RAADSBESLUIT

ZAAKNUMMER	BEHANDELEND AMBTENAAR	SECTOR	PORT. HOUDER
2121304		GRI	

ONDERWERP

Rekenkameronderzoek Telewerken

DE RAAD VAN DE GEMEENTE HENGELO BESLUIT:

- kennis te nemen van het Rekenkameronderzoek 'Telewerken'
- de aanbevelingen uit het Rekenkameronderzoek 'Telewerken' ter opvolging mee te geven aan het college, ter vergroting van het i-bewustzijn van medewerkers.

PUBLIEKSVRIENDELIJKE SAMENVATTING

Binnen gemeenten is er een toename van telewerken. Zo maakt ook de gemeente Hengelo het voor haar medewerkers mogelijk niet langer op een vaste werkplek in een gemeentelijk pand te werken, maar ook daarbuiten. Een probleem is dat mogelijk ook privacygevoelige gegevens kunnen worden vrijgegeven. In tal van wetten en besluiten zijn eisen gesteld aan het opslaan en verwerken van persoonsgegevens. Daarnaast heeft de gemeente Hengelo zelf spelregels opgesteld met betrekking tot het omgaan met persoonsgegevens.

Het onderzoek van de rekenkamercommissie richt zich op het veiligheidsbewustzijn en veiligheidsgedrag van gemeenteambtenaren bij het gebruik van telewerken en doet hiertoe een aantal aanbevelingen.

DE GEMEENTERAAD VAN HENGELO, **DATUM**

De griffier

De voorzitter

RAADSADVIES

ZAAKNUMMER	BEHANDELEND AMBTENAAR	SECTOR	PORT. HOUDER
2121304	C.H. Hartendorp	GRI	--

ONDERWERP

Rekenkameronderzoek 'Telewerken'

AANLEIDING, DOEL EN WAT GING ER AAN VOORAF

Aanleiding

Binnen gemeenten is er een toename van telewerken. Zo maakt ook de gemeente Hengelo het voor haar medewerkers mogelijk niet langer op een vaste werkplek in een gemeentelijk pand te werken, maar ook daarbuiten. Door gebruik te maken van een token of door middel van een code op de smartphone kunnen medewerkers inloggen op het gemeentelijk netwerk en zo alle applicaties ontsluiten die ook beschikbaar zijn op de werkplek.
Een probleem is dat met deze applicaties ook privacygevoelige gegevens kunnen worden vrijgegeven. In tal van wetten en besluiten zijn eisen gesteld aan het opslaan en verwerken van persoonsgegevens. Daarnaast heeft de gemeente Hengelo zelf spelregels opgesteld met betrekking tot het omgaan met persoonsgegevens. Maar terwijl er op gemeentelijke panden allerlei beveiligingsmaatregelen aanwezig zijn, is er op afstand geen controle op de vraag of individuele medewerkers zich aan de voorschriften en spelregels houden. Hierdoor is het onvoldoende duidelijk of het werken op afstand door gemeenteambtenaren voldoende veilig gebeurt.
Het onderzoek van de rekenkamercommissie richt zich op het veiligheidsbewustzijn en veiligheidsgedrag van gemeenteambtenaren bij het gebruik van telewerken.

In opdracht van de Rekenkamercommissie heeft Nathalie de Vries, studente Public Administration aan de Universiteit Twente, dit onderzoek uitgevoerd. In het onderzoek staan de volgende onderzoeksvragen centraal:

1. Welke eisen stellen de Wet Bescherming Persoonsgegevens, de Wet Basisregistratie Personen en de interne regels van de gemeente Hengelo aan het werken met persoonsgegevens middels telewerken?
2. Welke risico's spelen een rol bij dit telewerken met de door de gemeente beheerde gegevens?
3. In welke mate maken gemeenteambtenaren gebruik van de mogelijkheid persoonsgegevens op afstand te raadplegen en/of te bewerken?
4. In welke mate gedragen gemeenteambtenaren zich risicovol bij het op afstand raadplegen of bewerken van persoonsgegevens?

Doel

Het doel van het voorliggende voorstel is uw raad te informeren over de uitkomsten van het rekenkameronderzoek en daarbij de conclusies en aanbevelingen met elkaar te bespreken. Uw raad wordt daarbij verzocht om kennis te nemen van het onderzoek en de conclusies/aanbevelingen en deze concrete aanbevelingen aan het college ter opvolging mee te geven.

INHOUD VAN HET VOORSTEL

Conclusies en aanbevelingen

De WBP en WBRP stellen verschillende eisen aan de omgang met persoonsgegevens. Een belangrijk onderdeel daarvan is dat de persoonsgegevens die door een gemeente worden verwerkt slechts mogen worden verwerkt door de verantwoordelijke bewerker en niet in handen van derden mogen komen. Om dit te kunnen waarborgen heeft de gemeente Hengelo interne spelregels opgesteld. Deze regels zijn echter niet altijd bekend bij de gemeenteambtenaren die op afstand met persoonsgegevens werken. Zo meent ongeveer één derde van deze ambtenaren dat er bij het verlenen van de bevoegdheid geen aanwijzingen zijn gegeven over de veiligheid van het gebruik. Daarnaast geven een aantal van deze ambtenaren aan niet bekend te zijn met de gedragscode ambtelijke integriteit.

Verder bestaat er bij een deel van de gemeenteambtenaren die op afstand persoonsgegevens kunnen raadplegen en/of wijzigen een potentieel gevaar dat vertrouwelijke gegevens in handen van derden kunnen komen. Zo werkt het merendeel van de ambtenaren op afstand met persoonsgegevens in de keuken en/of woonkamer. Daarnaast bewaart een aantal gemeenteambtenaren tokens en/of codes voor de smartphone op plekken die duidelijk toegankelijk en zichtbaar zijn voor derden. Iets meer dan een kwart van de ambtenaren die op afstand met persoonsgegevens werken verschaffen andere gezinsleden/derden ook toegang tot hun apparatuur.

De commissie komt op grond van het rapport tot twee aanbevelingen:
1. Zorg ervoor dat de spelregels die zijn opgesteld (interne richtlijnen, gedragscode) bekend zijn bij alle betrokkenen en worden nageleefd;
2. Maak de betrokken medewerkers meer bewust van de gevaren die kleven aan het op afstand werken met persoonsgegevens, en licht ze voor over gedrag dat die gevaren zo veel mogelijk beperkt.

Bestuurlijke reactie en nawoord commissie
Alvorens het bijgevoegde onderzoeksrapport aan uw raad aan te bieden heeft de rekenkamercommissie het college bij wijze van bestuurlijk wederhoor in de gelegenheid gesteld om eventueel commentaar op dit onderzoek kenbaar te maken. Op 11 november 2016 heeft de commissie deze bestuurlijke reactie ontvangen.
De commissie stelt met genoegen vast dat het college het belang van het onderwerp i-bewustzijn onderschrijft. De activiteiten die nu plaatsvinden in het kader van de Baseline Informatiebeveiliging Gemeenten, de meldplicht Datalekken en de toolbox i-bewustzijn sluiten goed aan bij de aanbevelingen van de commissie. Deze activiteiten richten zich –terecht- niet alleen op informatieveiligheid in de thuis-/telewerksituatie, maar hebben een bredere reikwijdte. De commissie acht een structurele aanpak (met nulmeting) en terugkerende agendering, zoals voorgesteld door het college, van groot belang.
Specifiek ten aanzien van het telewerken, wijst de commissie op het belang van voldoende helderheid over de vraag wie nu –feitelijk- welke (persoons)gegevens via telewerken kan raadplegen, en welke keuzes ten aanzien van autorisatie daaraan ten grondslag liggen. Ondanks de rapportage, de antwoorden op enkele feitelijke vragen aan het college (februari 2016), en de bestuurlijke reactie (november 2016) blijft er op dit punt onduidelijkheid bestaan bij de commissie.

BESPREEK- EN BESLISPUNTEN

De raad wordt voorgesteld:
- kennis te nemen van het Rekenkameronderzoek 'Telewerken'
- de aanbevelingen uit het Rekenkameronderzoek ‘Telewerken’ ter opvolging mee te geven aan het college, ter vergroting van het i-bewustzijn van medewerkers.

FINANCIËLE ASPECTEN

Niet van toepassing

BIJLAGE(N)

- Aanbiedingsbrief resultaat onderzoek ‘Telewerken,’ inclusief onderzoek en bestuurlijke reactie.

Rekenkamercommissie

Postbus 18
7550 AA Hengelo

Gemeenteraad van Hengelo
Postbus 18
7550 AA Hengelo

Onderwerp	**Kenmerk**	**Datum**
Aanbieding resultaat onderzoek naar "Telewerken"	2017-V008	30-03-2017

Geachte leden van de raad,

De Rekenkamercommissie Hengelo biedt u hierbij het resultaat aan van het onderzoek 'Telewerken' naar het op afstand werken met persoonsgegevens binnen de gemeente Hengelo. In opdracht van de Rekenkamercommissie heeft Nathalie de Vries, studente Public Administration aan de Universiteit Twente, dit onderzoek uitgevoerd. Het onderzoeksrapport treft u aan als bijlage bij deze brief. De Rekenkamercommissie heeft de resultaten en conclusies integraal overgenomen.

Aanleiding en doelstelling onderzoek
Binnen gemeenten is er een toename van telewerken. Zo maakt ook de gemeente Hengelo het voor haar medewerkers mogelijk niet langer op een vaste werkplek in een gemeentelijk pand te werken, maar ook daarbuiten. Door gebruik te maken van een token of door middel van een code op de smartphone kunnen medewerkers inloggen op het gemeentelijk netwerk en zo alle applicaties ontsluiten die ook beschikbaar zijn op de werkplek.
Een probleem is dat met deze applicaties ook privacygevoelige gegevens kunnen worden vrijgegeven. In tal van wetten en besluiten zijn eisen gesteld aan het opslaan en verwerken van persoonsgegevens. Daarnaast heeft de gemeente Hengelo zelf spelregels opgesteld met betrekking tot het omgaan met persoonsgegevens. Maar terwijl er op gemeentelijke panden allerlei beveiligingsmaatregelen aanwezig zijn, is er op afstand geen controle op de vraag of individuele medewerkers zich aan de voorschriften en spelregels houden. Hierdoor is het onvoldoende duidelijk of het werken op afstand door gemeenteambtenaren voldoende veilig gebeurt. Het onderzoek richt zich derhalve op het veiligheidsbewustzijn en veiligheidsgedrag van gemeenteambtenaren bij het gebruik van telewerken.

Onderzoeksvragen
De hoofdvraag in het onderzoek was:

'Op welke wijze gaan gemeenteambtenaren van de gemeente Hengelo die kunnen telewerken om met de beveiliging van door de gemeente beheerde gegevens?'

Om tot de beantwoording van de hoofdvraag te komen is deze opgedeeld worden in enkele deelvragen;

1. Welke eisen stellen de Wet Bescherming Persoonsgegevens, de Wet Basisregistratie Personen en de interne regels van de gemeente Hengelo aan het werken met persoonsgegevens middels telewerken?
2. Welke risico's spelen een rol bij dit telewerken met de door de gemeente beheerde gegevens?
3. In welke mate maken gemeenteambtenaren gebruik van de mogelijkheid persoonsgegevens op afstand te raadplegen en/of te bewerken?
4. In welke mate gedragen gemeenteambtenaren zich risicovol bij het op afstand raadplegen of bewerken van persoonsgegevens?

Behandeld door
C.H. Hartendorp
074-245 9519

Conclusies

De WBP en WBRP stellen verschillende eisen aan de omgang met persoonsgegevens. Een belangrijk onderdeel daarvan is dat de persoonsgegevens die door een gemeente worden verwerkt slechts mogen worden verwerkt door de verantwoordelijke bewerker en niet in handen van derden mogen komen. Om dit te kunnen waarborgen heeft de gemeente Hengelo interne spelregels opgesteld. Deze regels zijn echter niet altijd bekend bij de gemeenteambtenaren die op afstand met persoonsgegevens werken. Zo meent ongeveer één derde van deze ambtenaren dat er bij het verlenen van de bevoegdheid geen aanwijzingen zijn gegeven over de veiligheid van het gebruik. Daarnaast geven een aantal van deze ambtenaren aan niet bekend te zijn met de gedragscode ambtelijke integriteit.

Verder bestaat er bij een deel van de gemeenteambtenaren die op afstand persoonsgegevens kunnen raadplegen en/of wijzigen een potentieel gevaar dat vertrouwelijke gegevens in handen van derden kunnen komen. Zo werkt het merendeel van de ambtenaren op afstand met persoonsgegevens in de keuken en/of woonkamer. Daarnaast bewaart een aantal gemeenteambtenaren tokens en/of codes voor de smartphone op plekken die duidelijk toegankelijk en zichtbaar zijn voor derden. Iets meer dan een kwart van de ambtenaren die op afstand met persoonsgegevens werken verschaffen andere gezinsleden/derden ook toegang tot hun apparatuur.

Aanbevelingen

De rekenkamercommissie komt op grond van het rapport tot twee aanbevelingen:

1. Zorg ervoor dat de spelregels die zijn opgesteld (interne richtlijnen, gedragscode) bekend zijn bij alle betrokkenen en worden nageleefd;
2. Maak de betrokken medewerkers meer bewust van de gevaren die kleven aan het op afstand werken met persoonsgegevens, en licht ze voor over gedrag dat die gevaren zo veel mogelijk beperkt.

Bestuurlijke reactie & nawoord

Alvorens het bijgevoegde onderzoeksrapport aan uw raad aan te bieden hebben wij het college bij wijze van ons bestuurlijk wederhoor in de gelegenheid gesteld om zijn eventuele commentaar op dit onderzoek aan ons kenbaar te maken. Op 11 november 2106 ontvingen wij de eveneens bijgevoegde brief van het college.
Wij stellen met genoegen vast dat het college het belang van het onderwerp i-bewustzijn onderschrijft. De activiteiten die nu plaatsvinden in het kader van de Baseline Informatiebeveiliging Gemeenten, de meldplicht Datalekken en de toolbox i-bewustzijn sluiten goed aan bij de aanbevelingen van de rekenkamercommissie. Deze activiteiten richten zich –terecht- niet alleen op informatieveiligheid in de thuis-/telewerksituatie, maar hebben een bredere reikwijdte. De rekenkamercommissie acht een structurele aanpak (met nulmeting) en terugkerende agendering, zoals voorgesteld door het college, van groot belang.
Specifiek ten aanzien van het telewerken, wijst de rekenkamercommissie op het belang van voldoende helderheid over de vraag wie nu –feitelijk- welke (persoons)gegevens via telewerken kan raadplegen, en welke keuzes ten aanzien van autorisatie daaraan ten grondslag liggen. Ondanks de rapportage, de antwoorden op enkele feitelijke vragen aan het college (februari 2016), en de bestuurlijke reactie (november 2016) blijft er op dit punt onduidelijkheid bestaan bij de rekenkamercommissie.

Behandelvoorstel
De rekenkamer stelt de raad het volgende voor:
- Neem middels een raadsbesluit kennis van het opgestelde rapport 'Telewerken';
- Biedt middels dit besluit de gepresenteerde aanbevelingen aan het college aan ter opvolging;
- Organiseer in samenwerking met het college een bijeenkomst betreffende het onderwerp "i-bewustzijn" waarin de voorgestelde structurele aanpak, zoals voorgesteld door het college, een plek krijgt.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Namens de Rekenkamercommissie gemeente Hengelo,
de secretaris,

C.H. Hartendorp

Bijlagen:
- Onderzoeksrapport 'Telewerken'
- Bestuurlijke reactie van het college dd 11-11-2016

Onderzoeksrapport Rekenkamer

Een onderzoek naar het op afstand werken met persoonsgegevens binnen de gemeente Hengelo

Nathalie de Vries
Haaksbergen, 12 april 2016

Samenvatting

Bij veel gemeenten is telewerken een onlosmakelijk onderdeel van de organisatie geworden. Telewerken wordt in het onderzoek gedefinieerd als ‘werk dat buiten het kantoor wordt verricht met behulp van informatie- en communicatie technologie, onafhankelijk van tijd en plaats’. Bij het uitvoeren van werkzaamheden op andere plaatsen dan het kantoor is toegang nodig tot (privacygevoelige) informatie en informatiesystemen die onder de verantwoordelijkheid vallen van de gemeente. Deze informatie dient goed beschermd te worden. Dat geldt temeer als deze informatie over personen gaat.

