

HANDREIKING INFORMATIEVEILIGHEID SOCIAAL DOMEIN

VISD is een programma van de VNG dat wordt uitgevoerd in samenwerking met KING

Opgesteld door VNG/KING
Datum 21 juni 2014
Versie 0.9

Colofon

Naam document

Handreiking informatieveiligheid sociaal domein

Versiebeheer

Het beheer van dit document berust bij het Programma Vervolg Informatievoorziening Sociaal Domein tot uiterlijk 31-12-2014.

Copyright

© 2014 Kwaliteitsinstituut Nederlandse Gemeenten (KING).

Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:

1. KING wordt als bron vermeld;
2. Het document en de inhoud mogen commercieel niet geëxploiteerd worden;
3. Publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door KING;
4. Iedere kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Rechten en vrijwaring

KING is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan KING geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. KING aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Leeswijzer

Dit product maakt onderdeel uit van het programma VISD (informatievoorziening Sociale Domein) en helpt gemeenten om hun informatiehuishouding op tijd en veilig aan te passen aan de nieuwe taken.

Doel

Het doel van dit document (informatiebeveiliging sociale domein) is het leveren van een overzicht van beveiligingsproducten die gemeenten helpen de juiste aandacht te geven aan de gewenste beveiligingseisen die noodzakelijk zijn. Deze beveiligingseisen zijn afhankelijk van onderkende risico's die voortvloeien uit de gewijzigde taakstelling en/of bedrijfsvoering en van invloed zijn op de processen, informatiesystemen en informatie en dienen te passen binnen het stamien van de geaccepteerde Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Het helpt gemeenten bij het borgen van goede en zorgvuldig en veilige gegevensuitwisseling en procesuitvoering en dit is een noodzakelijke randvoorwaarde.

Doelgroep

Dit document is van belang voor onder andere de informatiebeveiligingsfunctionarissen / Chief Information Security Officers (CISO) van gemeenten, de verantwoordelijke voor het inrichten van de nieuwe taken naar aanleiding van de decentralisaties binnen gemeenten en de betrokken architecten, proces- en informatiesysteemeigenaren bij de decentralisaties.

Inhoud

1	Inleiding	6
1.1	Sectorale normenkaders	6
1.2	Informatiebeveiligingsdienst	7
1.3	Informatiebeveiliging en de decentralisaties	7
1.4	Hoe te lezen	8
2	Programma van eisen	9
2.1	inleiding	9
2.2	Archetype	9
2.3	Belang thema informatieveiligheid	10
2.4	Uitwisseling (persoons)gegevens binnen het sociale domein	10
3	Informatieveiligheid	13
3.1	Wat is informatieveiligheid?	13
3.2	Veiligheid, privacy en beveiliging in het kader van 3D	13
3.3	Verantwoordelijkheden en afstemming	15
3.4	Proces informatiebeveiliging bij decentralisaties	16
4	Aan de slag	23
4.1	Algemeen en archetype onafhankelijk	23
4.2	Archetype 1 Transitie-proof	24
4.3	Archetype 2 Totaal integraal	36
4.4	Archetype 3 Geclusterd integraal	48
4.5	Archetype 4 Integraal in 2e instantie	60
4.6	Archetype 5 Geclusterde integraliteit elders	72
5	Organisaties in het kader van informatieveiligheid	85
5.1	Informatiebeveiligingsdienst voor gemeenten	85
5.2	Nationaal Cyber Security Centrum (NCSC)	88
5.3	Taskforce Bestuur en Informatieveiligheid Dienstverlening	89
5.4	Centrum voor Informatiebeveiliging en Privacybescherming	90
5.5	College bescherming persoonsgegevens	91
5.6	Overige organisaties	93
5.7	Ondersteunde documenten	93

1 Inleiding

Gemeenten worden vanaf 1 januari 2015 verantwoordelijk voor jeugdzorg, werk en inkomen en zorg aan langdurig zieken en ouderen.¹ Een deel van deze taken heeft de gemeente nu ook al, een deel neemt zij over van de Rijksoverheid. Deze (drie) decentralisaties bieden gemeenten een kans om de zorg voor kwetsbare inwoners, vanuit één visie en in samenhang uit te voeren. Dan ontstaan er mogelijkheden om gezinnen beter te ondersteunen dan nu het geval is. Met een integrale aanpak kan maatwerk worden geleverd en dienstverlening van de gemeente worden gestroomlijnd. Integrale aanpak betekent ook informatie delen en processen optimaliseren, niet alleen tussen de interne afdelingen maar ook tussen diverse ketenpartners.

Als professionele organisatie past hierbij dat gemeenten ook de beveiliging van informatie professioneel organiseren. Informatie moet immers beschikbaar en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien. Bij de uitwisseling moeten gemeenten voldoende rekening houden met beveiligings- en privacyaspecten en de huidige wet- en regelgeving.

De Wet bescherming persoonsgegevens (Wbp) bevat regels voor het verwerken van persoonsgegevens, waarbij de nadruk ligt op het geautomatiseerd verwerken van persoonsgegevens. Hoofdregel is dat persoonsgegevens alleen in overeenstemming met de wet en op behoorlijke, noodzakelijke en zorgvuldige wijze worden verwerkt. De Wbp staat niet op zichzelf. In materiewetten worden nadere regels gesteld ten aanzien van het verwerken van die persoonsgegevens. Voorbeelden hiervan zijn de wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI)², de wet Geneeskundige Behandelingsovereenkomsten (WGBO)³ en de Archiefwet⁴. In deze handreiking wordt niet ingegaan op de specifieke privacy- en de doelbindingsaspecten die in de Wbp en andere materiewetten zijn opgenomen, maar wel op de beveiligingsaspecten die hieruit voortkomen. Deze beveiligingsaspecten worden vastgesteld met behulp van een Privacy Impact Assessment (PIA).⁵

1.1 Sectorale normenkaders

Het belang van beveiliging van persoonsgegevens neemt toe door de groeiende omvang van het aantal uitgewisselde (gevoelige)gegevens, de toename van het aantal aansluitingen en het breder gebruik van deze persoonsgegevens. Hierdoor wordt de beveiliging van gegevens steeds complexer. Een belangrijke vraag die gemeenten zichzelf moeten stellen is; “Voldoet onze organisatie aan de eisen met betrekking tot vertrouwelijkheid (persoonsgegevens kunnen alleen worden verwerkt door daartoe gemachtigde personen), transparantie (kan aangetoont worden dat de geleverde diensten voorzien zijn van effectieve beveiligingsmaatregelen), juistheid, nauwkeurigheid en noodzakelijkheid?”

Het organisatiemodel dat een gemeente voor ogen heeft, beïnvloedt de mate van complexiteit rondom de informatieveiligheid. Gemeenten die ervoor kiezen om vanaf 1 januari 2015 ‘transitie-proof’ te zijn, krijgen in mindere mate te maken met een gewijzigde inrichting en uitvoering van hun informatieveiligheidsbeleid, voor zover de gemeente dit al (optimaal) heeft

¹ <http://www.rijksoverheid.nl/onderwerpen/gemeenten/decentralisatie-van-overheidstaken-naar-gemeenten>

² <http://wetten.overheid.nl/BWBR0013060/>

³ <http://wetten.overheid.nl/BWBR0007021/>

⁴ <http://wetten.overheid.nl/BWBR0007376/>

⁵ Zie voor meer informatie paragraaf 2.4 uitwisseling (persoons)gegevens binnen het sociale domein.

ingericht.⁶ Gemeenten die voor een totale integrale aanpak kiezen krijgen op dit moment te maken met verschillende wet- en regelgevingen en de eventueel daarbij behorende normenkaders.⁷

In dit document zullen we ook nader ingaan op de verhoudingen tussen de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de sectorale normenkaders.

1.2 Informatiebeveiligingsdienst

Sinds januari 2013 is de Informatiebeveiligingsdienst voor gemeenten (IBD)⁸ operationeel. De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger niveau te tillen. De IBD heeft drie concrete doelen. Allereerst het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging. In de tweede plaats het leveren van integrale coördinatie en concrete ondersteuning op gemeentespecifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging. En tot slot, gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alledag naar een hoger niveau te tillen.

Om de informatieveiligheid goed te richten dan wel naar een hoger niveau te tillen stelt het IBD gemeenten een toolkit ter beschikking. Deze toolkit bevat onder meer de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en operationele producten behorend bij de BIG. Met behulp van deze operationele producten kan iedere gemeente tot implementatie van de BIG overgaan.

1.3 Informatiebeveiliging en de decentralisaties

De BIG is een richtlijn die een totaalpakket aan informatiebeveiligingsmaatregelen omvat die voor iedere gemeente geldt. Deze baseline is opgezet rondom bestaande normen; de NEN/ISO 27002:2007 en NEN/ISO 27001:2005. Deze standaard is voor de Nederlandse Overheid gekozen en algemeen aanvaard als de norm voor informatiebeveiliging. Voor specifieke maatregelen is voor het tactische deel van de baseline ook gebruik gemaakt van de Wbp, de SUWI-wet, Gemeentelijke Basisadministratie (GBA)⁹, Basisregistraties Adressen en Gebouwen (BAG)¹⁰ en Paspoortuitvoeringsregeling Nederland (PUN)¹¹.

De drie decentralisaties voor jeugd, zorg en werk zijn niet als uitgangspunt genomen bij het opstellen van de BIG waardoor het waarschijnlijk nodig is om voor de drie decentralisaties additionele specifieke maatregelen te treffen.¹² Binnen de drie gedecentraliseerde domeinen wordt (zeer) privacygevoelige informatie van burgers verzameld, verwerkt en uitgewisseld. Er is gemeenten en partners veel aan gelegen om deze informatie goed te beveiligen.

⁶ Transitie-proof is een van de vijf inrichtingsmodellen (archetype) en wordt toegelicht in paragraaf 2.2.

⁷ Totaal integraal is een van de vijf inrichtingsmodellen (archetype) en wordt toegelicht in paragraaf 2.2.

⁸ <https://www.ibdgemeenten.nl/>

⁹ De GBA-wet (<http://wetten.overheid.nl/BWBR0006723/>) is per 6 januari 2014 vervallen vanaf dat moment is de wet Basisregistratie Personen (BRP) (<http://wetten.overheid.nl/BWBR0033715/>) in werking getreden.

¹⁰ <http://wetten.overheid.nl/BWBR0023466/>

¹¹ <http://wetten.overheid.nl/BWBR0012811/>

¹² Om vast te stellen dat het niveau van de BIG voldoende is, moet een baselinetoets uitgevoerd worden (zie paragraaf 3.3 'Proces informatiebeveiliging bij decentralisaties'.

Het doel van dit document is de veilige gegevensverwerking en -uitwisseling ook binnen de drie gedecentraliseerde domeinen te waarborgen en om mogelijke additionele informatiebeveiligingsrisico's die door de decentralisatie kunnen ontstaan voor gemeenten en partners te verminderen. Deze additionele risico's moeten worden geanalyseerd. Om de informatiebeveiligingsrisico's te verminderen dienen passende maatregelen te worden geselecteerd die genomen moeten worden bij gemeenten, partners, op knooppunten, op koppelvlakken en bij en/of door leveranciers. De maatregelen kunnen technisch, procedureel, organisatorisch of beleidsmatig van aard zijn (integraliteit) en dienen aan te sluiten bij het niveau van gevoeligheid en de kwetsbaarheid van de informatie.

1.4 Hoe te lezen

Afhankelijk van de informatiebeveiligingsrisico's en de door de gemeente gemaakte inrichtingskeuzes voor de drie decentralisaties zijn mogelijk additionele specifieke maatregelen nodig ten opzichte van de BIG. Om gemeenten handvatten te bieden welke relevante documenten kunnen worden gebruikt om informatiebeveiliging vanaf het begin mee te nemen wordt een koppeling gelegd met de aandachtspunten vanuit de decentralisaties. In dit document wordt een overzicht gegeven van (operationele) documenten die gemeenten helpen bij de implementatie van de beveiligingsmaatregelen. Uiteraard is hierbij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) het uitgangspunt.

Structuur

De indeling van dit document is als volgt:

Hoofdstuk 1 geeft de algemene inleiding over de Informatiebeveiligingsdienst en informatiebeveiliging in relatie tot de decentralisaties.

Hoofdstuk 2 gaat kort in op het programma van eisen, de verschillende Archetype en Thema's.

Hoofdstuk 3 geeft een uitgebreidere beschrijving van informatieveiligheid in het sociale domein.

Hoofdstuk 4 geeft een overzicht van relevante informatiebeveiligingsonderwerpen en een koppeling van deze onderwerpen met de door gemeenten te gebruiken producten.

In hoofdstuk 5 wordt een beschrijving gegeven van de producten op het gebied van informatiebeveiliging, waar in hoofdstuk 4 naar wordt gerefereerd, en de organisaties die deze producten hebben of op korte termijn worden gepubliceerd.

2 Programma van eisen

2.1 inleiding

Gemeenten zijn op zoek naar ICT-voorzieningen en systemen die hun werk kunnen ondersteunen. De markt confronteert gemeenten met hun oplossingen. Ter ondersteuning van de verwerving van een “regiesysteem” is een Programma van Eisen (versie 0.92) beschikbaar. Het doel van dit Programma van Eisen is niet het beschrijven van de functionaliteiten die benodigd zijn voor de feitelijke uitvoering van ondersteuningsmaatregelen, maar voor de regie daarover. Het PvE richt zich daarom primair op een informatievoorziening ten behoeve van de regiefunctie in het sociale domein.

Bij het verwerven van een nieuw informatiesysteem of het (laten) aanpassen van bestaande informatiesystemen dient de gemeente te weten waaraan dit informatiesysteem minimaal moet voldoen. Feitelijk gebruik en inrichting zullen per gemeente kunnen verschillen. Gemeenten moeten eerst een goed beeld vormen van het eigen beleid en de inrichting van hun eigen bedrijfsvoering en de informatieveiligheid. Het programma van Eisen kan daarna op het gekozen beleid, bedrijfsvoering en informatieveiligheid worden aangepast.

Het PvE is dus een basis voor een aanbestedingsbestek - of een aanzet tot een functioneel ontwerp wanneer de gemeente zelf reeds aanwezige applicaties gaat inzetten. Voor een specifieke gemeente zal een en ander nog moeten worden herschreven naar de eigen specifieke situatie.

In dit hoofdstuk wordt beschreven welke activiteiten de gemeente moet uitvoeren om de risico's vast te stellen die voortvloeien uit de gewijzigde taakstelling en/of bedrijfsvoering.

2.2 Archetype

Alle gemeenten zullen op een manier vorm moeten gaan geven aan de drie decentralisaties. Gemeenten zullen dit doen op een wijze passend bij hun lokale situatie, de kenmerken van hun bewoners en hun visie op het sociaal domein en dienstverlening. Hierdoor ontstaan lokale verschillen maar ook tot overeenkomsten. Op basis van deze overeenkomsten zijn een aantal archetypen (zie document Archetypen in het sociaal domein) uitgewerkt. Deze archetypen schrijven in de basis de inrichtingsmodellen die zich in den lande aftekenen. Geen enkele archetype zal één op één op een gemeente passen. Om de risico's te kunnen vaststellen, zullen gemeenten allereerst moeten vaststellen welke vorm van bedrijfsvoering (archetype) voor ogen staat. De volgende archetypes worden onderscheiden:

- Archetype 1 Transitie-proof.
- Archetype 2 Totaal integraal
- Archetype 3 Geclusterd integraal
- Archetype 4 Integraal in 2e instantie
- Archetype 5 Geclusterde integraliteit elders

Meer informatie met betrekking tot bovenstaande archetypen is te vinden op de volgende websites

<https://www.visd.nl/visd/producten/producten-actielijn-programma-van-eisen> en http://www.gemmaonline.nl/index.php/Uitgebreid_overzicht_archetypen

Thema's

Ter ondersteuning van de beleidskeuze is een aantal thema's uitgewerkt:

- Signalering en melding
- Registratie en Zaakgericht werken
- Informatieveiligheid
- Sturing & bekostiging

Deze thema's bieden gemeenten handvatten voor de beleidskeuze procesinrichting. In de volgende paragraaf wordt het thema informatieveiligheid kort toegelicht.

Meer informatie met betrekking tot bovenstaande thema's is te vinden op de website <http://www.visd.nl/>

2.3 Belang thema informatieveiligheid

De komende decentralisaties maken het voor gemeenten mogelijk om de dienstverlening beter, integraler en meer in samenhang te organiseren, maar dit moet natuurlijk wel veilig gedaan worden.

Het uiteindelijke doel van het project 'informatieveiligheid sociale domein' is het leveren van beveiligingsproducten die gemeenten helpen de juiste aandacht te geven aan de noodzakelijke beveiligingseisen. Deze beveiligingseisen zijn afhankelijk van onderkende risico's die voortvloeien uit de gewijzigde taakstelling en/of bedrijfsvoering. Deze zijn van invloed op de processen, informatiesystemen en informatie. Ze dienen te passen binnen het stramien van de geaccepteerde Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Het helpt gemeenten bij het borgen van goede, zorgvuldige en veilige gegevensuitwisseling en procesuitvoering. Dit is een noodzakelijke randvoorwaarde.

Goed en zorgvuldig gegevensdelen in het sociale domein vraagt namelijk ook aandacht van een goede beveiliging die betrekking heeft op processen & organisatie, kennis & bewustwording en gedrag.

2.4 Uitwisseling (persoons)gegevens binnen het sociale domein

Zoals eerder aangegeven zullen door de decentralisaties gemeenten meer (gevoelige) persoonsgegevens van burgers gaan verwerken. Daarbij gaat het ook om medische en strafrechtelijke persoonsgegevens. Bovendien zullen gegevens uit het ene sociale domein ook in een ander domein worden gebruikt. Om dit op een adequate manier te kunnen beveiligen zullen de privacyrisico's nauwkeurig in kaart moeten worden gebracht. Een middel om deze risico's en privacywaarborgen van burgers in kaart te brengen is het uitvoeren van een Privacy Impact

Assessment (PIA).¹³ In paragraaf 3.4 'Proces informatiebeveiliging bij decentralisaties' wordt een toelichting gegeven op het operationele product 'Privacy Impact Assessment' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), die door gemeenten kan worden uitgevoerd.

Hierbij is het van belang om te weten uit welke bronnen deze gegevens betrokken kunnen worden, wie is de eigenaar van deze gegevens (broneigenaar) en hoe partijen (gemeenten, ketenpartners en burgers) deze informatie met elkaar kunnen uitwisselen.

Risico's

Risico's die in de 'Handreiking - Financiën en de 3 decentralisaties' van het ministerie van Binnenlandse Zaken zijn onderkend, zijn onderverdeeld in: sociaal inhoudelijk, personeel, juridisch, informatisering, economie / financieel, politiek, organisatie & leiderschap en samenwerking.¹⁴ Relevante risico's met betrekking tot informatiebeveiliging en privacy zijn:

- Sociaal inhoudelijk
 - Dienstverlening komt niet op het gewenste niveau
- Personeel
 - Betrokken medewerkers implementeren de gewenste planning & controle maatregelen onvoldoende.
- Juridisch
 - Hulpverleners krijgen privégegevens onder ogen.
 - Het werkproces (en de daarvoor gebouwde ICT) blijkt strijdig met de Wet Bescherming Persoonsgegevens (Wbp).
 - De proeftuinen gaan van start zonder duidelijkheid over (on)mogelijkheden vanwege privacywetgeving.
 - De privacy is onvoldoende geborgd in de manier waarop de informatiesystemen worden ingericht en bijhorende handelswijze.
 - De inkoopcontracten blijken juridische onjuistheden te bevatten.
- Informatisering
 - De ICT-voorziening voldoet niet aan de gewenste kwaliteit.
 - De gemeente slaagt er niet in om per 1 januari 2015 goed werkende automatiseringssystemen te implementeren.
 - Meer personen kunnen informatie (van cliënten) raadplegen en muteren dan degenen die daartoe vanuit hun functie geautoriseerd zijn.
- Economisch/financieel
 - De planning & controlcyclus prioriteert de werkzaamheden verkeerd.
 - Het kwaliteitsniveau lijdt te veel onder de aandacht voor het budget
- Samenwerking
 - De afstemming met ketenpartijen en concernpartijen is onvoldoende. Ketenpartijen hebben meer invloed op projectresultaten dan vooraf gedacht.

Juridisch kader

Gegevens, die gemeenten en zorgaanbieders in hun dossiers registreren, hebben veelal een medische of justitiële achtergrond. De organisatorische en technische beveiliging van de gegevens, en de bescherming van de privacy van de betrokkenen is van absoluut belang.

¹³ Het College bescherming persoonsgegevens (CBP) dringt bij het Rijk aan om een Privacy Impact Assessment (PIA) uit te voeren die de risico's en privacywaarborgen in kaart brengt (http://www.cbppweb.nl/Pages/pb_20131030_privacyrisico-taken-gemeenten.aspx)

¹⁴ http://gemeentenvandetoekomst.nl/item/Handreiking-Financin-en-de-3-decentralisaties_021153

Er zal een gedegen juridisch kader moeten komen die de gegevensuitwisseling over de verschillende deeldomeinen mogelijk maakt, tezamen met een helder afwegingskader over wat wel en niet is toegestaan ten behoeve van één gezin, één plan, één regie.

Voor uitwisseling van persoonsgegevens is dan ook een wettelijke basis vereist. Bijvoorbeeld tussen bestuursorganen en uitvoeringsinstanties. Bij deze samenwerkingsverbanden moet steeds goed inzichtelijk zijn wie de verantwoordelijke¹⁵ en wie de bewerker¹⁶ van persoonsgegevens is. De richtlijnen van het College Bescherming Persoonsgegevens (CBP) over Informatie delen in samenwerkingsverbanden zijn hierbij leidend.¹⁷

De wet- en regelgeving met betrekking tot de decentralisaties¹⁸ gaan er onder andere vanuit dat informatie slechts mag worden gebruikt voor die doelen waarvoor zij verzameld zijn. Om zicht te krijgen op de aspecten van gegevensbescherming bij de uitvoering van de wetten is een analyse nodig. Een analyse van gegevens die voor verschillende processen nodig zijn, de bronnen waar die gegevens vandaan moeten komen, de vraag of er een wettelijke grondslag is en die het gebruik van die gegevens toestaat (zie hiervoor ook paragraaf 3.4 'Proces informatiebeveiliging bij decentralisaties').

Hieronder een niet limitatieve opsomming van relevante algemene en materiewetten met betrekking tot de drie decentralisaties.

- Algemene wet- en regelgeving:
 - Wet bescherming persoonsgegevens¹⁹
 - Wet algemene bepalingen burgerservicenummer²⁰
- Materiewetten:
 - Wet maatschappelijke ondersteuning 2015²¹
 - Invoeringswet Participatie²²
 - Jeugdwet²³

Bij iedere gegevensuitwisseling zullen (in het kader van de Wbp) de volgende vragen beantwoord moet worden:

- Welke gegevens worden in welke situaties tussen welke partijen uitgewisseld?
- Wat is het doel van die uitwisseling?
- Waarom is de uitwisseling noodzakelijk? Houdt hierbij rekening met proportionaliteit.
- Wie is de geveenseigenaar?
- Wie is de bewerker?

¹⁵ De verantwoordelijke in de zin van de Wbp is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (Artikel 1 sub d). De verantwoordelijke bepaalt welke persoonsgegevens, voor welk doel, op welke manier en met welke middelen worden verwerkt.

¹⁶ 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 overeenkomstig 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 gegevens enz.

¹⁷ http://www.privacyindezorg.nl/assets/files/inf_va_samenwerkingsverbanden.pdf

¹⁸ Wet maatschappelijke ondersteuning (Wmo) 2015, Invoeringswet Participatie, Jeugdwet en de Wet bescherming persoonsgegevens (Wbp)

¹⁹ http://www.eerstekamer.nl/wetsvoorstel/25892_wet_bescherming

²⁰ http://www.eerstekamer.nl/wetsvoorstel/30312_wet_algemene_bepalingen

²¹ http://www.eerstekamer.nl/wetsvoorstel/33841_wet_maatschappelijke

²² http://www.eerstekamer.nl/wetsvoorstel/33161_invoeringswet

²³ http://www.eerstekamer.nl/wetsvoorstel/33684_jeugdwet

3 Informatieveiligheid

3.1 Wat is informatieveiligheid?

Door de toenemende digitalisering is het zorgvuldig omgaan met de informatie en gegevens van burgers en organisaties voor gemeenten van groot belang. Uitval van computers of telecommunicatiesystemen, het in ongerede raken van gegevensbestanden of het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens heeft ernstige gevolgen voor de continuïteit van de bedrijfsvoering en het primaire proces. Een betrouwbare, beschikbare en correcte informatiehuishouding is essentieel voor de dienstverlening van gemeenten. Het is niet ondenkbaar dat hieraan ook politieke consequenties verbonden zijn of dat het imago van de gemeente, en daarmee van de overheid in het algemeen, wordt geschaad. Om informatieveiligheid (doel) te waarborgen wordt gebruik gemaakt van informatiebeveiliging (maatregel).²⁴

Informatiebeveiliging is de verzamelnaam voor de processen die worden ingericht om de betrouwbaarheid van gemeentelijke processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk incidenten. Hierbij wordt onderscheid gemaakt tussen beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid.

