niveau 4. Daartoe is een centraal team met Security en Privacy officers (SPO team) aangesteld.

Met het SPO team is er extra capaciteit en kennis in de organisatie gekomen om de proceseigenaar te ondersteunen bij privacy en informatiebeveiligingsvraagstukken.



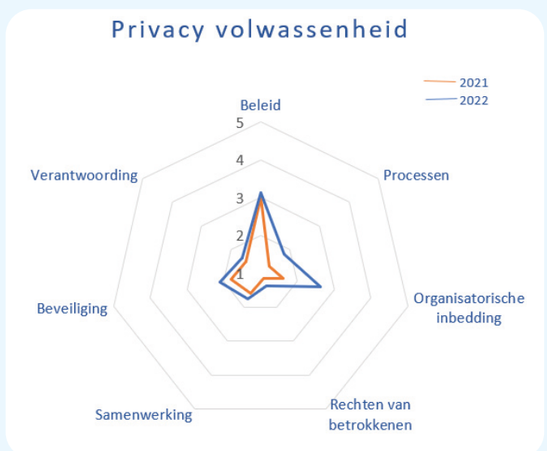
Daarnaast is in 2022 het aangekochte bewustwordings-programma live gegaan. Metingen tonen aan dat het bewustzijn bij medewerkers is toegenomen.

De veilige verwerking van (persoons)gegevens staat echter niet op zichzelf. Een steviger IT fundament is daarvoor noodzakelijk.

Jaarverslag Privacy

De gemeente Helmond wil een betrouwbare partner zijn en betrokkenen op een open en respectvolle wijze benaderen. Goede bescherming van persoonsgegevens is daarbij cruciaal. Er wordt op toegezien of dit gebeurt door de onafhankelijke interne toezichthouder, de functionaris voor de gegevensbescherming (FG). Met dit jaarverslag brengt de FG verslag uit van haar werkzaamheden, bevindingen en aanbevelingen. De FG heeft de volwassenheid van de organisatie beoordeeld op 7 thema's. Hiermee is inzicht in waar de organisatie staat en waar in de toekomst nog aan gewerkt moet worden.

Eén van de privacy-thema's is de beveiliging van de persoonsgegevens. Over de stand van zaken rondom de beveiliging van onze informatie en de digitale weerbaarheid, wordt jaarlijks ook verantwoording afgelegd. Deze verantwoording gaat dus niet enkel over persoonsgegevens. Bij het kopje beveiliging vindt u de bevindingen van deze verantwoording terug.



Gemeente Helmond

Verantwoording privacy en (digitale) weerbaarheid 2022

Beleid

Het privacybeleid beschrijft hoe de organisatie ervoor zorgt dat persoonsgegevens veilig en behoorlijk worden verwerkt. Op 10 november 2020 is het privacybeleid 2020-2024 vastgesteld. In 2023 wordt een Informatiebeveiliging en privacy beleid 2024-2028 opgesteld.

Processen

Om betrokkenen van dienst te kunnen zijn worden binnen de processen persoonsgegevens gebruikt. Om dit zorgvuldig te kunnen doen is inzicht nodig in de processen, in de persoonsgegevens, die in de processen worden gebruikt en afspraken hierover. De gemeente heeft een procesbeleid een procesverbeterteam, een project gegevensmanagement en werkt onder architectuur. Dit helpt bij het krijgen van een organisatiebreed overzicht. Verdere groei is nodig.

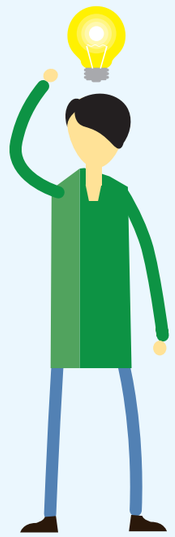
Risicomanagement

Door in een vroeg stadium na te denken over de risico's, die het gebruik van persoonsgegevens met zich meebrengen, kunnen de juiste maatregelen worden getroffen. Risicomanagement zorgt hier voor. Het risico bewustzijn van de organisatie neemt toe, dit blijkt uit het feit dat het aantal uitgevoerde risico analyses toeneemt.

Organisatorische inbedding

Om daadwerkelijk invulling te geven aan de bescherming van privacy, moeten de taken organisatorisch zijn ingebed. Dit wordt bereikt met een goede taakverdeling, voldoende middelen en een management dat het beleid voldoende actief uitdraagt.