Om de veiligheid in de gemeente Hengelo te kunnen waarborgen is het van belang om te onderzoeken hoe gemeenteambtenaren die op afstand kunnen werken met persoonsgegevens en voorzien zijn van een token of code omgaan met de beveiliging van persoonsgegevens. De rekenkamercommissie Hengelo richt zich daarbij vooral op het *gebruik van telewerken en op de omgang ermee door de ambtenaren zelf*.
Om dit te kunnen onderzoeken is de volgende onderzoeksvraag opgesteld:

‘Op welke wijze gaan gemeenteambtenaren van de gemeente Hengelo die kunnen telewerken om met de beveiliging van door de gemeente beheerde gegevens?’

Om deze onderzoeksvraag te beantwoorden is gebruik gemaakt van de volgende deelvragen:

1.Welke eisen stellen de Wet Bescherming Persoonsgegevens, de Wet Basisregistratie Personen en de interne regels van de gemeente Hengelo aan het werken met persoonsgegevens middels telewerken?

2.Welke risico’s spelen een rol bij dit telewerken met de door de gemeente beheerde gegevens?

3.In welke mate maken gemeenteambtenaren gebruik van de mogelijkheid persoonsgegevens op afstand te raadplegen en/of te bewerken?

4.In welke mate gedragen gemeenteambtenaren zich risicovol bij het op afstand raadplegen of bewerken van persoonsgegevens?

Uit de analyse van de eerste twee deelvragen komt naar voren dat de Wet Bescherming Persoonsgegevens (WBP) en de Wet Basisregistratie Personen (WBP) verschillende technische en organisatorische eisen stellen aan het werken met persoonsgegevens. Een belangrijk onderdeel hiervan is dat de persoonsgegevens die door een gemeente worden verwerkt slechts mogen worden verwerkt door de verantwoordelijke bewerker en niet in handen van derden mogen komen. Om dit te kunnen waarborgen heeft de gemeente Hengelo spelregels opgesteld die deels toegespitst lijken op gegevensverwerking binnen de door de gemeente beheerde gebouwen. Met telewerken is echter sprake van verwerking van gegevens buiten die gebouwen en ontstaan er diverse nieuwe risico’s. Om erachter te komen in welke mate de gemeente Hengelo persoonsgegevens verwerkt buiten de door de gemeente beheerde gebouwen en of dit risicovol is zijn deelvraag drie en vier gesteld.

Om deelvraag drie en vier zo breed mogelijk uit te kunnen zetten in de organisatie is ervoor gekozen om dit te doen aan de hand van een enquête. De onderzoekspopulatie bestaat daarbij

uit gemeenteambtenaren van de gemeente Hengelo die in het bezit zijn van een token en/of code voor de smartphone en op afstand kunnen werken met persoonsgegevens.

Uit de resultaten van deelvraag drie is gebleken dat de perceptie van ongeveer één derde van de onderzoekspopulatie is dat werkzaamheden op afstand wel verricht kunnen worden zonder hierbij de beschikking te hebben over persoonsgegevens.
Kenmerkend voor de gemeente Hengelo is het VDI-concept. Met VDI wordt de beveiliging in het rekencentrum geregeld. Hierdoor zouden medewerkers zonder bezwaar op elke locatie moeten kunnen werken. De resultaten van deelvraag vier laten echter zien dat er gevaren kleven aan de locatie waar ambtenaren van de gemeente Hengelo op afstand met persoonsgegevens werken. Daarnaast hanteert de gemeente Hengelo beleidsregels met betrekking tot het op afstand werken met persoonsgegevens. Uit de resultaten van het onderzoek komt naar voren dat een deel van de gebruikers onvoldoende op de hoogte lijkt van het beveiligingsbeleid van de gemeente en van de gedragscode ambtelijke integriteit en lijkt hier ook onvoldoende naar te handelen.

Geconcludeerd kan worden dat een deel van deze gemeenteambtenaren zich te weinig bewust is van de verantwoordelijkheden.

Inhoudsopgave

1. Inleiding

1.1 Probleemstelling

Technologische ontwikkelingen en een snel groeiende dienstensector hebben ertoe geleid dat het fenomeen telewerken in de jaren 90 doorbrak (Hoogendijk & van Schajik, 2011). Anno 2015 groeit het aantal telewerkers in Nederland nog steeds. Bij veel gemeenten is telewerken een onlosmakelijk onderdeel van de organisatie geworden. Maar wat is telewerken precies? Bij telewerken hebben we het over 'werk dat buiten het kantoor wordt verricht met behulp van informatie- en communicatie technologie, onafhankelijk van tijd en plaats. Daarnaast kan er behalve thuis ook op andere plaatsen worden gewerkt' (Horsten, 2011). Bij het uitvoeren van die werkzaamheden op andere plaatsen dan het kantoor 'is toegang nodig tot informatie en informatiesystemen die onder de verantwoordelijkheid vallen van de organisatie' (IBD, 2014). Bij het ontsluiten van deze informatie buiten de beheersbare omgeving dient deze informatie goed beschermd te worden. Dat geldt temeer als deze informatie over personen gaat en mogelijk privacygevoelig is.

Binnen gemeenten is er een toename van telewerken (IBD, 2014). Zo maakt ook de gemeente Hengelo het voor haar medewerkers mogelijk niet langer op een vaste werkplek in een gemeentelijk pand te werken, maar ook daarbuiten, waarbij de nadruk wordt gelegd op het thuiswerken, ook wel telewerken genoemd. Door gebruik te maken van een token of door middel van een code op de smartphone kunnen medewerkers inloggen op het gemeentelijk netwerk en zo alle applicaties ontsluiten die ook beschikbaar zijn op de werkplek. Deze applicaties kunnen vanaf elke locatie worden ontsloten (bijvoorbeeld thuis/in de trein of/op straat). Een probleem is dat met deze applicaties ook privacygevoelige gegevens kunnen worden vrijgegeven. In tal van wetten en besluiten zijn eisen gesteld aan het opslaan en verwerken van persoonsgegevens (Wet bescherming persoonsgegevens en de Wet basisregistratie personen). Daarnaast heeft de gemeente Hengelo zelf spelregels opgesteld met betrekking tot het omgaan met persoonsgegevens. Denk daarbij aan de verklaring omtrent gedrag en de verplicht te ondertekenen geheimhoudingsverklaring. Maar terwijl er op gemeentelijke panden allerlei beveiligingsmaatregelen aanwezig zijn, is er op afstand geen controle op de vraag of individuele medewerkers zich aan de voorschriften en spelregels houden. Hierdoor is het onvoldoende duidelijk of het werken op afstand door gemeenteambtenaren voldoende veilig gebeurt. De rekenkamercommissie van de gemeente Hengelo heeft daarom besloten tot een onderzoek naar het veiligheidsbewustzijn en veiligheidsgedrag van gemeenteambtenaren bij het gebruik van telewerken.

1.2 Doelstelling

Dit onderzoek vormt grotendeels een replicatie van het onderzoek 'Op afstand werken met persoonsgegevens binnen de gemeente Enschede' (de Vries, 2015). Het onderzoek geeft inzicht in de wijze waarop gemeenteambtenaren die op afstand kunnen werken met persoonsgegevens omgaan met de beveiliging van persoonsgegevens als zij telewerken.
Om de veiligheid in de gemeente Hengelo te kunnen waarborgen is het van belang om te onderzoeken hoe deze gemeenteambtenaren op afstand omgaan met de beveiliging van persoonsgegevens. De rekenkamercommissie Hengelo richt zich daarbij vooral op het *gebruik van telewerken en op de omgang ermee door de ambtenaren zelf*.

1.3 Onderzoeksvraag en deelvragen

De hoofdvraag in het onderzoek is:
'*Op welke wijze gaan gemeenteambtenaren van de gemeente Hengelo die kunnen telewerken om met de beveiliging van door de gemeente beheerde gegevens?'*

Om tot de beantwoording van de hoofdvraag te komen zal deze opgedeeld worden in enkele deelvragen:

1.Welke eisen stellen de Wet Bescherming Persoonsgegevens, de Wet Basisregistratie Personen en de interne regels van de gemeente Hengelo aan het werken met persoonsgegevens middels telewerken?

2.Welke risico's spelen een rol bij dit telewerken met de door de gemeente beheerde gegevens?

3.In welke mate maken gemeenteambtenaren gebruik van de mogelijkheid persoonsgegevens op afstand te raadplegen en/of te bewerken?

4.In welke mate gedragen gemeenteambtenaren zich risicovol bij het op afstand raadplegen of bewerken van persoonsgegevens?

Deze deelvragen zullen per hoofdstuk worden uitgewerkt. In het volgende hoofdstuk wordt het normatieve kader beschreven; welke eisen stelt de wet en de gemeente Hengelo aan het (ver)werken met persoonsgegevens? Op deze manier komt eerst naar voren welke organisatorische en technische maatregelen genomen moeten worden om gegevens te beveiligen. In het kader van deelvraag drie worden in het tweede deel van het normatieve kader de risico's van het op afstand werken met persoonsgegevens besproken. In hoofdstuk vier komt de methode van onderzoek aan bod. Dit vormt de onderzoekspopulatie, selectie, manier van onderzoek (enquête), operationalisering en respons. Het vijfde hoofdstuk presenteert de resultaten van de enquête onder de gemeenteambtenaren in Hengelo (die in het bezit zijn van een token of code op de smartphone en op afstand kunnen werken met persoonsgegevens).
In het allerlaatste hoofdstuk zullen de resultaten van de enquête leiden tot een conclusie voor de gemeente Hengelo.

2. Omgang met persoonsgegevens: normatief kader

Welke eisen stellen de Wet Bescherming Persoonsgegevens (WBP), de Wet Basisregistratie personen (BRP) en de interne regels van de gemeente Hengelo aan het werken met persoonsgegevens (middels telewerken)?

2.1 Inleiding

Paragraaf 2.2 van dit hoofdstuk bespreekt kort de totstandkoming van de Wet Bescherming Persoonsgegevens (WBP). In paragraaf 2.3 zal het karakter van de WBP aan bod komen. Paragraaf 2.4 gaat in op de definiëring van de belangrijkste begrippen uit de WBP. Vervolgens benoemt paragraaf 2.5 de eisen die de WBP stelt aan het werken met persoonsgegevens. Paragraaf 2.6 zal ingegaan op de Wet Basisregistratie Personen (Wet BRP). Paragraaf 2.7 bespreekt de administratie van de BRP. Paragraaf 2.8 benoemt de gebruikers van de BRP gegevens. Paragraaf 2.9 gaat in op de kenmerken van de BRP. In paragraaf 2.10 komen de eisen van de Wet BRP naar voren. Als laatste worden de interne spelregels van de gemeente Hengelo in paragraaf 2.11 besproken.

2.2 Wet Bescherming Persoonsgegevens (WBP)

De veiligheid van informatie is in de loop der jaren hoog in het vaandel komen te staan, hierdoor moest de wetgeving op een aantal punten worden aangepast (BMC, 2011). Zo is het recht op privacy binnen de rechtsstaat momenteel een fundamenteel recht. Dit belang wordt benadrukt in de Europese Privacyrichtlijn en in artikel 10 van de Grondwet. Om waarborgen te kunnen bieden voor een evenwicht tussen deze privacybescherming en andere grondrechten, is op 1 september 2001 de Wet Bescherming Persoonsgegevens (WBP) in werking getreden (Van der Sloot, 2010).

2.3 Karakterisering WBP

De Jong, Visser & Sibma (2008) beschrijven in hun evaluatierapport dat de WBP het doel heeft persoonsgegevens te beschermen die geregistreerd worden. De WBP heeft een eigen karakter en bestaat uit verschillende onderdelen. Subjectieve rechten worden verleend aan degenen van wie persoonsgegevens worden verwerkt. Daarnaast is de WBP een organieke wet gericht op de vormgeving van een grondrecht. In de memorie van toelichting komt naar voren dat na een zorgvuldige afweging van belangen van de verantwoordelijke en belanghebbende persoonsgegevens kunnen worden verwerkt. Door betrokkenen het recht toe te kennen en aan verantwoordelijken plichten op te leggen, wordt de positie van personen van wie gegevens worden verwerkt versterkt' (De Jong, Visser & Sibma, 2008). Deze rechten en plichten komen naar voren in paragraaf 2.5.

2.4 Belangrijke begrippen uit de WBP

De wet definieert in artikel 1 van hoofdstuk 1 een aantal belangrijke begrippen (Overheid, 2015).
Persoonsgegevens in de zin van de WBP zijn alle gegevens 'betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'. Een persoon is identificeerbaar 'indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden'.
Een ***verwerking*** van persoonsgegevens in de zin van de WBP is 'elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens'. Verwerkingen zijn 'in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van

terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens'.
De ***verantwoordelijke*** in de zin van de WBP is degene die 'het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'. De verantwoordelijke bepaalt welke persoonsgegevens, voor welk doel, op welke manier en met welke middelen worden verwerkt. De ***betrokkene*** is degene 'op wie een persoonsgegeven betrekking heeft' of 'waarover de gegevens informatie bevatten'. Bij de verwerking van persoonsgegevens kan de verantwoordelijke een bewerker inschakelen. 'De ***bewerker*** is een buiten de organisatie van de verantwoordelijke staande persoon of instelling'. Hij 'bewerkt gegevens ten behoeve van de verantwoordelijke, dat wil zeggen in overeenstemming met diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid'. De bewerker 'beperkt zich tot het verwerken van persoonsgegevens zonder zeggenschap te hebben over het doel van en de middelen voor de verwerking van persoonsgegevens. Hij neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegeven.

2.5 Eisen WBP rechtmatige verwerking persoonsgegevens

Persoonsgegevens worden door vele instanties, zoals gemeenten, vastgelegd. BMC (2011) beschrijft dat het vastleggen in principe geen probleem is, echter moet er wel zorgvuldig worden omgegaan met deze gegevens (BMC, 2011). Als gemeenten persoonsgegevens verwerken moeten zij aan een aantal eisen van de WBP voldoen. In het tweede hoofdstuk van de WBP zijn de voorwaarden aangegeven waaronder de verwerking van persoonsgegevens rechtmatig is (Overheid, 2014). ***Artikel 6*** geeft aan dat de eerste voorwaarde inhoudt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze moeten worden verwerkt. Vervolgens moet worden gekeken naar het vooraf vastgestelde doel. ***Artikel 7*** bepaalt dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Dit houdt in dat voor de gegevens worden verzameld een duidelijke omschrijving moet worden gegeven van het doel. ***Artikel 8*** geeft een opsomming van de rechtvaardiging van verwerking van persoonsgegevens. Daaropvolgend vormt ***artikel 9*** dat gegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Getoetst moet worden of het gebruik voor andere doeleinden verenigbaar is met het doel waarvoor de gegevens zijn verkregen. ***Artikel 10*** geeft weer dat persoonsgegevens niet langer bewaard worden in een vorm die het mogelijk maakt de betrokkene te identificeren dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt. De inhoudelijke kwaliteit van de gegevens komt in ***artikel 11*** naar voren: gegevens moeten toereikend, ter zake dienend, niet bovenmatig, juist en nauwkeurig zijn. In de ***artikelen 12, 13 en 14*** zijn technische en organisatorische bepalingen opgenomen met betrekking tot de beveiliging van gegevens. BMC (2011) geeft aan dat deze bepalingen nodig zijn om verlies of onrechtmatige verwerking tegen te gaan. 'Mocht de verwerking van gegevens zijn uitbesteed, dan dient de derde partij in deze maatregelen te voorzien. Alle instanties die gegevens verwerken dienen dit aan te melden bij het CPB, tenzij een onafhankelijke functionaris hier toezicht op houdt' (BMC, 2011).