- **beschikbaarheid:** het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen (informatiesystemen) op de juiste tijd en plaats voor de gebruikers. Hierdoor hebben burgers en bedrijven toegang tot voor hen relevante informatie en hebben medewerkers toegang tot relevante informatie om hun werk en hun dienstverlening richting onze burgers en bedrijven ongestoord voort te zetten.
- **integriteit:** het waarborgen van de correctheid, volledigheid, tijdigheid (actualiteit) en controleerbaarheid van informatie en informatieverwerking. Voor een efficiënte en effectieve bedrijfsvoering is het voor de gemeente van belang dat de correcte informatie tijdig aanwezig is in de informatiesystemen. Maar ook dat zelfs na een bepaalde periode de correctheid en de volledigheid van informatie eenvoudig gecontroleerd kan worden (=controleerbaarheid).
- **vertrouwelijkheid:** het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.
- **controleerbaarheid:** de mogelijkheid om met voldoende zekerheid vast te kunnen stellen of wordt voldaan aan de eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

3.2 Veiligheid, privacy en beveiliging in het kader van 3D

Voor het ondersteunen van de 'eigen kracht', krijgt de burger toegang tot zijn of haar (gezins)dossier. Met behulp van deze 'toegang' kan de burger waar en wanneer mogelijk zelf regie voeren. Desgewenst kan een mantelzorger door de burger gemachtigd worden van deze toegang gebruik te maken (bijvoorbeeld aan zelf afspraken plannen en combineren en het voeren van persoonlijk budgetbeheer). De burger ziet welke ondersteuning wordt gegeven en

²⁴ Zie hiervoor ook het operationele product 'Voorbeeld Informatiebeveiligingsbeleid Gemeenten' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) dat algemene beleidsuitgangspunten over informatiebeveiliging geeft.

welke (informele) zorg wordt georganiseerd door zijn/haar sociale omgeving. De burger ziet welke informatie over hem/haar/het gezin uitgewisseld wordt tussen de gemeente en de tweedelijns ondersteuners (inkijk).

Voor de regierol van de gemeente bij multiprobleemgezinnen²⁵ is een totaaloverzicht van alle betrokken ondersteuners (professionele én informele zorg) nodig in de vorm van de registratie van één plan. Voor de regierol is het tevens noodzakelijk dat de regisseur de voortgang van de hulpverlening bewaakt en er met de diverse ondersteuners (professioneel en informeel) en de burger kan worden gecommuniceerd (berichtgeving). Deze communicatie kan gestructureerd (verstrekking start dienstverlening, ketenbericht) of ongestructureerd (bijvoorbeeld stellen en beantwoorden van een vraag) plaatsvinden.

Persoonsgegevens in de zin van de Wet Bescherming Persoonsgegevens (Wbp) zijn alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.²⁶ Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.²⁷ De gevoeligheid hierbij is dat de veiligheid van een geïdentificeerde natuurlijk persoon in het geding kan zijn. Bijvoorbeeld doordat persoonsgegevens uitlekken of onterecht worden verwerkt bestaat de mogelijkheid dat de betrokkene gehanteerd wordt en fysieke en/of geestelijke schade oploopt.

Privacy en beveiliging

Privacy en beveiliging zijn zeer belangrijke uitgangspunten voor de te organiseren informatievoorziening. Het gaat immers om vertrouwelijke informatie over mensen in kwetsbare situaties.

Zowel voor alle informatie-uitwisseling tussen professionals als ook voor de inkijsfunctionaliteit door de burger (inzage in het eigen dossier) geldt dat privacy voorop staat. Ongeoorloofde toegang door derden tot bijvoorbeeld het dossier (doordat men zich voordoeft als de burger zelf) moet te allen tijde voorkomen worden. Dit vraagt niet alleen om strenge beveiliging in de zin van autorisaties op het dossier, het vereist met name aandacht voor de organisatorische kant van de informatiebeveiliging en voor een sluitende identificatie/authenticatie van de burger voor de toegang tot het informatiesysteem.

Dit geldt ook voor de regisseur, professional en/of medewerker, zeker als die in het veld toegang moeten hebben tot nog meer informatie dan de burger zelf.

Zowel bij regievoering als voor de informatiehuishouding moet rekening worden gehouden met reguliere trajecten (uitgangspunt: de burger zelf kan veel inzien en eventueel corrigeren; hij/zij heeft het heft zelf in handen) en trajecten waar sprake is van dwang (waar geen toestemming van de burger is vereist en de burger veelal zelf veel minder inzage en geen correctierecht zal of mag hebben in het eigen dossier).

Opdrachtverstrekking

²⁵ Een multiprobleemgezin is een gezin dat langdurig kampt met een combinatie van sociaal-economische en psychosociale problemen. De gezinnen hebben problemen op verschillende gebieden: huishouden, opvoeding, maatschappelijke positie (werkloosheid, financiële problemen), individueel functioneren van de gezinsleden en de relatie tussen de (ex-)partners. De problemen zijn meervoudig, complex en onderling verweven. Hulpverleners hebben vaak moeite deze gezinnen te helpen en vaak zijn er veel verschillende hulpverleners betrokken.

²⁶ Een natuurlijk persoon kan direct of indirect identificeerbaar zijn. Direct identificeerbaar is men aan de hand van naam, adres en woonplaats (NAW-gegevens), een persoonsnummer, een pseudo-identiteit die in brede kring bekend is of een biometrisch kenmerk (zoals een vingerafdruk). Indirect identificeerbaar is men aan de hand van andere unieke kenmerken of attributen of een combinatie van beide, waaruit voldoende informatie is af te leiden voor de identificatie.

²⁷ <http://www.cbpweb.nl/wbpnaslag/1/Paginas/wbp-artikel-1-a.aspx>

Bij de opdrachtverstrekking is het belangrijk dat gemeenten de privacy en informatiebeveiliging borgen. Daarom raden wij aan om bij uit- of aanbesteding van gegevensverwerking aan een private partij contractuele afspraken te maken over²⁸:

- Het serviceniveau. Welke kwaliteits- of prestatieniveaus horen bij de te leveren producten en diensten.
- Het niveau van informatiebeveiliging.
- Continuïteit van dienstverlening.
- Eigenaarschap van de gegevens.
- Wie heeft toegang tot de gegevens.
- Een exitstrategie. Zorg dat een gecontroleerde overgang naar een andere partij mogelijk is bij einde contract. Bijvoorbeeld datamigratie.
- Ondernemingsrechtelijke structuur met het oog op voorkoming van doorgifte van persoonsgegevens aan derde landen.

3.3 Verantwoordelijkheden en afstemming

Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd en belegd binnen gemeenten.²⁹

- Het **college van Burgemeester en Wethouders** (B&W) is integraal verantwoordelijk voor de beveiliging (beslissende rol) van informatie binnen de werkprocessen van de gemeente. Het college van B&W stelt kaders voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders.
- De **Directie** (in sturende rol) is verantwoordelijk voor kaderstelling en sturing. De directie stuurt op concern risico's, controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden en evalueert periodiek beleidskaders en stelt deze waar nodig bij.
- De **afdelingen binnen de gemeente** (in vragende rol) zijn verantwoordelijk voor de integrale beveiliging van hun organisatieonderdelen. De clusterdirectie:
 - stelt op basis van een expliciete risicoafweging betrouwbaarheidseisen voor zijn informatiesystemen vast (classificatie);
 - is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
 - stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
 - rapporteert over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de managementrapportages.
- De **gemeentelijke Service Organisatie** of gelijkwaardig (Bedrijfsvoering, Facilitaire zaken, Huisvesting, Human Resource / Personeel & Organisatie, Juridische Zaken, et cetera, in uitvoerende rol) is verantwoordelijk voor uitvoering.

Met deze verschillende verantwoordelijke partijen binnen de gemeente dient afstemming plaats te vinden met betrekking tot de (extra) beveiligingsmaatregelen die getroffen moeten worden. De maatregelen dienen belegd te worden binnen de 'juiste' organisatorische eenheid. Zie hiervoor ook paragraaf 3.4 'Proces informatiebeveiliging bij decentralisaties'.

²⁸ zoals artikel 14, lid 2 Wpb voorschrijft (<http://www.cbppweb.nl/wbpnaslag/2/Paginas/wbp-artikel-14-2.aspx>).

²⁹ Zie hiervoor ook het operationele product 'Voorbeeld Informatiebeveiligingsbeleid Gemeenten' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

3.4 Proces informatiebeveiliging bij decentralisaties

Deze paragraaf geeft een handreiking over hoe de implementatie van informatiebeveiliging bij decentralisaties (het beste) kan worden aangepakt. Het implementeren kan het beste in een aantal stappen gebeuren. Iedere stap is afhankelijk van de voorgaande stap en is belangrijk voor de volgende stap. Iedere stap heeft een bepaald doel en het resultaat is een gecontroleerde invoering met een verankering binnen de organisatie. Afhankelijk van de uitkomsten van de GAP-analyse en de prioritering kan het zijn dat sommige maatregelen eerder of later geïmplementeerd worden. Dit dient vastgelegd te worden in een informatiebeveiligingsplan per informatiesysteem.

Baseline Informatiebeveiliging Nederlandse Gemeenten

Nadat de Informatiebeveiligingsdienst voor gemeenten (IBD) de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) in mei 2013 had opgeleverd kon worden gestart met de volgende stap. Deze stap is het implementeren van de BIG door gemeenten. Het document Implementatie BIG³⁰ geeft een handreiking over hoe dit kan worden aangepakt.

Implementatie

De voorgestelde volgorde in deze paragraaf is gebaseerd op de volgorde uit hoofdstuk 3 van de tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).³¹ De daar benoemde stappen zijn aangepast aan de voor de decentralisaties relevante aspecten. Deze stappen worden schematisch weergegeven in figuur 1. De volgende stappen zijn onderkend:

1. Verzamel noodzakelijke input
2. Voer baselinetoets uit
3. Voer (eventueel) diepgaande risicoanalyse uit
4. Voer Privacy Impact Assessment uit
5. Voer GAP- en Impactanalyse uit
6. Stel informatiebeveiligingsplan (per informatiesysteem) op

Ad 1: Verzamel noodzakelijke input

Een groot afbreukrisico is dat meer personen informatie van cliënten kunnen raadplegen en muteren dan degenen die daartoe vanuit hun functie geautoriseerd zijn. Gemeenten zullen inzicht moeten hebben in de vereisten op het gebied van privacy en informatiebeveiliging met betrekking tot de drie decentralisaties.

Om de informatiebeveiliging met betrekking tot de drie decentralisaties adequaat in te richten is het van belang om inzicht te krijgen in de noodzakelijke informatievoorziening, de gegevensuitwisseling en ICT-voorzieningen en de afhankelijkheden te analyseren. Hierbij zullen gesprekken over de informatievoorziening en toepassing van ICT met gemeenten, departementen en andere betrokkenen gevoerd dienen te worden. Tijdens deze gesprekken zal inzicht verkregen moeten worden in onder andere:

- Inzicht in de (noodzakelijke) processen.
- Inzicht in de noodzakelijke informatiesystemen die deze processen ondersteunen.
- Inzicht in de noodzakelijke gegevens.
- Inzicht in waar en hoe de gegevens worden bewaard.
- Inzicht in de informatiestromen die plaats vinden.

³⁰ Zie hiervoor ook het operationele product 'Implementatie BIG' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

³¹ Zie hiervoor de Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

- Inzicht tussen welke partijen (welke) gegevens worden uitgewisseld.
- Inzicht in de (noodzakelijke) koppelingen tussen de verschillende informatiesystemen.
- Inzicht in het Programma van Eisen (PvE).
- Inzicht in de contracten voor de informatiesystemen.
- Autorisatiematrix van bevoegdheden in de informatiesystemen. Denk hierbij aan:
 - Wie welke gegevens mag inzien, wijzigen en (eventueel) verwijderen?
 - Welke rollen worden onderkend?
- Inzicht wie het beheer over de ICT uitvoert? Denk hierbij aan: de gemeente, departement, ketenpartners of is dit uitbesteed (denk hierbij ook aan een Software as a Service (SaaS) oplossing).
- Inzicht in de informatiebeveiliging.
- Inzicht in de van toepassing zijnde wet- en regelgeving.
- Inzicht in de (relevante) bedreigingen.
- Inzicht in de (relevante) risico's.

Volgens de Strategische Baseline moet er een risicoafweging plaatsvinden. De mogelijke methodes hiervoor zijn baselinetoets³² en diepgaande risicoanalyse³³. Het beveiligingsniveau van deze Tactische Baseline is zo gekozen dat dit voor de meeste processen en ondersteunende ICT-voorzieningen bij gemeenten voldoende is. Hiermee wordt voorkomen dat er voor ieder informatiesysteem een uitgebreide risicoanalyse uitgevoerd moet worden. Om vast te stellen dat het niveau van de Tactische Baseline voldoende is, moet een baselinetoets uitgevoerd worden.

Ad 2: Voer baselinetoets uit

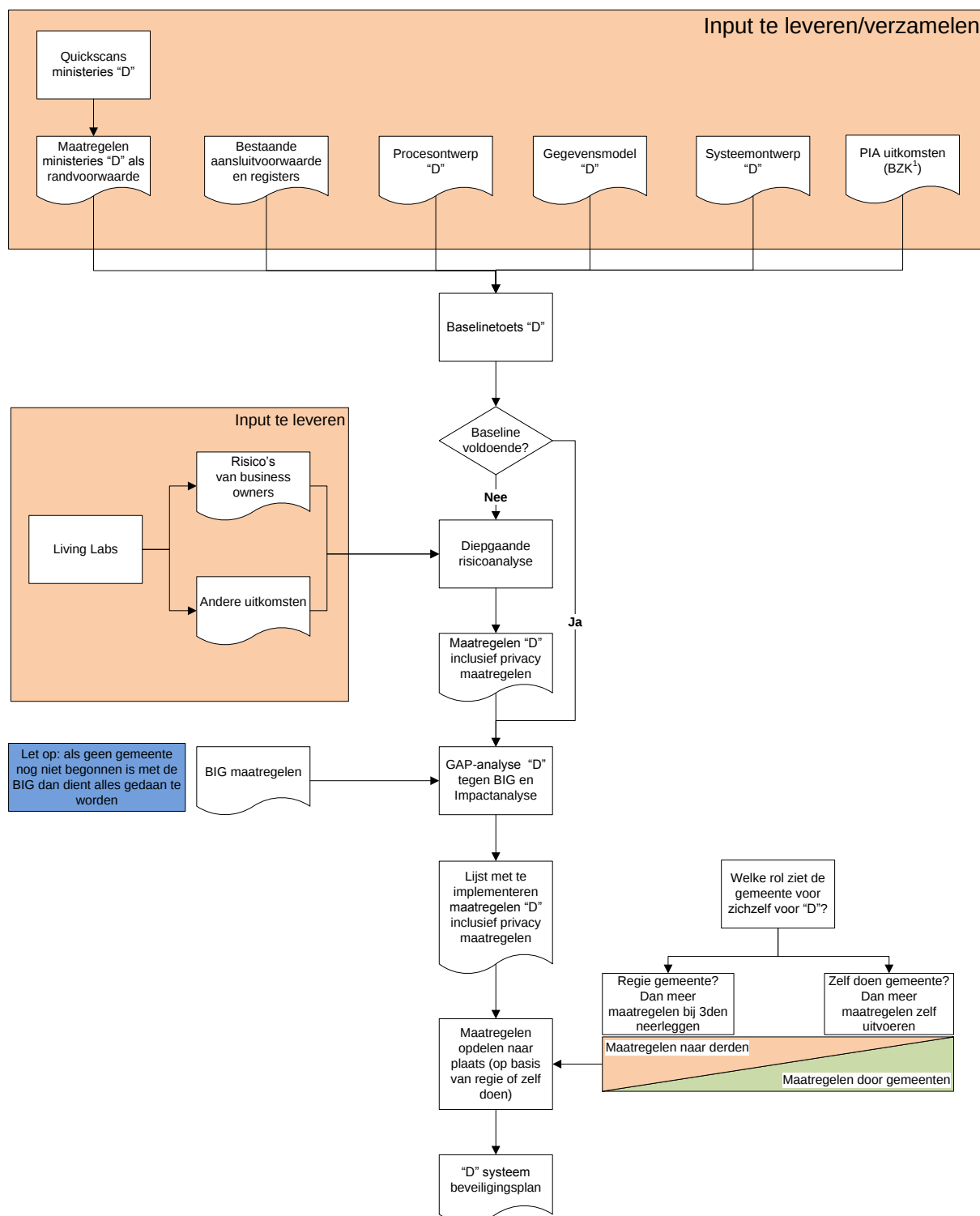
Als eerste stap om te toetsen of een proces en onderliggend informatiesysteem voldoende beveiligd wordt door de maatregelen in de BIG, dient deze baselinetoets uitgevoerd te worden. In de baselinetoets wordt onder meer bekeken of er geheime of geclassificeerde informatie verwerkt wordt, er sprake is van persoonsvertrouwelijke informatie zoals bedoeld in Artikel 16 van de Wet bescherming persoonsgegevens (Wbp), er hogere beschikbaarheidseisen vereist zijn en/of er dreigingen relevant zijn die niet in het dreigingsprofiel van de Tactische Baseline³⁴ meegenomen zijn.

Het resultaat van de baselinetoets is bedoeld voor lijn- en procesmanagers die resultaatverantwoordelijkheid dragen. Deze managers hebben belang bij de juiste kwaliteit casu quo betrouwbaarheid van het proces, hun informatiesysteem en de bijbehorende informatie. Daarbij hebben ze ook belang bij zo min mogelijk verstoring van het proces, zoveel mogelijk zekerheid omtrent het verloop van het proces en de kwaliteit van het informatiesysteem en de informatie. De resultaten van deze baselinetoets kunnen ook weer gebruikt worden bij de diepgaande risicoanalyse.

³² Zie hiervoor ook het operationele product 'Baselinetoets' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

³³ Zie hiervoor ook het operationele product 'Diepgaande Risicoanalysemethode gemeenten' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

³⁴ Zie hiervoor de Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).



¹ Zie de Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Kamer van 10 februari 2014 (vergaderjaar 2013 – 2014, Kamerstuk 33 750 VII, nr. 45, kenmerk 2014-0000052865)

Figuur 1 Schematische weergave proces informatiebeveiliging bij decentralisaties

De baselinetoets bestaat uit een aantal korte vragenlijsten en een methode om het belang van processen te bepalen. De antwoorden op de vragen worden gewaardeerd met een cijfer. Op basis van het totaal van de antwoorden wordt duidelijk of de standaard beveiliging (BIG) voldoende is of dat er een aanvullend onderzoek nodig is (diepgaande risicoanalyse).

Deze vragenlijst kan op twee manieren worden gebruikt:

1. Om te bepalen of een proces, informatiesysteem en informatie binnen de BIG valt of dat er meer maatregelen nodig zijn, nadat de GAP analyse en impactanalyse ten opzichte van de BIG gemeentebreed is uitgevoerd. De uitkomsten kunnen dan worden gebruikt om te bepalen of er meer maatregelen nodig zijn voor een proces en onderliggende informatiesystemen. Deze maatregelen kunnen worden verkregen uit een voorgedefinieerde lijst met maatregelen bovenop de baseline, of door een diepgaande risicoanalyse.
2. Voor het starten van een project of voor invoering van een nieuw informatiesysteem. Laat de baselinetoets opstellen door de procesverantwoordelijke. De vragenlijst vormt dan input voor de te nemen additionele beveiligingsmaatregelen welke in de definitiefase van het project nader worden uitgewerkt. Bijvoorbeeld door middel van een diepgaande risicoanalyse.

Ad 3: Voer diepgaande risicoanalysemethode gemeenten uit

Voor iedere informatiesysteem wijziging of als er een project wordt opgestart om te komen tot een nieuw informatiesysteem binnen de gemeente, dient een baselinetoets te worden uitgevoerd. Wanneer hieruit volgt dat de wijziging of het informatiesysteem binnen de BIG valt, kan worden volstaan met het implementeren van de BIG. Wanneer de eisen boven een bepaalde grens uitstijgen, moet ook een diepgaande risicoanalyse worden uitgevoerd.

Doelstelling van de diepgaande risicoanalyse is om in kaart te brengen welke maatregelen aanvullend op de baseline moeten worden getroffen om het juiste niveau van beveiliging te realiseren. De diepgaande risicoanalyse volgt een quick scan aanpak om ervoor te zorgen dat op een pragmatische en effectieve manier de juiste zaken in kaart worden gebracht. Uitgangspunt is dat de baselinetoets volledig is uitgevoerd en dat de resultaten daarvan beschikbaar zijn.

De uitgebreide risicoanalyse bestaat uit 3 hoofdstappen (voorafgegaan door de verkorte risicoanalyse):

1. Het in kaart brengen van de onderdelen van de informatievoorziening conform het MAPGOOD model.³⁵
2. Het in kaart brengen van de dreigingen die relevant zijn voor het te onderzoeken informatiesysteem, met per dreiging het potentiële effect en de kans op optreden.
3. Het vertalen van de meest relevante dreigingen naar maatregelen die moeten worden getroffen.

Let op, bij stap 3 mag men geen rekening houden met reeds bestaande maatregelen die dreigingen verminderen. Dit omdat anders de uitslag van de risicoanalyse wordt gekleurd. Risico's kunnen lager ingeschat worden omdat de respondenten ervan uitgaan dat er toch al maatregelen zijn genomen. Het zou zelfs zo kunnen zijn dat bepaalde BIG maatregelen nog niet zijn geïmplementeerd terwijl de informatiesysteemeigenaar dit niet weet.

Ad 4: Voer Privacy Impact Assessment uit

De Privacy Impact Assessment (PIA)³⁶ legt in de eerste plaats de risico's bloot die te maken hebben met privacy en dragen bij aan het vermijden of verminderen van deze privacyrisico's bij het verwerken van persoonsgegevens. Op basis van de antwoorden van de PIA wordt op systematische wijze inzichtelijk gemaakt of er een kans is dat de privacy van de betrokkene wordt geschaad, hoe hoog deze is en op welke gebieden deze is.

³⁵ Mapgood staat voor: mens, apparatuur, programmatuur, gegevens, organisatie, omgeving en diensten.

³⁶ Zie hiervoor ook het operationele product 'Toelichting PIA' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

De PIA doet dit door op gestructureerde wijze:

- de mogelijk (negatieve) gevolgen van het gebruik van persoonsgegevens voor de betrokken personen en organisaties in kaart te brengen en
- de risico's voor de betrokken personen en organisaties zo veel mogelijk te lokaliseren.

Op basis van de uitkomsten van de PIA kunnen door gemeenten gerichte acties worden genomen om deze risico's te verkleinen, beheersen of zelfs te voorkomen. Door het gebruik van de PIA kan bescherming van persoonsgegevens op een gestructureerde manier onderdeel uitmaken van de belangenafweging en besluitvorming over een proces, informatiesysteem of project. Hierdoor kunnen kostbare aanpassingen in processen, herontwerp van informatiesystemen of stopzetten van een project worden voorkomen door vroegtijdig inzicht in de belangrijkste privacyrisico's.

Een PIA kan het beste in een zo vroeg mogelijk stadium uitgevoerd worden. Bijvoorbeeld de definitiefase van een project, als vervolg op de baselinetoets. De PIA kan ook worden uitgevoerd bij een bestaand informatiesysteem als men twijfelt of er wel voldoende privacy maatregelen gedefinieerd en genomen zijn.

Ook aanpassingen of wijzigingen van bestaande informatiesystemen of projecten rechtvaardigen een PIA. Op die manier kan worden voorkomen dat later kostbare aanpassingen nodig zijn om alsnog de noodzakelijke beheersmaatregelen met betrekking tot privacy te implementeren. Ook wanneer de omstandigheden van een project tijdens de looptijd veranderen, is het raadzaam de PIA te herhalen en/of te evalueren bij de afsluiting van een project.

Ad 5: Voer GAP- en Impactanalyse uit

Het doel van de GAP-analyse³⁷ is te controleren of en in welke mate de maatregelen uit de tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten geïmplementeerd zijn bij de gemeente die het onderzoek uitvoert of laat uitvoeren. De GAP-analyse bevat alle maatregelen uit de tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) met daarbij controlevragen. De GAP-analyse is een methode om een vergelijking te maken tussen een bestaande of huidige situatie en de gewenste situatie, de maatregelen uit de baseline.

De GAP-analyse geeft als instrument antwoord op vragen als: 'Waar zijn we nu' en 'Waar willen we heen'. Met het gebruiken van de Tactische Baseline weet de gemeente nog niet wat er gedaan moet worden om de Tactische Baseline ingevoerd te krijgen. Door middel van de GAP-analyse kan de gemeente met het stellen van vragen vaststellen welke Tactische Baseline-maatregelen al ingevoerd zijn, en belangrijker, welke maatregelen uit deze Tactische Baseline nog niet ingevoerd zijn.

Met het gevonden resultaat kan vervolgens planmatig worden omgegaan en kunnen de actiehouders beginnen met het invoeren van maatregelen en hierover periodiek in de managementrapportages rapporteren.

Vervolgens onderzoek je welke maatregelen al genomen zijn en geef per maatregel aan:

- of er iets over beschreven is, en zo ja, waar dat opgelegd is (opzet) en
- of de verantwoordelijken bekend zijn met de maatregel (bestaan)

³⁷ Zie hiervoor ook het operationele product 'GAP-analyse' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

(rest) risico's

Het management speelt een cruciale rol. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Hierbij zal de verantwoordelijke manager, na de risicoafweging, een beslissing moeten nemen hoe met de (rest) risico's omgegaan dient te worden. Er zijn verschillende manieren hoe met deze (rest) risico's kan worden omgegaan. De meest gebruikelijke strategieën zijn:

1. **Risicodragend.** Risicodragend wil zeggen dat risico's geaccepteerd worden. Dat kan zijn omdat de kosten van de beveiligingsmaatregelen de mogelijke schade overstijgen. Maar het management kan ook besluiten om niets te doen, ondanks dat de kosten niet hoger zijn dan de schade die kan optreden. De maatregelen die een risicodragende organisatie neemt op het gebied van informatiebeveiliging zijn veelal van repressieve aard.
2. **Risiconeutraal.** Onder risiconeutraal wordt verstaan dat er dusdanige beveiligingsmaatregelen worden genomen dat dreigingen óf niet meer manifest worden óf, wanneer de dreiging wel manifest wordt, de schade als gevolg hiervan geminimaliseerd is. De meeste maatregelen die een risiconeutrale organisatie neemt op het gebied van informatiebeveiliging zijn een combinatie van preventieve, detectieve en repressieve maatregelen.
3. **Risicomijdend.** Onder risicomijdend verstaan we dat er zodanige maatregelen worden genomen dat de dreigingen zo veel mogelijk worden geneutraliseerd, zodat de dreiging niet meer tot een incident leidt.
Denk hierbij aan het invoeren van nieuwe software waardoor de fouten in de oude software geen dreiging meer vormen. In simpele bewoordingen: een ijzeren emmer kan roesten. Neem een kunststof emmer en de dreiging, roest, valt weg. Veel van de maatregelen binnen deze strategie hebben een preventief karakter.

