GEMEENTE Berg en Dal

Informatiebeveiligingsbeleid 2020-2023

Gemeente Berg en Dal

Vastgesteld: December 2019

Managementsamenvatting

Deze beleidsnota beschrijft het informatiebeveiligingsbeleid voor de jaren 2020 – 2023. Met dit 'Informatiebeveiligingsbeleid 2020-2023' zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en door te gaan met de stappen die in de voorgaande jaren zijn gezet. De basis voor dit beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO).

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen met als doel om de beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere gevoelige informatie te waarborgen binnen de organisatie. Het is de primaire verantwoordelijkheid van de afdelingsmanagers om de eigen processen, systemen en gegevens te beveiligen en hier voldoende middelen voor beschikbaar te stellen. En de benodigde maatregelen uit het jaarplan uit te voeren. De CISO adviseert, coördineert en ondersteund hierbij.

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de gehele levenscyclus van informatiesystemen. Het beperkt zich echter niet alleen tot de ICT en heeft betrekking op het bestuur, alle medewerkers, inwoners, gasten/bezoekers en externe relaties.

Informatie is een belangrijk bedrijfsmiddel. Beveiliging van deze informatie is nodig om een goede en veilige dienstverlening naar burgers, bedrijven en ketenpartners te garanderen. Daarom is het volgende doel gesteld voor de informatiebeveiliging:

De gemeente Berg en Dal wil *een betrouwbare partner* zijn voor inwoners, bedrijven en ketenpartners.

1. Inleiding

Deze beleidsnota beschrijft het informatiebeveiligingsbeleid voor de jaren 2020 - 2023. Deze vervangt het in 2016 vastgestelde ‘Gemeentelijk Informatiebeveiligingsbeleid 2016-2021’. Dit laatste beleid was nog gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De BIG wordt per 1 januari 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO). De BIO vormt de basis voor dit strategische beleid.

Met dit ‘Gemeentelijk Informatiebeveiligingsbeleid 2020-2023’ zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te borduren op stappen die in de voorgaande jaren gezet zijn. Deze nota is richtinggevend en kader stellend en wordt aangevuld met onderwerp-specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

2. Wat is Informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan het zorgen voor een bewust en veilig omgaan met informatie door het toepassen van een combinatie van organisatorische en technische maatregelen. Deze maatregelen zijn erop gericht de betrouwbaarheid van gemeentelijke processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens aantoonbaar te beschermen tegen al dan niet opzettelijk onheil.

De maatregelen borgen de juiste toegankelijkheid van informatie, het opbouwen en onderhouden van het bewustzijn over informatieveiligheid en, in het geval van incidenten, de eventuele gevolgschade (impact) van deze incidenten te beperken. Hoe vertrouwelijker informatie is, hoe meer maatregelen er getroffen moeten worden.

Bij het organiseren van informatiebeveiliging moeten de gemeenten voldoen aan de relevante wet- en regelgeving. Daarbij zal zoveel als mogelijk een goede balans gevonden moeten worden met het faciliteren van een optimale bedrijfsvoering en het bereiken van de dienstverleningsambities van de gemeenten.

Kernpunten van informatiebeveiliging zijn:

- **Beschikbaarheid (of continuïteit):** het zorgdragen voor het beschikbaar zijn van informatie en informatie-verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- **Integriteit:** het waarborgen van de correctheid (juistheid), volledigheid, tijdigheid van informatie en informatieverwerking oftewel het in overeenstemming zijn van informatie met de werkelijkheid;
- **Vertrouwelijkheid:** het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe bevoegd en geautoriseerd zijn.
- **Controleerbaarheid:** waarborgen dat de beoogde toegang tot gegevens en de juiste werking van systemen continu alsook achteraf te controleren is.

3. Onze ambitie

De hoofddoelstelling van dit informatiebeveiligingsbeleid is het richting geven aan het inrichten van informatiebeveiliging binnen de gemeente. Er worden doelen gesteld, verantwoordelijkheden beschreven, structuur geschetst en middelen aangegeven waarmee dit beleid moet worden vormgegeven.