Er is in 2022 een centraal team van Security en privacy offiers benoemd. Daarmee heeft de organisatie haar slagkracht in potentie vergroot. Daarnaast is een juiste houding ten opzichte van de thema's Informatiebeveiliging en privacy nodig. Het omarmen van de thema's als onderwerpen die de kwaliteit van de dienstverlening verbeteren en ze te zien als een integrale management taak zal bijdragen aan de groei in volwassenheid.



Bewustwording in 2022

E-learning

Nieuwe medewerkers volgen bij indiensttreding een E-learning en maken hierbij een kennistest.

Bewustwordingsworkshop

Er is een workshop in de vorm van een pubquiz "digitale veiligheid" ontwikkeld. Deze workshop is onderdeel geworden van het onboarding programma voor nieuwe medewerkers en kan ook op verzoek worden afgenomen.

Continue leren

Medewerkers ontvangen periodiek korte berichten (nano learnings) in hun inbox. Met dit bericht worden zij geïnformeerd over belangrijke onderwerpen. Zij worden daarmee gemotiveerd om veilig te handelen. De berichten stimuleren continue bewustwording rondom informatiebeveiliging en privacy.

Nieuwsberichten

Er is een site "Veilig werken" ingericht. Deze site bevat richtlijnen om digitaal veilig te werken. Daarnaast worden er regelmatig nieuwsberichten gepubliceerd op het Knaal.

Mystery guest

Met deze test is heeft een medewerker van het ingehuurde bedrijf geprobeerd of hij toegang kon krijgen tot onze gebouwen en informatie. Van de actie is een video gemaakt die wordt ingezet voor bewustwordingsactiviteiten.

Social Hack training:

Tijdens de Social Hack training, hebben de medewerkers van de klantcontactcentra geleerd hoe ze een social hack kunnen herkennen. De training is ook tijdens de "Helmond ben ik dag" aangeboden.

Landelijke cyberoefening

In oktober is tijdens de cyber security week deelgenomen aan de landelijke cyberoefening. Doel van deze cyberoefening was om beter voorbereid te zijn, mocht zich in Helmond een cyberaanval voordoen. Verder werd inzicht gegeven in de bestuurlijke gevolgen van een cybercrisis.

Phishing competitie

Door middel van een phishing campagne en cultuurvideo's werden medewerkers getraind om phishing mails te herkennen en adequaat te handelen.

Cyberbarometer:

In 2022 is gemeten hoe bewust onze organisatie is van de risico's. Deze meting toont aan dat het bewustzijn bij medewerkers is toegenomen.

Rechten van betrokkenen

Betrokkenen hebben het recht op informatie en inzage. Zo kunnen ze controleren of er op een juiste wijze wordt omgegaan met hun gegevens. Ze hebben het recht om aanpassing van de gegevens te vragen of een klacht in te dienen bij de FG. Ook hebben ze het recht op menselijke tussenkomst, bij geautomatiseerde besluiten. In 2022 heeft de FG 1 klacht behandeld. De inwoner meende dat de organisatie teveel informatie van hem had gevraagd. Zijn klacht was ongegrond.

De gemeente heeft (nog) geen bestuurlijke besluitvorming geautomatiseerd. Digitalisering neemt toe en daarmee ook de hoeveelheid data. Het is de ambitie van de gemeente Helmond om de data(stromen) te gebruiken om enerzijds te komen tot nieuwe inzichten en opgaven uit de stad en anderzijds slimme (geautomatiseerde) beslissingen te nemen. Meer inzicht in het gebruik van automatisch verwerkte persoonsgegevens of algoritmes en opstellen van principes rondom het gebruik zal de rechten van betrokkenen beter beschermen.