2.6 Basisregistratie Personen (BRP)

Een basisregistratie is een door de overheid officieel aangewezen registratie. De gegevens in deze registratie worden geacht van hoge kwaliteit, actueel en betrouwbaar te zijn. Bij alle overheidsinstellingen worden deze verplicht, en zonder nader onderzoek gebruikt bij de uitvoering van publiekrechtelijke taken. De Basisregistratie personen (BRP) is één van de 12 basisregistraties. (Alle basisregistraties samen vormen het Stelsel van basisregistraties). 'De

BRP bevat persoonsgegevens over alle ingezetenen van Nederland en over personen die niet in Nederland wonen (of hier slechts kort verblijven) maar die een relatie hebben met de Nederlandse overheid, de 'niet-ingezetenen' (BMC, 2011, p.9). De Basisregistratie Personen (BRP) is een samenvoeging van de Gemeentelijke Basisadministratie Personen (GBA) en Register Niet Ingezetenen (RNI). De invoering van de BRP vindt plaats in de periode juni 2013 – juni 2016' (Overheid, 2015)[1].

2.7 Inhoud administratie BRP

In de BRP bevinden zich een aantal persoonsgegevens, deze bestaan onder meer uit: (artikel 2.7)

- Naam, voornamen, geboortedatum, geboorteplaats en geboorteland;
- Gegevens over de ouders;
- Gegevens over huwelijk en geregistreerd partnerschap;
- Gegeven over kinderen;
- Gegevens over nationaliteit en eventueel over het verblijfsrecht;
- Verblijfplaats (adres);
- Het burgerservicenummer (BSN)

2.8 Gebruikers BRP gegevens

Gebruikers van de gegevens zijn de gemeente en de desbetreffende burgers zelf. Verder worden de gegevens in de BRP ook gebruik door (semi)- overheidsorganisaties die voor de uitoefening van hun publiekrechtelijke taken persoonsgegevens nodig hebben. Hieronder vallen onder meer de politie, belastingdienst, het waterschap, notarissen en pensioenfondsen. Afhankelijk van de afspraken die er over de aanlevering van gegevens zijn gemaakt en van hun behoeften, krijgen deze organisaties een selectie uit de BRP. Een voorbeeld hiervan is het bevolkingsonderzoek naar borstkanker: hiervoor verkrijgen screeningsorganisaties een beperkte set gegevens van alle in de BRP geregistreerde vrouwen onder de 50 jaar (BMC, 2011, p.10).

2.9 Eisen BRP

De kenmerken van een basisregistratie zijn aangeduid in 12 eisen waaraan de basisregistratie moet voldoen. In een brief aan de Tweede Kamer van 3 maart 2009 zijn 12 eisen geformuleerd waaraan wetgeving van basisregistraties moet voldoen, de zogenaamde 12 eisen aan basisregistraties. De eerste eis geeft aan dat de ***registratie bij wet geregeld*** moet zijn. Eis twee bepaalt dat ***afnemers een terug meldplicht hebben***. Dit houdt in dat wanneer afnemers twijfelen aan de juistheid van de gegevens in de basisregistratie zij de plicht hebben dit te melden aan de houder. De houder heeft vervolgens ook de plicht deze melding serieus te onderzoeken en zo waar nodig correcties door te voeren. Eis drie geeft aan dat ***de basisregistratie verplicht wordt gebruikt door de hele overheid***, en de als authentiek aangewezen gegevens kunnen in de werkprocessen zonder nader onderzoek gebruikt worden. Op deze manier bereik je het effect dat 1) bedrijven en burgers slechts eenmaal gegevens hoeven aan te leveren, (2) de kwaliteit van de registratie goed is en (3) de uitwisseling van gegevens tussen overheden gestroomlijnd wordt, is het gebruik van basisregistraties (indien

beschikbaar) verplicht voor alle private en publieke instanties die uitvoering geven aan publieke taken. Daaropvolgend vormt eis vier dat er ***duidelijkheid*** bestaat ***over de aansprakelijkheid***. Eis vijf heeft betrekking op de transparante financiën, en geeft weer dat ***de realisatie en exploitatie geschieden tegen redelijke kosten en er eenduidigheid is over de verdeling ervan***. De duidelijkheid omtrent ***inhoud en het bereik van de registratie*** komen in eis zes naar voren. In eis zeven, acht, negen en tien zijn bepalingen opgenomen omtrent de duidelijkheid van verantwoordelijkheden en procedures. Zo laat eis zeven zien dat er ***alleen sluitende afspraken en procedures tussen de houder van het register enerzijds en de leveranciers en de afnemers van gegevens anderzijds***. Eis acht geeft aan dat er ***duidelijke procedures*** dienen te zijn ***met betrekking tot de toegankelijkheid van de basisregistratie***. Eis negen stuit op het belang van een ***strikt regime van kwaliteitsborging***. In eis tien komt naar voren dat er is ***vastgelegd dat en hoe afnemers van gegevens op een niet-vrijblijvende wijze betrokken worden bij de besluitvorming over de registratie***. Daaropvolgend geven eis elf en twaalf aan dat ***de positie van de basisregistratie binnen het stelsel van basisregistraties duidelijk*** is en de relaties met de basisregistraties zijn ***beschreven***. De zeggenschap over de basisregistratie berust bij een bestuursorgaan en er is een minister verantwoordelijk voor het realiseren, respectievelijk het functioneren van de registratie.

2.10 Wet BRP

Met de Wet basisregistratie personen (Wet BRP), die sinds januari 2014 van kracht is, is de plicht voor gemeenten ontstaan om jaarlijks een onderzoek uit te voeren. Het onderzoek vindt plaats door middel van een zelfevaluatie (Overheid, 2015). De zelfevaluatie vervangt de driejaarlijkse GBA-audit[2], waar aan de hand van een vragenlijst getoetst werd of gemeenten voldeden aan allerlei materiële vereisten. Deze eisen bestonden onder meer uit:

- Toegangscontrole tot het gebouw;
- Geen onbevoegden mogen ruimte betreden;
- Inbraakbeveiliging door middel van alarminstallatie;
- Beveiliging tegen kennisneming door onbevoegden;
- Richtlijnen met betrekking tot zorgvuldig omgaan met wachtwoorden, afdrukken van gegevens en inzage als gevolg van meekijken.

In het onderzoek zelfevaluatie BRP die dit jaar bij gemeenten voor eerst plaatsvindt, zal er gekeken worden naar BRP-processen. Dit zijn:

- De beveiliging van de basisregistratie;
- De inrichting van de basisregistratie;
- De werking van de basisregistratie;
- De verwerking van gegevens in de basisadministratie (BRP- gegevens) voor zover het om de gemeentelijke voorziening gaat of voor zover het college verantwoordelijk is voor de bijhouding.

Voor het onderzoek maakt de gemeente gebruik van het door het Agentschap BPR beschikbaar gesteld evaluatie-instrument. Voor het onderzoek en de rapportage in 2014 bestaat het evaluatie-instrument uit:

[2] Gemeentelijke Basisadministratie Personen

- De webapplicatie kwaliteitsmonitor;
- De digitale vragenlijst BRP;
- De bestandscontrolemodule.

De minister voert in aanvulling op de door de gemeente uitgevoerde controles een nader onderzoek (steekproef) bij 35 gemeenten uit om de bevindingen te controleren (Overheid, 2015).

2.11 Interne regels gemeente Hengelo

Zeeuwen (2011) beschrijft dat gemeenten als eigenaar en hoeder van gegevensadministraties zorg dienen te dragen voor de beveiliging van vastgelegde gegevens en de bescherming tegen onrechtmatig gebruik daarvan. Voor het werken met persoonsgegevens zijn vanuit de overheid in verschillende wet en regelgeving (WBP en Wet BRP) een aantal regels opgesteld met betrekking tot het werken met persoonsgegevens. Vanuit deze wet en regelgeving zijn gedragsregels afgeleid. Deze gelden voor medewerkers van gemeenten in relatie tot al hun werkzaamheden, dus ook bij het gebruik van Suwinet. Suwinet betreft een computersysteem waarin vrijwel alle denkbare persoonsgegevens (o.a. loon, hypotheek, bankrekeningnummer) van burgers zijn opgeslagen.

Voor de gemeente Hengelo geldt de 'gedragscode ambtelijke integriteit gemeente Hengelo 2004'. Hierin staat een aantal gedragsregels die samen deze gedragscode vormen. De code brengt naar voren wat de organisatie van integer handelen vindt. Het gaat bij deze code niet om strak omlijnde regels, maar een aantal basisbeginselen die als uitgangspunt kunnen gelden voor houding en gedrag. Elke nieuwe medewerker die een aanstelling krijgt bij de gemeente Hengelo tekent ervoor kennis te hebben genomen van deze gedragscode. Voor medewerkers die in het kader van hun functie gebruik dienen te maken van Suwinet volgt er een aanvullend document, de 'zorgvuldigheidsverklaring Suwi-inkijk'. De medewerker tekent in dit document dat hij /zij op de hoogte is van de regels met betrekking tot Suwinet. Tevens worden er in het beveiligingsplan van de gemeente Hengelo (2014) tien gouden regels besproken die betrekking hebben op het gebruik.

Deze eerste gouden regel heeft betrekking op het feit dat wachtwoorden strikt persoonlijk zijn en uitsluitend door de betreffende medewerker gebruikt dienen te worden om toegang tot de betreffende systemen te krijgen. 'Geef je wachtwoord dus niet aan derden of een collega en ***bewaar ze op een veilige plek, dus niet in de agenda of op een geel briefje'.*** De tweede gouden regel betreft het ***melden van beveiligingsincidenten bij de servicedesk*****.** **'**De servicedesk is belast met de algemene registratie van beveiligingsincidenten, incidenten dienen daarom zo snel mogelijk bij hen gemeld te worden'**.** Voorbeelden van incidenten zijn: een virusmelding op het systeem waarmee je op dat moment werkt, een deur of lade dat op slot had moeten zijn maar niet op slot is, een inbraak of een poging tot inbraak. De derde gouden regel maakt duidelijk dat er sprake is van een ***geheimhoudingsplicht.*** Persoonsgegevens mogen niet verder bekend gemaakt worden dan voor de uitoefening van de functie noodzakelijk is. Het gaat hier om persoonsgegevens die uit hoofde van de functie bekend worden, alsmede overige informatie waarvan de medewerker weet of redelijkerwijze kan vermoeden dat geheimhouding verplicht is. Gouden regel vier bespreekt ***de gedragscode***

Internet en e-mailgebruik. In deze gedragscode zijn regels neergelegd die aangeven hoe medewerkers dienen om te gaan met e-mail en internet op de werkplek. Regel vijf doelt op de ***kennisname van het informatiebeveiligingsbeleid en het beveiligingsplan Suwi***. Regel zes heeft te maken met ***gegevensverstrekking aan derden via de telefoon*.** Het uitgangspunt hierbij is dat er niet aan verzoeken om telefonische informatie over betrokkenen tegemoet gekomen wordt. Dat betekent dat wanneer personen of instanties beweren namens een betrokkene te bellen, er geen telefonische informatie over deze klant verstrekt mag worden. Regel zeven bespreekt de ***clear desk/clear screen policy***. Dit betekent dat de vertrouwelijke omgang met persoonsgegevens o.a. inhoudt dat elke werkplek zodanig is ingericht, dat onbevoegden in geval van afwezigheid van de medewerker niet aan deze gegevens kunnen komen. Gouden regel acht gaat nader in op de correcte omgang met vertrouwelijke gegevens. Deze regel geeft aan dat ***vertrouwelijke gegevens niet in de prullenbak thuishoren*.** De inhoud van alle papierprullenbakken wordt door een speciaal bedrijf vernietigd. Waardoor afval dus op de juiste manier afgescheiden dient te worden: papier in de papierbakken en de rest in vuilnisemmers. Regel negen heeft te maken met het ***aanspreken van onbekende personen***. Wanneer de medewerker iemand binnen het gebouw tegenkomt waar officieel geen publiek zonder begeleiding mag komen en de medewerker niet weet wie deze persoon is en wat hij/zij daar te doen heeft. 'Spreek je deze persoon aan, stel je jezelf voor en vraag je wat hij/zij hier komt doen. Personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor aangesproken op hun overtreding'. Wijs hun vervolgens beleefd, maar duidelijk de weg naar het publieke gedeelte van het gebouw en begeleid ze daar naartoe. De laatste gouden regel geeft aan dat informatiebeveiliging niet gratis is, 'het kost energie en werkt vaak tegen je als je haast hebt en de werkdruk hoog is. ***Echter is informatiebeveiliging uitermate belangrijk voor je werk en hoort bij de professionele en bekwame uitvoering van het werk. Neem het daarom zeer serieus'*** (Beveiligingsplan Suwinet, 2014).

2.12 Samenvattend

De WBP en de WBRP vermelden dat de gemeente als eigenaar en hoeder van gegevensregistraties verplicht is daar zorgvuldig mee om te gaan. Daarnaast stellen de WBP en de WBRP verschillende eisen aan de omgang met persoonsgegevens. Een belangrijk onderdeel daarvan is dat persoonsgegevens die door een gemeente worden verwerkt slechts mogen worden verwerkt door de verantwoordelijke bewerker en niet in handen van derden mogen komen. De gemeente Hengelo geeft daar invulling aan door middel van de gemeentelijke gedragscode ambtelijke integriteit en een beveiligingsplan. Deze interne spelregels lijken deels toegespitst op gegevensverwerking door ambtenaren binnen de door de gemeente beheerde gebouwen. Bij telewerken is er echter sprake van verwerking buiten die gebouwen, waardoor er diverse nieuwe risico's ontstaan. Deze risico's zullen in het volgende hoofdstuk worden besproken.

3. Mogelijke risico's bij telewerken

3.1 Inleiding

Persoonsgegevens dienen in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze te worden verwerkt. Wanneer deze verwerking van persoonsgegevens op afstand plaatsvindt bestaan er verschillende risico's. Deze risico's zijn volgens de informatiebeveiligingsdienst voor gemeenten (IBD) in te delen naar de schakels van de telewerkketen. Deze bestaan uit de volgende vijf schakels:

- De telewerklocatie;
- De telewerkvoorziening (apparatuur);
- De verbinding tussen het apparaat en de ICT- infrastructuur van de gemeente;
- De toegang en informatie die aan de telewerker beschikbaar wordt gesteld;
- De telewerker zelf'.

Dit hoofdstuk beschrijft nader deze vijf schakels. Paragraaf 3.2 bespreekt de risico's rondom de telewerklocatie. De gevaren rondom de telewerkvoorziening en de verbinding van het apparaat met de ICT van de gemeente komen in Paragraaf 3.3 en 3.4 naar voren. Paragraaf 3.5 gaat in op de beschikbare toegang van de telewerker en de risico's die hierbij komen kijken. En als laatste bespreekt paragraaf 3.6 de laatste schakel, de telewerker zelf.

3.2 De telewerklocatie

De IBD (2014) laat in het document telewerkbeleid zien dat de grootste bedreiging van telewerken is dat (vertrouwelijke) informatie wordt onderschept. Wanneer een medewerker op een openbare locatie telewerkt, bestaat er een kans dat een buitenstaander gevoelige informatie vanaf het beeldscherm leest of een telefoongesprek afluistert. Daarnaast kan de apparatuur van de telewerker zoekraken. Door verlies of diefstal is er een mogelijkheid dat de daarop opgeslagen informatie in handen kan komen van een buitenstaander.
'Gebruikt een telewerker een computer van een ander dan bestaat de mogelijkheid dat de volgende gebruiker van deze computer, de in de cache opgeslagen informatie van de vorige sessie kan inzien' (IBD, 2014).