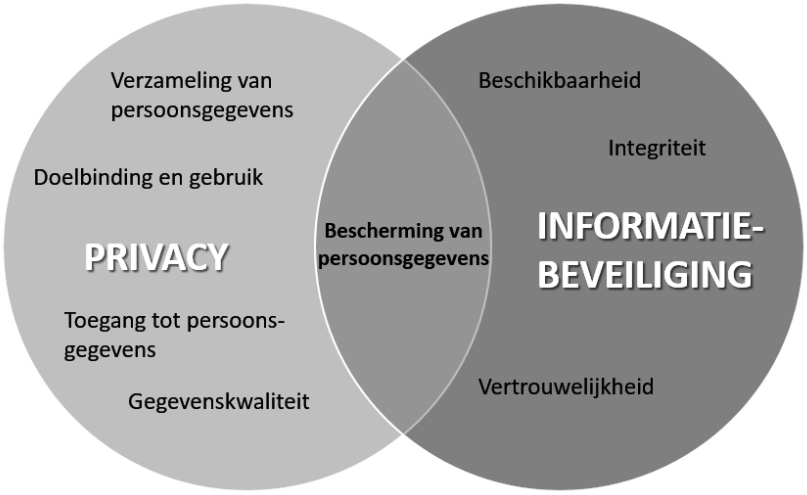
Informatie is een belangrijk bedrijfsmiddel dat de gemeente op gepaste wijze willen beschermen. Daarom is het volgende doel gesteld voor informatiebeveiliging:

> De gemeente Berg en Dal wilt *een betrouwbare partner* zijn voor onze inwoners, bedrijven en ketenpartners.

De gemeente zet daarom de komende jaren in op het optimaliseren van informatieveiligheid en het verder professionaliseren van de informatiebeveiligingsfunctie. Dit zodat inwoners, bedrijven en ketenpartners erop kunnen vertrouwen dat hun gegevens goed beveiligd worden en dit te kunnen verantwoorden. Dit doen wij binnen de geldende kaders.

4. Relatie tussen informatiebeveiliging en privacy

Informatiebeveiliging en privacy zijn termen die soms door elkaar worden gebruikt. Informatiebeveiliging en privacy zijn echter twee verschillende begrippen. Ze hebben wel een gemeenschappelijk raakvlak.



Informatiebeveiliging heeft een bredere scope dan de bescherming van enkel persoonsgegevens (gegevens privacy1). Informatiebeveiliging draait om de bescherming van alle gevoelige informatie tegen aantasting van integriteit, vertrouwelijkheid en beschikbaarheid. Bijvoorbeeld ook de beveiliging van politiek gevoelige of financiële gegevens. Een informatiebeveiligingsincident hoeft daarom niet altijd een datalek te betreffen. Dat is enkel het

[1] Gegevens privacy is één van de verschillende soorten privacy. Andere soorten zijn: lichamelijke privacy, huiselijke privacy en communicatie privacy.

geval wanneer er persoonsgegevens betrokken zijn.

Een adequate informatiebeveiliging (van persoonsgegevens) is wettelijk verplicht voor gemeenten om te kunnen voldoen aan de Algemene Verordening Gegevensbescherming (AVG), de Europese privacywet. Artikel 32 van de AVG schrijft voor dat:

"Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen".

Informatiebeveiliging maakt daarmee een onderdeel uit van de bescherming van persoonsgegevens. De AVG laat de inschatting van risico's en het bepalen van de benodigde maatregelen over aan de verwerkingsverantwoordelijke (de gemeente). Normenkaders als de BIO helpen de gemeente om de risico's goed in te schatten en de benodigde maatregelen te treffen. Hoe de gemeente omgaat met privacy en de AVG is beschreven in het privacybeleid van de gemeente Berg en Dal.

5. Landelijke ontwikkelingen en kaders

Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de voorgaande baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Van de afzonderlijke BIG, BIR, BIR2017, IBI en BIWA naar één gezamenlijke BIO. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek. Helder, actueel en veilig.

Baseline Informatiebeveiliging Overheid (BIO)

De BIO (Baseline Informatiebeveiliging Overheid) is per 2020 het nieuwe normenkader voor de gehele overheid. Het jaar 2020 geldt als overgangsjaar. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude BIG. Dat wil zeggen dat de afdelingsmanagers nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid. De BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Afhankelijk van de inschatting van het risico (risicoanalyse), zal het management op generiek of proces niveau een beveiligingsniveaumoeten bepalen.