Samenwerking

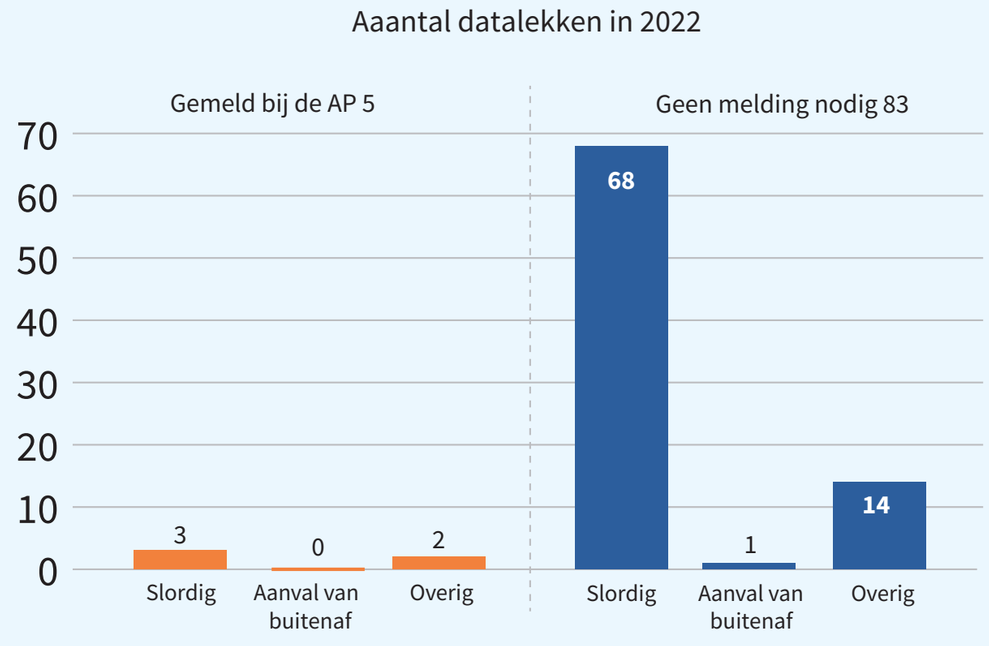
Met haar partners deelt de gemeente Helmond gegevens. Betrokkenen moeten er op kunnen vertrouwen dat dit zorgvuldig en veilig gebeurt. De gemeente maakt hierover met haar partners afspraken. Dit gebeurt op afdelingsniveau, een totaaloverzicht ontbreekt nog.

Beveiliging

Betrokkenen moeten er op kunnen vertrouwen dat hun persoonsgegevens passend zijn beveiligd, zodat hun gegevens niet kunnen worden misbruikt. Dit betekent ook dat zij kunnen rekenen op goede dienstverlening, omdat de juiste persoonsgegevens op het juiste moment voor de juiste mensen beschikbaar zijn. De gemeente legt via ENSIA verantwoording af. Uit deze verantwoording blijkt dat het volwassenheidsniveau van informatieveiligheid van de gemeente Helmond 2,1 is.

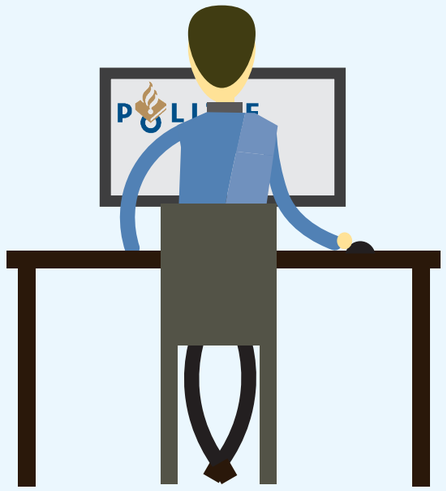
Datalekken

Wanneer er bij de beveiliging iets mis gaat, waardoor gegevens verloren gaan, veranderd worden of in verkeerde handen terechtkomen is er sprake van een datalek. Datalekken worden altijd geregistreerd. Zijn de betrokken persoonsgegevens gevoelig? Dan moet het lek gemeld worden bij de Autoriteit Persoonsgegevens (AP). We hebben in 2022 5 keer een melding gedaan. In de andere 83 gevallen was geen melding nodig. In de meeste gevallen was het datalek een gevolg van “slordig handelen”. Denk aan situaties waarbij brieven naar een verkeerd adres zijn gestuurd.



WPG

Naast persoonsgegevens verwerkt de gemeente ook politiegegevens. Dit gebeurt door de bijzondere opsporingsambtenaren en op deze gegevens is de Wet politiegegevens van toepassing. Er wordt jaarlijks een audit uitgevoerd op de verwerking van de politiegegevens. In 2022 is de audit over 2021 toegestuurd aan de Autoriteit Persoonsgegevens. Daarnaast is een verbeterplan opgesteld en uitgevoerd.