Welke strategie een organisatie ook kiest, de keuze dient bewust door het management te worden gemaakt en de gevolgen ervan dienen te worden gedragen.

Impactanalyse

Nadat bij de GAP-analyse in kaart is gebracht, welke maatregelen wel of niet genomen zijn, volgt de Impactanalyse. De Impactanalyse geeft antwoord op de vraag in welke volgorde maatregelen geïmplementeerd gaan worden. Dit is belangrijk omdat niet alle ontbrekende maatregelen in één keer genomen kunnen worden. Afwegingen hierbij zijn:

- Geaccepteerd risico;
- Beschikbaar budget;
- Wachten op maatregelen die beter eerder uitgevoerd kunnen worden;
- Ontwikkelingen op het gebied van uitbesteding of samenwerking;
- Landelijke ontwikkelingen.

De Impactanalyse concentreert zich op de kosten dan wel de tijd en moeite die nodig is om een maatregel te implementeren. De uitkomst van de Impactanalyse is de GAP tussen wat er al is en wat er nog niet is én een volgorde voor de implementatie van de maatregelen. Er is een opzet gemaakt waarin eigenaren benoemd zijn voor iedere maatregel; een maatregel zonder eigenaar en aansturing wordt niet genomen.

Ad 6: Stel informatiebeveiligingsplan (per informatiesysteem) op

Het informatiebeveiligingsplan beschrijft de uitkomst van de hiervoor uitgevoerde stappen. In het informatiebeveiligingsplan is per informatiesysteem vastgelegd welke maatregelen aanvullend genomen moeten worden ten opzicht van de BIG en welke besluiten daarover genomen zijn. Dit informatiebeveiligingsplan per systeem is dan ook een aanvulling op het informatiebeveiligingsplan van de BIG, waarin de status en voortgang van de maatregelen uit de BIG in worden beschreven. Het informatiebeveiligingsplan per systeem, net zoals het informatiebeveiligingsplan voor de BIG, is een “levend” document. Het moet periodiek, minimaal per kwartaal, worden bijgesteld. De informatiesysteemeigenaar is verantwoordelijk voor dit informatiebeveiligingsplan en verzorgt de rapportages met betrekking tot de voortgang aan de CISO/Management/Directie. Deze rapportages over de voortgang zorgen ervoor dat het op de agenda blijft staan en continue aandacht krijgt op verschillende niveaus in de organisatie. De basis voor een planmatige aanpak en het implementeren en borgen van informatiebeveiliging is het informatiebeveiligingsplan.

4 Aan de slag

In dit hoofdstuk wordt aangegeven welke operationeel ondersteunde documenten relevant zijn voor de verschillende archetype. In de eerste paragraaf wordt als eerste ingegaan op informatiebeveiligingsaspecten die niet gerelateerd worden aan één specifiek archetype maar algemeen toepasbaar zijn. De overige paragrafen wordt ingezoomd op ieder afzonderlijk archetype. Hierbij zijn de bedrijfs- en applicatiefuncties als uitgangspunt genomen. Er wordt per applicatiefunctie een korte algemene toelichting gegeven specifiek voor het archetype, een toelichting met betrekking tot informatiebeveiliging en een koppeling met de relevante informatiebeveiligingsonderwerpen (zie ook paragraaf 5.7 'ondersteunde documenten') en operationele BIG producten (BIG-OP).

4.1 Algemeen en archetype onafhankelijk

In deze paragraaf wordt ingegaan op informatiebeveiligingsaspecten die niet gerelateerd kunnen worden aan één specifiek archetype maar algemeen toepasbaar zijn. Hierbij wordt een korte algemene toelichting gegeven en een koppeling met de relevante informatiebeveiligingsonderwerpen (zie ook paragraaf 5.7 'ondersteunde documenten') en operationele BIG producten (BIG-OP).

Achtergrondinformatie informatiebeveiliging	BIG en BIG-OP producten
Onafhankelijk welk archetype je als gemeente kiest, je moet als gemeente aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) voldoen.³⁸ Als de informatiebeveiliging bij gemeenten zijn ingericht volgens de Strategische Baseline in opzet, bestaan en werking, dan is dat afdoende garantie dat gemeenten hun eigen informatie en die van andere overheidsinstellingen zowel centraal als decentraal veilig behandelen. Dit bevordert het vertrouwen van de burger in de overheid waar ze hun zaken veilig en makkelijk digitaal kunnen afhandelen en tevens wordt het vertrouwen vergroot van ketenpartners, dat serieus wordt omgegaan met gegevensbescherming. Gemeenten moeten de verantwoordelijkheid voor informatieveiligheid zowel bestuurlijk als ambtelijk op de juiste plaats in de organisatie beleggen en op deze manier informatieveiligheid borgen. Binnen gemeenten is het College van Burgemeester en Wethouders integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente. Het lijnmanagement is verantwoordelijk voor de kwaliteit van de bedrijfsvoering waar informatiebeveiliging een integraal onderdeel van uitmaakt. Zo is het lijnmanagement ook verantwoordelijk voor informatiebeveiliging. Het primaire uitgangspunt voor informatiebeveiliging is en blijft risicomanagement. Het uitvoeren van een baselinetoets en/of een risicoanalyse ondersteunt het management bij het vaststellen van de risico's die worden gelopen en hoe groot die risico's zijn. Daarmee kan vervolgens bepaald worden welke informatiebeveiligingsmaatregelen getroffen moeten worden om de risico's terug te dringen. Bij de vertaling van risico naar informatiebeveiligingsmaatregel is classificatie een belangrijk hulpmiddel om de ernst van een risico en de reikwijdte van een informatiebeveiligingsmaatregel te kunnen bepalen.	Inrichten informatiebeveiliging: • Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten mei 2013 versie 1.0 IBD • Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten mei 2013 versie 1.0 IBD • Bijlage hoofdstuk 15.1.1 Identificatie toepasselijke wetgeving • Implementatie BIG • Handreiking CISO functieprofiel • Voorbeeld Informatiebeveiligingsbeleid Gemeenten Risicoanalyse (inclusief GAP-analyse): • Baselinetoets (in ontwikkeling) • Diepgaande risicoanalyse methode (in ontwikkeling) • GAP-analyse (colofon, resultaat, vragenlijst en uitleg) Dataclassificatie: • Handreiking dataclassificatie Awareness informatiebeveiliging: • Communicatieplan gemeente (in ontwikkeling)

³⁸ Op 29 november 2013 is tijdens de Buitengewone Algemene Ledenvergadering (BALV) van de VNG de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeenten' met 95% van de stemmen aangenomen. Hierdoor is de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) als basisnormenkader voor het gemeentelijke domein erkend.

Gemeenten zullen risicoanalyses uit moeten voeren en een methode voor classificatie hebben. De classificatiemethode kan beschouwd worden als een vereenvoudigde vorm van een risicoanalyse. Gemeenten zouden een informatiebeveiligingsfunctionaris moeten benoemen zoals een Chief Information Security Officer (CISO) die kan helpen bij het stellen van de juiste beveiligingsvragen en adviseren bij bepalen van informatiebeveiligingsmaatregelen door middel van een baselinetoets en/of een risicoanalyse. De uitkomst van die risicoanalyse, de informatiebeveiligingsmaatregelen dienen meegenomen te worden in ontwerpen en vragen (Programma van Eisen) aan de markt. Gemeenten moeten continue aandacht besteden aan bewustwording met betrekking tot informatiebeveiliging.	• Presentatie Bewustwording Informatieveiligheid bij gemeenten
--	--

4.2 Archetype 1 Transitie-proof

In deze paragraaf wordt ingezoomd op het archetype transitie-proof. Hierbij wordt als eerste een korte toelichting gegeven specifiek voor dit archetype en een koppeling met de relevante informatiebeveiligingsonderwerpen (zie ook paragraaf 5.7 ‘ondersteunde documenten’) en operationele BIG producten (BIG-OP). Daarna wordt ingezoomd op de bedrijfs- en applicatiefuncties. Hierbij wordt per applicatiefunctie een korte algemene toelichting gegeven specifiek voor het archetype, een toelichting met betrekking tot informatiebeveiliging en een koppeling met de relevante informatiebeveiligingsonderwerpen (zie ook paragraaf 5.7 ‘ondersteunde documenten’) en operationele BIG producten (BIG-OP).

Achtergrondinformatie informatiebeveiliging	BIG en BIG-OP producten
In dit model wordt de continuïteit van ondersteuning en het huidige kwaliteitsniveau van de dienstverlening geborgd. Je blijft de huidige ‘kolommen’ (lees domeinen) hanteren waardoor deze ‘kolommen’ naast elkaar blijven bestaan. Er wordt weinig tot niets gedaan aan het delen van informatie over de kolommen heen. De informatiestromen lopen hier dan over het algemeen ook in de ‘kolom’. Hierbij kunnen de informatiestromen digitaal of ‘fysiek’ (= op papier / in dossiers) verwerkt worden. Alleen wanneer dit (wettelijk) noodzakelijk is worden koppelingen (bijvoorbeeld advies- en meldpunt huiselijk geweld en kindermishandeling (AMHK)) gebouwd. Burgers moeten erop kunnen vertrouwen dat er zorgvuldig wordt omgegaan met persoonsgegevens wanneer zij bepaalde zorg of dienstverlening ontvangen. Natuurlijk hebben gemeenten nu al de verantwoordelijkheid voor het goed en zorgvuldig omgaan met persoonsgegevens van burgers. De drie decentralisaties kunnen betekenen dat gemeenten meer gegevens zullen verwerken en hiervoor ook meer zullen samenwerken met andere keten- en contractpartners. Dat roept andere vragen op. Bijvoorbeeld over het delen van gegevens tussen professionals, in een wijkteam. Het is dan ook zaak om privacybeleid te (her)formuleren en dit te implementeren in de (bestaande en nieuwe) werkprocessen. De gevoeligheid zit vooral in medische en / of strafrechtelijke gegevens. Op dit moment worden in de WMO-kolom ook medische gegevens verwerkt. Ervan uitgaande dat met de huidige werkwijze voldaan wordt aan de geldende informatieveiligheidsnormen, kan hierbij voor de nieuwe werkwijze van WMO-taken aangesloten worden. Zo wordt qua informatieveiligheid aan de norm voldaan. Met de nieuwe taken komen ook strafrechtelijke gegevens binnen het gemeentelijk bereik. Ervan uitgaande dat de werkprocessen binnen de	Privacy impact assessment: • Toelichting bij het Privacy Impact Assessment (PIA) • PIA – Vragenlijst • PIA - Verslag Persoonsgegevens: • Handreiking dataclassificatie • Bewerkersovereenkomst Authenticatie en Autorisatie (inclusief wachtwoorden): • Toegangsbeleid • Wachtwoordbeleid • Telewerken beleid • Aanwijzing Logging Communicatie & Opslag: • Encryptiebeleid (PKI) (in ontwikkeling) Inkopen / aanbesteding: • Contractmanagement • Inkoopvoorwaarden en informatiebeveiligingseisen • Bewerkersovereenkomst • Geheimhoudingsverklaringen BIG • Handleiding screening personeel

bestaande kolom blijven (huidige jeugdzorgkolom) en in deze kolom op dit moment voldaan wordt aan de geldende informatieveiligheidsnormen, hoeft je qua informatieveiligheid voor de reguliere werkzaamheden niets additioneel in te regelen. Uitwisseling van informatie gaat veelal over netwerken. Het is zaak hierbij oog te hebben voor de juiste beveiliging (encryptie) van informatie. Zeker als er gebruik wordt gemaakt van uitwisseling met derden over mogelijk onveilige kanalen buiten de gemeente. Het gaat hierbij niet alleen over het transport maar ook over de opslag zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie. Als gevoelige informatie buiten het gemeentelijke domein wordt opgeslagen (bij derde, als die al de gegevens lokaal mogen opslaan) zal dit extra eisen opleveren voor de beveiliging van deze informatie. Het gaat hierbij dan zowel over het transport als de opslag van informatie. Voor een juiste inrichting van toegangsrechten binnen systemen en tot informatie is het van belang goed te definiëren wie (functietype) welke (wat/dat informatie) te zien mag/moet krijgen. Daarnaast is een auditlogging van belang om achteraf te controleren wie wat heeft ingezien en wanneer en voor welke taak. De kans bestaat dat de bestaande systemen die binnen dit archetype aanwezig zijn dit nog niet op orde hebben. Ondanks dat bij dit model (tijdelijk) veel bij het oude blijft, moet je als gemeente de zaken geregeld hebben die in paragraaf 4.1 'Algemeen en archetype onafhankelijk' zijn beschreven.	
--	--

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
1. Behoeftebepaling - Bieden triage-instrumenten In dit archetype worden geen instrumenten anders dan dat nu al gebruikt wordt, verworven.	Gemeenten moeten vaststellen welke (persoons)gegevens noodzakelijk zijn met betrekking tot de triageprocessen³⁹ en welke (persoons)gegevens worden vastgelegd. De ondersteunende triage-instrumenten (bijvoorbeeld het gebruikte registratiesysteem) en processen dienen de privacy te borgen (noodzaak⁴⁰, subsidiariteit⁴¹ en proportionaliteit⁴² van gegevensverwerking). Dit geldt voor zowel de huidige als nieuw te verwerven triage-instrumenten. Bij de nieuwe systemen is privacy bij design⁴³ het uitgangspunt. Hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (bijvoorbeeld burger en/of professional), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft uitgevoerd en voor welke taak met betrekking tot een signaal/melding. Bij BRP wordt dit protocolleren genoemd.⁴⁴ Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de (persoons)gegevens beschikbaar, juist en actueel zijn.⁴⁵ Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
2. Behoeftebepaling - Ondersteunen ontvangen en beoordelen van signalen Binnen dit archetype worden meldingen en signalen via de beschikbare 'systemen' afgegeven (bestaande systematieken).	Gemeenten moeten vaststellen welke (persoons)gegevens de verschillende meldingen en/of signalen (dienen te) bevatten en welke (persoons)gegevens worden vastgelegd (wat- en dat-informatie). Denk hierbij ook aan meldingen uit verschillende probleemgebieden die gecombineerd en geverifieerd moeten kunnen worden (bijvoorbeeld gebeurtenissen vanuit basisregistraties	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

³⁹ Triage is het proces van verhelderen, routeren en escaleren van vragen en casussen.

⁴⁰ Het bepalen van het doel van informatiedeling (doelbinding).

⁴¹ subsidiariteit van de gegevensverwerking: is het doel ook te bereiken met een minder ingrijpende methode?

⁴² proportionaliteit van de gegevensverwerking: hoe verhouden het doel en de daarvoor noodzakelijke gegevensuitwisseling zich tot de schending van de persoonlijke levenssfeer van de betrokkene en zijn omgeving

⁴³ Bron: CBP -Privacy by Design gaat uit van het principe dat er in een vroeg stadium nagedacht wordt over het goede gebruik van persoonsgegevens binnen een organisatie, de noodzaak van het gebruik van deze gegevens en de bescherming ervan. Door al bij het ontwikkelen van systemen privacy en bescherming van persoonsgegevens in te bouwen is de kans op het succes ervan het grootst.

⁴⁴ Bron: Operatie BRP – binnengemeentelijke leveringen ([http://www.operatiebrp.nl/sites/operatie-brp/files/Binnengemeentelijke leveringen - Verdieping van inrichtingseisen v1.0.pdf](http://www.operatiebrp.nl/sites/operatie-brp/files/Binnengemeentelijke%20leveringen%20-%20Verdieping%20van%20inrichtingseisen%20v1.0.pdf)) Iedere vorm van administratie kent methoden om de juistheid van een administratieve handeling te waarborgen. Een onjuiste handeling die niet wordt opgemerkt, leidt immers tot fouten in de administratie. Voor geautomatiseerde systemen wordt een systeem gehanteerd waarmee alle handelingen van het systeem in beginsel door het systeem zelf worden vastgelegd. Dit vastleggen wordt protocolleren genoemd. Via protocolleren wordt ook vastgelegd welke gegevens wanneer en aan wie uit de administratie zijn verstrekt. Het doel hiervan is tweeledig. Ten eerste kan uit de protocollen worden afgeleid of het systeem de verstrekking juist heeft uitgevoerd. Ten tweede is de vastlegging van een gegevensverstrekking een belangrijk bestanddeel in het stelsel tot bescherming van de persoonlijke levenssfeer van de burger. Het is het sluitstuk. Achteraf kan dan immers worden herleid of de gegevensverstrekking rechtmatig heeft plaatsgevonden: dit wordt de privacyfunctie genoemd.

⁴⁵ Dit betekent onder andere dat gebruik wordt gemaakt van de juiste bron/basisregistratie en dat er geen gebruik wordt gemaakt van 'eigen' bestanden.

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
3. Klantcontact – Signaleren Er wordt gebruik gemaakt van de bestaande structuren (en dus verschillende portalen) waarbij meldingen direct bij de verantwoordelijke functies binnenkomen.	en kernregistraties, signalen uit de samenloopvoorziening van het inlichtingenbureau). De ondersteunende informatiesystemen (bijvoorbeeld een centraal signaal- en meldingenregister) en processen (bijvoorbeeld één centrale toegangspoort of meerdere, melden van problemen via een e-formulier of een (web)service.) dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (bijvoorbeeld burger en/of professional), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft uitgevoerd en voor welke taak met betrekking tot een signaal/melding. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de (persoons)gegevens beschikbaar, juist en actueel zijn.⁴⁵ Denk hierbij aan: dat een melding/signaal niet verloren gaat, dat de ontvangst van de melding/signaal wordt bevestigd (bijvoorbeeld geautomatiseerd); dat de melding/signaal direct bij de verantwoordelijke functies binnenkomen en dat de melding/signaal ook wordt verwerkt en opgevolgd. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Denk hierbij aan: gebeurtenissen die vanuit bronsystemen worden gemeld; signalen die worden geregistreerd; dat meldingen op één plek samen komen en het informeren van de verantwoordelijke professional.	
4. Financiële afhandeling - Afhandelen en beheren declaraties en facturen Afhandeling van declaraties en facturen conform de nu geldende werkwijze.	Gemeenten moeten vaststellen welke gegevens worden vastgelegd. Gemeenten moeten ook vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Hierbij is het van belang dat alleen geautoriseerde personen van de (contract)partners declaraties mogen indienen bij gemeenten. (Contract)partners mogen ook alleen hun eigen declaraties indienen en de afhandeling van hun declaraties volgen. Hierbij dient functiescheiding toegepast te worden om het risico op fraude te	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
5. Financiële afhandeling - Ondersteunen budgetbewaking De budgetbewaking verandert niet ten opzichte van de huidige situatie.		

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
6. Verantwoording - Declareren geleverde diensten Bij dit archetype wordt de bestaande situatie in principe niet gewijzigd tenzij vanuit de transitie een andere werkwijze wordt voorgeschreven. Hierbij kan gedacht worden aan elektronische uitwisseling van declaraties tussen zorgaanbieders en gemeenten daar waar het gaat om de overheveling van de extramurale begeleiding van de AWBZ naar de WMO.	voorkomen/verkleinen. Denk hierbij aan het klaarzetten van betalingen, het wijzigen van gegevens van crediteuren, het autoriseren van betalingen en het monitoren en bewaken van budgetten. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	
7. Verantwoording - Inzage in afhandeling declaraties Er wordt geen specifieke functionaliteit aangeboden.		
8. Financiële afhandeling - Leveren van statistische informatie	Bij de uitwisseling van verantwoordings-, stuur-, en beleidsinformatie dient nagedacht te worden over welke informatie nodig is voor welke vraag. Is het bijvoorbeeld nodig om detail gegevens te verstrekken over verantwoordings-, stuur -, en beleidsinformatie of kan er worden geanonimiseerd? Kan (geanonimiseerde) verantwoordings-, stuur -, en beleidsinformatie in kleine gemeenschappen toch inzicht geven in het individu? Met de gecontracteerde (keten)partner moeten afspraken worden over welke informatie wordt aangeleverd en op welke wijze (bijvoorbeeld via een clearinghouse⁴⁶). Hierbij dienen de (bestaande) aanleveringsprotocollen de integriteit, vertrouwelijkheid en privacy te waarborgen. Er moet voor de nieuwe taken (en bestaande taken) en de daarop verzamelde en ten aanzien van de eventueel over leefdomeinen heen gekoppelde stuur- en/of beleidsinformatie een privacyprotocol te worden uitgewerkt.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag • Inkopen / aanbesteding
9. Financiële afhandeling - Leveren van verantwoordingsinformatie		
10. Verantwoording - Bieden horizontale en verticale verantwoording De huidige kolommen zijn bepalend voor de te genereren verantwoordingsinformatie. Waar vanuit de horizontale⁴⁷ en verticale⁴⁸ verantwoording informatie gewenst is, is de te genereren minimale (en facultatieve) gegevensset leidend. Het aanleveren van deze informatie is vanuit de kolommen een extra administratieve last en mogelijk niet in alle gevallen te genereren.		

⁴⁶ Het clearinghouse zorgt als derdepartij voor de administratie en afhandeling van transacties tussen twee of meer partijen. De gestandaardiseerde registratie is goed mogelijk met behulp van een zogenaamde 'clearinghouse'-constructie waarbij de gegevens op cliëntniveau worden aangeleverd aan een organisatorisch onafhankelijk clearinghouse, die zorgt voor: enerzijds controle op de standaard (zijn alle basis- en aanvullende gegevens op de juiste manier ingevoerd?) en anderzijds voor (geanonimiseerde) verdeling van de informatie richting de verschillende belanghebbende actoren.

⁴⁷ verantwoording vanuit het College van B&W aan de gemeenteraad, de lokale rekenkamer en het lokale publiek over geleverde diensten en bereikte resultaten, vanuit de gemeentelijke verantwoordelijkheid in het sociaal domein

⁴⁸ verantwoording vanuit de gemeente aan het rijk, ten behoeve van de systeemverantwoordelijkheid van de minister.