De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO2 en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

[2] Deze principes worden tegelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG).

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes zijn nader uitgewerkt in bijlage 1.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

Overige normenkaders

Het Informatiebeveiligingsbeleid is een algemene basis. Vanuit domeinwetgeving kunnen aanvullende eisen worden gesteld. Deze worden in aanvullende beleidsdocumenten geformuleerd. Dit geldt o.a. voor de Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de Basisregistratie Personen (BRP) en Waardedocumenten (WD), de beveiligingsnorm DigiD of de Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Algemene verordening gegevensbescherming (AVG).

6. Rollen/taken en verantwoordelijkheden

In dit hoofdstuk wordt op hoofdlijnen uiteengezet welke rollen/taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de gemeenten en ketenpartners.

College van B&W

Het college van B&W is verantwoordelijk voor informatiebeveiliging binnen de gestelde kaders. Het college stelt hiervoor de beleidskaders en specifieke regelingen en procedures vast. Jaarlijks legt ze verantwoording af aan de gemeenteraad over informatiebeveiliging en de toepassing van het informatiebeveiligingsbeleid. Dit gebeurt in de paragraaf bedrijfsvoering in de jaarstukken.

Gemeenteraad

De gemeenteraad controleert het college van B&W op de naleving van het informatiebeveiligingsbeleid.

Directie en lijnmanagement

De directie en het lijnmanagement zijn verantwoordelijk voor het sturen op en monitoren van de uitvoering van het beleid. Ze stimuleren bewustwording over informatiebeveiliging bij medewerkers. Het vaststellen van doelen en middelen betreft informatiebeveiliging is aan de lijnmanagers gemandateerd. Zij zijn ook verantwoordelijk voor de afhandeling van data-incidenten binnen hun afdeling. De CISO adviseert en ondersteund in de uitvoering waar nodig.

Chief Information Security Officer (CISO)

De CISO ondersteunt, coördineert en adviseert vanuit een onafhankelijke positie over de te nemen maatregelen voor informatiebeveiliging. Hij rapporteert jaarlijks hierover aan het bestuur, de directie en het management.

Functionaris Gegevensbescherming (FG)

De FG coördineert de privacy werkzaamheden en adviseert de organisatie bij vragen of problemen. De FG is ook contactpersoon voor de Autoriteit Persoonsgegevens.

Beveiliging Implementatie Team (BIT)

Er zal een Beveiliging Implementatie team (BIT) ingericht worden onder de verantwoordelijkheid van de CISO. De CISO zal dit overleg organiseren en voorzitten. Deelnemers aan deze overleggen zijn de beveiligingsbeheerders vanuit de afdelingen. De commissie komt periodiek bij elkaar om de maatregelen uit het jaarplan voor informatiebeveiliging uit te voeren en daarover verantwoording af te leggen via ENSIA.

Beveiligingsbeheerders

Binnen de verschillende vakgebieden zijn beveiligingsbeheerders aangewezen. Zij zijn binnen hun vakgebied het eerste aanspreekpunt voor informatiebeveiligingsvragen. En zorgen ervoor dat de nodige taken worden uitgevoerd.

Controle en verantwoording (ENSIA)

De gemeente Berg en Dal verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek (Eenduidige Normatiek Single Information Audit). Dit betekent dat jaarlijks een ENSIA-coördinator wordt aangewezen. De ENSIA-coördinator zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA per gemeente wordt opgehaald bij de verantwoordelijke managers. De managers zijn er voor verantwoordelijk dat alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten wordt aangeleverd.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van de individuele gemeente aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad.

Middels deze verantwoording worden het college en de raad van de gemeente Berg en Dal geïnformeerd. De betrokkenheid van het bestuur is essentieel en laat zien dat de gemeente informatiebeveiliging serieus nemen.