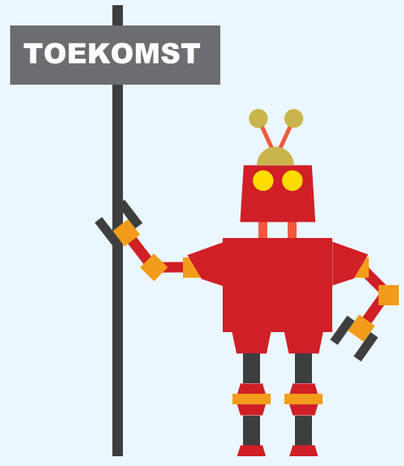
Aanbevelingen

- Zorg voor meer inzicht in de persoonsgegevens die worden verwerkt binnen processen. Zorg dat alle processen zijn beschreven en het register van verwerkingen volledig en actueel is en blijft.
- Pas risicomanagement toe Zorg dat besluiten worden gebaseerd op een risicoafweging. Betrek daarbij de privacy risico's van betrokkenen. Onderzoek voor alle bestaande processen de privacyrisico's en de maatregelen die nodig zijn om deze risico's te verkleinen. Begin bij de meest risicovolle processen.
- Zie informatiebeveiliging en privacy, net als financiën en personeel, als een integrale managementtaak en maak ook op de werkvloer capaciteit vrij voor deze thema's. Draag als management uit dat privacy en informatiebeveiliging de kwaliteit van de dienstverlening verbeteren. Omarm beide thema's in plaats ze te zien als een struikelblok.

Dit zorgt voor:

- Snellere groei op alle thema's.
- Beter inzicht in de persoonsgegevens die worden verwerkt en de daarmee samenhangende risico's.
- Betere informatie zodat inwoners nog beter kunnen worden bediend.
- Zekerheid voor inwoners en andere betrokkenen dat er zorgvuldig en veilig met hun gegevens wordt omgegaan.

Helmond wil een innovatieve stad zijn die gebruik maakt van de mogelijkheden die digitalisering biedt. Vanwege de impact die de digitalisering heeft op de publieke waarden beveelt de FG bovendien aan om data-ethiek in de organisatie te implementeren en uitvoering te geven aan de agenda digitale grondrechten en ethiek 2022-2026.



Rapportage (digitale) weerbaarheid.

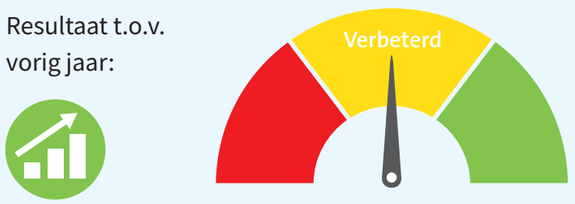
Met deze rapportage laat de gemeente zien waar zij staat op het gebied van informatieveiligheid.

Baseline informatiebeveiliging Overheid (BIO)

De overheid heeft een gemeenschappelijk normenkader vastgesteld, de Baseline Informatiebeveiliging (BIO). Dit normenkader bevat de richtlijnen waaraan gemeenten moeten voldoen om haar gegevens te beschermen. Met behulp van een zelfevaluatie verantwoordt de gemeente of zij voldoet aan de BIO. Dit doet zij op 5 thema's.

- **Beleid en organisatie**
- **Continuïteit en incidenten**
- **Databescherming**
- **Personeel en Toegang**
- **Informatiesystemen**

Resultaat t.o.v. vorig jaar:



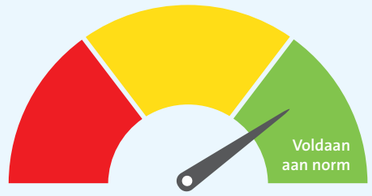
goed verbeterd verdient aandacht

We zien op al deze thema's groei ten opzichte van vorig jaar.

Basisregistraties en DigiD

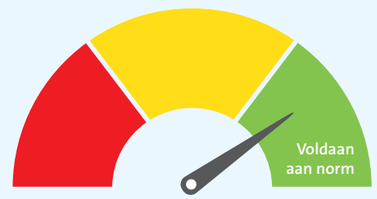
Daarnaast heeft de gemeente Helmond te maken met specifieke normenkaders van een aantal basisregistraties en DigiD. De basisregistraties maken delen uit van een landelijk stelsel. Het doel van dit stelsel van basisregistraties is om de dienstverlening te verbeteren en de hele overheid gebruik te laten maken van dezelfde basisgegevens. Daarnaast gebruikt de gemeente DigiD voor haar dienstverlening. DigiD is een middel om vast te stellen dat de gebruiker is wie hij zegt dat hij is.

De gemeente Helmond voldoet aan de landelijke normenkaders die gelden voor deze voorzieningen.



Uitzondering is de Basisregistratie Personen (BRP) en Reisdocumenten. Hier voldoet de gemeente aan de minimale norm. De inzet die in 2022 is gepleegd heeft geleid tot verbetering ten opzichte van 2021.

Resultaat t.o.v. vorig jaar:



voldaan aan de norm niet voldaan aan de norm