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
11. Verantwoording - Bieden statistische informatie De huidige kolommen zijn bepalend voor de te genereren statistische informatie.		
12. Verantwoording - Bieden van managementinformatie De huidige kolommen zijn bepalend voor de te genereren managementinformatie.		
13. Bedrijfsfunctie Inkoop en contractbeheer - Beheren van contracten en SLA's De inkoop van ondersteuning verandert niet ten opzichte van de huidige situatie. Inkoop van zorg vindt per kolom plaats tenzij anders georganiseerd (bv centrale of regionale inkooporganisatie). Daar worden ook de contracten beheerd	In bestaande en/of nieuwe contracten dienen mogelijk beveiligingsaspecten meegenomen te worden, zoals de bewerkersovereenkomst. Met de (keten)partners moeten ook afspraken worden gemaakt over de wijze waarop verantwoording (monitoring) aan de gemeente wordt afgelegd.	• Inkopen / aanbesteding
14. Klantcontact - Beheren klantcontacten Het beheren van klantcontacten gebeurt nu ook al vanuit de bestaande frontoffice dan wel Klant Contact Centrum (KCC). De hiervoor reeds aanwezige functionaliteit in bijvoorbeeld Customer Relationship Management (CRM)-achtige systemen zijn afdoende.	Gemeenten moeten vaststellen welke (persoons)gegevens worden vastgelegd. Gemeenten moeten tevens vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd.Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de klantgegevens beschikbaar, juist en actueel zijn.⁴⁵ Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
15. Klantcontact - Maken afspraken Op dit moment kunnen zowel de burger, de zaakwaarnemer en de professionals per 'kolom' en/of dienst en/of product op (diverse) manieren afspraken maken. Wanneer deze voldoen hoeft u 'enkel' wat in te regelen voor nieuwe producten en/of diensten. U moet wel afspraken kunnen maken.	Burgers, zaakwaarnemers en professionals moet er op kunnen vertrouwen dat de mogelijkheden (systemen) om afspraken te maken beschikbaar zijn en juiste en actuele gegevens bevatten.	• Communicatie & Opslag
16. Klantcontact – Inzage in klantgegevens en lopende zaken De klantgegevens zijn niet anders beschikbaar dan in de huidige systemen en dossiers reeds vastgelegd.	Voor het opvolgen van meldingen, signalen en/of het voeren van het gesprek moet de regisseur kunnen beschikken over (een beperkte) set gegevens over de burger. Deze gegevens komen zowel uit bronsystemen van organisaties die betrokken zijn bij de ondersteuning van die burger (en zijn gezin) als uit de gemeentelijke systemen. Bij de hulpverlenende organisaties is in het algemeen veel informatie bekend over de situatie van de burger op een bepaald leefgebied en de al geleverde dienstverlening. Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. Tevens moeten gemeenten vaststellen welke (persoons)gegevens worden uitgewisseld tussen de ketenpartner en gemeenten. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (medewerkers, ketenpartners), welke gegevens mogen raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Denk hierbij aan de regisseur, de medewerker van het gemeentelijke KCC. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers en ketenpartners moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling van informatie tussen de voorziening van de ketenpartner en gemeentelijke voorziening dient de vertrouwelijkheid en integriteit te worden gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
17. Klantcontact – Tonen en bijwerken lopende zaken en mijn gegevens Een eigen klant dossier is hier leuk (maar ook niet meer dan dat), de burger kan ook bellen of per brief naar de bijvoorbeeld de status van een aanvraag te informeren. Inregelen van iets dergelijks past niet goed bij het archetype.	Burgers, zaakwaarnemers en professionals moeten er op kunnen vertrouwen dat het klant dossier beschikbaar is en de juiste en actuele gegevens bevatten. Gemeenten moeten vaststellen wie (burgers, medewerkers en ketenpartners), welke gegevens mogen raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een audit logging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs burgers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeenten moeten ook vaststellen via welke kanalen het klant dossier wordt ontsloten, lokaal toegankelijk of (op termijn) ook via mijnOverheid.nl. Bij de uitwisseling van informatie dient de vertrouwelijkheid en integriteit te worden gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
18. Klantcontact – Tonen gemeentelijke producten en diensten Om zaken te kunnen doen met de gemeente is het allereerst noodzakelijk dat voor burgers alle relevante informatie over gemeentelijke producten en diensten digitaal beschikbaar is en actueel wordt gehouden.	De burger moet er op kunnen vertrouwen dat de aangeboden informatie over gemeentelijke producten en diensten digitaal beschikbaar, juist en actueel is. Tevens moet de burger er op kunnen vertrouwen dat de aangeboden relevante informatie ook daadwerkelijk van de gemeente afkomstig is. De manier waarop gemeentelijke producten en diensten kunnen worden aangevraagd is minder van belang (een aanvraagformulier per product/dienst of 1 startpunt met een soort vraagboom). Als gemeenten producten en diensten van ketenpartners	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
19. Klantcontact – Aanvragen producten en diensten Wanneer je het van belang acht dat de burger alle diensten en producten digitaal kan aanvragen, zul je dit moeten inrichten.	beschikbaar stellen moeten gemeenten beslissen hoe met aanvragen voor deze producten en diensten van ketenpartners wordt omgegaan. Gemeenten moeten vaststellen of gebruikers die producten en/of diensten aanvragen zich moeten aanmelden/registreren voordat ze gebruik kunnen maken van deze dienstverlening. Tevens moeten gemeenten vaststellen of (persoons)gegevens noodzakelijk zijn met betrekking tot deze gemeentelijke dienstverlening. Zo ja, om welke (persoons)gegevens gaat het hier dan. Gemeenten moeten vaststellen wie welke gegevens mag plaatsen en onderhouden/bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Burgers kunnen vaak via meerdere kanalen (bijvoorbeeld met papieren aanvragen) gemeentelijke producten en diensten aanvragen. Wanneer gemeenten het van belang acht dat de burger alle diensten en producten digitaal kan aanvragen, moeten ze dit inrichten. Bij de uitwisseling van informatie tussen de ketenpartner en gemeenten dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	
20. Stimulering zelfredzaamheid - Matchen vraag en aanbod Het matchen van vraag en aanbod is in dit archetype geen doel op zich.	Ongeacht de rol (deze kan variëren van ondersteunend, faciliterend tot regulerend en initiërend) die de gemeente hierin kiest, kan bij eventuele fouten/misstanden de gemeente hierop aangesproken worden. Dit ondanks het feit dat deze informatie aangeleverd kan worden door derden (bijvoorbeeld burgers, buurten, wijken, regio's, dienstverleners en instellingen). Het is mogelijk dat de ondersteunende websites en aangeboden informatie los staan van de gemeentelijke website. De burger moet er op kunnen vertrouwen dat de getoonde informatie (bijvoorbeeld vraag en aanbod, buurt-/wijk- en burgerinitiatieven en zelfdiagnose, welke partijen lokaal of regionaal beschikbaar zijn voor welke diensten) beschikbaar, juist en actueel is. Gemeenten moeten vaststellen of gebruikers die informatie aanleveren (content plaatsen) zich moeten aanmelden/registreren voordat ze gebruik	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag ○ Denk hierbij aan SSL (PKIoverheid) certificaten.
21. Stimulering zelfredzaamheid - Ondersteunen buurt-/wijk- en burgerinitiatieven Het verhogen van de zelfredzaamheid dan wel het faciliteren van burgerinitiatieven is geen direct doel binnen dit archetype.		
22. Stimulering zelfredzaamheid - Ondersteunen zelfdiagnose Het ondersteunen van zelfdiagnose is in dit archetype geen doel.		

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
23. Stimulering zelfredzaamheid - Tonen content wijkteam Voor de huidige diensten is de website en het KCC reeds in functie. Het inrichten van wijkteams is zeer onwaarschijnlijk in dit archetype en daarmee het tonen van hun content evenzeer.	kunnen maken van deze dienstverlening. Tevens moeten gemeenten vaststellen of (persoons)gegevens noodzakelijk zijn met betrekking tot de geleverde dienstverlening. Zo ja, om welke (persoons)gegevens gaat het hier dan. Bij de uitwisseling en opslag van (persoons)gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Op het moment dat wordt aangehaakt bij bestaande initiatieven/applicaties moeten gemeenten vaststellen of deze voldoen aan de eisen en wensen van de gemeenten. Denk hierbij aan privacy en beveiligingseisen.	
24. Stimulering zelfredzaamheid - Tonen sociale kaart Geen direct doel binnen dit archetype. Wanneer er reeds een sociale kaart is is het indien enigszins mogelijk gewenst aan te sluiten bij de gemeentelijke (het tonen van) producten en diensten.		
25. Planvorming - Beheren groepstraject Het kunnen beheren van groepstrajecten ter uitvoering van 1 plan maakt geen onderdeel uit van dit archetype.	Gemeenten moeten vaststellen welke (persoons)gegevens worden vastgelegd, zowel voor het beheren van een groepstraject als bij het opstellen van het plan. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (de professional en/of regisseur), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (de professional en/of regisseur) moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van (persoons)gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bijvoorbeeld het regiesysteem dat in deze functionaliteit voorziet.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
26. Planvorming - Opstellen plan In dit archetype wordt geen integraal plan opgesteld		

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
27. Regievoering – Uitzetten en monitoren opdrachten Het uitzetten en monitoren van opdrachten is in dit archetype geen doel.	Gemeenten moeten vaststellen welke (persoons)gegevens nodig zijn bij het uitzetten van de verschillende opdrachten, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (regisseurs), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd.Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (regisseurs) moeten er op kunnen vertrouwen dat de getoonde informatie, welke zorgaanbieders welke diensten bieden- en tegen welke kosten, beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van gegevens de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bijvoorbeeld bij het uitzetten van de opdrachten online (via eigen zaakstelsel of via transitiebericht (toewijzing) conform de AWBZ-brede zorgregistratie (AZR) standaarden).	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
28. Specifieke ondersteuning - Beheren werkvoorraad Werkvoorraad wordt bijgehouden door de systemen die de gemeente nu al gebruikt. Veelal zullen dit taakspecifieke applicaties zijn. Indien deze applicaties de status van de lopende zaken doorgeeft aan het zakenmagazijn dan heeft de gemeente via het zakenmagazijn inzicht in alle lopende zaken. Indien een dergelijke koppeling niet geïmplementeerd is dan is de gemeente voor inzicht in de lopende zaken afhankelijk van de taakspecifieke applicaties.	Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt (zakensysteem⁴⁹ /-magazijn), zodat de werkzaamheden adequaat kunnen worden uitgevoerd. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd.Fout! Bladwijzer niet	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

⁴⁹ Systeem voor beheer van zaken, bij voorkeur conform het Referentiemodel Gemeentelijke Basisgegevens Zaken (RGBZ) en de Zaaktypencatalogus

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
29. Specifieke ondersteuning - Beheren zaken Zakenbeheer wordt gerealiseerd via de systemen die de gemeente nu al gebruikt. Dit kan via een gemeentebreed zaaksysteem zijn, of een taakspecifieke applicaties, eventueel in combinatie met een generiek zakenmagazijn.	gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (regisseurs, teamleden en/of professionals) moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	
30. Specifieke ondersteuning - Bijwerken status van levering product of dienst Terugkoppeling van geleverde diensten en producten gewenst	Gemeenten moeten vaststellen of ketenpartners de terugkoppeling of inhoudelijke afhandeling rechtstreeks in de gemeentelijke voorzieningen kunnen/mogen aanbrengen. Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag • Inkopen / aanbesteding

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
31. Specifieke ondersteuning - Ondersteunen inhoudelijke afhandeling Voor de huidige diensten is de website en het KCC reeds in functie en de inhoudelijke afhandeling van zaken is geregeld via taakspecifieke applicaties. Er wordt zoveel mogelijk aansluiting gezocht bij de beschikbare elektronische uitwisseling van de opdracht- en declaratieberichten. Bijvoorbeeld de overheveling van de extramurale begeleiding naar de WMO.	bijgewerkt, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. Tevens moeten gemeenten vaststellen welke (persoons)gegevens worden uitgewisseld tussen de voorziening van de ketenpartner en hun eigen voorziening in verband met de afhandeling van specialistische zaken. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers en ketenpartners moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling van informatie tussen de voorziening van de ketenpartner en gemeentelijke voorziening, via koppelvlakken of een webbased applicatie, dient de vertrouwelijkheid en integriteit gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie. Mogelijk moeten er met betrekking tot de terugkoppeling of inhoudelijke afhandeling extra afspraken worden gemaakt tussen gemeenten en ketenpartners. Bijvoorbeeld: Gemeenten moeten als verantwoordelijke⁵⁰ een schriftelijke overeenkomst (bewerkerovereenkomst) afsluiten met de ketenpartners (de bewerker⁵¹). De bewerkerovereenkomst kan zelfstandig worden gebruikt maar is meestal een onderdeel van een overeenkomst met een breder bereik.⁵²	

4.3 Archetype 2 Totaal integraal

In deze paragraaf wordt ingezoomd op het archetype totaal integraal. Hierbij wordt als eerste een korte toelichting gegeven specifiek voor dit archetype en een koppeling met de relevante informatiebeveiligingsonderwerpen (zie ook paragraaf 5.7 ‘ondersteunde documenten’) en

⁵⁰ De verantwoordelijke is volgens de Wet bescherming persoonsgegevens (Wbp) degene die het doel en de middelen voor de verwerking van persoonsgegevens bepaalt (Art. 1 sub d Wbp).

⁵¹ De Wbp definieert de bewerker als ‘degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen’ (Art. 1 sub e Wbp).

⁵² zie hiervoor het document Inkoop voorwaarden en beveiligingseisen van de IBD

operationele BIG producten (BIG-OP). Daarna wordt ingezoomd op de bedrijfs- en applicatiefuncties. Hierbij wordt per applicatiefunctie een korte algemene toelichting gegeven specifiek voor het archetype, een toelichting met betrekking tot informatiebeveiliging en een koppeling met de relevante informatiebeveiligingsonderwerpen (zie ook paragraaf 5.7 ‘ondersteunde documenten’) en operationele BIG producten (BIG-OP).

Achtergrondinformatie informatiebeveiliging	BIG en BIG-OP producten
Om als gemeente integrale dienstverlening te kunnen bieden aan burgers in het kader van de drie decentralisaties, is het kunnen delen van gegevens binnen en over domeinen een randvoorwaarde. Burgers moeten erop kunnen vertrouwen dat er zorgvuldig wordt omgegaan met persoonsgegevens wanneer zij bepaalde zorg of dienstverlening ontvangen. Natuurlijk hebben gemeenten nu al de verantwoordelijkheid voor het goed en zorgvuldig omgaan met persoonsgegevens van burgers. De drie decentralisaties kunnen betekenen dat gemeenten meer gegevens zullen verwerken en hiervoor ook meer zullen samenwerken met andere keten- en contractpartners. Omdat in dit model veel informatie bij elkaar wordt gebracht is informatiebeveiliging binnen dit type een majeur thema. Het is zeer waarschijnlijk dat hier bijzondere/gevoelige persoonsgegevens worden verwerkt. Daardoor zullen de vertrouwelijkheidseisen toenemen. Dit roept andere vragen op en daarmee ook de te implementeren informatiebeveiligingsmaatregelen. Bijvoorbeeld over het delen van gegevens tussen professionals in een wijkteam. Het is dan ook zaak om privacybeleid te (her)formuleren en dit te implementeren in de (bestaande en nieuwe) werkprocessen. De informatiebeveiligingsmaatregel die, naast de normale te implementeren maatregelen, de nadruk krijgen in dit archetype is encryptie van informatie die getransporteerd wordt over (on)veilige netwerken. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie, het verregaand vaststellen van toegangsrechten tot op medewerkerniveau, auditlogging en controle van alle activiteiten. Deze eisen zullen ook worden opgelegd aan derde partijen die met gemeentelijke informatie gaan werken en deze maatregelen dienen te worden vastgelegd in contracten, SLA's en bewerkersovereenkomsten. De gemeente is aan zet om die afspraken ook te (laten) controleren. Gemeenten moeten ook de zaken geregeld hebben die in paragraaf 4.1 ‘Algemeen en archetype onafhankelijk’ zijn beschreven.	Privacy impact assessment: • Toelichting bij het Privacy Impact Assessment (PIA) • PIA – Vragenlijst • PIA - Verslag Persoonsgegevens: • Handreiking dataclassificatie • Bewerkersovereenkomst Authenticatie en Autorisatie (inclusief wachtwoorden): • Toegangsbeleid • Wachtwoordbeleid • Telewerken beleid • Aanwijzing Logging Communicatie & Opslag: • Encryptiebeleid (PKI) (in ontwikkeling) Inkopen / aanbesteding: • Contractmanagement • Inkoopvoorwaarden en informatiebeveiligingseisen • Bewerkersovereenkomst • Geheimhoudingsverklaringen BIG • Handleiding screening personeel

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
1. Behoeft bepaling - Bieden triage-instrumenten Het triageproces is in dit archetype van groot belang.	Gemeenten moeten vaststellen welke (persoons)gegevens noodzakelijk zijn met betrekking tot de triageprocessen⁵³ en welke (persoons)gegevens worden vastgelegd. De ondersteunende triage-instrumenten (bijvoorbeeld het gebruikte registratiesysteem) en processen dienen de privacy te borgen (noodzaak⁵⁴, subsidiariteit⁵⁵ en proportionaliteit⁵⁶ van gegevensverwerking). Dit geldt voor zowel de huidige als nieuw te verwerven triage-instrumenten, bij de nieuwe systemen is privacy bij design⁵⁷ het uitgangspunt. Hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (bijvoorbeeld burger en/of professional), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft uitgevoerd en voor welke taak met betrekking tot een signaal/melding. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de (persoons)gegevens beschikbaar, juist en actueel zijn.⁴⁵ Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
2. Behoeft bepaling - Ondersteunen ontvangen en beoordelen van signalen Vroegsignalering is een van de doelen binnen dit archetype.	Gemeenten moeten vaststellen welke (persoons)gegevens de verschillende meldingen en/of signalen (dienen te) bevatten en welke (persoons)gegevens vastgelegd (wat- en dat-informatie). Denk hierbij ook aan meldingen uit verschillende probleemgebieden die gecombineerd en geverifieerd	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

⁵³ Triage is het proces van verhelderen, routeren en escaleren van vragen en casussen.

⁵⁴ Het bepalen van het doel van informatiedeling (doelbinding).

⁵⁵ subsidiariteit van de gegevensverwerking: is het doel ook te bereiken met een minder ingrijpende methode?

⁵⁶ proportionaliteit van de gegevensverwerking: hoe verhouden het doel en de daarvoor noodzakelijke gegevensuitwisseling zich tot de schending van de persoonlijke levenssfeer van de betrokkene en zijn omgeving

⁵⁷ Bron: CBP -Privacy by Design gaat uit van het principe dat er in een vroeg stadium nagedacht wordt over het goede gebruik van persoonsgegevens binnen een organisatie, de noodzaak van het gebruik van deze gegevens en de bescherming ervan. Door al bij het ontwikkelen van systemen privacy en bescherming van persoonsgegevens in te bouwen is de kans op het succes ervan het grootst.

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
3. Klantcontact – Signaleren Voor de burger is er één centrale toegang die is ingericht om meldingen door te geleiden naar de juiste verantwoordelijke. Meldingen met betrekking tot de openbare ruimte of huiselijk geweld en kindermishandeling hebben (mogelijk) een ander toegangspoort. Via welk kanaal een melding ook binnenkomt, een melding wordt geregistreerd en bevestigd.	moeten kunnen worden (bijvoorbeeld gebeurtenissen vanuit basisregistraties en kernregistraties, signalen uit de samenloopvoorziening van het inlichtingenbureau). De ondersteunende informatiesystemen (bijvoorbeeld een centraal signaal- en meldingenregister) en processen (bijvoorbeeld één centrale toegangspoort of meerdere, melden van problemen via een e-formulier of een (web)service.) dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (bijvoorbeeld burger en/of professional), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft uitgevoerd en voor welke taak met betrekking tot een signaal/melding. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de (persoons)gegevens beschikbaar, juist en actueel zijn.⁴⁵ Denk hierbij aan: dat een melding/signaal niet verloren gaat, dat de ontvangst van de melding/signaal wordt bevestigd (bijvoorbeeld geautomatiseerd); dat de melding/signaal direct bij de verantwoordelijke functies binnenkomen en dat de melding/signaal ook wordt verwerkt en opgevolgd. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Denk hierbij aan: gebeurtenissen die vanuit bronsystemen worden gemeld; signalen die worden geregistreerd; dat meldingen op één plek samen komen en het informeren van de verantwoordelijke professional.	
4. Financiële afhandeling - Afhandelen en beheren declaraties en facturen Niet onderscheidend. Op zich niet onderscheidend maar wel van belang is dat ontschotting ook aan de backoffice kant is geregeld.	Gemeenten moeten vaststellen welke gegevens worden vastgelegd. Gemeenten moeten ook vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Hierbij is het van belang dat alleen geautoriseerde personen van de (contract)partners declaraties mogen indienen bij gemeenten. (Contract)partners mogen ook alleen hun eigen	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
5. Financiële afhandeling - Ondersteunen budgetbewaking Waar binnen dit archetype het uitgangspunt is integrale dienstverlening, is het ook aan de regisseur te sturen op kosten(efficiency) van de in te zetten interventies. Hiervoor is (ontschotte) budgetbewaking noodzakelijk.	declaraties inzien en de afhandeling van hun declaraties volgen. Hierbij dient functiescheiding toegepast te worden om het risico op fraude te voorkomen/verkleinen. Denk hierbij aan het klaarzetten van betalingen, het wijzigen van gegevens van crediteuren, het autoriseren van betalingen en het monitoren en bewaken van budgetten. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd.Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	
6. Verantwoording - Declareren geleverde diensten		
7. Verantwoording - Inzage in afhandeling declaraties Ketenpartners hebben de mogelijkheid inzage te plegen in alle door hen ingediende declaraties.		
8. Financiële afhandeling - Leveren van statistische informatie	Bij de uitwisseling van verantwoordings-, stuur-, en beleidsinformatie dient nagedacht te worden over welke informatie nodig is voor welke vraag. Is het bijvoorbeeld nodig om detail gegevens te verstrekken over verantwoordings-, stuur -, en beleidsinformatie of kan er worden geanonimiseerd? Kan (geanonimiseerde) verantwoordings-, stuur -, en beleidsinformatie in kleine gemeenschappen toch inzicht geven in het individu? Met de gecontracteerde (keten)partner moeten afspraken worden over welke informatie wordt aangeleverd en op welke wijze (bijvoorbeeld via een clearinghouse⁵⁸). Hierbij dienen de (bestaande) aanleveringsprotocollen de integriteit, vertrouwelijkheid en privacy te waarborgen. Er moet voor de nieuwe taken (en bestaande taken) en de daarop verzamelde en ten aanzien van de eventueel over leefdomeinen heen gekoppelde stuur- en/of beleidsinformatie een privacyprotocol te worden uitgewerkt.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag • Inkopen / aanbesteding
9. Financiële afhandeling - Leveren van verantwoordingsinformatie		
10. Verantwoording - Bieden horizontale en verticale verantwoording Waar vanuit de horizontale en verticale verantwoording informatie gewenst is, is de te genereren minimale (en facultatieve) gegevensset leidend Het aanleveren van de horizontale en verticale verantwoording informatie is vanuit dit archetype een minimale inspanning, aangezien deze informatie reeds in het regiesysteem wordt vastgelegd. Tevens is er behoefte aan beleidsinformatie en financiële informatie.		

⁵⁸ Het clearinghouse zorgt als derdepartij voor de administratie en afhandeling van transacties tussen twee of meer partijen. De gestandaardiseerde registratie is goed mogelijk met behulp van een zogenaamde 'clearinghouse'-constructie waarbij de gegevens op cliëntniveau worden aangeleverd aan een organisatorisch onafhankelijk clearinghouse, die zorgt voor: enerzijds controle op de standaard (zijn alle basis- en aanvullende gegevens op de juiste manier ingevoerd?) en anderzijds voor (geanonimiseerde) verdeling van de informatie richting de verschillende belanghebbende actoren.

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
11. Verantwoording - Bieden statistische informatie Statistische informatie wordt integraal geboden over alle zaken die spelen binnen de clusters van de decentralisaties		
12. Verantwoording - Bieden van managementinformatie Managementinformatie wordt integraal geboden over alle zaken die spelen binnen de clusters van de decentralisaties		
13. Bedrijfsfunctie Inkoop en contractbeheer - Beheren van contracten en SLA's Inkoop van zorg en het beheren van de contracten vindt centraal vanuit de gemeente plaats inclusief het wijkoverstijgend en gespecialiseerd aanbod.	In bestaande en/of nieuwe contracten dienen mogelijk beveiligingsaspecten meegenomen te worden, zoals de bewerkersovereenkomst. Met de (keten)partners moeten ook afspraken worden gemaakt over de wijze waarop verantwoording (monitoring) aan de gemeente wordt afgelegd.	• Inkopen / aanbesteding
14. Klantcontact - Beheren klantcontacten Het uitgangspunt is het huishouden⁵⁹ in dit archetype. Hiervoor worden klantcontacten altijd gebundeld naar het plan dat betrekking heeft op het huishouden.	Gemeenten moeten vaststellen welke (persoons)gegevens worden vastgelegd. Gemeenten moeten tevens vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd.Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de klantgegevens beschikbaar, juist en actueel zijn.⁴⁵ Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

⁵⁹ Voor 'het' huishouden wordt verwezen naar de definitie van 'groep' uit het bedrijfsobjectenmodel van de 'handreiking zaakgericht werken in het sociaal domein: "Een groep bestaat uit de personen die –naar beoordeling van de regisseur- samen onderwerp vormen van, of randvoorwaardelijk zijn voor een plan."

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
15. Klantcontact - Maken afspraken Je moet afspraken kunnen maken, dat heeft prioriteit 1. Op termijn wil je dat de afsprakenmodule gekoppeld, dan wel geïntegreerd is in mijn klantdossier. Dat past binnen dit archetype (dat heeft prioriteit 3).	Burgers, zaakwaarnemers en professionals moet er op kunnen vertrouwen dat de mogelijkheden (systemen) om afspraken te maken beschikbaar zijn en juiste en actuele gegevens bevatten.	• Communicatie & Opslag
16. Klantcontact – Inzage in klantgegevens en lopende zaken De klantgegevens zijn integraal beschikbaar op één plaats. Hierbij moet onderscheid gemaakt in wat⁶⁰ en dat⁶¹ informatie en is stringente autorisatiebeheer noodzakelijk.	Voor het opvolgen van meldingen, signalen en/of het voeren van het gesprek moet de regisseur kunnen beschikken over (een beperkte) set gegevens over de burger. Deze gegevens komen zowel uit bronsystemen van organisaties die betrokken zijn bij de ondersteuning van die burger (en zijn gezin) als uit de gemeentelijke systemen. Bij de hulpverlenende organisaties is in het algemeen veel informatie bekend over de situatie van de burger op een bepaald leefgebied en de al geleverde dienstverlening. Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. Tevens moeten gemeenten vaststellen welke (persoons)gegevens worden uitgewisseld tussen de ketenpartner en gemeenten. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (medewerkers, ketenpartners), welke gegevens mogen raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Denk hierbij aan de regisseur, de medewerker van het gemeentelijke KCC. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers en ketenpartners moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling van informatie tussen de voorziening van de ketenpartner en gemeentelijke voorziening dient de vertrouwelijkheid en integriteit te worden gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

⁶⁰ de gegevens over wat er aan de hand, d.w.z. de inhoudelijke dossier gegevens van de hulp- of dienstverlenende organisatie of afdeling.

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
17. Klantcontact – Tonen en bijwerken lopende zaken en mijn gegevens Een eigen klantdossier is integraal beschikbaar op één plaats. Functionaliteit waarmee de burger zijn gegevens kan inzien, lopende zaken kan volgen en waarmee persoonlijke gegevens, zoals het e-mail adres of telefoonnummer, kan worden gewijzigd.	Burgers, zaakwaarnemers en professionals moeten er op kunnen vertrouwen dat het klantdossier beschikbaar is en de juiste en actuele gegevens bevatten. Gemeenten moeten vaststellen wie (burgers, medewerkers en ketenpartners), welke gegevens mogen raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs burgers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeenten moeten ook vaststellen via welke kanalen het klantdossier wordt ontsloten, lokaal toegankelijk of (op termijn) ook via mijnOverheid.nl. Bij de uitwisseling van informatie dient de vertrouwelijkheid en integriteit te worden gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
18. Klantcontact – Tonen gemeentelijke producten en diensten Je creëert een nieuwe integrale toegang voor alle gemeentelijke diensten op gebied van het sociale domein. Dit betekent dat je deze informatie ook integraal toegankelijk moet maken.	De burger moet er op kunnen vertrouwen dat de aangeboden informatie over gemeentelijke producten en diensten digitaal beschikbaar, juist en actueel is. Tevens moet de burger er op kunnen vertrouwen dat de aangeboden relevante informatie ook daadwerkelijk van de gemeente afkomstig is. De manier waarop gemeentelijke producten en diensten kunnen worden aangevraagd is minder van belang (een aanvraagformulier per product/dienst of 1	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

⁶¹ informatie over het feit dat een gezin of persoon bekend is bij een instantie en/ of een hulpverlener. Ook deze informatie valt onder de werking van de Wbp.