3.3 De telewerkvoorziening (apparaat)

Govcert (2009) omschrijft dat indien een telewerker over apparatuur van de gemeente beschikt, de gemeente zelf kan bepalen welke beveiligingsmaatregelen zij hierop aanbrengt. Daarmee kan de gemeente de risico's voor de apparatuur grotendeels afdekken. Voor de privéapparatuur is dat anders. Deze apparatuur is namelijk niet in het beheer bij de gemeente en daardoor kunnen de risico's aanmerkelijk groter zijn dan bij een door de gemeente beheerd systeem. Kwaadwillende buitenstaanders kunnen via malware (zoals virussen) informatie op de thuis apparatuur inzien of op het netwerk van de gemeente inloggen als de telewerker geen up-to-date anti malware software gebruikt. Ook bestaat er een mogelijkheid dat andere gezinsleden de op de thuis apparatuur opgeslagen informatie kunnen inzien (Govcert, 2009).

3.4 De verbinding tussen het apparaat en de ICT- infrastructuur van de gemeente

De IBD (2014) beschrijft dat de netwerkverbinding tussen het apparaat en de ICT-infrastructuur van de gemeente op verschillende manieren tot stand kan worden gebracht.

Deze verbinding kan bijvoorbeeld worden afgeluisterd door kwaadwillende, waardoor zij inzage kunnen krijgen in informatie die tussen de gemeente en telewerker wordt uitgewisseld. Het wachtwoord en de gebruikersnaam kunnen op deze manier bemachtigd worden, waardoor een kwaadwillende zich mogelijk toegang kan verschaffen tot de informatie waarvoor de gemeente verantwoordelijk is (IBD, 2014).

3.5 Toegang tot informatie

Govcert (2009) geeft aan dat een gemeente via een webserver e-mail beschikbaar kan stellen aan de telewerker. 'De telewerker kan dan via de browser zijn e-mail behandelen. In sommige gevallen worden er zelfs interne applicaties met bedrijfsinformatie via het internet beschikbaar gesteld aan de telewerker. Indien men alleen gebruik maakt van een gebruikersnaam en wachtwoord om deze toegang te beveiligen, loopt men het risico dat dit wachtwoord wordt gekraakt' (Govcert, 2009).

3.6 De telewerker zelf

De IBD (2014) beschrijft dat de mens zelf vaak de zwakste schakel in de telewerkketen is. Zeker wanneer deze zich niet bewust is van risico's die verbonden zijn aan het telewerken:

- Het apparaat wordt onbeheerd achtergelaten in een ruimte waar derden toegang tot hebben, wat derden meer mogelijkheden geeft om in te breken
- Vaak is men zich niet bewust van het feit dat men slachtoffer is van 'Social engineering'. De IBD (2014) omschrijft dat er bij Social engineering gebruik wordt gemaakt van kwaadwillende personen om zodoende informatie van medewerkers te ontfutselen. Dit kan gaan om bedrijfsgeheimen of informatie die niet voor iedereen bestemd is uit gemeentelijk systemen. Om zijn doel te bereiken maakt de Social engineer gebruik van zwakheden in de mens.
- Privé apparatuur wordt niet goed beheerd en kan besmet raken met malware
(IBD, 2014).

In onderstaande tabel zijn per ketenonderdeel bovenstaande risico's samengevat.

Tabel 1. Mogelijke risico's bij telewerken

Ketenonderdeel	**Nadere duiding onderdeel**	**Risico's**
Telwerklocatie	Openbare ruimte algemeen	Onbevoegden kunnen informatie vanaf het beeldscherm meelezen
		Onbevoegden kunnen informatie onderscheppen door het afluisteren van een telefoongesprek
		Informatie in handen van buitenstaande door verlies of diefstal van de apparatuur
	Openbare ruimte op een openbare PC	In cache opgeslagen gegevens van de vorige gebruiker zijn nog achtergebleven en beschikbaar voor een volgende gebruiker
Telewerkvoorziening	Privé apparatuur	beveiligingsmaatregelen kunnen bij de gebruiker niet (technisch) worden afgedwongen
		Informatie in handen van buitenstaander door zoekraken/diefstal apparaat
		Oplopen van een malware besmetting waardoor de gemeente ook geïnfecteerd raakt
		Andere gezinsleden of derden kunnen bij gegevens
Verbinding tussen het apparaat en de ICT- infrastructuur van de gemeente		Afluisteren van kwaadwillende
		Ongeautoriseerde toegang tot server omgeving
De toegang en informatie die aan de telewerker beschikbaar wordt gesteld	Interne applicaties	Kraken van gebruikersnaam en wachtwoord
De telewerker zelf		Onbeheerd achterlaten apparatuur in een ruimte waar derden toegang toe hebben
		Slachtoffer van 'Social engineering' (kwaadwillende ontfutselen vertrouwelijke informatie bij medewerkers)
		Onvoldoende beheer PC, deze kan besmet raken met malware

4. Methode van onderzoek

4.1 Inleiding

Het onderzoek van de rekenkamercommissie richt zich op de risico's die verband houden met het gedrag van de gebruikers zelf: de ambtenaren in Hengelo die van telewerken gebruik kunnen maken. Om in deze risico's inzicht te krijgen is gebruik gemaakt van het instrument online enquête (online survey) onder deze medewerkers. Dit hoofdstuk bespreekt de wijze waarop deze survey is uitgevoerd.

Paragraaf 4.2 bespreekt de onderzoekspopulatie en selectie van respondenten uit deze populatie. Paragraaf 4.3 betreft de opzet van de vragenlijst en gaat nader in op de bekende risico's vanuit het normatieve kader. Paragraaf 4.4 gaat over de benadering van de respondenten en de verkregen respons.

4.2 Onderzoekspopulatie en selectie

Kenmerkend voor de gemeente Hengelo is dat er in de meeste applicaties wordt gewerkt met persoonsgegevens. Van de 850 medewerkers hebben ongeveer 675 medewerkers toegang tot persoonsgegevens (op de werkplek). Afgezien van de buitendienst (175 personen) hebben dus vrijwel alle overige medewerkers toegang tot persoonsgegevens.

De onderzoekspopulatie wordt gevormd door alle gemeenteambtenaren binnen de gemeente Hengelo die in het bezit zijn van een token of een code om op afstand te kunnen werken met persoonsgegevens. Van de 850 medewerkers hebben 547 medewerkers van de gemeente Hengelo een token of en code en kunnen dus op afstand werken. De 547 personen blijken werkzaam in grote diversiteit aan onderdelen van de gemeente Hengelo; van het College van B&W, Griffie, de Directies en de afdeling Financiën tot Secretariaat en Flexpool, Terugvordering en Administratie, Regionale Organisatie Zelfstandigen, Cultuurtechniek, Sportservice en Twentebad.

4.3 De vragenlijst

De vragenlijst die onder de geselecteerde onderzoekspopulatie wordt afgenomen is ontworpen om over de volgende onderwerpen informatie te verzamelen:

1. De mate en aard van het gebruik telewerken in de gemeente Hengelo;
2. De mate waarin bij dit telewerken sprake is van de uit de theorie bekende risico's ten aanzien van de schakels: telewerklocatie, telewerkvoorziening en de telewerker zelf;
3. De risico-inschatting van de gebruikers zelf;
4. De noodzakelijkheid van het telewerken voor de gebruikers.

4.3.1 De mate en aard van het gebruik telewerken in de gemeente Hengelo

Wat betreft deelvraag twee, het aantal ambtenaren dat op afstand persoonsgegevens kan raadplegen, is op grond van de administratie van de gemeente al vastgesteld dat 547 van de 850 gemeenteambtenaren deze mogelijkheid tot telewerken in beginsel hebben. In het eerste deel van de enquête wordt dit gegeven geverifieerd en nader gespecificeerd. Hebben de

betreffende medewerkers daadwerkelijk toegang en over welk type toegang beschikken de medewerkers dan precies? Daarnaast is het ook van belang om te kijken hoe frequent ze van die mogelijkheid gebruik maken. Om daar achter te komen zijn in de vragenlijst de volgende vragen gesteld:

Tabel 2. Enquête vragen omtrent de mate en aard van het gebruik telewerken

Vraag nummer	Vraag
3	Heeft u voor het uitvoeren van uw functie de bevoegdheid om persoonsgegevens op afstand te raadplegen? (Dus op andere plaatsen dan op het stadskantoor/ uw reguliere werkplek)
4	Heeft u voor het uitvoeren van uw functie de bevoegdheid om persoonsgegevens op afstand te wijzigen? (Zo ja, welke?)
7	Hoe vaak raadpleegt u op afstand persoonsgegevens?
8	Hoe vaak wijzigt u op afstand persoonsgegevens?

4.3.2 Risico's ten aanzien van de schakels

Wat betreft deelvraag drie, de mate van risicovol gedrag van ambtenaren op afstand, is er een selectie van risico's gemaakt. Deze risico's hebben betrekking op de schakels telewerklocatie, telewerkvoorziening en de telewerker zelf.

Telewerklocatie

In de literatuur wordt er op gewezen dat telewerken in openbare locaties risico's met zich mee brengt. Om er achter te komen in hoeverre die risico's van telewerken bij de telewerkers van de gemeente Hengelo spelen is daarom in de vragenlijst de volgende vraag gesteld:

Tabel 3. Enquête vraag omtrent de telewerklocatie

Vraag nummer	Vraag
12	Op welke plaatsen maakt u gebruik van het werken op afstand?
13	Op welke plek werkt u thuis?

Telewerkvoorziening

Uit de literatuur komt verder naar voren dat er verschillende risico's bestaan rondom de apparatuur die op afstand wordt gebruikt. Om erachter te komen in hoeverre deze risico's van toepassing zijn op de telewerkers van de gemeente Hengelo zijn in de vragenlijst de volgende vragen gesteld:

Tabel 4. Enquête vragen omtrent de telewerkvoorziening

Vraag nummer	Vraag

17	Van wie is de apparatuur waarmee u op afstand werkt?
18	Wie maken er van deze apparatuur gebruik?
21	Welke toepassingen heeft u op de apparatuur waarmee u op afstand werkt?

Telewerker zelf

De telewerker zelf wordt in de literatuur als zwakste schakel beschouwd. In hoeverre de telewerkers van de gemeente Hengelo een risico vormen wordt onderzocht door het stellen van de volgende vragen:

Tabel 5. Enquête vragen omtrent de telewerker zelf

Vraagnummer	Vraag
9	Heeft u kennis genomen van de gedragscode ambtelijke integriteit?
6	Zijn er door of vanwege de gemeente Hengelo bij het verlenen van deze bevoegdheid aanwijzingen gegeven over veiligheid van het gebruik?
11	Op welke plek bewaart u de token/ code voor de smartphone?
19	Hoe vaak bent u op de apparatuur in aanraking gekomen met virussen?
20	Wat heeft u gedaan toen u in aanraking kwam met een virus?
22	Waar zoekt u hulp bij problemen met uw apparatuur?

4.3.3 Risico-inschatting van de gebruikers zelf

Om er achter te komen hoe de gebruikers het risico rondom telewerken zelf schatten zijn de ambtenaren op basis van een 5-punt schaal (1=geheel oneens, 2=oneens, 3=noch oneens/noch eens, 4=eens, 5=geheel eens) de volgende stellingen voorgelegd:

Tabel 6. Stellingen omtrent de risico-inschatting van de gebruikers zelf

Stelling nummer	Vraag
24	Ik beschik op de kamer waarin ik op afstand thuiswerk over een afsluitbare kast of la.
25	De ruimte waarin ik op afstand werk is veilig.
29	Ik ben ervan overtuigd dat niemand anders dan ik bij de persoonsgegevens kan.
30	Wanneer een persoon of instantie beweert volgens een betrokkene te bellen verstrek ik telefonisch informatie.

4.3.4 De noodzakelijkheid van het telewerken voor de gebruikers

Om te kijken of telewerken onder de telewerkers in Hengelo noodzakelijk is, zijn de respondenten wederom stellingen voorgelegd op basis van een 5-punt schaal (1=geheel oneens, 2=oneens, 3=noch oneens/noch eens, 4=eens, 5=geheel eens).

Tabel 7. Stellingen omtrent de noodzakelijkheid van het telewerken voor de gebruikers

Stelling	Vraag

nummer	
26	Voor mijn werk is het noodzakelijk dat ik op afstand toegang heb tot netwerken van de gemeente Hengelo.
27	Voor mijn werk is het noodzakelijk dat ik op afstand toegang heb tot persoonsgegevens van burgers.

4.4 Respons

In de mail met de uitnodiging om deel te nemen aan het onderzoek is duidelijk gemaakt dat de gegevens vertrouwelijk worden verwerkt. De antwoorden zijn niet terug te voeren naar individuele personen. De mail met de uitnodiging is op maandag 17 augustus 2015 (week 34) naar alle respondenten gestuurd. Het enquête onderzoek is ondersteund met een bericht op het Intranet van de gemeente Hengelo. Na twee weken is er een mail gestuurd om de respondenten eraan te herinneren dat ze nog de mogelijkheid hebben om mee te doen. Dit is gedaan om de respons te verhogen. Op vrijdag 4 september 2015 (week 36) is de vragenlijst gesloten. Er is gekozen voor dit tijdspad omdat de zomervakantie in de gemeente Hengelo officieel begon op 4 juli en eindigde op 16 augustus 2015. In totaal zijn er 547 gemeenteambtenaren (die in het bezit zijn van een token/code voor de smartphone en op afstand kunnen werken met persoonsgegevens) benaderd om de enquête in te vullen. Van deze populatie hebben 237 de enquête ingevuld. Daarnaast zijn er na het versturen van de eerste mail 97 mails ontvangen omtrent het niet kunnen invullen van de enquête wegens vakantie/ziekte/verlof. Uit deze 97 mails is naar voren gekomen dat een aantal van 74 respondenten voor 4 september 2015 (sluiting van de vragenlijst) weer terug zouden zijn van vakantie/verlof. Een totaal aantal van 23 respondenten waren dus niet in staat om de enquête in te vullen voor de sluiting van de vragenlijst. Na het versturen van de herinneringsmail op maandag 31 augustus zijn er 46 mails ontvangen omtrent het niet kunnen invullen van de enquête wegens vakantie/ziekte/verlof. 33 respondenten gaven in de mail aan dat ze de enquête niet konden in vullen voor de sluiting van de vragenlijst. Gezien het feit dat bij deze 33 respondenten, ook de 23 respondenten van daarnet inbegrepen zijn. Zijn er na het versturen van de herinneringsmail in totaal 10 respondenten niet in staat geweest om de enquête in te vullen wegens vakantie/verlof voor de sluiting van de vragenlijst. Daarnaast zijn er ook nog een aantal (7) mails ontvangen waarin naar voren komt dat er voor deze respondent geen mogelijkheid is om op afstand te werken met persoonsgegevens. In totaal is er een respons verkregen van 47%. Naar aanleiding van de resultaten van het onderzoek is er op 18 januari 2016 een lijst met vragen naar het college gestuurd. Op 12 februari 2016 heeft het college antwoord gegeven op deze vragen (zie bijlage). De antwoorden van het college op deze vragen zijn in dit onderzoeksrapport verwerkt.