Ketenpartners

De gemeente Berg en Dal neemt deel aan verschillende samenwerkingsverbanden zoals het Werkbedrijf Rijk van Nijmegen (WBRN) voor de uitvoering van de Participatiewet en het samenwerkingsverband Instituut Bijzonder Onderzoek (IBO) voor de fraude handhaving bij uitkeringen. Bij deze samenwerkingen is sprake van uitwisseling van informatie, waarvan de gemeente eigenaar of beheerder is. Informatiebeveiliging dient onderdeel te zijn van een samenwerkingsovereenkomst en deze mag niet strijdig zijn met het informatiebeveiligingsbeleid van de gemeente. Bijzondere aandacht is er voor de Gemeenschappelijke Regeling ICT Rijk van Nijmegen (iRvN) waarbij de iRvN de ICT (automatisering) voor de gemeente uitvoert. En ook de technische maatregelen vanuit de BIO zijn belegd en worden beheerd door de iRvN. Deze categorieën en regels per thema komen terug in de toegewezen rollen binnen de informatiebeveiligingsorganisatie van Berg en Dal.

Bijlage 1. Principes voor informatiebeveiliging

Gemeenten wisselen op alle beleidsterreinen informatie uit en beheren dat op vele manieren, zowel binnen de eigen organisatie, maar ook daarbuiten. Als professionele organisatie past hierbij dat de gemeente ook de beveiliging van informatie adequaat organiseert. Informatie moet immers beschikbaar, actueel, volledig en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien. Bij de uitwisseling moet de gemeente te allen tijde rekening houden met beveiligings- en privacyaspecten omdat ze een maatschappelijke en wettelijke verantwoordelijkheid heeft om de gegevens van de inwoners onder alle omstandigheden te beschermen.

Bestuurlijke aanvulling op de normen en regels

De principes gaan over waarden die de bestuurders en afdelingsmanagers zichzelf opleggen. Deze waarden zijn verbonden aan de waarden van de organisatie. Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de organisatie. Om dat te bewerkstelligen zijn de volgende principes belangrijk:

1. Bestuurders bevorderen een veilige cultuur

Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium. Zonder open cultuur waar iedereen vrij is om te spreken is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als de organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunnen we adequaat reageren op dreigingen en samenhangende risico's.

2. Informatiebeveiliging is van iedereen

Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.

Iedereen moet betrokken worden bij risicomanagement, in alle lagen van de organisatie. Maak gebruik van de kennis en verantwoordelijkheid van proces- en systeem eigenaren. Gebruik de Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en Controller als onafhankelijke adviseur en laat ze samenwerken in een risicoteam, waar u vanzelfsprekend ook zitting in heeft. Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen de organisatie. Goed uitgevoerd risicomanagement creëert waarde voor de organisatie omdat de kwaliteit van besluiten toeneemt en de kans op falen afneemt.

3. Informatiebeveiliging is risicomanagement

Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten. Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten. Maak afdelingsmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken over uw risicobereidheid. Afdelingsmanagers zijn verantwoordelijk voor de maatregelen en rapportage daarover.

4. Risicomanagement is onderdeel van de besluitvorming

Risicomanagement is onderdeel van alle besluiten en risicomanagement is 'chefsache'. U kunt als bestuurder alleen de juiste richting aangeven als informatie u bereikt. Door dreigingen en risico's mee te nemen in de vragen die u stelt aan uw afdelingsmanagers kunt u er in uw beslissingen ook rekening mee houden. Zo kunt u bijsturen voordat risico's manifest worden en escalatie voorkomen.

5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking

Het risicomanagementproces moet passen bij de organisatie en ondersteunen aan de organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.

6. Informatiebeveiliging is een proces

Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.

Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert. Indien u in uw risicomanagement geen rekening houdt met een veranderende omgeving, dan zijn uw maatregelen op termijn wellicht niet doeltreffend of doelmatig.

7. Informatiebeveiliging kost geld

Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.

Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieve- en/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt.

8. Onzekerheid dient te worden ingecalculeerd

De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele

beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.

Zonder goede informatie kunt u geen goede risico-inschattingen en besluiten nemen. Zonder goede en tijdige informatie bent u niet bekend met de risico's die uw organisatie loopt. Verbetering komt voort uit leren en ervaring

9. Risicobeheer wordt voortdurend verbeterd door leren en ervaring.

Risicomanagement gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert. Hoe goed de informatiehuishouding ook beveiligd is, incidenten zullen altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren bouwt u doorlopend aan het verhogen van uw digitale weerbaarheid.

10. Het bestuur controleert en evalueert

Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.

Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie omgaat met het onderwerp.

Medewerkers kunnen erop vertrouwen dat besluiten op bestuursniveau genomen worden, wanneer de situatie daar om vraagt.