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
19. Klantcontact – Aanvragen producten en diensten Het digitaal aanvragen van producten en diensten wordt hier noodzakelijk uit doelstelling digitale overheid 2017⁶². Wanneer alles integraal beoordeeld dient te worden, zul je daar een 'selectiemechanisme' voor moeten inbouwen. Daarom is het inregelen van digitaal aanvragen hier belangrijker.	startpunt met een soort vraagboom). Als gemeenten producten en diensten van ketenpartners beschikbaar stellen moeten gemeenten beslissen hoe met aanvragen voor deze producten en diensten van ketenpartners wordt omgegaan. Gemeenten moeten vaststellen of gebruikers die producten en/of diensten aanvragen zich moeten aanmelden/registreren voordat ze gebruik kunnen maken van deze dienstverlening. Tevens moeten gemeenten vaststellen of (persoons)gegevens noodzakelijk zijn met betrekking tot deze gemeentelijke dienstverlening. Zo ja, om welke (persoons)gegevens gaat het hier dan. Gemeenten moeten vaststellen wie welke gegevens mag plaatsen en onderhouden/bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Burgers kunnen vaak via meerdere kanalen (bijvoorbeeld met papieren aanvragen) gemeentelijke producten en diensten aanvragen. Wanneer gemeenten het van belang acht dat de burger alle diensten en producten digitaal kan aanvragen, moeten ze dit inrichten. Bij de uitwisseling van informatie tussen de ketenpartner en gemeenten dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	
20. Stimulering zelfredzaamheid - Matchen vraag en aanbod Dit is goed om te hebben, past ook bij dit archetype. Het zou uiteindelijk wellicht gelieerd kunnen zijn aan het eigen dossier van burgers.	Ongeacht de rol (deze kan variëren van ondersteunend, faciliterend tot regulerend en initiërend) die de gemeente hierin kiest, kan bij eventuele fouten/misstanden de gemeente hierop aangesproken worden. Dit ondanks het feit dat deze informatie aangeleverd kan worden door derden (bijvoorbeeld burgers, buurten, wijken, regio's,	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag ○ Denk hierbij aan SSL (PKIoverheid)

⁶² Zie hiervoor de visiebrief digitale overheid 2017 van minister Plasterk van Binnenlandse Zaken en Koninkrijksrelatie (<https://zoek.officielebekendmakingen.nl/kst-26643-280.pdf>).

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
21. Stimulering zelfredzaamheid - Ondersteunen buurt-/wijk- en burgerinitiatieven Het ondersteunen van de buurt- en wijkinitiatieven kan het beste plaats vinden vanuit dit archetype. Vanuit dit archetype is dit ook een van de belangrijkste doelstellingen, voordat regie vanuit het wijkteam plaatsvindt.	dienstverleners en instellingen). Het is mogelijk dat de ondersteunende websites en aangeboden informatie los staan van de gemeentelijke website. De burger moet er op kunnen vertrouwen dat de getoonde informatie (bijvoorbeeld vraag en aanbod, buurt-/wijk- en burgerinitiatieven en zelfdiagnose, welke partijen lokaal of regionaal beschikbaar zijn voor welke diensten) beschikbaar, juist en actueel is. Gemeenten moeten vaststellen of gebruikers die informatie aanleveren (content plaatsen) zich moeten aanmelden/registreren voordat ze gebruik kunnen maken van deze dienstverlening. Tevens moeten gemeenten vaststellen of (persoons)gegevens noodzakelijk zijn met betrekking tot de geleverde dienstverlening. Zo ja, om welke (persoons)gegevens gaat het hier dan. Bij de uitwisseling en opslag van (persoons)gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Op het moment dat wordt aangehaakt bij bestaande initiatieven/applicaties moeten gemeenten vaststellen of deze voldoen aan de eisen en wensen van de gemeenten. Denk hierbij aan privacy en beveiligingseisen.	certificaten.
22. Stimulering zelfredzaamheid - Ondersteunen zelfdiagnose Het ondersteunen van zelfdiagnose is goed om te hebben en past binnen dit archetype. Het zou uiteindelijk wellicht gelieerd kunnen zijn aan het eigen dossier van burgers.		
23. Stimulering zelfredzaamheid - Tonen content wijkteam Past binnen dit archetype en in de doelstelling om samen met de burger op transparante manier hulp en ondersteuning vorm te geven.		
24. Stimulering zelfredzaamheid - Tonen sociale kaart Past binnen het archetype. Geen hoge prioriteit. Zou uiteindelijk mooi zijn om aan te haken bij het eigen dossier.		

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
25. Planvorming - Beheren groepstraject Een groep komt vaak overeen met een gezin, maar kan bijvoorbeeld ook een buurman bevatten die daar vaak over de vloer komt. De combinatie van personen maakt een groep uniek. Personen kunnen in meerdere groepen voorkomen. Ook kunnen groepen dus gemeentete overstijgend zijn. In dit geval is afstemming tussen de verschillende gemeenten aangewezen.	Gemeenten moeten vaststellen welke (persoons)gegevens worden vastgelegd, zowel voor het beheren van een groepstraject als bij het opstellen van het plan. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (de professional en/of regisseur), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (de professional en/of regisseur) moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van (persoons)gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bijvoorbeeld het regiesysteem dat in deze functionaliteit voorziet.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
26. Planvorming - Opstellen plan Naast het huishouden is ook het opstellen van een plan het uitgangspunt bij dit archetype. Deze functionaliteit wordt voorzien door het regiesysteem.		

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
27. Regievoering – Uitzetten en monitoren opdrachten Waar binnen dit archetypen wordt uitgegaan van inhoudelijke regie, is het kunnen uitzetten en monitoren van opdrachten een vereiste. Dit kan, waar het binnengemeentelijke dienstverlening betreft, met het eigen zaakstelsel. Waar het dienstverlening door zorgaanbieders betreft, kan dit met het transitiebericht (toewijzing) conform de AWBZ-brede zorgregistratie (AZR) standaarden.	Gemeenten moeten vaststellen welke (persoons)gegevens nodig zijn bij het uitzetten van de verschillende opdrachten, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (regisseurs), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (regisseurs) moeten er op kunnen vertrouwen dat de getoonde informatie, welke zorgaanbieders welke diensten bieden- en tegen welke kosten, beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van gegevens de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bijvoorbeeld bij het uitzetten van de opdrachten online (via eigen zaakstelsel of via transitiebericht (toewijzing) conform de AWBZ-brede zorgregistratie (AZR) standaarden).	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
28. Specifieke ondersteuning - Beheren werkvoorraad In dit archetype wordt zoveel als mogelijk integraal afgehandeld. Het beheren van de werkvoorraad (sturen op caseload en een juiste verdeling van de werkzaamheden) is een belangrijke functionaliteit. De werkvoorraad wordt bijgehouden door de systemen die de gemeente nu al gebruikt. Dit kan via een gemeentebreed zaakstelsel zijn, of taakspecifieke applicaties, eventueel in combinatie met een generiek zakenmagazijn.	Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt (zakensysteem⁶³ /-magazijn), zodat de werkzaamheden adequaat kunnen worden uitgevoerd. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

⁶³ Systeem voor beheer van zaken, bij voorkeur conform het Referentiemodel Gemeentelijke Basisgegevens Zaken (RGBZ) en de Zaaktypencatalogus

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
29. Specifieke ondersteuning - Beheren zaken Zakenbeheer wordt gerealiseerd via de systemen die de gemeente nu al gebruikt. Dit kan via een gemeentebreed zaaksysteem zijn, of taakspecifieke applicaties, eventueel in combinatie met een generiek zakenmagazijn.	genoemd.Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (regisseurs, teamleden en/of professionals) moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	
30. Specifieke ondersteuning - Bijwerken status van levering product of dienst Terugkoppeling van geleverde diensten en producten gewenst.	Gemeenten moeten vaststellen of ketenpartners de terugkoppeling of inhoudelijke afhandeling rechtstreeks in de gemeentelijke voorzieningen kunnen/mogen aanbrengen. Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag • Inkopen / aanbesteding

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
31. Specifieke ondersteuning - Ondersteunen inhoudelijke afhandeling Inhoudelijke afhandeling van de verstrekking van diensten of producten via hetzij een integraal zaaksysteem dan wel via taakspecifieke applicaties. Gemeenten stellen koppelvlakken beschikbaar om uitwisseling van en naar hun voorzieningen mogelijk te maken.	bijgewerkt, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. Tevens moeten gemeenten vaststellen welke (persoons)gegevens worden uitgewisseld tussen de voorziening van de ketenpartner en hun eigen voorziening in verband met de afhandeling van specialistische zaken. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers en ketenpartners moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling van informatie tussen de voorziening van de ketenpartner en gemeentelijke voorziening, via koppelvlakken of een webbased applicatie, dient de vertrouwelijkheid en integriteit gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie. Mogelijk moeten er met betrekking tot de terugkoppeling of inhoudelijke afhandeling extra afspraken worden gemaakt tussen gemeenten en ketenpartners. Bijvoorbeeld: Gemeenten moeten als verantwoordelijke⁶⁴ een schriftelijke overeenkomst (bewerkerovereenkomst) afsluiten met de ketenpartners (de bewerker⁶⁵). De bewerkerovereenkomst kan zelfstandig worden gebruikt maar is meestal een onderdeel van een overeenkomst met een breder bereik.⁶⁶	

4.4 Archetype 3 Geclusterd integraal

In deze paragraaf wordt ingezoomd op het archetype geclusterd integraal. Hierbij wordt als eerste een korte toelichting gegeven specifiek voor dit archetype en een koppeling met de relevante informatiebeveiligingsonderwerpen (zie ook paragraaf 5.7 'ondersteunde

⁶⁴ De verantwoordelijke is volgens de Wet bescherming persoonsgegevens (Wbp) degene die het doel en de middelen voor de verwerking van persoonsgegevens bepaalt (Art. 1 sub d Wbp).

⁶⁵ De Wbp definieert de bewerker als 'degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen' (Art. 1 sub e Wbp).

⁶⁶ zie hiervoor het document Inkoop voorwaarden en beveiligingseisen van de IBD

documenten') en operationele BIG producten (BIG-OP). Daarna wordt ingezoomd op de bedrijfs- en applicatiefuncties. Hierbij wordt per applicatiefunctie een korte algemene toelichting gegeven specifiek voor het archetype, een toelichting met betrekking tot informatiebeveiliging en een koppeling met de relevante informatiebeveiligingsonderwerpen (zie ook paragraaf 5.7 'ondersteunde documenten') en operationele BIG producten (BIG-OP).

Achtergrondinformatie informatiebeveiliging	BIG en BIG-OP producten
Per cluster zal per burger/huishouden informatie worden vergaard. Dit brengt, afhankelijk van de clusterkeuze, met zich mee dat er meer informatie van een burger/huishouden op één (digitale) locatie bewaard wordt. Afhankelijk van de clustering gebeurt dit over leefdomenien heen. Burgers moeten erop kunnen vertrouwen dat er zorgvuldig wordt omgegaan met persoonsgegevens wanneer zij bepaalde zorg of dienstverlening ontvangen. Natuurlijk hebben gemeenten nu al de verantwoordelijkheid voor het goed en zorgvuldig omgaan met persoonsgegevens van burgers. De drie decentralisaties kunnen betekenen dat gemeenten meer gegevens zullen verwerken en hiervoor ook meer zullen samenwerken met andere keten- en contractpartners. Dat roept andere vragen op bijvoorbeeld over het delen van gegevens tussen professionals, bijvoorbeeld in een wijkteam. Dit vraagt het een en ander van informatiebeveiliging. Het is dan ook zaak om privacybeleid te (her)formuleren en dit te implementeren in de (bestaande en nieuwe) werkprocessen. Voor een juiste inrichting van toegangsrechten binnen systemen en tot informatie is het van belang goed te definiëren wie (functietype) welke (wat/dat informatie) te zien mag krijgen. Daarnaast is een auditlogging van belang om achteraf te controleren wie wat heeft ingezien en wanneer en voor welke taak. De kans bestaat dat de bestaande systemen die binnen dit archetype aanwezig zijn dit nog niet op orde hebben. Uitwisseling van informatie gaat veelal over netwerken en het is zaak hierbij oog te hebben voor de juiste beveiliging (encryptie) van informatie. Zeker als er gebruik wordt gemaakt van uitwisseling met derden over mogelijk onveilige kanalen buiten de gemeente. Het gaat hierbij niet alleen over het transport maar ook over de opslag zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie. Als gevoelige informatie buiten het gemeentelijke domein wordt opgeslagen (bij derde, als die al de gegevens lokaal mogen opslaan) zal dit extra eisen opleveren voor de beveiliging van deze informatie. Gemeenten moeten ook de zaken geregeld hebben die in paragraaf 4.1 'Algemeen en archetype onafhankelijk' zijn beschreven.	Privacy impact assessment: • Toelichting bij het Privacy Impact Assessment (PIA) • PIA – Vragenlijst • PIA - Verslag Persoonsgegevens: • Handreiking dataclassificatie • Bewerkersovereenkomst Authenticatie en Autorisatie (inclusief wachtwoorden): • Toegangsbeleid • Wachtwoordbeleid • Telewerken beleid • Aanwijzing Logging Communicatie & Opslag: • Encryptiebeleid (PKI) (in ontwikkeling) Inkopen / aanbesteding: • Contractmanagement • Inkoopvoorwaarden en informatiebeveiligingseisen • Bewerkersovereenkomst • Geheimhoudingsverklaringen BIG • Handleiding screening personeel

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
1. Behoeftbepaling - Bieden triage-instrumenten Het triageproces is in dit archetype per cluster georganiseerd. Elk cluster hanteert hierbij haar eigen triage-instrumenten.	Gemeenten moeten vaststellen welke (persoons)gegevens noodzakelijk zijn met betrekking tot de triageprocessen⁶⁷ en welke (persoons)gegevens worden vastgelegd. De ondersteunende triage-instrumenten (bijvoorbeeld het gebruikte registratiesysteem) en processen dienen de privacy te borgen (noodzaak⁶⁸, subsidiariteit⁶⁹ en proportionaliteit⁷⁰ van gegevensverwerking). Dit geldt voor zowel de huidige als nieuw te verwerven triage-instrumenten, bij de nieuwe systemen is privacy by design⁷¹ het uitgangspunt. Hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (bijvoorbeeld burger en/of professional), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft uitgevoerd en voor welke taak met betrekking tot een signaal/melding. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de (persoons)gegevens beschikbaar, juist en actueel zijn.⁴⁵ Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
2. Behoeftbepaling - Ondersteunen ontvangen en beoordelen van signalen Meldingen en signalen worden via de beschikbare 'systemen' per cluster afgegeven.	Gemeenten moeten vaststellen welke (persoons)gegevens de verschillende meldingen en/of signalen (dienen te) bevatten en welke (persoons)gegevens vastgelegd (wat- en dat-informatie). Denk hierbij ook aan meldingen uit verschillende probleemgebieden die gecombineerd en geverifieerd moeten kunnen worden (bijvoorbeeld	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

⁶⁷ Triage is het proces van verhelderen, routeren en escaleren van vragen en casussen.

⁶⁸ Het bepalen van het doel van informatiedeling (doelbinding).

⁶⁹ subsidiariteit van de gegevensverwerking: is het doel ook te bereiken met een minder ingrijpende methode?

⁷⁰ proportionaliteit van de gegevensverwerking: hoe verhouden het doel en de daarvoor noodzakelijke gegevensuitwisseling zich tot de schending van de persoonlijke levenssfeer van de betrokkene en zijn omgeving

⁷¹ Bron: CBP -Privacy by Design gaat uit van het principe dat er in een vroeg stadium nagedacht wordt over het goede gebruik van persoonsgegevens binnen een organisatie, de noodzaak van het gebruik van deze gegevens en de bescherming ervan. Door al bij het ontwikkelen van systemen privacy en bescherming van persoonsgegevens in te bouwen is de kans op het succes ervan het grootst.

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
3. Klantcontact – Signaleren Voor de burger is er per cluster één centrale toegang die is ingericht om meldingen binnen dat cluster door te geleiden naar de juiste verantwoordelijke. Via welk kanaal een melding ook binnenkomt, een melding wordt per cluster geregistreerd en bevestigd.	gebeurtenissen vanuit basisregistraties en kernregistraties, signalen uit de samenloopvoorziening van het inlichtingenbureau). De ondersteunende informatiesystemen (bijvoorbeeld een centraal signaal- en meldingenregister) en processen (bijvoorbeeld één centrale toegangspoort of meerdere, melden van problemen via een e-formulier of een (web)service.) dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (bijvoorbeeld burger en/of professional), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft uitgevoerd en voor welke taak met betrekking tot een signaal/melding. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de (persoons)gegevens beschikbaar, juist en actueel zijn.⁴⁵ Denk hierbij aan: dat een melding/signaal niet verloren gaat, dat de ontvangst van de melding/signaal wordt bevestigd (bijvoorbeeld geautomatiseerd); dat de melding/signaal direct bij de verantwoordelijke functies binnenkomen en dat de melding/signaal ook wordt verwerkt en opgevolgd. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Denk hierbij aan: gebeurtenissen die vanuit bronsystemen worden gemeld; signalen die worden geregistreerd; dat meldingen op één plek samen komen en het informeren van de verantwoordelijke professional.	
4. Financiële afhandeling - Afhandelen en beheren declaraties en facturen	Gemeenten moeten vaststellen welke gegevens worden vastgelegd. Gemeenten moeten ook vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Hierbij is het van belang dat alleen geautoriseerde personen van de (contract)partners declaraties mogen indienen bij gemeenten. (Contract)partners mogen ook alleen hun eigen declaraties indienen en de afhandeling van hun declaraties volgen. Hierbij dient functiescheiding toegepast te worden om het risico op fraude te voorkomen/verkleinen. Denk hierbij aan het	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
5. Financiële afhandeling - Ondersteunen budgetbewaking De budgetbewaking vindt plaats per cluster of - als de gemeente heeft gekozen van het ontschotten van de budgetten - integraal.		

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
6. Verantwoording - Declareren geleverde diensten	klaarzetten van betalingen, het wijzigen van gegevens van crediteuren, het autoriseren van betalingen en het monitoren en bewaken van budgetten. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	
7. Verantwoording - Inzage in afhandeling declaraties		
8. Financiële afhandeling - Leveren van statistische informatie	Bij de uitwisseling van verantwoordings-, stuur-, en beleidsinformatie dient nagedacht te worden over welke informatie nodig is voor welke vraag (over de clusters heen). Is het bijvoorbeeld nodig om detail gegevens te verstrekken over verantwoordings-, stuur -, en beleidsinformatie of kan er worden geanonimiseerd? Kan (geanonimiseerde) verantwoordings-, stuur -, en beleidsinformatie in kleine gemeenschappen toch inzicht geven in het individu? Met de gecontracteerde (keten)partner moeten afspraken worden over welke informatie wordt aangeleverd en op welke wijze (bijvoorbeeld via een clearinghouse⁷²). Hierbij dienen de (bestaande) aanleveringsprotocollen de integriteit, vertrouwelijkheid en privacy te waarborgen. Er moet voor de nieuwe taken (en bestaande taken) en de daarop verzamelde en ten aanzien van de eventueel over leefdomeinen heen gekoppelde stuur- en/of beleidsinformatie een privacyprotocol te worden uitgewerkt.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag • Inkopen / aanbesteding
9. Financiële afhandeling - Leveren van verantwoordingsinformatie		
10. Verantwoording - Bieden horizontale en verticale verantwoording		
De gehanteerde clusters zijn bepalend voor de te genereren verantwoordingsinformatie. Waar vanuit de verticale verantwoording informatie gewenst is, is de te genereren minimale (en facultatieve) gegevensset leidend. Tevens is er behoefte aan beleidsinformatie en financiële informatie.		
11. Verantwoording - Bieden statistische informatie		
Statistische informatie wordt geleverd binnen één cluster maar niet over verschillende clusters heen.		
12. Verantwoording - Bieden van managementinformatie		
Managementinformatie wordt geleverd binnen één cluster maar niet over verschillende clusters heen.		

⁷² Het clearinghouse zorgt als derde partij voor de administratie en afhandeling van transacties tussen twee of meer partijen. De gestandaardiseerde registratie is goed mogelijk met behulp van een zogenaamde 'clearinghouse'-constructie waarbij de gegevens op cliëntniveau worden aangeleverd aan een organisatorisch onafhankelijk clearinghouse, die zorgt voor: enerzijds controle op de standaard (zijn alle basis- en aanvullende gegevens op de juiste manier ingevoerd?) en anderzijds voor (geanonimiseerde) verdeling van de informatie richting de verschillende belanghebbende actoren.

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
13. Bedrijfsfunctie Inkoop en contractbeheer - Beheren van contracten en SLA's Inkoop van zorg vindt per cluster plaats tenzij anders georganiseerd (bv centrale of regionale inkooporganisatie). Daar worden ook de contracten beheerd	In bestaande en/of nieuwe contracten dienen mogelijk beveiligingsaspecten meegenomen te worden, zoals de bewerkersovereenkomst. Met de (keten)partners moeten ook afspraken worden gemaakt over de wijze waarop verantwoording (monitoring) aan de gemeente wordt afgelegd.	• Inkopen / aanbesteding
14. Klantcontact - Beheren klantcontacten Per cluster zal per burger / huishouden de klantcontacten worden vastgelegd. Mogelijk, afhankelijk van de clusterkeuze, brengt dit met zich mee dat er meerdere klantcontacten van een burger / huishouden binnen de gemeente wordt geregistreerd.	Gemeenten moeten vaststellen welke (persoons)gegevens worden vastgelegd. Gemeenten moeten tevens vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de klantgegevens beschikbaar, juist en actueel zijn.⁴⁵ Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
15. Klantcontact - Maken afspraken Je moet afspraken kunnen maken, dat heeft prioriteit 1. Passend bij de doelstelling van dit archetype wil je uiteindelijk per cluster 1 soort afspraak kunnen maken. Dat heeft prioriteit 3.	Burgers, zaakwaarnemers en professionals moet er op kunnen vertrouwen dat de mogelijkheden (systemen) om afspraken te maken beschikbaar zijn en juiste en actuele gegevens bevatten.	• Communicatie & Opslag

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
16. Klantcontact – Inzage in klantgegevens en lopende zaken De klantgegevens zijn per sector op één plaats beschikbaar. Hierbij is onderscheid gemaakt in wat- en dat-informatie en is stringente autorisatiebeheer mogelijk.	Voor het opvolgen van meldingen, signalen en/of het voeren van het gesprek moet de regisseur kunnen beschikken over (een beperkte) set gegevens over de burger. Deze gegevens komen zowel uit bronsystemen van organisaties die betrokken zijn bij de ondersteuning van die burger (en zijn gezin) als uit de gemeentelijke systemen. Bij de hulpverlenende organisaties is in het algemeen veel informatie bekend over de situatie van de burger op een bepaald leefgebied en de al geleverde dienstverlening. Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. Tevens moeten gemeenten vaststellen welke (persoons)gegevens worden uitgewisseld tussen de ketenpartner en gemeenten. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (medewerkers, ketenpartners), welke gegevens mogen raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Denk hierbij aan de regisseur, de medewerker van het gemeentelijke KCC. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers en ketenpartners moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling van informatie tussen de voorziening van de ketenpartner en gemeentelijke voorziening dient de vertrouwelijkheid en integriteit te worden gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
17. Klantcontact – Tonen en bijwerken lopende zaken en mijn gegevens Eigen klantdossier en / of statusoverzichten worden gegenereerd per cluster. Niet direct noodzakelijk wel wenselijk.	Burgers, zaakwaarnemers en professionals moeten er op kunnen vertrouwen dat het klantdossier beschikbaar is en de juiste en actuele gegevens bevatten. Gemeenten moeten vaststellen wie (burgers, medewerkers en ketenpartners), welke gegevens mogen raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs burgers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeenten moeten ook vaststellen via welke kanalen het klantdossier wordt ontsloten, lokaal toegankelijk of (op termijn) ook via mijnOverheid.nl. Bij de uitwisseling van informatie dient de vertrouwelijkheid en integriteit te worden gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
18. Klantcontact – Tonen gemeentelijke producten en diensten Je maakt een nieuwe toegang per cluster. Zo zul je je producten en dienst ook inzichtelijk moeten maken.	De burger moet er op kunnen vertrouwen dat de aangeboden informatie over gemeentelijke producten en diensten digitaal beschikbaar, juist en actueel is. Tevens moet de burger er op kunnen vertrouwen dat de aangeboden relevante informatie ook daadwerkelijk van de gemeente afkomstig is. De manier waarop gemeentelijke producten en diensten	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
19. Klantcontact – Aanvragen producten en diensten Wanneer je het van belang acht dat de burger digitaal alle diensten en producten kan, aanvragen zul je dit moeten inregelen per 'cluster'.	kunnen worden aangevraagd is minder van belang (een aanvraagformulier per product/dienst of 1 startpunt met een soort vraagboom). Als gemeenten producten en diensten van ketenpartners beschikbaar stellen, moeten gemeenten beslissen hoe met aanvragen voor deze producten en diensten van ketenpartners wordt omgegaan. Gemeenten moeten vaststellen of gebruikers die producten en/of diensten aanvragen zich moeten aanmelden/registreren voordat ze gebruik kunnen maken van deze dienstverlening. Tevens moeten gemeenten vaststellen of (persoons)gegevens noodzakelijk zijn met betrekking tot deze gemeentelijke dienstverlening. Zo ja, om welke (persoons)gegevens gaat het hier dan. Gemeenten moeten vaststellen wie welke gegevens mag plaatsen en onderhouden/bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Burgers kunnen vaak via meerdere kanalen (bijvoorbeeld met papieren aanvragen) gemeentelijke producten en diensten aanvragen. Wanneer gemeenten het van belang acht dat de burger alle diensten en producten digitaal kan aanvragen, moeten ze dit inrichten. Bij de uitwisseling van informatie tussen de ketenpartner en gemeenten dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	
20. Stimulering zelfredzaamheid - Matchen vraag en aanbod Dit is goed om te hebben. Past ook binnen de doelstelling van het archetype, maar heeft geen prioriteit.	Ongeacht de rol (deze kan variëren van ondersteunend, faciliterend tot regulerend en initiërend) die de gemeente hierin kiest, kan bij eventuele fouten/misstanden de gemeente hierop aangesproken worden. Dit ondanks het feit dat deze informatie aangelevert kan worden door derden (bijvoorbeeld burgers, buurten, wijken, regio's, dienstverleners en instellingen). Het is mogelijk dat de ondersteunende websites en aangeboden informatie los staan van de gemeentelijke website. De burger moet er op kunnen vertrouwen dat de	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag ○ Denk hierbij aan SSL (PKIoverheid) certificaten.
21. Stimulering zelfredzaamheid - Ondersteunen buurt-/wijk- en burgerinitiatieven		

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
22. Stimulering zelfredzaamheid - Ondersteunen zelfdiagnose Dit is goed om te hebben. Past ook binnen de doelstelling van het archetype, maar heeft geen prioriteit.	getoonde informatie (bijvoorbeeld vraag en aanbod, buurt-/wijk- en burgerinitiatieven en zelfdiagnose, welke partijen lokaal of regionaal beschikbaar zijn voor welke diensten) beschikbaar, juist en actueel is. Gemeenten moeten vaststellen of gebruikers die informatie aanleveren (content plaatsen) zich moeten aanmelden/registreren voordat ze gebruik kunnen maken van deze dienstverlening. Tevens moeten gemeenten vaststellen of (persoons)gegevens noodzakelijk zijn met betrekking tot de geleverde dienstverlening. Zo ja, om welke (persoons)gegevens gaat het hier dan. Bij de uitwisseling en opslag van (persoons)gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Op het moment dat wordt aangehaakt bij bestaande initiatieven/applicaties moeten gemeenten vaststellen of deze voldoen aan de eisen en wensen van de gemeenten. Denk hierbij aan privacy en beveiligingseisen.	
23. Stimulering zelfredzaamheid - Tonen content wijkteam In dit archetype is niet zozeer de wijk het vertrekpunt, maar meer het cluster van (samenhangende) taken. Het tonen van de content van een wijkteam is hier dus niet van toepassing		
24. Stimulering zelfredzaamheid - Tonen sociale kaart Past binnen het archetype. Geen hoge prioriteit. Zou uiteindelijk mooi zijn om aan te haken bij het eigen dossier.		
25. Planvorming - Beheren groepstraject Het beheren van een groepstraject gebeurt binnen dit archetype binnen het betreffende cluster	Gemeenten moeten vaststellen welke (persoons)gegevens worden vastgelegd, zowel voor het beheren van een groepstraject als bij het opstellen van het plan. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (de professional en/of regisseur), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd.Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (de professional en/of regisseur) moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van (persoons)gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bijvoorbeeld het regiesysteem dat in deze functionaliteit voorziet.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
26. Planvorming - Opstellen plan Het opstellen van een plan is hier beperkt tot de gehanteerde clustering. Het kan dus zijn dat per cluster een plan wordt opgesteld.		