5. Resultaten

Dit hoofdstuk beschrijft de resultaten van het onderzoek. In paragraaf 5.1 wordt in het kader van deelvraag drie eerst een overzicht gegeven van het gebruik van telewerken door de ambtenaren die daar volgens de gemeente Hengelo toegang toe hebben. De paragrafen 5.2 tot en met 5.5 hebben betrekking op deelvraag vier, de mate van risicovol gedrag van ambtenaren op afstand. Paragraaf 5.2 bespreekt het gebruik van risicovolle telewerklocaties. Paragraaf 5.3 gaat over het risico rondom de telewerkvoorziening. Paragraaf 5.4 gaat in op het risico rondom de telewerker zelf. Vervolgens geeft paragraaf 5.5 weer hoe gebruikers zelf het risico schatten. En als laatste geeft paragraaf 5.6 de noodzakelijkheid van telewerken weer.

5.1 Overzicht van de mate en aard van het gebruik telewerken in de gemeente Hengelo

Vanuit de gemeente is vastgesteld dat **547 van de 850** gemeenteambtenaren op afstand persoonsgegevens kunnen raadplegen met een token of een code. Maar dit zegt natuurlijk weinig over het daadwerkelijk gebruik van deze mogelijkheid. Aan de hand van de tabellen 8 tot en met 12, die op basis van de enquête zijn geproduceerd, is meer duidelijkheid te verschaffen.

Tabel 8 laat aan de hand van de antwoorden op de gestelde verificatievraag zien dat 120 van de 237 respondenten aangeven dat ze voor het uitvoeren van hun functie de mogelijkheid hebben om persoonsgegeven op afstand te raadplegen. 117 respondenten geven daarentegen aan die mogelijkheid niet te hebben. Dit is merkwaardig omdat volgens de door de gemeente verstrekte informatie alle respondenten die toegang zouden hebben. De antwoorden op de verificatievraag lijken slechts op twee manieren te verklaren. Hetzij zijn de gegevens van de gemeente over de ambtenaren die toegang hebben tot de persoonsgegevens in hoge mate onjuist (en veel minder dan de 547 ambtenaren heeft daadwerkelijk toegang). Hetzij veel van de ambtenaren die deze toegang hebben zijn hiervan niet op de hoogte. De brief van 12 februari 2016 (zie bijlage) van het college verschaft over deze twee manieren meer duidelijkheid. De brief maakt duidelijk dat 675 medewerkers van de gemeente Hengelo toegang hebben tot persoonsgegevens en dat 547 medewerkers hiervan over een token of een code beschikken om op afstand (met persoonsgegevens) te werken (Brief college; antwoord A+B, p.1). Hiermee is het verschil nog niet geheel verklaard. Het beeld blijft immers anders dan de uitkomsten van de enquête laten zien. Wellicht is het onderscheid te verklaren uit de actualiteit van de administratiegegevens. Wat betreft de tweede manier schetst de brief van het college dat er bij de uitgifte van een fysiek of digitaal token (waarmee men dus kan telewerken) een voorlichting geregeld is. Dit betekent dat ambtenaren die deze toegang hebben hiervan op de hoogte dienen te zijn. Daarnaast kan de afdeling ICT het gebruik van de uitgegeven tokens monitoren. Bij geen gebruik van de tokens kan via het afdelingshoofd worden gevraagd het token weer in te leveren. Bij afgifte van het token aan de medewerker is dit token meteen actief. Mocht het token binnen 7 weken niet worden gebruikt (geactiveerd) dan kan de medewerker het token niet meer gebruiken. Na deze periode wordt het token gedeactiveerd als de medewerker het langer dan drie maanden niet gebruikt (Brief college; antwoord C, p.2).

Tabel 9 geeft vervolgens inzicht in de mogelijkheid tot het wijzigen van persoonsgegevens. Over deze mogelijkheid blijkt krap 37 procent van de 120 personen met toegang tot persoonsgegevens te beschikken. Dit komt grotendeels overeen met het antwoord in de brief van het college van 12 februari 2016, waarin staat vermeld dat van de 675 medewerkers die toegang hebben tot persoonsgegevens er ongeveer 30 medewerkers beschikken over autorisatie om daarin te muteren (Brief college; antwoord A, p.1). Tabel 10 laat zien welke persoonsgegevens dit betreft.

De tabellen 11 en 12 geven een overzicht van de frequentie waarmee ambtenaren gebruik maken van het op afstand raadplegen, respectievelijk wijzigen van persoonsgegevens. Te zien is dat deze frequentie sterk verschilt. Slechts een klein deel raadpleegt dagelijks op afstand persoonsgegevens. Het merendeel van de respondenten doet dat duidelijk minder frequent. 40 procent van de respondenten die de mogelijkheid heeft om op afstand persoonsgegevens te raadplegen doet dat in de praktijk nauwelijks tot nooit. Voor de respondenten die op afstand persoonsgegevens kunnen wijzigen is het beeld vergelijkbaar. Het merendeel van de respondenten met die mogelijkheid geeft aan dit sporadisch of zelfs nooit te doen.

Kortom, de resultaten van de enquête laten zien dat de mate van gebruik van telewerken door medewerkers van de gemeente aanmerkelijk minder is dan de registratiecijfers van de verstrekte codes en tokens suggereren.

- In de praktijk hebben niet 547 van de 850 medewerkers maar ongeveer de helft daarvan de mogelijkheid om bij telewerken persoonsgegevens te raadplegen.
- Een beperkt deel daarvan (een kleine 40 procent) kan persoonsgegevens wijzigen.
- Van de personen die persoonsgegevens op afstand kunnen raadplegen en/of wijzigen maakt enkel een beperkt deel van deze mogelijkheid intensief of redelijk intensief gebruik. Een aanzienlijk deel doet dat niet of nauwelijks.

Tabel 8. Heeft u voor het uitvoeren van uw functie de bevoegdheid om persoonsgegevens op afstand te raadplegen?

	Aantal (N)	Percentage (%)
1)Ja	120	50,6
2)Nee	117	49,4
Totaal	237	100,0

Tabel 9. Heeft u voor het uitvoeren van uw functie de bevoegdheid om vanuit huis persoonsgegevens te wijzigen? Zo ja, welke?

	Aantal (N)	Percentage (%)
1)Ja	43	36,8
2)Nee	74	63,2
Totaal	117	100,0
Missing	3	
Totaal	120	

Tabel 10. Welke persoonsgegevens kunt u op afstand wijzigen?

	Aantal (N)	Percentage (%)
1)Uitkeringsgegevens	3	12,0
2)Klant/bedrijfsgegevens (NAW gegevens)	5	20,0
3)Gegevens vastgelegd in applicaties als GWS, You force, SoZa, WMO en Jeugd.	5	20,0
4)Parkeervergunning/ ontheffing gegevens	1	4,0
5)Salarisadministratie	1	4,0
6)Melddesksysteem	1	4,0
7)Verlofregistratie/ opwerkvergoedingen	1	4,0
8)Alle gegevens	6	24,0
9)Wachtwoorden resetten/accounts vrijgeven/ rapportages	2	8,0
Totaal	25	100,0
Missing	18	
Totaal	43	

Tabel 11. Hoe vaak raadpleegt u op afstand persoonsgegevens?

	Aantal (N)	Percentage (%)
1)Vrijwel dagelijks	11	9,5
2)2-3 keer per week	18	15,5
3)Circa 1 keer per week	18	15,5
4)Minder dan 1 keer per week	21	18,1
5)Sporadisch	28	24,1
6)Nooit	20	17,2
Totaal	116	100,0
Missing	4	
Totaal	120	

Tabel 12. Hoe vaak wijzigt u op afstand persoonsgegevens?

	Aantal (N)	Percentage (%)
1)Vrijwel dagelijks	4	9,3
2)2-3 keer per week	4	9,3
3)Circa 1 keer per week	4	9,3
4)Minder dan 1 keer per week	7	16,3
5)Sporadisch	11	25,6
6)Nooit	13	30,2
Totaal	43	100,0

5.2 Gebruik risicovolle telewerklocaties

In de literatuur wordt er op gewezen dat telewerken in openbare locaties risico's met zich mee brengt. De tabellen 13 en 14, die op basis van de enquête zijn geproduceerd, geven inzicht in de mate waarin door telewerkers van de gemeente Hengelo op risicovolle plaatsen wordt gewerkt.

Tabel 13 laat zien dat het overgrote deel van de respondenten thuis op afstand werkt. Een kleine 6 procent werkt op afstand in de trein en ongeveer 4 procent werkt tijdens de taakuitvoering op straat. De literatuur signaleert dat het werken op openbare locaties als in de trein of op straat extra risico's met zich mee brengt. Buitenstaanders kunnen op deze manier mogelijk vertrouwelijke informatie van het beeldscherm lezen of een telefoongesprek afluisteren dat gaat over de betreffende gegevens.

Tabel 14 laat zien in welke ruimte de respondenten werken als zij thuis van de gegevens gebruik maken. Te zien is dat de helft van de 94 respondenten die thuis werkt, dat in de woonkamer doet en dat daarnaast een kleine 10 procent in de keuken werkt. In die woonkamer en keuken kunnen allicht andere gezinsleden of bekenden aanwezig zijn of op bezoek komen. Dit gaat met enige risico's gepaard.

Kortom, de resultaten van de enquête laten zien dat er gevaren kleven aan de locatie waar ambtenaren van de gemeente Hengelo op afstand werken met persoonsgegevens. De brief van het college van 12 februari 2016 geeft echter aan dat de gemeente Hengelo gebruik maakt van VDI. Met het VDI concept wordt de beveiliging in de rekencentrum geregeld (Brief college; antwoord A, p.2). Hierdoor zouden medewerkers zonder bezwaar op elke locatie moeten kunnen werken. Een kanttekening die hierbij kan worden gemaakt is dat het VDI concept puur gericht is op de techniek en de beveiliging hiervan. Het (risico) gedrag en de omgang van medewerkers met persoonsgegevens op afstand kan hiermee niet direct worden afgedekt.

Tabel 13. Op welke plaatsen maakt u gebruik van het werken op afstand? (N=120)
**Meerdere antwoorden mogelijk*

	Aantal (N)	Percentage (%)
1)Thuis	94	78,3%
2)Tijdens uw taakuitvoering op straat	5	4,2%
3)In de trein	7	5,8%
4)Anders	23	19,2%

Tabel 14. Op welke plek werkt u thuis?

	Aantal (N)	Percentage (%)
1)In de studeerkamer	33	35,1
2)In de woonkamer	47	50,0
3)In de keuken	8	8,5
4)Anders	6	6,4
Totaal	94	100%

5.3 Gebruik van risicovolle telewerkvoorzieningen

Uit de literatuur komt naar voren dat er verschillende risico's bestaan rondom de apparatuur die op afstand wordt gebruikt. En dat de mate van risico afdekking hierbij samenhangt met het beheer van de apparatuur. Aan de hand van de tabellen 15 tot en met 19, die op basis van de enquête zijn geproduceerd, kan ook wat dit betreft meer inzicht worden verkregen.

Tabel 15 geeft een overzicht van het eigenaarschap van de apparatuur. Te zien is dat een meerderheid (63%) van de respondenten zelf eigenaar is van de apparatuur waarmee op afstand wordt gewerkt. Ongeveer een derde beschikt over apparatuur die afkomstig is van de gemeente Hengelo. Dit laatste valt volgens de literatuur te prefereren, omdat dit impliceert dat de gemeente Hengelo kan bepalen welke beveiligingsmaatregelen zij op deze apparatuur aanbrengt, waardoor risico's grotendeels kunnen worden verminderd.

Tabel 16 laat vervolgens zien of ook anderen gebruik maken van de apparatuur waarmee op afstand wordt gewerkt. Het blijkt dat veel van de apparatuur waarop wordt getelewerkt niet exclusief door de telewerker wordt gebruikt, maar ook door anderen. Ook dit houdt een zeker risico in. Van de privacy gevoelige informatie kan een print screen gemaakt worden en dit kan wel op de thuis pc gezet worden. Waardoor deze informatie mogelijk toegankelijk is voor derden die ook gebruik maken van de apparatuur.

Tabel 17 geeft een overzicht van de applicaties op de gebruikte apparatuur. Opvallend is dat 20 procent van de respondenten toegeeft wel gebruik te maken van software voor het downloaden van films, muziek en/of spellen, hetgeen risico's met zich meebrengt van kwaadaardige software.

Daarnaast laat de tabel zien dat ongeveer een derde van de respondenten aangeeft niet over een virusscanner te beschikken, en dat iets minder dan de helft van de respondenten geen gebruik maakt van een automatische slaapfunctie. Dit is merkwaardig want volgens de gemeente Hengelo werkt iedere gemeenteambtenaar op afstand in 'de Cloud' waardoor beveiligingstoepassingen als bijvoorbeeld een virusscanner aanwezig (horen te) zijn. Dit kan twee dingen betekenen. Hetzij beschikken de ambtenaren daadwerkelijk niet over de benodigde beveiligingstoepassingen. Hetzij veel van de ambtenaren die over deze toepassingen beschikken zijn hiervan niet op de hoogte. De brief van 12 februari 2016 van het college verschaft over deze twee manieren meer duidelijkheid. Wat betreft het eerste punt geeft het college in de brief aan dat met het VDI- concept de beveiliging centraal wordt geregeld (Brief college; antwoord A, p.2) wat zou betekenen dat de ambtenaren over de benodigde beveiligingstoepassingen als een virusscanner beschikken. Aangaande het tweede punt geeft de brief aan dat er bij de uitgifte van een fysiek of een digitaal token wat betreft voorlichting en instructie geen extra zaken zijn geregeld (Brief college; antwoord C, p.2). In hoeverre die voorlichting en instructie reikt komt in de brief niet duidelijk naar voren. Er bestaat dus een mogelijkheid dat ambtenaren daadwerkelijk niet zijn ingelicht over de toepassingen waarover zij beschikken op de apparatuur.

Tabel 18 en 19 gaan nader in op de relatie tussen het gebruik van deze beveiligingstoepassingen op de apparatuur en het vertonen van risicovol gedrag. Tabel 18

laat zien dat van de 26 respondenten die beschikken over software voor het downloaden van films, muziek en/of spellen 3 respondenten geen virusscanner hebben. Tabel 19 laat zien dat van de 47 respondenten die in de woonkamer werken, er 22 respondenten niet beschikken over een automatische slaapfunctie met wachtwoord.

Kortom, de resultaten van de enquête laten het volgende zien:

- Gebruikers van de telewerkvoorzieningen werken hiermee veelvuldig op apparatuur die ook door anderen wordt gebruikt
- Op die apparatuur is niet zelden download software geïnstalleerd hetgeen risico's met zich meebrengt.
- Een aanzienlijk deel van de gebruikers geeft aan geen gebruik te maken van beveiligingstoepassingen als een virusscanner die risico's kunnen helpen verminderen en lijkt daarmee onvoldoende op de hoogte te zijn van de voorlichting en/of instructie van de gemeente.

Tabel 15. Van wie is de apparatuur waarmee u op afstand werkt?

	Aantal (N)	Percentage (%)
1)Gemeente Hengelo	43	35,8%
2)Persoonlijk eigendom	75	62,5%
3)Anders	2	1,7%
Totaal	120	100%

Tabel 16. Wie maken er gebruik van de apparatuur?

	Aantal (N)	Percentage (%)
1)Alleen ikzelf	55	45,8%
2)Andere gezinsleden	37	30,8%
3)Anders	6	5,0%
Totaal	98	100%
Missing	22	
Totaal	120	

Tabel 17. Welke toepassingen heeft u op de apparatuur waarmee u op afstand werkt?
**Meerdere antwoorden mogelijk*
(N=120)

	Aantal (N)	Percentage (%)
1)Office pakket	91	75,8%
2)Automatisch slaapfunctie beveiligd met wachtwoord	66	55,0%
3)Software voor het downloaden van films, muziek en/of spellen	26	21,7%
4)Chatprogramma's	10	8,3%
5)Virusscanner	79	65,8%
6)Cloud diensten	40	33,3%
7)Personal firewall	42	35%

8)Anti malware tool	37	30,8%

Tabel 18. Veiligheid van toepassingen 1

			Heeft u een up-to-date virus scanner?		Totaal
			Nee	Ja	
Beschikt u over software voor het downloaden van films, muziek en/of spellen?	Nee	Aantal	38	56	94
		% van totaal	31,6%	46,7%	78,3%
	Ja	Aantal	3	23	26
		% van totaal	2,5%	19,2%	21,7%
		Aantal	41	79	120
		% van totaal	34,2%	65,8%	100,0%

Tabel 19. Veiligheid van toepassingen 2

			Heeft u een automatische slaapfunctie beveiligd met wachtwoord?		Totaal
			Nee	Ja	
Op welke plek werkt u thuis?	In de studeerkamer	Aantal	7	26	33
		% van totaal	7,4%	27,7%	35,1%
	In de woonkamer	Aantal	22	25	47
		% van totaal	23,4%	26,6%	50,0%
	In de keuken	Aantal	1	7	8
		% van totaal	1,1%	7,4%	8,5%
	Anders	Aantal	2	4	6
		% van totaal	2,1%	4,3%	6,4%
		Aantal	32	62	94
		% van totaal	34,0%	66,0%	100%

5.4 Risico's rondom de telewerker zelf

De telewerker zelf wordt in de literatuur als zwakste schakel beschouwd. Hoe staat het met die telewerker in Hengelo? De tabellen 20 tot en met 25 zijn gemaakt om inzicht te krijgen in de risico's die er rondom de telewerker zelf spelen.

Tabel 20 en 21 gaan over de kennis van het beleid van de gemeente Hengelo. Te zien is dat ongeveer een derde van de respondenten die persoonsgegevens op afstand kunnen raadplegen of wijzigen aangeven geen indicatie te hebben gekregen over de veiligheid van het gebruik hiervan. Ook voor de gedragscode ambtelijke integriteit geldt dat een beperkt deel van de respondenten aangeeft geen kennis te hebben genomen van deze code.

Tabel 22 geeft inzicht in de bewaarplek van de token of code. Te zien is dat de token of code in een aantal gevallen wordt bewaard op plekken die toegankelijk zijn voor derden.

Tabel 23, 24 en 25 laten zien of gemeenteambtenaren in aanraking zijn gekomen met een virus en welke handelingen zij hierbij vervolgens hebben verricht. Naar voren komt dat ongeveer een vijfde deel van de respondenten in aanraking is gekomen met een virus, maar dat slechts twee van hen hiervan melding hebben gemaakt bij de servicedesk van de gemeente Hengelo. Terwijl dit conform het beveiligingsreglement daar zo snel mogelijk gemeld dient te worden.

Kortom, de resultaten van de enquête geven de indruk dat de risico's rond de telewerker zelf beter kunnen worden afgedekt.

- Het college geeft in de brief van 12 februari 2016 aan dat er beleidsregels zijn met betrekking tot het op afstand werken met persoonsgegevens. Uit het onderzoek komt naar voren dat een deel van de gebruikers onvoldoende op de hoogte lijkt van het beveiligingsbeleid van de gemeente en van de gedragscode ambtelijke integriteit en lijkt hier ook onvoldoende naar te handelen.

Tabel 20. Zijn er door of vanwege de gemeente Hengelo bij het verlenen van deze bevoegdheid (raadplegen en/of wijzigen van persoonsgegevens) aanwijzingen gegeven over de veiligheid van het gebruik?

	Aantal (N)	Percentage (%)
1)Ja	77	64,2
2)Nee	41	34,2
Totaal	118	100,0
Missing	2	
Totaal	120	

Tabel 21. Heeft u kennis genomen van de gedragscode ambtelijke integriteit Hengelo?

	Aantal (N)	Percentage (%)
1)Ja	90	92,8%
2)Nee	7	7,2%
Totaal	97	100%
Missing	23	
Totaal	120	

Tabel 22. Op welke plek bewaart u de token en/of code voor de smartphone?

	Aantal (N)	Percentage (%)
1) Thuis (keukenla/kast/bureau/map)	19	20,0
2) (Werk)tas	8	8,4
3) Op de telefoon/smartphone	27	28,4
4) Op het werk	1	1,0
5) Uit het hoofd geleerd	27	28,4
6) Binnen handbereik	3	3,2
7) Geheime plek	6	6,4
8) Sleutelbos	4	4,2
Totaal	95	100,0
Missing	25	
Totaal	120	

Tabel 23. Hoe vaak bent u op de apparatuur in aanraking gekomen met virussen?

	Aantal (N)	Percentage (%)
1)Nooit	80	66,7
2)1-4 keer	18	15,0
3)5-10 keer	0	0,0
4)>10 keer	0	0,0
Totaal	98	100
Missing	22	
Totaal	120	

Tabel 24. Wat heeft u gedaan toen u in aanraking kwam met een virus?

	Aantal (N)	Percentage (%)
1)Weggegooid	6	33,0
2)Op gereageerd	5	27,8
3)Gemeld bij de servicedesk	2	11,1
4)Anders	5	27,8
Totaal	18	100,0

Tabel 25. Waar zoekt u hulp bij problemen met uw apparatuur?
**Meerdere antwoorden mogelijk (N=120)*

	Aantal (N)	Percentage (%)
1)Bij de servicedesk van de gemeente Hengelo	59	49,2
2)Bij het bedrijf waar ik de apparatuur heb gekocht	19	15,8
3)Bij een reparateur	9	7,5
4)Ik heb een kennis/familielid die dit voor mij doet	27	22,5
5)Anders	23	19,2

5.5 Risico-inschatting door de telewerkers zelf

Om er achter te komen hoe de gebruikers het risico rondom telewerken zelf inschatten is hun op basis van een 5-punt schaal (1=geheel oneens, 2=oneens, 3=noch oneens/noch eens, 4=eens, 5=geheel eens) een aantal stellingen voorgelegd.

De figuren 1 en 2 geven inzicht in de veiligheid van de ruimte op afstand. Te zien is dat veel respondenten op afstand niet beschikken over een afsluitbare lade of kast. Een grote meerderheid zegt op afstand in een veilige ruimte te werken. Één respondent meent op afstand in een onveilige ruimte te werken.

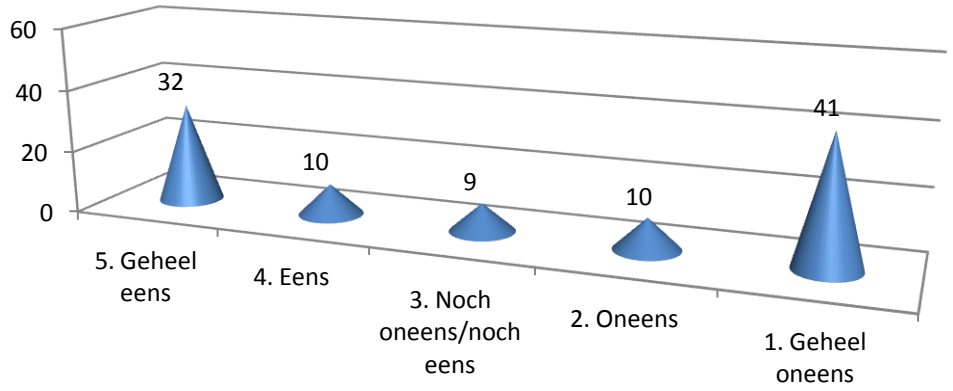
Figuur 3 geeft weer hoe de ambtenaren de beveiliging van persoonsgegevens inschatten. Te zien is dat de een groot deel van de respondenten denkt dat de persoonsgegevens bij hen veilig zijn en dat niemand anders dan zij zelf bij de persoonsgegevens kunnen. Enkele respondenten lijken hier echter twijfels over te hebben.

Figuur 4 heeft betrekking op de telefonische verstrekking van persoonsgegevens. Meer dan de helft van de respondenten zegt telefonisch geen informatie te verstrekken wanneer een persoon of instantie hierover belt. Een klein aantal van de respondenten geeft aan dit wel te doen. Dit komt niet overeen met het huidige beveiligingsbeleid dat stelt dat er niet aan verzoeken om telefonische informatie tegemoet mag worden gekomen.

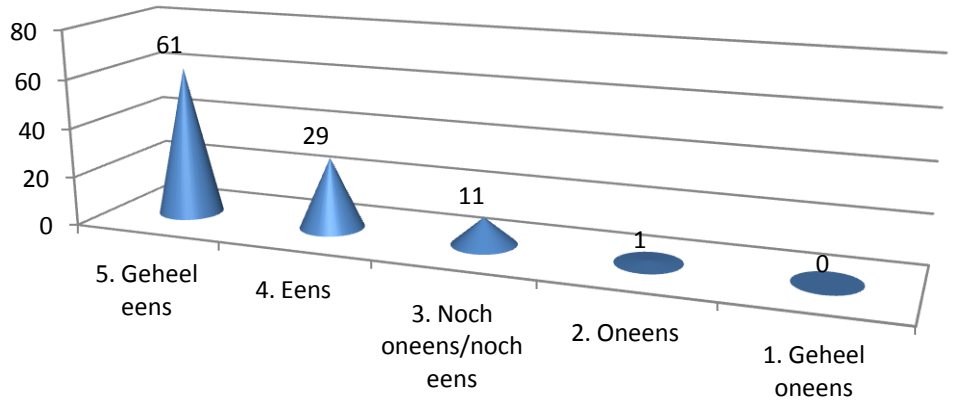
Kortom, de resultaten van de enquête laten zien dat:

- De perceptie van het merendeel van de ambtenaren is dat ze op afstand in een veilige ruimte werken. Slechts een beperkt deel geeft aan er niet zeker van te zijn dat niemand anders dan zij zelf bij de persoonsgegevens kunnen;
- Gezien het huidige beveiligingsbeleid van de gemeente Hengelo is het opmerkzaam dat een aantal telewerkers zegt telefonisch informatie te verstrekken. Een gevaar dat daaraan kleeft is dat op deze manier privacy gevoelige informatie in handen kan komen van een persoon/instantie waarvoor deze informatie niet toegankelijk hoort te zijn/bestemd is.

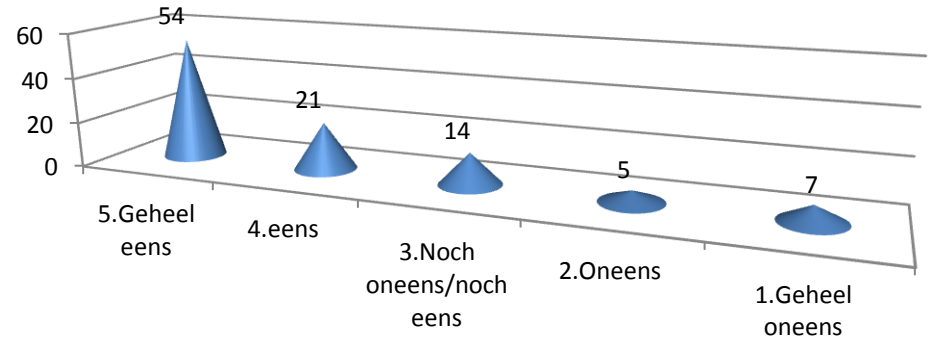
Figuur 1. Ik beschik op de kamer waarin ik op afstand thuiswerk over een afsluitbare kast of la (N=102).



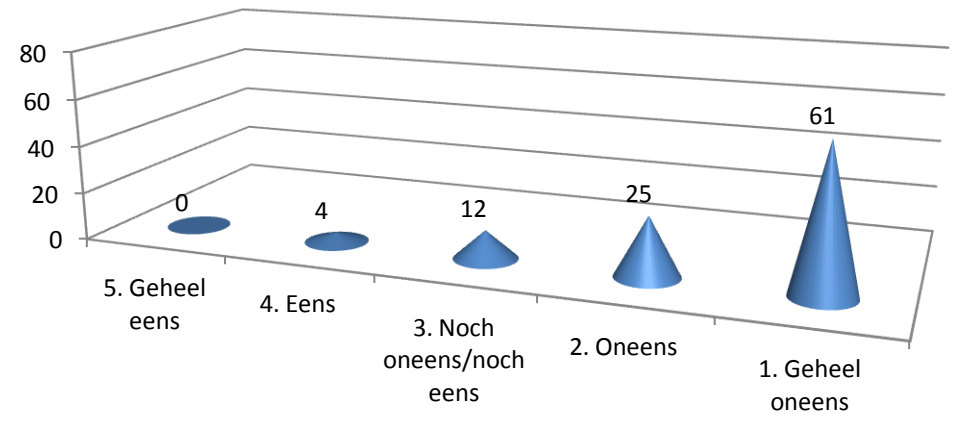
Figuur 2. De ruimte waarin ik op afstand werk is veilig (N=102).



Figuur 3. Ik ben ervan overtuigd dat niemand anders dan ik bij de persoonsgegevens kan (N=101).



Figuur 4. Wanneer een persoon of instantie beweert volgens een betrokkene te bellen verstrek ik telefonisch informatie (N=102).



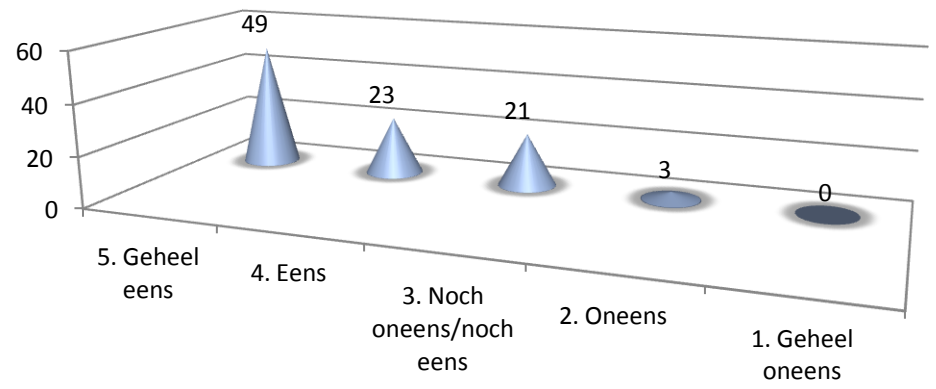
5.6 Noodzakelijkheid van telewerken

Tot slot zijn de telewerkers bevraagd over de noodzakelijkheid van de telewerkvoorziening voor hun werk. Hiertoe zijn wederom stellingen voorgelegd op basis van een 5-punt schaal (1=geheel oneens, 2=oneens, 3=noch oneens/noch eens, 4=eens, 5=geheel eens). De antwoorden zijn samengevat in de figuren 5 en 6.

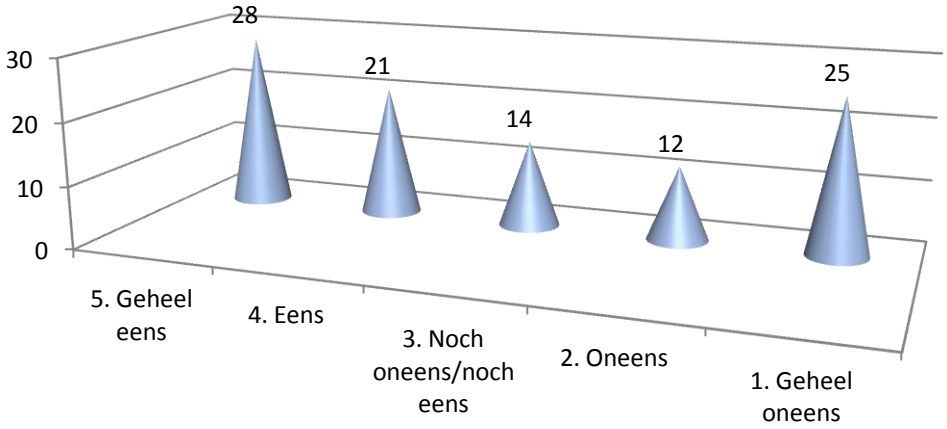
Figuur 5 gaat over de toegang tot het netwerk van de gemeente (intranet). Het blijkt dat een grote meerderheid van de respondenten deze toegang noodzakelijk acht om hun werkzaamheden op afstand te kunnen verrichten, maar dat een deel ook zonder lijkt te kunnen.