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
27. Regievoering – Uitzetten en monitoren opdrachten Regie binnen dit archetype is per cluster afgebakend. Daarbinnen worden opdrachten uitgezet en gemonitord.	Gemeenten moeten vaststellen welke (persoons)gegevens nodig zijn bij het uitzetten van de verschillende opdrachten, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (regisseurs), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd.Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (regisseurs) moeten er op kunnen vertrouwen dat de getoonde informatie, welke zorgaanbieders welke diensten bieden- en tegen welke kosten, beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van gegevens de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bijvoorbeeld bij het uitzetten van de opdrachten online (via eigen zaakstelsel of via transitiebericht (toewijzing) conform de AWBZ-brede zorgregistratie (AZR) standaarden).	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
28. Specifieke ondersteuning - Beheren werkvoorraad In dit archetype wordt zoveel als mogelijk integraal afgehandeld binnen het cluster van taken. Het beheren van de werkvoorraad (sturen op caseload en een juiste verdeling van de werkzaamheden) is hier dus beperkt tot de afbakening van het cluster. De werkvoorraad wordt bijgehouden door de systemen die de gemeente nu al gebruikt. Dit kan via een gemeentebreed zaakstelsel zijn, of taakspecifieke applicaties, eventueel in combinatie met een generiek zakenmagazijn.	Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt (zakensysteem⁷³ /-magazijn), zodat de werkzaamheden adequaat kunnen worden uitgevoerd. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd.Fout! Bladwijzer niet	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

⁷³ Systeem voor beheer van zaken, bij voorkeur conform het Referentiemodel Gemeentelijke Basisgegevens Zaken (RGBZ) en de Zaaktypecatalogus

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
29. Specifieke ondersteuning - Beheren zaken Zakenbeheer wordt gerealiseerd via de systemen die de gemeente nu al gebruikt. Dit kan via een gemeentebreed zaaksysteem zijn, of taakspecifieke applicaties, eventueel in combinatie met een generiek zakenmagazijn.	gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (regisseurs, teamleden en/of professionals) moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	
30. Specifieke ondersteuning - Bijwerken status van levering product of dienst Terugkoppeling van geleverde diensten en producten gewenst	Gemeenten moeten vaststellen of ketenpartners de terugkoppeling of inhoudelijke afhandeling rechtstreeks in de gemeentelijke voorzieningen kunnen/mogen aanbrengen. Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag • Inkopen / aanbesteding

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
31. Specifieke ondersteuning - Ondersteunen inhoudelijke afhandeling Het ligt voor de hand om voor de inhoudelijke afhandeling specifieke systemen en voorzieningen te gebruiken (cluster specifieke werkwijze). Gemeenten stellen per cluster koppelvlakken beschikbaar om uitwisseling van en naar hun sectorale voorzieningen mogelijk te maken.	bijgewerkt, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. Tevens moeten gemeenten vaststellen welke (persoons)gegevens worden uitgewisseld tussen de voorziening van de ketenpartner en hun eigen voorziening in verband met de afhandeling van specialistische zaken. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers en ketenpartners moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling van informatie tussen de voorziening van de ketenpartner en gemeentelijke voorziening, via koppelvlakken of een webbased applicatie, dient de vertrouwelijkheid en integriteit gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie. Mogelijk moeten er met betrekking tot de terugkoppeling of inhoudelijke afhandeling extra afspraken worden gemaakt tussen gemeenten en ketenpartners. Bijvoorbeeld: Gemeenten moeten als verantwoordelijke⁷⁴ een schriftelijke overeenkomst (bewerkerovereenkomst) af sluiten met de ketenpartners (de bewerker⁷⁵). De bewerkerovereenkomst kan zelfstandig worden gebruikt maar is meestal een onderdeel van een overeenkomst met een breder bereik.⁷⁶	

4.5 Archetype 4 Integraal in 2e instantie

In deze paragraaf wordt ingezoomd op het archetype integraal in 2^e instantie. Hierbij wordt als eerste een korte toelichting gegeven specifiek voor dit archetype en een koppeling met de relevante informatiebeveiligingsonderwerpen (zie ook paragraaf 5.7 ‘ondersteunde

⁷⁴ De verantwoordelijke is volgens de Wet bescherming persoonsgegevens (Wbp) degene die het doel en de middelen voor de verwerking van persoonsgegevens bepaalt (Art. 1 sub d Wbp).

⁷⁵ De Wbp definieert de bewerker als ‘degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen’ (Art. 1 sub e Wbp).

⁷⁶ zie hiervoor het document Inkoop voorwaarden en beveiligingseisen van de IBD

documenten') en operationele BIG producten (BIG-OP). Daarna wordt ingezoomd op de bedrijfs- en applicatiefuncties. Hierbij wordt per applicatiefunctie een korte algemene toelichting gegeven specifiek voor het archetype, een toelichting met betrekking tot informatiebeveiliging en een koppeling met de relevante informatiebeveiligingsonderwerpen (zie ook paragraaf 5.7 'ondersteunde documenten') en operationele BIG producten (BIG-OP).

Achtergrondinformatie informatiebeveiliging	BIG en BIG-OP producten
Om als gemeente integrale dienstverlening te kunnen bieden aan burgers in het kader van de drie decentralisaties is het kunnen delen van gegevens binnen en over domeinen een randvoorwaarde. Burgers moeten erop kunnen vertrouwen dat er zorgvuldig wordt omgegaan met persoonsgegevens wanneer zij bepaalde zorg of dienstverlening ontvangen. Natuurlijk hebben gemeenten nu al de verantwoordelijkheid voor het goed en zorgvuldig omgaan met persoonsgegevens van burgers. De drie decentralisaties kunnen betekenen dat gemeenten meer gegevens zullen verwerken en hiervoor ook meer zullen samenwerken met andere keten- en contractpartners. Dat roept andere vragen op bijvoorbeeld over het delen van gegevens tussen professionals, bijvoorbeeld in een wijkteam. Het is dan ook zaak om privacybeleid te (her)formuleren en dit te implementeren in de (bestaande en nieuwe) werkprocessen. In 1e instantie wijzigt er, anders dan de bijkomende taken, niet veel aan de huidige manier van informatievoorziening- en verwerking. Wanneer de huidige werkwijze voldoet aan de eisen van informatieveiligheid, dan zal in de nieuwe situatie de informatieveiligheid ook geborgd zijn. Vooral in 2e instantie heb je veel gegevens over een burger/huishouden beschikbaar en wanneer je met een zaakssysteem werkt zal je die gegevens verwerken. Dit brengt andere informatieveiligheids-issues met zich mee dan degenen waar nu in is voorzien. Uitwisseling van informatie gaat veelal over netwerken en het is zaak hierbij oog te hebben voor de juiste beveiliging (encryptie) van informatie. Zeker als er gebruik wordt gemaakt van uitwisseling met derden over mogelijk onveilige kanalen buiten de gemeente. Het gaat hierbij niet alleen over het transport maar ook over de opslag zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie. Als gevoelige informatie buiten het gemeentelijke domein wordt opgeslagen (bij derde, als die al de gegevens lokaal mogen opslaan) zal dit extra eisen opleveren voor de beveiliging van deze informatie. Gemeenten moeten ook de zaken geregeld hebben die in paragraaf 4.1 'Algemeen en archetype onafhankelijk' zijn beschreven.	Privacy impact assessment: • Toelichting bij het Privacy Impact Assessment (PIA) • PIA – Vragenlijst • PIA - Verslag Persoonsgegevens: • Handreiking dataclassificatie • Bewerkersovereenkomst Authenticatie en Autorisatie (inclusief wachtwoorden): • Toegangsbeleid • Wachtwoordbeleid • Telewerken beleid • Aanwijzing Logging Communicatie & Opslag: • Encryptiebeleid (PKI) (in ontwikkeling) Inkopen / aanbesteding: • Contractmanagement • Inkoopvoorwaarden en informatiebeveiligingseisen • Bewerkersovereenkomst • Geheimhoudingsverklaringen BIG • Handleiding screening personeel

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
1. Behoeftbepaling - Bieden triage-instrumenten Het triageproces is ook in dit archetype van belang, maar pas op het moment dat gekozen wordt voor een integrale benadering.	Gemeenten moeten vaststellen welke (persoons)gegevens noodzakelijk zijn met betrekking tot de triageprocessen⁷⁷ en welke(persoons)gegevens worden vastgelegd. De ondersteunende triage-instrumenten (bijvoorbeeld het gebruikte registratiesysteem) en processen dienen de privacy te borgen (noodzaak⁷⁸, subsidiariteit⁷⁹ en proportionaliteit⁸⁰ van gegevensverwerking). Dit geldt voor zowel de huidige als nieuw te verwerven triage-instrumenten, bij de nieuwe systemen is privacy bij design⁸¹ het uitgangspunt. Hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (bijvoorbeeld burger en/of professional), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft uitgevoerd en voor welke taak met betrekking tot een signaal/melding. Bij BRP wordt dit protocolleren genoemd.Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de (persoons)gegevens beschikbaar, juist en actueel zijn.⁴⁵ Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
2. Behoeftbepaling - Ondersteunen ontvangen en beoordelen van signalen Meldingen en signalen worden primair afgehandeld via de bestaande systematieken. Wel moet aanvullend een systematiek worden ingericht voor signalen en meldingen vanuit de bestaande kanalen naar de integrale voorziening in tweede instantie.	Gemeenten moeten vaststellen welke (persoons)gegevens de verschillende meldingen en/of signalen (dienen te) bevatten en welke(persoons)vastgelegd (wat- en dat-informatie). Denk hierbij ook aan meldingen uit verschillende probleemgebieden die gecombineerd en geverifieerd moeten kunnen worden (bijvoorbeeld gebeurtenissen vanuit basisregistraties en kernregistraties, signalen uit de samenloopvoorziening van het inlichtingenbureau). De ondersteunende informatiesystemen	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

⁷⁷ Triage is het proces van verhelderen, routeren en escaleren van vragen en casussen.

⁷⁸ Het bepalen van het doel van informatiedeling (doelbinding).

⁷⁹ subsidiariteit van de gegevensverwerking: is het doel ook te bereiken met een minder ingrijpende methode?

⁸⁰ proportionaliteit van de gegevensverwerking: hoe verhouden het doel en de daarvoor noodzakelijke gegevensuitwisseling zich tot de schending van de persoonlijke levenssfeer van de betrokkene en zijn omgeving

⁸¹ Bron: CBP -Privacy by Design gaat uit van het principe dat er in een vroeg stadium nagedacht wordt over het goede gebruik van persoonsgegevens binnen een organisatie, de noodzaak van het gebruik van deze gegevens en de bescherming ervan. Door al bij het ontwikkelen van systemen privacy en bescherming van persoonsgegevens in te bouwen is de kans op het succes ervan het grootst.

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
3. Klantcontact – Signaleren Voor de burger is er per cluster één centrale toegang die is ingericht om meldingen binnen dat cluster door te geleiden naar de juiste verantwoordelijke. Via welk kanaal een melding ook binnenkomt, een melding wordt per cluster geregistreerd en bevestigd. Op een later moment worden de verschillende toegangspoorten samengevoegd tot één toegangspoort en worden alle meldingen centraal geregistreerd. Een geregistreerde melding wordt altijd bevestigd.	(bijvoorbeeld een centraal signaal- en meldingenregister) en processen (bijvoorbeeld één centrale toegangspoort of meerdere, melden van problemen via een e-formulier of een (web)service.) dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (bijvoorbeeld burger en/of professional), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft uitgevoerd en voor welke taak met betrekking tot een signaal/melding. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de (persoons)gegevens beschikbaar, juist en actueel zijn.⁴⁵ Denk hierbij aan: dat een melding/signaal niet verloren gaat, dat de ontvangst van de melding/signaal wordt bevestigd (bijvoorbeeld geautomatiseerd); dat de melding/signaal direct bij de verantwoordelijke functies binnenkomen en dat de melding/signaal ook wordt verwerkt en opgevolgd. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Denk hierbij aan: gebeurtenissen die vanuit bronsystemen worden gemeld; signalen die worden geregistreerd; dat meldingen op één plek samen komen en het informeren van de verantwoordelijke professional.	
4. Financiële afhandeling - Afhandelen en beheren declaraties en facturen	Gemeenten moeten vaststellen welke gegevens worden vastgelegd. Gemeenten moeten ook vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Hierbij is het van belang dat alleen geautoriseerde personen van de (contract)partners declaraties mogen indienen bij gemeenten. (Contract)partners mogen ook alleen hun eigen declaraties indienen en de afhandeling van hun declaraties volgen. Hierbij dient functiescheiding toegepast te worden om het risico op fraude te voorkomen/verkleinen. Denk hierbij aan het klaarzetten van betalingen, het wijzigen van gegevens	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
5. Financiële afhandeling - Ondersteunen budgetbewaking		
6. Verantwoording - Declareren geleverde diensten		

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
7. Verantwoording - Inzage in afhandeling declaraties	van crediteuren, het autoriseren van betalingen en het monitoren en bewaken van budgetten. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	
8. Financiële afhandeling - Leveren van statistische informatie	Bij de uitwisseling van verantwoordings-, stuur-, en beleidsinformatie dient nagedacht te worden over welke informatie nodig is voor welke vraag. Is het bijvoorbeeld nodig om detail gegevens te verstrekken over verantwoordings-, stuur-, en beleidsinformatie of kan er worden geanonimiseerd? Kan (geanonimiseerde) verantwoordings-, stuur-, en beleidsinformatie in kleine gemeenschappen toch inzicht geven in het individu? Met de gecontracteerde (keten)partner moeten afspraken worden over welke informatie wordt aangeleverd en op welke wijze (bijvoorbeeld via een clearinghouse⁸²). Hierbij dienen de (bestaande) aanleveringsprotocollen de integriteit, vertrouwelijkheid en privacy te waarborgen. Er moet voor de nieuwe taken (en bestaande taken) en de daarop verzamelde en ten aanzien van de eventueel over leefdomeinen heen gekoppelde stuur- en/of beleidsinformatie een privacyprotocol te worden uitgewerkt.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag • Inkopen / aanbesteding
9. Financiële afhandeling - Leveren van verantwoordingsinformatie		
10. Verantwoording - Bieden horizontale en verticale verantwoording		
Primair doel is het ondersteunen van Multiprobleemgezinnen (MPG) en daarmee het voorkomen van recidive en verdere escalatie. Hier is de verantwoording primair op gericht.		
11. Verantwoording - Bieden statistische informatie		
Statistische informatie wordt zowel geleverd vanuit één cluster als over de clusters heen voor burgers met meervoudige problematiek.		
12. Verantwoording - Bieden van managementinformatie		
Managementinformatie wordt zowel geleverd vanuit één cluster als over de clusters heen voor burgers met meervoudige problematiek.		

⁸² Het clearinghouse zorgt als derde partij voor de administratie en afhandeling van transacties tussen twee of meer partijen. De gestandaardiseerde registratie is goed mogelijk met behulp van een zogenaamde 'clearinghouse'-constructie waarbij de gegevens op cliëntniveau worden aangeleverd aan een organisatorisch onafhankelijk clearinghouse, die zorgt voor: enerzijds controle op de standaard (zijn alle basis- en aanvullende gegevens op de juiste manier ingevoerd?) en anderzijds voor (geanonimiseerde) verdeling van de informatie richting de verschillende belanghebbende actoren.

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
13. Bedrijfsfunctie Inkoop en contractbeheer - Beheren van contracten en SLA's Inkoop van zorg vindt per kolom plaats tenzij anders georganiseerd (bv centrale of regionale inkooporganisatie). Daar worden ook de contracten beheerd. Binnen dit archetype is inkoop en het beheren van contracten met betrekking tot wijkoverstijgend en gespecialiseerd aanbod centraal binnen de gemeente belegd.	In bestaande en/of nieuwe contracten dienen mogelijk beveiligingsaspecten meegenomen te worden, zoals de bewerkersovereenkomst. Met de (keten)partners moeten ook afspraken worden gemaakt over de wijze waarop verantwoording (monitoring) aan de gemeente wordt afgelegd.	• Inkopen / aanbesteding
14. Klantcontact - Beheren klantcontacten Het huishouden is niet primair het vertrekpunt in dit archetype. In eerste instantie worden de klantcontacten beheerd per kanaal. In tweede instantie wordt integraal gewerkt en is de groep het vertrekpunt om bestaande klantcontacten te bundelen en te koppelen aan het op te stellen plan.	Gemeenten moeten vaststellen welke (persoons)gegevens worden vastgelegd. Gemeenten moeten tevens vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de klantgegevens beschikbaar, juist en actueel zijn.⁴⁵ Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
15. Klantcontact - Maken afspraken Op dit moment kun je per 'kolom' en/of dienst en/of product ook op (diverse) manieren afspraken. Wanneer deze voldoen hoeft je 'enkel' wat in te regelen voor nieuwe producten en/of diensten. Voor de eerste instantie kun je het op deze manier inrichten. In tweede instantie heb je een contactpersoon en kun je het dus ook op die manier (persoonlijk) regelen. Dit is een tussenoplossing. Uiteindelijk wil je voor zowel de eerste als de tweede instantie een 'gestroomlijnder' proces.	Burgers, zaakwaarnemers en professionals moet er op kunnen vertrouwen dat de mogelijkheden (systemen) om afspraken te maken beschikbaar zijn en juiste en actuele gegevens bevatten.	• Communicatie & Opslag

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
16. Klantcontact – Inzage in klantgegevens en lopende zaken De klantgegevens zijn via sectorale klantdossiers beschikbaar. Hierbij is onderscheid gemaakt in wat- en dat-informatie en is stringente autorisatiebeheer mogelijk.	Voor het opvolgen van meldingen, signalen en/of het voeren van het gesprek moet de regisseur kunnen beschikken over (een beperkte) set gegevens over de burger. Deze gegevens komen zowel uit bronsystemen van organisaties die betrokken zijn bij de ondersteuning van die burger (en zijn gezin) als uit de gemeentelijke systemen. Bij de hulpverlenende organisaties is in het algemeen veel informatie bekend over de situatie van de burger op een bepaald leefgebied en de al geleverde dienstverlening. Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. Tevens moeten gemeenten vaststellen welke (persoons)gegevens worden uitgewisseld tussen de ketenpartner en gemeenten. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (medewerkers, ketenpartners), welke gegevens mogen raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Denk hierbij aan de regisseur, de medewerker van het gemeentelijke KCC. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers en ketenpartners moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling van informatie tussen de voorziening van de ketenpartner en gemeentelijke voorziening dient de vertrouwelijkheid en integriteit te worden gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
17. Klantcontact – Tonen en bijwerken lopende zaken en mijn gegevens Eigen klantdossier is hier leuk (maar ook niet meer dan dat) in eerste instantie. Je kunt ook bellen om de status van je aanvraag te zien. Je kunt per brief informeren. Je zult uiteindelijk per kolom wel wat dienen in te regelen (in sommige kolomen zal dat nu al geregeld zijn). In tweede instantie (integraal) is het op termijn wel noodzakelijk.	Burgers, zaakwaarnemers en professionals moeten er op kunnen vertrouwen dat het klantdossier beschikbaar is en de juiste en actuele gegevens bevatten. Gemeenten moeten vaststellen wie (burgers, medewerkers en ketenpartners), welke gegevens mogen raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs burgers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeenten moeten ook vaststellen via welke kanalen het klantdossier wordt ontsloten, lokaal toegankelijk of (op termijn) ook via mijnOverheid.nl. Bij de uitwisseling van informatie dient de vertrouwelijkheid en integriteit te worden gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
18. Klantcontact – Tonen gemeentelijke producten en diensten Voor de huidige diensten is de website en het KCC reeds in functie. Je kunt opteren om de 'nieuwe' functies ook een plek te geven. Je kunt ook kiezen om for the time being de bestaande kanalen open te laten.	De burger moet er op kunnen vertrouwen dat de aangeboden informatie over gemeentelijke producten en diensten digitaal beschikbaar, juist en actueel is. Tevens moet de burger er op kunnen vertrouwen dat de aangeboden relevante informatie ook daadwerkelijk van de gemeente afkomstig is. De manier waarop gemeentelijke producten en diensten kunnen worden aangevraagd is minder van belang (een aanvraagformulier per product/dienst of 1 startpunt met een soort vraagboom). Als gemeenten	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
19. Klantcontact – Aanvragen producten en diensten Wanneer je het van belang acht dat burger digitaal alle diensten en producten kunnen aanvragen. Zul je dit moeten inregelen per 'kolom'.	producten en diensten van ketenpartners beschikbaar stellen moeten gemeenten beslissen hoe met aanvragen voor deze producten en diensten van ketenpartners wordt omgegaan. Gemeenten moeten vaststellen of gebruikers die producten en/of diensten aanvragen zich moeten aanmelden/registreren voordat ze gebruik kunnen maken van deze dienstverlening. Tevens moeten gemeenten vaststellen of (persoons)gegevens noodzakelijk zijn met betrekking tot deze gemeentelijke dienstverlening. Zo ja, om welke (persoons)gegevens gaat het hier dan. Gemeenten moeten vaststellen wie welke gegevens mag plaatsen en onderhouden/bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Burgers kunnen vaak via meerdere kanalen (bijvoorbeeld met papieren aanvragen) gemeentelijke producten en diensten aanvragen. Wanneer gemeenten het van belang acht dat de burger alle diensten en producten digitaal kan aanvragen, moeten ze dit inrichten. Bij de uitwisseling van informatie tussen de ketenpartner en gemeenten dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	
20. Stimulering zelfredzaamheid - Matchen vraag en aanbod Dit is goed om te hebben. Past binnen de doelstelling, maar heeft geen prioriteit.	Ongeacht de rol (deze kan variëren van ondersteunend, faciliterend tot regulerend en initiërend) die de gemeente hierin kiest, kan bij eventuele fouten/misstanden de gemeente hierop aangesproken worden. Dit ondanks het feit dat deze informatie aangelevert kan worden door derden (bijvoorbeeld burgers, buurten, wijken, regio's, dienstverleners en instellingen). Het is mogelijk dat de ondersteunende websites en aangeboden informatie los staan van de gemeentelijke website. De burger moet er op kunnen vertrouwen dat de getoonde informatie (bijvoorbeeld vraag en aanbod, buurt-/wijk- en burgerinitiatieven en zelfdiagnose, welke partijen lokaal of regionaal beschikbaar zijn voor welke diensten) beschikbaar, juist en actueel is. Gemeenten moeten vaststellen of gebruikers die informatie aanleveren (content plaatsen) zich	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag ○ Denk hierbij aan SSL (PKIoverheid) certificaten.
21. Stimulering zelfredzaamheid - Ondersteunen buurt-/wijk- en burgerinitiatieven Geen direct doel binnen dit archetype waar de focus met name ligt op integraliteit bij niet zelfredzame doelgroepen dan wel bij trajecten waar tot op dat moment geen effectieve dienstverlening heeft kunnen plaatsvinden.		