Figuur 6 heeft betrekking op de toegang tot persoonsgegevens van burgers op afstand. Hier blijkt dat ongeveer de helft van de respondenten meent niet op afstand te kunnen werken zonder daarbij de beschikking te hebben over deze persoonsgegevens, maar dat daarnaast een aanzienlijk deel meent dat deze toegang tot de persoonsgegevens niet of niet per se nodig is.

Figuur 5. Voor mijn werk is het noodzakelijk dat ik op afstand toegang heb tot netwerken van de gemeente Hengelo (N=96)



Figuur 6. Voor mijn werk is het noodzakelijk dat ik op afstand toegang heb tot persoonsgegevens van burgers (N=100).



6. Conclusie

In dit onderzoek ging het om de vraag hoe gemeenteambtenaren van de gemeente Hengelo die kunnen telewerken omgaan met de beveiliging van de door de gemeente beheerde gegevens. Om deze onderzoeksvraag te beantwoorden zijn er een aantal deelvragen gesteld die in het onderzoek zijn beantwoord. In dit conclusie hoofdstuk vatten we allereerst deze antwoorden op die deelvragen samen, om vervolgens tot de beantwoording van de hoofdvraag te komen.

6.1 Beantwoording van de deelvragen

1.Welke eisen stellen de Wet Bescherming Persoonsgegevens, de Wet Basisregistratie Personen en de interne regels van de gemeente Hengelo aan het werken met persoonsgegevens middels telewerken?

De WBP en de WBRP stellen verschillende eisen aan de omgang met persoonsgegevens. Een belangrijk onderdeel daarvan is dat de persoonsgegevens die door een gemeente worden verwerkt slecht mogen worden verwerkt door de verantwoordelijke bewerker en niet in handen van derden mogen komen. Om dit te kunnen waarborgen heeft de gemeente Hengelo interne spelregels opgesteld. Een onderdeel hiervan is de gedragscode ambtelijke integriteit, waarin een aantal basisbeginselen voor houding en gedrag zijn verwoord.

2.Welke risico's spelen een rol bij dit telewerken met de door de gemeente beheerde gegevens?

De interne spelregels die de gemeente Hengelo heeft opgesteld lijken deels toegespitst op gegevensverwerking door ambtenaren binnen de door de gemeente beheerde gebouwen. Met telewerken is echter sprake van verwerking van gegevens buiten die gebouwen en ontstaan er diverse nieuwe risico's. Deze risico's zijn in te delen naar schakels van de telewerkketen en zijn samengevat in tabel 1.

3.In welke mate maken gemeenteambtenaren gebruik van de mogelijkheid persoonsgegevens op afstand te raadplegen en/of te bewerken?

Vanuit de gemeente Hengelo is aangegeven dat 547 van de 850 gemeenteambtenaren op afstand zouden kunnen werken met persoonsgegevens. Dit komt niet geheel overeen met de resultaten van de enquête onder de ambtenaren zelf, die uitwijzen dat van diegenen die toegang zouden moeten hebben, enkel de helft zelf meent toegang te hebben. Daarnaast is vastgesteld dat van die personen met toegang een aanzienlijk deel deze toegang in de praktijk niet of nauwelijks benut, en voor het werk op afstand ook niet nodig acht.

4.In welke mate gedragen gemeenteambtenaren zich risicovol bij het op afstand raadplegen of bewerken van persoonsgegevens?

Wat betreft de schakel telewerklocatie zijn er risico's gesignaleerd. Sommige telewerkers gebruiken de telewerkvoorziening op openbare locaties, zoals (op straat en, in de trein). Het gevaar hiervan is dat buitenstaanders op deze manier vertrouwelijk informatie van het beeldscherm kunnen lezen of een telefoongesprek afluisteren. Uit het onderzoek komt naar voren dat veel telewerkers van de gemeente Hengelo thuis telewerken in de keuken of woonkamer. Hieraan kunnen risico's verbonden zijn.

Wat betreft risico's rondom het gebruik van de apparatuur, zien we dat veel telewerkers bij de gemeente Hengelo gebruik maken van de eigen apparatuur in huis, waartoe ook gezinsleden toegang hebben. De gemeente Hengelo maakt gebruik van het concept VDI. Dit betekent dat er in de cloud wordt gewerkt, en dat minder geavanceerde apparatuur afdoende zou moeten zijn.

Tenslotte geeft het college in de brief van 12 februari 2016 aan dat er beleidsregels zijn met betrekking tot het op afstand werken met persoonsgegevens. De resultaten van de enquête geven de indruk dat een deel van de gebruikers niet of onvoldoende op de hoogte zijn van de voor het telewerken relevante gedragscodes.

6.2 Beantwoording van de hoofdvraag

'Op welke wijze gaan gemeenteambtenaren van de gemeente Hengelo die kunnen telewerken om met de beveiliging van de door de gemeente beheerde gegevens?'

De WBP en WBRP stellen verschillende eisen aan de omgang met persoonsgegevens. Een belangrijk onderdeel daarvan is dat de persoonsgegevens die door een gemeente worden verwerkt slechts mogen worden verwerkt door de verantwoordelijke bewerker en niet in handen van derden mogen komen. Om dit te kunnen waarborgen heeft de gemeente Hengelo interne spelregels opgesteld. Deze regels zijn echter niet altijd bekend bij de gemeenteambtenaren die op afstand met persoonsgegevens werken. Zo meent ongeveer één derde van deze ambtenaren dat er bij het verlenen van de bevoegdheid geen aanwijzingen zijn gegeven over de veiligheid van het gebruik. Daarnaast geven een aantal van deze ambtenaren aan niet bekend te zijn met de gedragscode ambtelijke integriteit.

Verder bestaat er bij een deel van de gemeenteambtenaren die op afstand persoonsgegevens kunnen raadplegen en/of wijzigen een potentieel gevaar dat vertrouwelijke gegevens in handen van derden kunnen komen. Zo werkt het merendeel van de ambtenaren op afstand met persoonsgegevens in de keuken en/of woonkamer, en beschikken daarbij dan niet over een automatische slaapfunctie met wachtwoord. Daarnaast bewaren een aantal gemeenteambtenaren tokens en/of codes voor de smartphone op plekken die duidelijk toegankelijk en zichtbaar zijn voor derden. Iets meer dan een kwart van de ambtenaren die op afstand met persoonsgegevens werken verschaffen andere gezinsleden/derden ook toegang tot hun apparatuur. Een gevaar dat hieraan kleeft is dat van deze privacy gevoelige informatie een print screen gemaakt kan worden en dit wel op de thuis pc gezet kan worden. Waardoor deze informatie mogelijk toegankelijk is voor derden die ook gebruik maken van de apparatuur.

7. Referenties

Babbie, E. (2010). *The practice of social research.* Belmont: Wadworth Cengage Learning.

BMC. (2011). *Informatiebeveiligingsbeheer*. Rotterdam: Adviesmanagement.

Govcert. (2009). *Telewerken: Veilig werken op afstand*. Den Haag: Nederlandse overheid.

Hoogendijk, L., & Van Schajik, J. (2011). Beveiliging van telewerken: Een praktische aanpak. *IT-Auditor*, 20(2), 7-14.

Horsten, F. (2011). *Het nieuwe werken*. Den Haag: Arbeidsmarkt- en opleidingsfonds gemeenten.

IBD. (2014). *Telewerkbeleid.* Verkregen op 28 juni, 2015 van https://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0410-Telewerkbeleid-gemeente-v1.0.pdf

Overheid. (2015). *Wet bescherming persoonsgegevens*. Verkregen op 2 juli, 2015 van http://wetten.overheid.nl/BWBR0011468/

Overheid. (2015). *Zelfevaluatie BRP*. Verkregen op 4 juli, 2015 van http://www.bprbzk.nl/BRP/Zelfevaluatie_BRP

Sloot van der, B. (2010). De evaluatie van de Wet bescherming persoonsgegevens. *Privacy & Informatie*, 13 (5), 224-236.

Suwinet(2014). Beveiligingsplan Gemeente Hengelo.

Vries, N.L. de (2015). Een onderzoek naar het op afstand werken met persoonsgegevens.

Winter, H. B., De jong, P. O., Sibma, A., Visser, F. W., Herweijer, M., Klingenberg, A. M., & Prakken, H. (2008). *Wat niet weet, wat niet deert: een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk.* Groningen: Pro facto.

Zeeuwen, R. (2011). *Werken op afstand, integriteit en informatiebeveiliging.* Enschede: Gemeente Enschede.

8. Bijlagen

8.1 Enquête: Een onderzoek onder gemeenteambtenaren van de gemeente Hengelo naar het werken op afstand met de door de gemeente beheerde gegevens.

De Rekenkamercommissie van de gemeente Hengelo doet op dit moment een onderzoek naar het werken op afstand met persoonsgegevens. Ik wil u daarom vragen deze vragenlijst in te vullen. Het invullen duurt ongeveer 5 minuten. De antwoorden zullen vertrouwelijk worden behandeld en al u gegevens blijven anoniem.

Ik wil u alvast bedanken voor uw tijd en bereidwillige medewerking! Als u verder vragen of opmerkingen heeft, kunt u mij natuurlijk mailen.

Met vriendelijke groet,

Nathalie de Vries
Masterstudent Public Safety Universiteit Twente
n.l.devries@student.utwente.nl

1.

Welk type functie heeft u?

- ○ Leidinggevende
- ○ Administratief medewerker
- ○ Beleidsmedewerker
- ○ Adviseur
- ○ Handhaving/Buitendienst
- ○ Projectmedewerker
- ○ Anders

2.

Wat voor soort arbeidsovereenkomst heeft u?

- ○ Arbeidsovereenkomst voor onbepaalde tijd (Vast contract)
- ○ Arbeidsovereenkomst voor bepaalde tijd (Tijdelijk contract)
- ○ Anders

3.

Heeft u voor het uitvoeren van uw functie de bevoegdheid om persoonsgegevens op afstand te raadplegen?(Dus op andere plaatsen dan op het stadskantoor/uw reguliere werkplek)

- Ja
- Nee

4.

Heeft u voor het uitvoeren van uw functie de bevoegdheid om persoonsgegevens op afstand te wijzigen? (Zo ja, welke?)

- Ja
- Nee

Wanneer u bij zowel vraag drie als vier nee heeft ingevuld mag u stoppen met het invullen van de enquête.

5.

Zijn er door of vanwege de gemeente Hengelo bij het verlenen van deze bevoegdheid beperkingen in het gebruik aan u opgelegd?

- Ja, namelijk
- Nee

6.

Zijn er door of vanwege de gemeente Hengelo bij het verlenen van deze bevoegdheid aanwijzingen gegeven over veiligheid van het gebruik?

- Ja
- Nee

7.

Hoe vaak raadpleegt u op afstand persoonsgegevens?

- Vrijwel dagelijks
- 2-3 keer per week
- Circa 1 keer per week
- Minder dan 1 keer per week
- Sporadisch
- Nooit

8.

Hoe vaak wijzigt u op afstand persoonsgegevens?

- Vrijwel dagelijks
- 2-3 keer per week
- Circa 1 keer per week
- Minder dan 1 keer per week
- Sporadisch
- Nooit

Wanneer u bij zowel vraag zeven als acht nooit heeft ingevuld mag u stoppen met het invullen van de enquête.

9.

Heeft u kennis genomen van 'De gedragscode ambtelijke integriteit Hengelo'?

- Ja
- Nee

10.

Heeft u de beschikking over een token of een code voor de smartphone om uw werk op afstand uit te kunnen voeren?

- Ja
- Nee
- Anders

11.

Op welke plek bewaart u de token/code voor de smartphone?

12.

Op welke plaatsen maakt u gebruik van het werken op afstand? (Meer dan één antwoord mogelijk)

- Thuis
- Tijdens uw taakuitvoering op straat
- In de trein
- Anders

Wanneer u bij vraag 12 heeft gekozen voor de optie 'Thuis'mag u doorgaan met vraag 13 De overige opties mogen de enquête vervolgen bij vraag 14.

13.

Op welke plek werkt u thuis?

- In de studeerkamer
- In de woonkamer
- In de keuken
- Anders

14.

Beschikt u op de apparatuur waarmee u op afstand werkt automatisch over een vergrendelingfunctie met wachtwoord?

- ○ Ja
- ○ Nee, ga door naar vraag 16

15.

Na hoeveel minuten wordt uw computer vergrendeld?

- ○ Minder dan 1 minuut
- ○ 1 a 2 minuten
- ○ Meer dan 3 minuten

16.

van welke apparatuur maakt u gebruik als u op afstand werkt? (Meer dan één antwoord mogelijk)

- ☐ Laptop
- ☐ Tablet
- ☐ Pc
- ☐ Mobiele telefoon

17.

Van wie is deze apparatuur?

- ☐ Gemeente Hengelo
- ☐ Persoonlijk eigendom
- ☐ Anders

18.

Wie maken er van deze apparatuur gebruik?

- Alleen ikzelf
- Andere gezinsleden
- Anders

19.

Hoe vaak bent u op die apparatuur in aanraking gekomen met virussen?

- Nooit, ga door naar vraag 21
- 1-4 keer
- 5-10 keer
- >10 keer

20.

Wat heeft u daarmee gedaan?

- Weggegooid
- Op gereageerd
- Gemeld bij de servicedesk
- Anders

21.

Welke toepassingen heeft u op uw apparatuur waarmee u op afstand werkt? (Meer dan één antwoord mogelijk)

- Office pakket
- automatische slaapfunctie beveiligd met wachtwoord
- Software voor het downloaden van films, muziek en/of spellen
- Chatprogramma's
- Virusscanner
- Cloud diensten (Dropbox, Gmail)

- [ ] Personal firewall
- [ ] Anti malware tool

22.

Waar zoekt u hulp bij problemen met uw apparatuur? (Meer dan één antwoord mogelijk)

- [ ] Bij de servicedesk van de gemeente
- [ ] Bij het bedrijf waar ik de apparatuur heb gekocht
- [ ] Bij een reparateur
- [ ] Ik heb een kennis/familielid die dit voor mij doet
- [ ] Anders

23.

Onderstaand vindt u een aantal stellingen. Wilt u aangeven of u het met de volgende stellingen geheel oneens, oneens, noch oneens/noch eens, eens, geheel eens bent. (Waarbij 1=geheel oneens en 5=geheel eens)

	1 Geheel oneens				**5 Geheel eens**
Ik vind het fijn dat ik op afstand kan werken.	○	○	○	○	○

24.

	1 Geheel oneens				**5 Geheel eens**
Ik beschik op de kamer waarin ik op afstand thuiswerk over een afsluitbare kast of la.	○	○	○	○	○

25.

	1 Geheel oneens				**5 Geheel eens**
De ruimte waarin ik op afstand werk is veilig.	○	○	○	○	○

26.

	1 Geheel oneens				5 Geheel eens
Voor mijn werk is het noodzakelijk dat ik op afstand toegang heb tot netwerken van de gemeente.	○	○	○	○	○

27.

	1 Geheel oneens				5 Geheel eens
Voor mijn werk is het noodzakelijk dat ik op afstand toegang heb tot persoonsgegevens van burgers.	○	○	○	○	○

28.

	1 Geheel oneens				5 Geheel eens
Mijn leidinggevende is van mening dat ik op afstand moet kunnen werken.	○	○	○	○	○

29.

	1 Geheel oneens				5 Geheel eens
Ik ben ervan overtuigd dat niemand anders dan ik bij de persoonsgegevens kan.	○	○	○	○	○

30.

	1 Geheel oneens				5 Geheel eens
Wanneer een persoon of instantie beweert volgens een betrokkene te bellen verstrek ik telefonisch informatie.	○	○	○	○	○

Dit is het einde van de vragenlijst.

Bedankt voor het invullen van de vragen!

8.2 Brief college tussenvragen 18-01-2016

GEMEENTE HENGELO

Postbus 18
7550 AA Hengelo

Aan het college
P/a de heer J. Eshuis

Onderwerp
Vragen n.a.v. onderzoek inzake telewerken.

Datum
18 januari 2016.

Geacht college,

In opdracht van de Rekenkamercommissie heeft Nathalie de Vries, studente Public Administration aan de Universiteit Twente, een onderzoek verricht naar het op afstand werken met persoonsgegevens binnen de gemeente Hengelo. Het voorlopige onderzoeksrapport treft u hierbij aan. Het rapport in de huidige vorm geeft de Rekenkamercommissie aanleiding tot het stellen van een aantal vragen; de antwoorden op onderstaande vragen zullen nog worden verwerkt in het eindrapoort.

Toegang tot persoonsgegevens (vanaf werkplek, op afstand)
Volgens opgave van de gemeente aan de onderzoeker kunnen 547 van de 847 medewerkers op afstand (d.w.z. met een token of code) persoonsgegevens raadplegen. De digitale vragenlijst is uitgezet onder deze 547 medewerkers; 237 daarvan hebben de vragenlijst daadwerkelijk ingevuld. Van deze 237 geven echter 127 respondenten aan géén toegang te hebben tot persoonsgegevens (en 7 medewerkers hebben per e-mail aangegeven de vragenlijst niet te hebben ingevuld omdat ze op afstand geen toegang hebben tot persoonsgegevens). Het rapport laat ook zien dat slechts een deel van de respondenten daadwerkelijk en intensief gebruik maakt van de mogelijkheid op afstand persoonsgegevens te raadplegen en/of te wijzigen.

a. Hoeveel van de 847 medewerkers heeft (op de werkplek) toegang tot persoonsgegevens? Is het mogelijk hierbij een nadere uitsplitsing te geven naar het soort toegang (leesrecht/wijzigingsrecht, aard van de persoonsgegevens)?
b. Hoeveel van de 847 medewerkers heeft de mogelijkheid op afstand te werken?
c. Is de autorisatie die medewerkers hebben op de werkplek gelijk aan die bij het op afstand werken, m.a.w. hebben medewerkers die op de werkplek wel/geen toegang hebben tot persoonsgegevens ook wél/geen toegang tot persoonsgegevens bij het op afstand werken, of wordt er verschil gemaakt in de autorisatie?
d. Is er sprake van beleid ten aanzien van op afstand werken met persoonsgegevens? Welke criteria worden toegepast bij het al dan niet toekennen van de mogelijkheid op afstand te werken, c.q. op afstand met persoonsgegevens te werken? Wie kent deze mogelijkheid binnen de gemeente toe? Wordt de toekenning wel eens geweigerd?
e. Wordt op enigerlei wijze gemonitord in hoeverre medewerkers die op afstand kunnen werken (al dan niet met persoonsgegevens) daadwerkelijk gebruik maken van deze mogelijkheid, en hoe vaak? Is er sprake van een in duur beperkte toekenning?
f. Het onderzoek richt zich op de omgang met persoonsgegevens bij op afstand werken. Zijn er andere werkzaamheden (te denken valt bijvoorbeeld aan aanbestedingsprocedures) waarbij de gemeente speciale autorisatie voor medewerkers toepast? Indien dat het geval is, hoe wordt hiermee omgegaan bij op afstand werken?

Behandeld door
Mr. R.H. Plomp
Tel. 06-53677769

Gebruik van beveilingsmaatregelen

a. Is overwogen om de (relatief kleine groep) medewerkers die (daadwerkelijk) op afstand met persoonsgegevens werkt dit niet te laten doen op eigen apparatuur, maar deze medewerkers uit te rusten met laptops, die uitsluitend voor het telewerken kunnen worden gebruikt en voorzien zijn van een hoge mate van beveiliging (slaapfunctie/wachtwoord, geen mogelijkheid zelf software te downloaden, virus- en malware scanners, privacy screens)?
b. Is overwogen om medewerkers bij gebruik van eigen apparatuur te verplichten bepaalde minimale beveiligingsmaatregelen aan de eigen apparatuur te treffen? Is overwogen om op afstand werken met persoonsgegevens te beperken tot bepaalde locaties (bijvoorbeeld niet in de trein)?
c. Voor alle medewerkers geldt de Gedragscode ambtelijke integriteit 2004. Daarnaast is er het Beveiligingsplan Suwinet 2014 met bijbehorende gedragscode voor internet- en e-mailgebruik en de zorgvuldigheidsverklaring Suwi. Op welke wijze worden medewerkers die op afstand gaan werken ingelicht over de risico's van telewerken? Op welke wijze worden medewerkers geïnformeerd over de genoemde codes en hoe wordt omgegaan met die zorgvuldigheidsverklaring?

Tot slot

Heeft u nog aanvullende informatie die van belang kan zijn in het kader van dit onderzoek?

Wij stellen u namens de Rekenkamercommissie graag in de gelegenheid deze vragen te beantwoorden. Wij verzoeken u uw eventuele (schriftelijke) reactie op uiterlijk vrijdag 12 februari a.s. aan de Rekenkamercommissie te doen toekomen.

Met vriendelijke groet,

N.S. Groenendijk
(voorzitter)

R. H. Plomp.
(secretaris)

8.3 Antwoord college vragen Telewerken 12-02-2016.

Gemeente Hengelo

Postbus 18
7550 AA Hengelo

Aan de Rekenkamercommissie
T.a.v. de heer N.S. Groenendijk
Postbus 18
7550AA Hengelo

Onderwerp	**Zaaknummer**	**Uw kenmerk**	**Datum**
Onderzoeksrapport Telewerken Rekenkamer	2005572		12-02-2016

VERZONDEN 12 FEB. 2016

Geachte heer Groenendijk,

Dank voor de toezending van het eerste versie van het onderzoeksrapport "Telewerken Rekenkamer". Onderstaand zijn de antwoorden op uw vragen geformuleerd .

Toegang tot persoonsgegevens (vanaf werkplek, op afstand)

a. In de meeste applicaties wordt gewerkt met persoonsgegevens. Afgezien van de buitendienst (175 personen) hebben dus vrijwel alle overige (ongeveer 675) medewerkers toegang tot persoonsgegevens.
In het systeem waarin de BASISREGISTRATIE PERSONEN wordt bijgehouden zijn alle burgers van Hengelo opgenomen. Van de genoemde 675 zijn er ongeveer 30 met autorisatie om daarin te muteren.

b. 547 medewerkers van de gemeente Hengelo hebben een token of een code en kunnen dus op afstand werken.

c. Het systeem waarin de BASISREGISTRATIE PERSONEN wordt bijgehouden kan alleen worden gebruikt op kantoor. Afgezien daarvan hebben de medewerkers die beschikken over een token of een code "op afstand" dezelfde autorisatie als op het werk.

d. Er zijn beleidsregels met betrekking tot het op afstand werken met persoonsgegevens. De direct leidinggevende beslist of een medewerker een token krijgt en vraagt dit aan bij de afdeling ICT. De afweging wordt gemaakt door de betreffende leidinggevende.

e. Nee

f. Bij vele applicaties is sprake van speciale autorisaties. Een van de meest persoonsgevoelige systemen is Suwinet. Aan het raadplegen van de gegevens in dat systeem zijn specifieke procedures vastgesteld. Autorisaties voor Suwinet lopen voor bepaalde tijd (zolang je die

taak waarvoor je de autorisatie hebt gekregen nog vervult).

Gebruik van beveiligingsgegevens

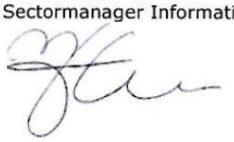
A. De gemeente Hengelo maakt gebruik van VDI. Door deze werkwijze is het niet relevant met welke apparatuur een medewerker op afstaand werkt. Met het VDI-concept wordt de beveiliging in het rekencentrum geregeld.

B. In het kader van het antwoord gegeven bij a is dit dus niet van toepassing. De medewerker kan zonder bezwaar op elke locatie werken.

C. Voor medewerkers geldt de gedragscode ambtelijke integriteit 2004. Voor het gebruik van Suwinet is een zorgvuldigheidsverklaring opgesteld. Iedere medewerker die toegang heeft tot Suwinet heeft deze zorgvuldigheidsverklaring getekend.
Met betrekking tot de uitgifte van een fysiek of een digitaal token (waarmee men dus kan telewerken) zijn wat betreft voorlichting en instructie geen extra zaken geregeld. Vooralsnog wordt uitgegaan van de bestaande regelingen.
Daarnaast kan de afdeling ICT het gebruik van de uitgegeven tokens monitoren. Bij geen gebruik van de tokens kan via het afdelingshoofd worden gevraagd het token weer in te leveren.
Bij afgifte van het token aan de medewerker is dit token meteen actief. Mocht het token binnen 7 weken niet worden gebruikt (geactiveerd) dan kan de medewerker het token niet meer gebruiken. Na deze periode wordt het token gedeactiveerd als de medewerker het langer dan drie maanden niet gebruikt.

We zien graag de definitieve versie van het onderzoeksrapport "Telewerken' tegemoet.

Met vriendelijke groet,
Burgemeester en Wethouders van Hengelo,
namens dezen,
Sectormanager Informatie en Faciliteiten



De heer M.G. Fleer

Vermeld altijd het zaaknummer als u contact opneemt met de gemeente.

Bezoekadres stadhuis
Burgemeester Jansenplein 1
Bezoekadres stadskantoor
Hazenweg 121

E-mailadres
gemeente@hengelo.nl
Telefoonnummer
14-074

Gemeente Hengelo

Postbus 18
7550 AA Hengelo

Rekenkamercommissie
T.a.v. de heer C. Hartendorp
Postbus 18
7550AA Hengelo

Onderwerp	**Zaaknummer**	**Uw kenmerk**	**Datum**
Reactie op onderzoek Telewerken	2065770		11 november 2016

Geachte heer Hartendorp,

Dank voor toezending van het definitieve rapport "Telewerken Hengelo". In uw brief met Onderwerp "Aanbieding resultaat onderzoek Telewerken" vraagt u naar een bestuurlijke reactie van het college op dit onderzoek.

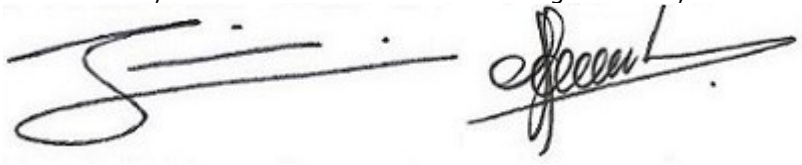
Op twee onderdelen van deze brief willen we graag reageren:

1. **Het onderdeel "Conclusies"**
   De gemeente Hengelo werkt met het VDI-Concept. Dit houdt in, dat wordt ingelogd op een virtuele computer op het netwerk van de gemeente. Dit concept biedt een optimaal veilige methodiek om thuis te kunnen inloggen en werken. Elke ambtenaar die thuis kan werken beschikt over een persoonlijke pincode. Deze code dient gecombineerd te worden met een inlogcode die verkregen wordt uit een token (hardware matig of softwarematig).
   Iedere keer dat wordt gestart met een nieuwe telewerksessie wordt een unieke inlogcode verstrekt. Tot slot moet met de inlognaam en het wachtwoord worden ingelogd.
   Deze methode van "thuis werken" is technisch veilig.
   Voor wat betreft de opmerking over de "automatische slaapfunctie" wordt opgemerkt , dat elke VDI-sessie na 15 minuten in de lockstand schiet. Dan dient men (ook in de thuissituatie) opnieuw aan te loggen.
   Verder willen wij erop wijzen, dat de gemeente Hengelo het onmogelijk heeft gemaakt thuis GBA en de Basisregistratie Personen te raadplegen.

2. **Het onderdeel "Aanbevelingen"**
   Net als andere gemeenten is Hengelo bezig met de invoering van de BIG (Baseline Informatiebeveiliging Gemeenten). Om aan de BIG te voldoen moet aan een veelheid van eisen worden voldaan. Een van de belangrijkste aandachtspunten hierbij is het ontwikkelen van bewustwording van informatieveiligheid. Een ander punt hierbij is zowel het hebben van procedures en gedragsregels als de kennis hebben van de procedures en gedragsregels.
   De aanbevelingen bij dit onderzoek Telewerken sluiten goed aan bij de aandachtspunten uit het project invoering van de BIG. Onderschreven wordt, dat op het terrein van i- bewustzijn de komende tijd nog stappen moeten worden gezet.
   In het kader van de Basisline Informatiebeveiliging Gemeente n (BIG) en de Meldplicht Datalekken is al een start gemaakt met de uitvoering van de aanbevelingen. Binnen de

gemeente Hengelo is een traject gestart om het onderwerp i-bewustzijn onder de aandacht te brengen. Dit traject vindt o.a. plaats binnen de domein Sociaal. Binnen de regio hebben de Twentse gemeenten gezamenlijk een toolbox i-bewustzijn ontwikkeld. Deze toolbox wordt medio november worden gelanceerd. Onderdelen van deze toolbox zullen in het Hengelose traject worden ingezet.
Het doel van dit traject in Hengelo is de bewustwording op het gebied van informatieveiligheid bij de organisatie te vergroten. Niet alleen bij de medewerker, maar ook bij bestuur en management. Doel bij bestuur en management is, dat zij het belang van informatieveiligheid inzien en uitdragen (het is een organisatieverantwoordelijkheid).
Voor de medewerkers is het traject gericht op meer operationele zaken (o.a. omgaan met wachtwoorden, phishing-mails, privacy). Gestart zal worden met een nulmeting om het huidige kennisniveau in kaart te brengen.
Dit onderwerp zal structureel op de agenda staan. Vanwege de veranderende omgeving zal de organisatie continue actuele kennis moeten hebben van het onderwerp informatieveiligheid. Jaarlijks zal dit onderwerp i-bewustzijn dan ook in het informatiebeveiligingsplan worden opgenomen.

Met vriendelijke groet,
Burgemeester en wethouders van Hengelo,
de secretaris, de burgemeester,



De heer J. Eshuis De heer S.W.J.G Schelberg

Bezoekadres
Hazenweg 121

E-mailadres
gemeente@hengelo.nl
Telefoonnummer
14-074

Rekenkamercommissie

Postbus 18
7550 AA Hengelo

Aan het college
P/a de heer J.Eshuis

Onderwerp	**Kenmerk**	**Datum**
Aanbieding resultaat onderzoek naar 'Telewerken'	2017_V009	30 maart 2017

Geacht college,

De Rekenkamercommissie Hengelo biedt u hierbij het resultaat aan van het in het jaar 2016 gehouden onderzoek naar Telewerken. Zoals ons onderzoeksprotocol voorschrijft versturen wij u hierbij het afschrift van de aanbiedingsbrief aan de gemeenteraad.

Behandelvoorstel
De rekenkamercommissie heeft de gemeenteraad voorgesteld om kennis te nemen van het uitgevoerde onderzoek en de daaruit voortkomende aanbeveling aan het college ter opvolging aan te bieden. Tevens stelt de rekenkamercommissie voor om in een–nader met u te organiseren- bijeenkomst door te spreken over het onderwerp "i-bewustzijn," waarin de door u voorgestelde structurele aanpak een plek krijgt.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Namens de Rekenkamercommissie gemeente Hengelo,
de secretaris,

C.H. Hartendorp

Bijlagen:
- Aanbiedingsbrief aan de gemeenteraad incl. bijlagen betreffende het Rekenkameronderzoek naar 'Telewerken'

Behandeld door
C.H. Hartendorp
074-245 9519