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
22. Stimulering zelfredzaamheid - Ondersteunen zelfdiagnose Dit is goed om te hebben. Past binnen de doelstelling, maar heeft geen prioriteit.	moeten aanmelden/registreren voordat ze gebruik kunnen maken van deze dienstverlening. Tevens moeten gemeenten vaststellen of (persoons)gegevens noodzakelijk zijn met betrekking tot de geleverde dienstverlening. Zo ja, om welke (persoons)gegevens gaat het hier dan. Bij de uitwisseling en opslag van (persoons)gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Op het moment dat wordt aangehaakt bij bestaande initiatieven/applicaties moeten gemeenten vaststellen of deze voldoen aan de eisen en wensen van de gemeenten. Denk hierbij aan privacy en beveiligingseisen.	
23. Stimulering zelfredzaamheid - Tonen content wijkteam Binnen dit archetype heeft een gemeente een specifieke voorziening voor Multiprobleemgezinnen (MPG). De wijk is hier dus geen uitgangspunt en daarmee het tonen van de content van het wijkteam ook niet.		
24. Stimulering zelfredzaamheid - Tonen sociale kaart Past binnen het archetype. Geen hoge prioriteit. Zou uiteindelijk mooi zijn om aan te haken bij het eigen dossier.		
25. Planvorming - Beheren groepstraject Het beheren van een groepstraject gebeurt in dit archetype pas in tweede instantie.	Gemeenten moeten vaststellen welke (persoons)gegevens worden vastgelegd, zowel voor het beheren van een groepstraject als bij het opstellen van het plan. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (de professional en/of regisseur), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (de professional en/of regisseur) moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van (persoons)gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bijvoorbeeld het regiesysteem dat in deze functionaliteit voorziet.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
26. Planvorming - Opstellen plan Het opstellen van een plan gebeurt pas in tweede instantie. De hiervoor benodigde functionaliteit en benodigde informatie is ook pas in tweede instantie benodigd. In eerste instantie is deze functionaliteit niet nodig.		

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
27. Regievoering – Uitzetten en monitoren opdrachten Binnen dit archetype wordt primair uitgegaan van regie op het proces in tweede instantie. Het uitzetten en monitoren van opdrachten gebeurt hier primair offline. Uiteraard kan gemeente ervoor kiezen de opdrachten ook online uit te zetten. Dit kan, waar het binnengemeentelijke dienstverlening betreft, met het eigen zaakstelsel. Waar het dienstverlening door zorgaanbieders betreft, kan dit met het transitiebericht (toewijzing) conform de AWBZ-brede zorgregistratie (AZR) standaarden	Gemeenten moeten vaststellen welke (persoons)gegevens nodig zijn bij het uitzetten van de verschillende opdrachten, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (regisseurs), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd.Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (regisseurs) moeten er op kunnen vertrouwen dat de getoonde informatie, welke zorgaanbieders welke diensten bieden- en tegen welke kosten, beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van gegevens de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bijvoorbeeld bij het uitzetten van de opdrachten online (via eigen zaakstelsel of via transitiebericht (toewijzing) conform de AWBZ-brede zorgregistratie (AZR) standaarden).	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
28. Specifieke ondersteuning - Beheren werkvoorraad Binnen dit archetype is de primaire doelstelling het integraal ondersteunen van Multiprobleemgezinnen (MPG) in tweede instantie. Het betreft hier een relatief klein volume en dus is het beheren van werkvoorraad geen belangrijke functionaliteit. De werkvoorraad wordt bijgehouden door de systemen die de gemeente nu al gebruikt. Dit kan via een gemeentebreed zaakstelsel zijn, of taakspecifieke applicaties, eventueel in combinatie met een generiek zakenmagazijn.	Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt (zakensysteem⁸³ /-magazijn), zodat de werkzaamheden adequaat kunnen worden uitgevoerd. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd.Fout! Bladwijzer niet gedefinieerd.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

⁸³ Systeem voor beheer van zaken, bij voorkeur conform het Referentiemodel Gemeentelijke Basisgegevens Zaken (RGBZ) en de Zaaktypencatalogus

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
29. Specifieke ondersteuning - Beheren zaken Zakenbeheer wordt gerealiseerd via de systemen die de gemeente nu al gebruikt. Dit kan via een gemeentebreed zaaksysteem zijn, of taakspecifieke applicaties, eventueel in combinatie met een generiek zakenmagazijn.	gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (regisseurs, teamleden en/of professionals) moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	
30. Specifieke ondersteuning - Bijwerken status van levering product of dienst Terugkoppeling van geleverde diensten en producten gewenst	Gemeenten moeten vaststellen of ketenpartners de terugkoppeling of inhoudelijke afhandeling rechtstreeks in de gemeentelijke voorzieningen kunnen/mogen aanbrengen. Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag • Inkopen / aanbesteding

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
31. Specifieke ondersteuning - Ondersteunen inhoudelijke afhandeling Het ondersteunen van de inhoudelijke afhandeling is niet het primaire doel, omdat de focus ligt op het voeren van procesregie. Gemeenten stellen een webapplicatie beschikbaar die de ketenpartners kunnen gebruiken voor de communicatie met gemeenten. Later stellen gemeenten koppelvlakken beschikbaar om uitwisseling van en naar hun voorzieningen mogelijk te maken	bijgewerkt, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. Tevens moeten gemeenten vaststellen welke (persoons)gegevens worden uitgewisseld tussen de voorziening van de ketenpartner en hun eigen voorziening in verband met de afhandeling van specialistische zaken. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers en ketenpartners moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling van informatie tussen de voorziening van de ketenpartner en gemeentelijke voorziening, via koppelvlakken of een webbased applicatie, dient de vertrouwelijkheid en integriteit gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie. Mogelijk moeten er met betrekking tot de terugkoppeling of inhoudelijke afhandeling extra afspraken worden gemaakt tussen gemeenten en ketenpartners. Bijvoorbeeld: Gemeenten moeten als verantwoordelijke⁸⁴ een schriftelijke overeenkomst (bewerkerovereenkomst) afsluiten met de ketenpartners (de bewerker⁸⁵). De bewerkerovereenkomst kan zelfstandig worden gebruikt maar is meestal een onderdeel van een overeenkomst met een breder bereik.⁸⁶	

4.6 Archetype 5 Geclusterde integraliteit elders

In deze paragraaf wordt ingezoomd op het archetype geclusterde integraliteit elders. Hierbij wordt als eerste een korte toelichting gegeven specifiek voor dit archetype en een koppeling met de relevante informatiebeveiligingsonderwerpen (zie ook paragraaf 5.7 ‘ondersteunde

⁸⁴ De verantwoordelijke is volgens de Wet bescherming persoonsgegevens (Wbp) degene die het doel en de middelen voor de verwerking van persoonsgegevens bepaalt (Art. 1 sub d Wbp).

⁸⁵ De Wbp definieert de bewerker als ‘degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen’ (Art. 1 sub e Wbp).

⁸⁶ zie hiervoor het document Inkoop voorwaarden en beveiligingseisen van de IBD

documenten') en operationele BIG producten (BIG-OP). Daarna wordt ingezoomd op de bedrijfs- en applicatiefuncties. Hierbij wordt per applicatiefunctie een korte algemene toelichting gegeven specifiek voor het archetype, een toelichting met betrekking tot informatiebeveiliging en een koppeling met de relevante informatiebeveiligingsonderwerpen (zie ook paragraaf 5.7 'ondersteunde documenten') en operationele BIG producten (BIG-OP).

Achtergrondinformatie informatiebeveiliging	BIG en BIG-OP producten
Per cluster zal per burger/huishouden informatie worden vergaard. Dit brengt, afhankelijk van de clusterkeuze, met zich mee dat er meer informatie van een burger/huishouden op één (digitale) locatie bewaard wordt. Burgers moeten erop kunnen vertrouwen dat er zorgvuldig wordt omgegaan met persoonsgegevens wanneer zij bepaalde zorg of dienstverlening ontvangen. Natuurlijk hebben gemeenten nu al de verantwoordelijkheid voor het goed en zorgvuldig omgaan met persoonsgegevens van burgers. De drie decentralisaties kunnen betekenen dat gemeenten meer gegevens zullen verwerken en hiervoor ook meer zullen samenwerken met andere keten- en contractpartners. Daarnaast is het zo dat in dit type het leeuwendeel van de informatieverwerking ten aanzien van de gegevens plaats vindt buiten de eigen organisatie. Dat roept andere vragen op bijvoorbeeld over het delen van gegevens tussen professionals, bijvoorbeeld in een wijkteam. Dit vraagt het een en ander van informatiebeveiliging. Het is dan ook zaak om privacybeleid te (her)formuleren en dit te implementeren in de (bestaande en nieuwe) werkprocessen. Voor een juiste inrichting van toegangsrechten binnen systemen en tot informatie is het van belang goed te definiëren wie (functietype) welke (wat/dat informatie) te zien mag krijgen. Daarnaast is een auditlogging van belang om achteraf te controleren wie wat heeft ingezien en wanneer en voor welke taak. De kans bestaat dat de bestaande systemen die binnen dit archetype aanwezig zijn dit nog niet op orde hebben. Uitwisseling van informatie gaat veelal over netwerken en het is zaak hierbij oog te hebben voor de juiste beveiliging (encryptie) van informatie. Zeker als er gebruik wordt gemaakt van uitwisseling met derden over mogelijk onveilige kanalen buiten de gemeente. Het gaat hierbij niet alleen over het transport maar ook over de opslag zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie. Als gevoelige informatie buiten het gemeentelijke domein wordt opgeslagen (bij derde, als die al de gegevens lokaal mogen opslaan) zal dit extra eisen opleveren voor de beveiliging van deze informatie. Daarnaast wil je, op meta-niveau, als gemeente informatie terug ontvangen. Deze informatie dient sturing & bekostiging en beleidsdoelen. Het verwerken van en door derde partijen, namelijk de partij elders, brengt ten aanzien van informatiebeveiliging additionele vereisten met zich mee. Aandachtspunt is uitwisseling van verantwoordings- en stuurinformatie tussen diverse partijen over mogelijk onvoldoende betrouwbare netwerken. Het is zaak om goed na te denken over welke informatie is nodig voor welke vraag. Is het bijvoorbeeld nodig om detailgegevens te verstrekken voor verantwoordings-, stuur-, en beleidsinformatie, kan er worden geanonimiseerd? Gemeenten moeten ook de zaken geregeld hebben die in paragraaf 4.1 'Algemeen en archetype onafhankelijk' zijn beschreven.	Privacy impact assessment: • Toelichting bij het Privacy Impact Assessment (PIA) • PIA – Vragenlijst • PIA - Verslag Persoonsgegevens: • Handreiking dataclassificatie • Bewerkersovereenkomst Authenticatie en Autorisatie (inclusief wachtwoorden): • Toegangsbeleid • Wachtwoordbeleid • Telewerken beleid • Aanwijzing Logging Communicatie & Opslag: • Encryptiebeleid (PKI) (in ontwikkeling) Inkopen / aanbesteding: • Contractmanagement • Inkoopvoorwaarden en informatiebeveiligingseisen • Bewerkersovereenkomst • Geheimhoudingsverklaringen BIG • Handleiding screening personeel

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
1. Behoeftbepaling - Bieden triage-instrumenten Het triageproces is in dit archetype per cluster georganiseerd. Elk cluster hanteert hierbij haar eigen triage-instrumenten.	Gemeenten moeten vaststellen welke (persoons)gegevens noodzakelijk zijn met betrekking tot de triageprocessen⁸⁷ en welke(persoons)gegevens worden vastgelegd. De ondersteunende triage-instrumenten (bijvoorbeeld het gebruikte registratiesysteem) en processen dienen de privacy te borgen (noodzaak⁸⁸, subsidiariteit⁸⁹ en proportionaliteit⁹⁰ van gegevensverwerking). Dit geldt voor zowel de huidige als nieuw te verwerven triage-instrumenten, bij de nieuwe systemen is privacy bij design⁹¹ het uitgangspunt. Hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (bijvoorbeeld burger en/of professional), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft uitgevoerd en voor welke taak met betrekking tot een signaal/melding. Bij BRP wordt dit protocolleren genoemd.Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de (persoons)gegevens beschikbaar, juist en actueel zijn.⁴⁵ Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
2. Behoeftbepaling - Ondersteunen ontvangen en beoordelen van signalen Meldingen en signalen worden via de beschikbare 'systemen' per cluster afgegeven. Dit geldt met name voor de formele kanalen. In geval van signalen uit het informele systeem is een goede 'routing' van belang, zodat signalen bij het juiste cluster terecht komen.	Gemeenten moeten vaststellen welke (persoons)gegevens de verschillende meldingen en/of signalen (dienen te) bevatten en welke(persoons)vastgelegd (wat- en dat-informatie). Denk hierbij ook aan meldingen uit verschillende probleemgebieden die gecombineerd en geverifieerd moeten kunnen worden (bijvoorbeeld gebeurtenissen vanuit basisregistraties en kernregistraties, signalen uit de samenloopvoorziening van het inlichtingenbureau). De ondersteunende informatiesystemen	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

⁸⁷ Triage is het proces van verhelderen, routeren en escaleren van vragen en casussen.

⁸⁸ Het bepalen van het doel van informatiedeling (doelbinding).

⁸⁹ subsidiariteit van de gegevensverwerking: is het doel ook te bereiken met een minder ingrijpende methode?

⁹⁰ proportionaliteit van de gegevensverwerking: hoe verhouden het doel en de daarvoor noodzakelijke gegevensuitwisseling zich tot de schending van de persoonlijke levenssfeer van de betrokkene en zijn omgeving

⁹¹ Bron: CBP -Privacy by Design gaat uit van het principe dat er in een vroeg stadium nagedacht wordt over het goede gebruik van persoonsgegevens binnen een organisatie, de noodzaak van het gebruik van deze gegevens en de bescherming ervan. Door al bij het ontwikkelen van systemen privacy en bescherming van persoonsgegevens in te bouwen is de kans op het succes ervan het grootst.

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
3. Klantcontact – Signaleren Voor de burger is er per cluster één centrale toegang die is ingericht om meldingen binnen dat cluster door te geleiden naar de juiste verantwoordelijke.	(bijvoorbeeld een centraal signaal- en meldingenregister) en processen (bijvoorbeeld één centrale toegangspoort of meerdere, melden van problemen via een e-formulier of een (web)service.) dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (bijvoorbeeld burger en/of professional), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft uitgevoerd en voor welke taak met betrekking tot een signaal/melding. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de (persoons)gegevens beschikbaar, juist en actueel zijn.⁴⁵ Denk hierbij aan: dat een melding/signaal niet verloren gaat, dat de ontvangst van de melding/signaal wordt bevestigd (bijvoorbeeld geautomatiseerd); dat de melding/signaal direct bij de verantwoordelijke functies binnenkomen en dat de melding/signaal ook wordt verwerkt en opgevolgd. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Denk hierbij aan: gebeurtenissen die vanuit bronsystemen worden gemeld; signalen die worden geregistreerd; dat meldingen op één plek samen komen en het informeren van de verantwoordelijke professional.	
4. Financiële afhandeling - Afhandelen en beheren declaraties en facturen	Gemeenten moeten vaststellen welke gegevens worden vastgelegd. Gemeenten moeten ook vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Hierbij is het van belang dat alleen geautoriseerde personen van de (contract)partners declaraties mogen indienen bij gemeenten. (Contract)partners mogen ook alleen hun eigen declaraties indienen en de afhandeling van hun declaraties volgen. Hierbij dient functiescheiding toegepast te worden om het risico op fraude te voorkomen/verkleinen. Denk hierbij aan het klaarzetten van betalingen, het wijzigen van gegevens van crediteuren, het autoriseren van betalingen en het monitoren en bewaken van budgetten. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
5. Financiële afhandeling - Ondersteunen budgetbewaking Op basis van de afgesloten contracten en de afgesloten vorm van financiering, vindt door de gemeente budgetbewaking plaats per cluster of - als de gemeente heeft gekozen voor het ontschotten van budgetten - integraal.		
6. Verantwoording - Declareren geleverde diensten		

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
7. Verantwoording - Inzage in afhandeling declaraties Niet van toepassing voor archetype 5.	genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	
8. Financiële afhandeling - Leveren van statistische informatie	Bij de uitwisseling van verantwoordings-, stuur-, en beleidsinformatie dient nagedacht te worden over welke informatie nodig is voor welke vraag. Is het bijvoorbeeld nodig om detail gegevens te verstrekken over verantwoordings-, stuur-, en beleidsinformatie of kan er worden geanonimiseerd? Kan (geanonimiseerde) verantwoordings-, stuur-, en beleidsinformatie in kleine gemeenschappen toch inzicht geven in het individu? Met de gecontracteerde (keten)partner moeten afspraken worden over welke informatie wordt aangeleverd en op welke wijze (bijvoorbeeld via een clearinghouse⁹²). Hierbij dienen de (bestaande) aanleveringsprotocollen de integriteit, vertrouwelijkheid en privacy te waarborgen. Er moet voor de nieuwe taken (en bestaande taken) en de daarop verzamelde en ten aanzien van de eventueel over leefdomeinen heen gekoppelde stuur- en/of beleidsinformatie een privacyprotocol te worden uitgewerkt.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag • Inkopen / aanbesteding
9. Financiële afhandeling - Leveren van verantwoordingsinformatie		
10. Verantwoording - Bieden horizontale en verticale verantwoording De gehanteerde clusters zijn bepalend voor de te genereren verantwoordingsinformatie. Waar vanuit de verticale verantwoording informatie gewenst is, is de te genereren minimale (en facultatieve) gegevensset leidend. Tevens is er behoefte aan beleidsinformatie en financiële informatie. In dit archetypen zijn de afspraken over te leveren verantwoordingsinformatie vastgelegd in de contractafspraken		
11. Verantwoording - Bieden statistische informatie Statistische informatie wordt door derde partijen aangeleverd conform het inkoopcontract of andere soortige overeenkomsten.		
12. Verantwoording - Bieden van managementinformatie Management informatie wordt door derde partijen aangeleverd conform het inkoopcontract of andere soortige overeenkomsten.		

⁹² Het clearinghouse zorgt als derde partij voor de administratie en afhandeling van transacties tussen twee of meer partijen. De gestandaardiseerde registratie is goed mogelijk met behulp van een zogenaamde 'clearinghouse'-constructie waarbij de gegevens op cliëntniveau worden aangeleverd aan een organisatorisch onafhankelijk clearinghouse, die zorgt voor: enerzijds controle op de standaard (zijn alle basis- en aanvullende gegevens op de juiste manier ingevoerd?) en anderzijds voor (geanonimiseerde) verdeling van de informatie richting de verschillende belanghebbende actoren.

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
13. Bedrijfsfunctie Inkoop en contractbeheer - Beheren van contracten en SLA's Het beheren van de contracten is hier buiten scope en verantwoordelijkheid van de uitvoerende partij elders.	In bestaande en/of nieuwe contracten dienen mogelijk beveiligingsaspecten meegenomen te worden, zoals de bewerkersovereenkomst. Met de (keten)partners moeten ook afspraken worden gemaakt over de wijze waarop verantwoording (monitoring) aan de gemeente wordt afgelegd.	• Inkopen / aanbesteding
14. Klantcontact - Beheren klantcontacten Per cluster zal per burger / huishouden de klantcontacten worden vastgelegd. Mogelijk, afhankelijk van de clusterkeuze, brengt dit met zich mee dat er meerdere klantcontacten van een burger / huishouden bij verschillende organisaties wordt geregistreerd.	Gemeenten moeten vaststellen welke (persoons)gegevens worden vastgelegd. Gemeenten moeten tevens vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers moeten er op kunnen vertrouwen dat de klantgegevens beschikbaar, juist en actueel zijn.⁴⁵ Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
15. Klantcontact - Maken afspraken Hier is het van belang dat je 'garandeert' afspraken met de derde partij kan maken. Hier is het van belang dat je daar iets voor inregeld. Dit hoeft niet meteen een afspraken module te zijn, maar wel een methode die dit faciliteert. Op de lange termijn wil je wel iets dergelijks ingeregeld hebben.	Burgers, zaakwaarnemers en professionals moet er op kunnen vertrouwen dat de mogelijkheden (systemen) om afspraken te maken beschikbaar zijn en juiste en actuele gegevens bevatten.	• Communicatie & Opslag

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
16. Klantcontact – Inzage in klantgegevens en lopende zaken De klantgegevens zijn via sectorale klantdossiers beschikbaar. Hierbij is onderscheid gemaakt in wat- en dat-informatie en is stringente autorisatiebeheer mogelijk. Via een aparte voorziening worden deze gegevens ook integraal zichtbaar gemaakt.	Voor het opvolgen van meldingen, signalen en/of het voeren van het gesprek moet de regisseur kunnen beschikken over (een beperkte) set gegevens over de burger. Deze gegevens komen zowel uit bronsystemen van organisaties die betrokken zijn bij de ondersteuning van die burger (en zijn gezin) als uit de gemeentelijke systemen. Bij de hulpverlenende organisaties is in het algemeen veel informatie bekend over de situatie van de burger op een bepaald leefgebied en de al geleverde dienstverlening. Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. Tevens moeten gemeenten vaststellen welke (persoons)gegevens worden uitgewisseld tussen de ketenpartner en gemeenten. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (medewerkers, ketenpartners), welke gegevens mogen raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Denk hierbij aan de regisseur, de medewerker van het gemeentelijke KCC. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers en ketenpartners moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling van informatie tussen de voorziening van de ketenpartner en gemeentelijke voorziening dient de vertrouwelijkheid en integriteit te worden gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
17. Klantcontact – Tonen en bijwerken lopende zaken en mijn gegevens Eigen klantdossier per cluster lijkt hier sneller van belang. Anders komen statusvragen over derde te leveren diensten en producten toch bij de gemeente uit.	Burgers, zaakwaarnemers en professionals moeten er op kunnen vertrouwen dat het klantdossier beschikbaar is en de juiste en actuele gegevens bevatten. Gemeenten moeten vaststellen wie (burgers, medewerkers en ketenpartners), welke gegevens mogen raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs burgers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeenten moeten ook vaststellen via welke kanalen het klantdossier wordt ontsloten, lokaal toegankelijk of (op termijn) ook via mijnOverheid.nl. Bij de uitwisseling van informatie dient de vertrouwelijkheid en integriteit te worden gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
18. Klantcontact – Tonen gemeentelijke producten en diensten Je zult als eindverantwoordelijke moeten verwijzen naar de juiste toegang. Wanneer je je zorgtaken (WMO 2015) integraal onderbrengt bij bijvoorbeeld zorgverzekeraar moet je op zijn minst een verwijzing naar die toegang opnemen en het liefst nog een directe koppeling naar een meldingsveld.	De burger moet er op kunnen vertrouwen dat de aangeboden informatie over gemeentelijke producten en diensten digitaal beschikbaar, juist en actueel is. Tevens moet de burger er op kunnen vertrouwen dat de aangeboden relevante informatie ook daadwerkelijk van de gemeente afkomstig is. De manier waarop gemeentelijke producten en diensten kunnen worden aangevraagd is minder van belang (een aanvraagformulier per product/dienst of 1 startpunt met een soort vraagboom). Als gemeenten producten en diensten van ketenpartners beschikbaar stellen moeten gemeenten beslissen hoe met aanvragen voor deze producten en diensten van	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
19. Klantcontact – Aanvragen producten en diensten Wanneer je het van belang acht de burger digitaal alle diensten en producten kan aanvragen zul je dit moeten inregelen per cluster. Hier is de vraag of je de aanvraag bij de derde partij 'wegzet' of de aanvraag op de 'eigen' omgeving neerzet en de aanvraag doorleidt naar de derde.	ketenpartners wordt omgegaan. Gemeenten moeten vaststellen of gebruikers die producten en/of diensten aanvragen zich moeten aanmelden/registreren voordat ze gebruik kunnen maken van deze dienstverlening. Tevens moeten gemeenten vaststellen of (persoons)gegevens noodzakelijk zijn met betrekking tot deze gemeentelijke dienstverlening. Zo ja, om welke (persoons)gegevens gaat het hier dan. Gemeenten moeten vaststellen wie welke gegevens mag plaatsen en onderhouden/bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Burgers kunnen vaak via meerdere kanalen (bijvoorbeeld met papieren aanvragen) gemeentelijke producten en diensten aanvragen. Wanneer gemeenten het van belang acht dat de burger alle diensten en producten digitaal kan aanvragen, moeten ze dit inrichten. Bij de uitwisseling van informatie tussen de ketenpartner en gemeenten dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie.	
20. Stimulering zelfredzaamheid - Matchen vraag en aanbod Dit is goed om te hebben. Past binnen de doelstelling, maar heeft geen prioriteit.	Ongeacht de rol (deze kan variëren van ondersteunend, faciliterend tot regulerend en initiërend) die de gemeente hierin kiest, kan bij eventuele fouten/misstanden de gemeente hierop aangesproken worden. Dit ondanks het feit dat deze informatie aangelevert kan worden door derden (bijvoorbeeld burgers, buurten, wijken, regio's, dienstverleners en instellingen). Het is mogelijk dat de ondersteunende websites en aangeboden informatie los staan van de gemeentelijke website. De burger moet er op kunnen vertrouwen dat de getoonde informatie (bijvoorbeeld vraag en aanbod, buurt-/wijk- en burgerinitiatieven en zelfdiagnose, welke partijen lokaal of regionaal beschikbaar zijn voor welke diensten) beschikbaar, juist en actueel is. Gemeenten moeten vaststellen of gebruikers die informatie aanleveren (content plaatsen) zich	• Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag ○ Denk hierbij aan SSL (PKIoverheid) certificaten.
21. Stimulering zelfredzaamheid - Ondersteunen buurt-/wijk- en burgerinitiatieven		
22. Stimulering zelfredzaamheid - Ondersteunen zelfdiagnose Dit is goed om te hebben. Past binnen de doelstelling, maar heeft geen prioriteit.		

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
23. Stimulering zelfredzaamheid - Tonen content wijkteam Wanneer je het van belang acht de burger de content van het wijkteam kan inzien, zal je dit moeten inregelen per cluster. Het ontsluiten daarvan voor de burger vanuit de verschillende organisaties vraagt dat men werkt in een gemeentelijke	moeten aanmelden/registreren voordat ze gebruik kunnen maken van deze dienstverlening. Tevens moeten gemeenten vaststellen of (persoons)gegevens noodzakelijk zijn met betrekking tot de geleverde dienstverlening. Zo ja, om welke (persoons)gegevens gaat het hier dan. Bij de uitwisseling en opslag van (persoons)gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Op het moment dat wordt aangehaakt bij bestaande initiatieven/applicaties moeten gemeenten vaststellen of deze voldoen aan de eisen en wensen van de gemeenten. Denk hierbij aan privacy en beveiligingseisen.	
24. Stimulering zelfredzaamheid – Tonen sociale kaart Dit is goed om te hebben. Past binnen de doelstelling, maar heeft geen prioriteit.		
25. Planvorming - Beheren groepstraject Het beheren van een groepstraject gebeurt binnen dit archetype binnen het betreffende cluster	Gemeenten moeten vaststellen welke (persoons)gegevens worden vastgelegd, zowel voor het beheren van een groepstraject als bij het opstellen van het plan. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (de professional en/of regisseur), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (de professional en/of regisseur) moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van (persoons)gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bijvoorbeeld het regiesysteem dat in deze functionaliteit voorziet.	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
26. Planvorming - Opstellen plan Het opstellen van een plan is hier beperkt tot de gehanteerde clustering. Het kan dus zijn dat per cluster een plan wordt opgesteld.		

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
27. Regievoering – Uitzetten en monitoren opdrachten Regie binnen dit archetype is per cluster afgebakend. Daarbinnen worden opdrachten uitgezet en gemonitord.	Gemeenten moeten vaststellen welke (persoons)gegevens nodig zijn bij het uitzetten van de verschillende opdrachten, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie (regisseurs), welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd.Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (regisseurs) moeten er op kunnen vertrouwen dat de getoonde informatie, welke zorgaanbieders welke diensten bieden- en tegen welke kosten, beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van gegevens de vertrouwelijkheid en integriteit gewaarborgd te zijn. Bijvoorbeeld bij het uitzetten van de opdrachten online (via eigen zaakstelsel of via transitiebericht (toewijzing) conform de AWBZ-brede zorgregistratie (AZR) standaarden).	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag
28. Specifieke ondersteuning - Beheren werkvoorraad In dit archetype wordt zoveel als mogelijk integraal afgehandeld binnen het cluster van taken. Het beheren van de werkvoorraad (sturen op caseload en een juiste verdeling van de werkzaamheden) is hier dus beperkt tot de afbakening van het cluster. De werkvoorraad wordt bijgehouden door de systemen die de gemeente nu al gebruikt. Dit kan via een gemeentebreed zaakstelsel zijn, of taakspecifieke applicaties, eventueel in combinatie met een generiek zakenmagazijn.	Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of bijgewerkt (zakensysteem⁹³ /-magazijn), zodat de werkzaamheden adequaat kunnen worden uitgevoerd. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd.Fout! Bladwijzer niet	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag

⁹³ Systeem voor beheer van zaken, bij voorkeur conform het Referentiemodel Gemeentelijke Basisgegevens Zaken (RGBZ) en de Zaaktypecatalogus

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
29. Specifieke ondersteuning - Beheren zaken Zakenbeheer wordt gerealiseerd via de systemen die de gemeente nu al gebruikt. Dit kan via een gemeentebreed zaaksysteem zijn, of taakspecifieke applicaties, eventueel in combinatie met een generiek zakenmagazijn.	gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers (regisseurs, teamleden en/of professionals) moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling en opslag van gegevens dient de vertrouwelijkheid en integriteit gewaarborgd te zijn.	
30. Specifieke ondersteuning - Bijwerken status van levering product of dienst Terugkoppeling van geleverde diensten en producten gewenst	Gemeenten moeten vaststellen of ketenpartners de terugkoppeling of inhoudelijke afhandeling rechtstreeks in de gemeentelijke voorzieningen kunnen/mogen aanbrengen. Gemeenten moeten vaststellen welke (persoons)gegevens kunnen worden geraadpleegd of	• Privacy impact assessment • Persoonsgegevens • Authenticatie en Autorisatie (inclusief wachtwoorden) • Communicatie & Opslag • Inkopen / aanbesteding

Achtergrondinformatie archetype	Achtergrondinformatie informatiebeveiliging	BIG-OP
31. Specifieke ondersteuning - Ondersteunen inhoudelijke afhandeling Het ligt voor de hand om voor de inhoudelijke afhandeling specifieke systemen en voorzieningen te gebruiken zoals die bij de uitvoerende organisatie voorhanden zijn. De inhoudelijke afhandeling wordt in principe niet gefaciliteerd door een eventueel door de gemeente beschikbaar gesteld regiesysteem. Niet relevant voor archetype	bijgewerkt, zodat de werkzaamheden adequaat kunnen worden uitgevoerd. Tevens moeten gemeenten vaststellen welke (persoons)gegevens worden uitgewisseld tussen de voorziening van de ketenpartner en hun eigen voorziening in verband met de afhandeling van specialistische zaken. De ondersteunende informatiesystemen en processen dienen de privacy te borgen (noodzaak, subsidiariteit en proportionaliteit van gegevensverwerking), hierbij is een goede toegangsbeveiliging essentieel. Gemeenten moeten vaststellen wie, welke gegevens mag raadplegen en bijwerken. Dit is onder andere afhankelijk van de functie. Daarnaast is een auditlogging van belang om achteraf te kunnen controleren wie, wat, wanneer heeft gedaan en voor welke taak. Bij BRP wordt dit protocolleren genoemd. Fout! Bladwijzer niet gedefinieerd. Wijs medewerkers op het belang van het geheimhouden van inlogcodes, zodat kan worden nagegaan door wie een wijziging is aangebracht. Gemeentelijke medewerkers en ketenpartners moeten er op kunnen vertrouwen dat de getoonde informatie beschikbaar, juist en actueel is. Bij de uitwisseling van informatie tussen de voorziening van de ketenpartner en gemeentelijke voorziening, via koppelvlakken of een webbased applicatie, dient de vertrouwelijkheid en integriteit gewaarborgd. Bovendien wordt er ook gevoelige informatie opgeslagen zodat ook maatregelen nodig zijn voor de beveiliging van opgeslagen informatie. Mogelijk moeten er met betrekking tot de terugkoppeling of inhoudelijke afhandeling extra afspraken worden gemaakt tussen gemeenten en ketenpartners. Bijvoorbeeld: Gemeenten moeten als verantwoordelijke⁹⁴ een schriftelijke overeenkomst (bewerkerovereenkomst) af sluiten met de ketenpartners (de bewerker⁹⁵). De bewerkerovereenkomst kan zelfstandig worden gebruikt maar is meestal een onderdeel van een overeenkomst met een breder bereik.⁹⁶	

⁹⁴ De verantwoordelijke is volgens de Wet bescherming persoonsgegevens (Wbp) degene die het doel en de middelen voor de verwerking van persoonsgegevens bepaalt (Art. 1 sub d Wbp).

⁹⁵ De Wbp definieert de bewerker als 'degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen' (Art. 1 sub e Wbp).

⁹⁶ zie hiervoor het document Inkoop voorwaarden en beveiligingseisen van de IBD

5 Organisaties in het kader van informatieveiligheid

Er zijn verschillende organisaties die een belangrijke rol spelen op het gebied van informatieveiligheid. Hieronder wordt een overzicht gegeven van die organisaties die van belang zijn in het kader van 3D. Tevens wordt per organisatie een overzicht gegeven van de producten op het gebied van informatiebeveiliging die door deze organisaties zijn of worden gepubliceerd.

5.1 Informatiebeveiligingsdienst voor gemeenten

De Informatiebeveiligingsdienst voor gemeenten (IBD)⁹⁷ is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen.

Hieronder volgt een overzicht van de relevante documenten die door de IBD zijn of worden gepubliceerd. Deze documenten zijn beschikbaar op de (publieke) website⁹⁸ en de community site⁹⁹ van de IBD. Ook toekomstige documentatie zal hier worden gepubliceerd.

Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft opdracht gegeven voor het ontwikkelen van een Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De Baseline Informatiebeveiliging Nederlandse Gemeenten is bedoeld om:

1. Gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging.
2. Gemeenten een hulpmiddel te geven om aan alle eisen op het gebied van Informatiebeveiliging te kunnen voldoen.
3. De auditlast bij gemeenten te verminderen.
4. Gemeenten een aantoonbaar betrouwbare partner te laten zijn.

Met deze baseline hebben bestuur en management van gemeenten een instrument in handen waarmee zij in staat zijn om te meten of de eigen organisatie 'in control' is op het gebied van informatiebeveiliging. Deze baseline is vervaardigd op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR) voor de gemeentelijke markt. Het betreft twee varianten: een Strategische- én een Tactische Baseline.

- De Strategische Baseline¹⁰⁰ kan gezien worden als de 'kapstok' waaraan de elementen van informatiebeveiliging opgehangen kunnen worden. Centraal staan de organisatie en de verantwoording over informatiebeveiliging binnen de gemeente.
- De Tactische Baseline¹⁰¹ beschrijft de normen en maatregelen ten behoeve van controle en risicomanagement. De Tactische Baseline beschrijft aan de hand van dezelfde indeling als de

⁹⁷ <https://www.ibdgemeenten.nl/>

⁹⁸ <https://www.ibdgemeenten.nl/producten/>

⁹⁹ <https://community.ibdgemeenten.nl/>

¹⁰⁰ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-0506-Strategische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.0.pdf>

¹⁰¹ <http://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-0506-Tactische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.0.pdf>

internationale beveiligingsnorm ISO/IEC 27002:2007, de controls/maatregelen die als baseline gelden voor gemeenten.

Operationele producten BIG

Op basis van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) ontwikkelt de Informatiebeveiligingsdienst voor gemeenten (IBD) operationele producten behorend bij de BIG. Met behulp van deze operationele producten kan iedere gemeente tot implementatie van de BIG overgaan. De IBD ontwikkelt deze operationele producten in samenwerking met de Taskforce BID en een groot aantal betrokken gemeenten die de producten reviewen voordat ze definitief worden.

Voor een actueel overzicht verwijzen wij naar de (publieke) website en community site van de IBD. De volgende operationele producten BIG zijn op het moment van publicatie van dit document door de IBD gepubliceerd:

Aanwijzing Logging: Het doel van dit document is een aanwijzing te geven over het gebruik van logging binnen gemeentelijke informatiesystemen.

Anti-malware beleid: Dit document geeft een mogelijke invulling van beleidsuitgangspunten voor het Anti-malware beleid weer. Deze beleidsuitgangspunten zijn afkomstig uit de BIG en het beleid is daarmee compliant aan de BIG.

Back-up en Recovery Gemeente: Het doel van dit document is een aanwijzing te geven over hoe het back-up en recovery beleid van een gemeente opgezet en uitgevoerd kan worden.

Bewerkersovereenkomst: Dit product bevat een standaard bewerkersovereenkomst en een voorbeeld bijlage met maatregelen voor de bewerker die de gemeente als verantwoordelijke kan gebruiken bij het laten bewerken van persoonsgegevens.

Cloud Computing: Dit document geeft uitgangspunten weer, gezien vanuit informatiebeveiliging, voor een invulling van het Cloud Computing beleid voor gemeenten. Deze beleidsuitgangspunten informatiebeveiliging zijn afkomstig uit de BIG en het beleid is daarmee compliant aan de BIG.

Contractmanagement: Het doel van dit document is aanwijzingen te geven omtrent contractmanagement.

GAP-analyse: Het doel van de GAP-analyse is om gemeenten te controleren of en in welke mate de maatregelen uit de tactische variant van de BIG zijn geïmplementeerd. Hierbij gaat het om gemeenten die het onderzoek uitvoeren of laten uitvoeren.

Geheimhoudingsverklaringen BIG: Dit product bevat voorbeelden van geheimhoudingsverklaringen, die door gemeenten te gebruiken zijn. Deze geheimhoudingsverklaringen zijn onderdeel van de BIG.

Handleiding screening personeel: Dit document geeft een handleiding over hoe invulling kan worden gegeven aan de verificatie van de achtergrond voor alle kandidaten (werknemers), ingehuurd personeel en externe gebruikers. Deze verificatie heet ook screening van personeel en wordt al binnen gemeenten gebruikt voor wat betreft het verkleinen van integriteitsrisico's.

Handreiking CISO functieprofiel: Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit de verschillende delen van de organisatie met relevante rollen en functies. De rollen van de Chief Information Security Officer (CISO) en het lijnmanagement zijn beschreven. Bij kleine gemeenten kan deze rol ook in deeltijd uitgevoerd worden, waarbij het ook mogelijk is om dit te combineren over verschillende gemeenten in een regionale opzet.

Handreiking dataclassificatie: Dit document bevat een good practice voor (data)classificatie. Data betekent in dit verband alle gegevens en informatie, ongeacht het medium waarop deze opgeslagen wordt en ongeacht de presentatie daarvan.

Handreiking Wijzigingsbeheer: Dit product bevat aanwijzingen voor het omgaan met het doorvoeren van wijzigingen in de ICT-middelen en -diensten, en aanwijzingen voor gebruik en inrichting van het proces wijzigingsbeheer.

Hardening beleid voor gemeenten: Dit document geeft een mogelijke invulling van beleidsuitgangspunten voor het hardening-beleid weer. Deze beleidsuitgangspunten zijn afkomstig uit de BIG en het beleid is daarmee compliant aan de BIG.

Implementatie BIG: Het doel van de 'Implementatie BIG' is om binnen de gemeente te toetsen of en in welke mate de gemeente voldoet aan de maatregelen uit de BIG.

Inkoopvoorwaarden en informatiebeveiligingseisen: Dit product bevat aanwijzingen voor beveiligingseisen in inkoopvoorwaarden van de gemeente.

Mobiele gegevensdragers: Dit product bevat aanwijzingen en beleid rondom het gebruik van mobiele gegevensdragers zoals USB sticks of back-up media.

Mobile Device Management: Er is een toename van het gebruik van mobiele gegevensdragers zoals smartphones, tablets en laptops binnen gemeenten. Deze aanwijzing is geschreven om vanuit verschillende gezichtspunten de risico's en oplossingen weer te geven die gemeenten kunnen inzetten bij de keuzes voor mobiele apparaten. Ook wordt een lijst met functionele eisen en wensen gegeven voor het geval dat men een MDM-oplossing wil implementeren voor het beheer van mobiele apparaten en de gemeentelijke gegevens die erop kunnen staan.

Patch management voor gemeenten: Patch Management is het proces waarmee patches op gecontroleerde beheerste (risico beperkende) wijze uitgerold kunnen worden. Patches zijn doorgaans kleine programma's die aanpassingen maken om fouten op te lossen of verbeteringen aan te brengen in bestaande programmatuur en/of hardware. Patch Management wordt meestal uitgevoerd door de ICT-afdeling binnen een organisatie. Het doel van Patch Management is tweeledig. Ten eerste is het gericht op het inzichtelijk maken van de actuele stand van kwetsbaarheden en toegepaste patches binnen de beheerde infrastructuur. Het tweede doel is op een zo efficiënt en effectief mogelijke wijze met zo min mogelijk verstoringen stabiele (veilige) informatiesystemen te creëren en te houden.

Presentatie Bewustwording Informatieveiligheid bij gemeenten: De presentatie is bedoeld voor iedere medewerker binnen de gemeente. Met als doel om alle medewerkers bewust te maken van de informatiebeveiligingsrisico's die de gemeente loopt en ook van de wijze waarop zij zich hiertegen kan beschermen. Elke gemeente kan de presentatie overigens aanpassen naar de eigen gemeentelijke situatie. De BIG en het informatiebeveiligingsplan, ook een operationeel product van de BIG, zijn als uitgangspunt genomen voor de presentatie.

Privacy Impact Assessment (PIA): Dit document is de toelichting bij het Privacy Impact Assessment (PIA) instrument ter ondersteuning bij het uitvoeren van de PIA.

Responsible Disclosure: In de ICT-wereld bestaan meerdere praktijken om kwetsbaarheden in ICT bekend te maken. Responsible Disclosure binnen de ICT-wereld is het op een verantwoorde wijze, en in gezamenlijkheid tussen melder en organisatie, openbaar maken van ICT-kwetsbaarheden op basis van een, door organisaties hiervoor, vastgesteld beleid voor Responsible Disclosure. Dit document geeft een template weer voor het beleid op het vlak van Responsible Disclosure, waarin een aantal aspecten standaard is opgenomen, zoals het delen van de meldingen met de IBD.

Telewerken beleid: Deze aanwijzing is geschreven om vanuit verschillende gezichtspunten de risico's en oplossingen weer te geven die gemeenten kunnen inzetten rondom telewerken.

Toegangsbeleid: Dit document bevat een good practice voor het toegangsbeleid van een gemeente. De in deze handreiking genoemde niveaus en (bewaar)termijnen zijn een voorstel en komen uit verschillende brondocumenten. Waaronder: wet- en regelgeving, PVIB-patronen, een gemeente en de Strategische deel van de BIG.

Procedure Afvoer ICT middelen: Dit product bevat aanwijzingen voor het omgaan met het afvoeren van IT middelen.

Voorbeeld Incident Management en responsebeleid: Dit document geeft een mogelijke invulling van beleidsuitgangspunten voor het Incident Management en Responsebeleid weer en aanwijzingen voor gebruik en inrichting van een Incident Management en responseteam. Deze beleidsuitgangspunten zijn afkomstig uit de BIG en het beleid is daarmee compliant aan de BIG.

Voorbeeld Informatiebeveiligingsbeleid Gemeenten: Dit document geeft algemene beleidsuitgangspunten over informatiebeveiliging van de gemeente.

Wachtwoordbeleid: Dit product bevat aanwijzingen en een beleid rondom het gebruik van wachtwoorden binnen de gemeente.

De volgende operationele producten BIG zijn in ontwikkeling:

Baselinetoets: Het doel van dit document is het leveren van een aanpak die gebruikt kan worden om voor nieuwe processen en informatiesystemen een methode te hebben om te bepalen of de BIG afdoende is of niet. Tevens kan deze aanpak ook gebruikt worden om bij een bestaand informatiesysteem te toetsen of deze voldoende beveiligd is door de BIG maatregelen.

Diepgaande risicoanalyse methode: Doelstelling van de diepgaande risicoanalyse is om in kaart te brengen welke maatregelen aanvullend op de baseline moeten worden getroffen om het juiste niveau van beveiliging te realiseren.

Encryptiebeleid (PKI): Deze handleiding is geschreven om vanuit verschillende gezichtspunten de risico's en oplossingen weer te geven die gemeenten kunnen inzetten rondom encryptie/versleuteling en Public Key Infrastructure (PKI).

Handreiking communicatieplan gemeente: Deze aanwijzing is geschreven om vanuit verschillende gezichtspunten de risico's en oplossingen weer te geven die gemeenten kunnen inzetten rondom telewerken.

Handreiking proces configuratiebeheer: Dit product bevat aanwijzingen voor het omgaan van alle componenten die deel uitmaken van de ICT-infrastructuur, en aanwijzingen voor gebruik en inrichting van het proces configuratiebeheer.

Logische toegangsbeveiliging: Dit product bevat aanwijzingen en een beleid rondom het inrichten van logische toegangsbeveiliging binnen de gemeente.

Procedure nieuwe ICT-voorzieningen: Dit product bevat aanwijzingen voor het vastleggen van de verschillende stappen die noodzakelijk zijn om nieuwe versies, releases of updates van ICT-voorzieningen goed te keuren alvorens deze in productie worden genomen.

5.2 Nationaal Cyber Security Centrum (NCSC)

Het Nationaal Cyber Security Centrum (NCSC)¹⁰² draagt bij aan het gezamenlijk vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein en daarmee aan een veilige, open en stabiele informatiesamenleving door het leveren van inzicht en het bieden van handelingsperspectief. De primaire doelgroepen van het NCSC zijn Rijksoverheid en organisaties in de vitale infrastructuur. Het centrum valt organisatorisch onder de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) van het ministerie van Veiligheid en Justitie maar is gestoeld op publiek-private samenwerking.

Gedegen kennis over de aard, urgentie en gevolgen van cyber crime is belangrijk om goede maatregelen te kunnen nemen. Het Nationaal Cyber Security Centrum (NCSC) publiceert

¹⁰² <https://www.ncsc.nl/>

kennisdocumenten zoals het Cyber Security Beeld Nederland en het Trendrapport Cybercrime en Digitale Veiligheid die gericht zijn op het informeren van hogere bestuurslagen in (vitale) organisaties, publiek en privaat. We publiceren ook uitgaven die specifiek bestemd zijn voor managers en bijvoorbeeld ICT-experts.

Wifi-beveiliging - De onderschatte schakel in netwerkbeveiliging: Draadloos werken biedt vele voordelen maar kent – zeker in vergelijking met een netwerk met vaste aansluitingen - ook ernstige en specifieke dreigingen, die de betrouwbaarheid van de informatievoorziening van een organisatie kunnen aantasten. Deze whitepaper brengt relevante informatie rondom de beveiliging van wifinetwerken in samenhang bij elkaar.

Beveiligingsrichtlijnen voor mobiele apparaten: Het toenemende gebruik van slimme mobiele apparaten biedt veel nieuwe mogelijkheden, maar er kleven ook risico's aan. Daarom publiceert het Nationaal Cyber Security Centrum (NCSC) richtlijnen voor de beveiliging van mobiele apparaten.

Consumerization en security: Slimme mobieltjes, data in 'de cloud' en altijd online: de manier waarop we ICT gebruiken is structureel veranderd. De opkomst van de tablets, smartphone's en slimme clouddiensten benadrukken dit. Dit consumentgedreven gebruik van ICT (consumerization) brengt beveiligingsrisico's met zich mee.

ICT-beveiligingsrichtlijnen voor webapplicaties: De ICT- beveiligingsrichtlijnen voor webapplicaties vormen een leidraad voor het veiliger ontwikkelen, beheren en aanbieden van webapplicaties en bijbehorende infrastructuur. De beveiligingsrichtlijnen zijn breed toepasbaar voor ICT- oplossingen die gebruik maken van webapplicaties. Hierdoor zijn ze zowel door afnemers, als door dienstaanbieders te gebruiken voor aan- en uitbestedingen, toezicht en onderlinge afspraken.

Cloudcomputing: Deze publicatie geeft informatie over cloudcomputing en mogelijke risico's ervan. Met andere woorden: als een organisatie kiest voor 'cloudcomputing', zijn er dan risico's voor de bedrijfsvoering en heeft deze keuze gevolgen voor de informatiebeveiliging van de organisatie?

Responsible Disclosure: Dit dossier bevat de leidraad Responsible Disclosure, voorbeelden van Responsible Disclosure beleid en voorbeelden van Responsible Disclosure.

De documentatie is beschikbaar op de (publieke) website van het NCSC.¹⁰³

5.3 Taskforce Bestuur en Informatieveiligheid Dienstverlening

De Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID) ¹⁰⁴ is ingesteld om het onderwerp informatieveiligheid hoog op de agenda te krijgen bij bestuurders en topmanagement van alle overheidslagen. Zowel qua bewustwording als sturing. De Taskforce BID bouwt voort op de huidige initiatieven op informatieveiligheidsvlak vanuit een intensieve samenwerking met de koepelorganisaties van elk van de overheidslagen.¹⁰⁵ Bovendien wordt nauw samengewerkt met betrokken organisaties op informatieveiligheidsvlak, zoals het Nationaal Cyber Security Centrum (NCSC), het Centrum Informatiebeveiliging en Privacybescherming (CIP), de Informatiebeveiligingsdienst voor gemeenten (IBD), het Waterschapshuis en Logius.

¹⁰³ <https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling>

¹⁰⁴ <http://www.taskforcebid.nl/>

¹⁰⁵ Betrokken koepelorganisaties zijn de Unie van Waterschappen, Interprovinciaal Overleg (IPO), Manifestgroep, Vereniging van Nederlandse Gemeenten (VNG) en Interdepartementale Commissie Chief Information Officers (ICCIO).

Doel van de Taskforce Bestuur en Informatieveiligheid Dienstverlening is om uiteindelijk te komen tot verplichtende zelfregulering per overheidslaag als het gaat om informatieveiligheid.

De volgende producten zijn door de Taskforce BID gepubliceerd:

Opleidingsaanbod: Het spoor 'leren' richt zich met name op de verandering in kennis, houding en vaardigheden bij bestuur en management.¹⁰⁶

Zelftest Informatieveiligheid: De Taskforce BID heeft voor u een online test ontwikkeld waarmee u in tien minuten zelf eenvoudig uw kennis en bewustzijn toetst op het gebied van informatieveiligheid. Onderwerpen die aan bod komen gaan over de verschillende aspecten van informatieveiligheid, verantwoordelijken bij informatieveiligheid, informatieveiligheid en ketens, sturen op informatieveiligheid en risicobewustzijn. Met de Zelftest Informatieveiligheid krijgt u een beter beeld van de verschillende aspecten van informatieveiligheid en hoe u daar als bestuurder of topmanager op kunt sturen.¹⁰⁷

De documentatie is beschikbaar op zowel de (publieke) website¹⁰⁸ als de (besloten) Pleio site¹⁰⁹ van de Taskforce BID.

5.4 Centrum voor Informatiebeveiliging en Privacybescherming

Het Centrum voor Informatiebeveiliging en Privacybescherming (CIP)¹¹⁰ is het expertisecentrum voor informatiebeveiliging en privacybescherming van, voor en door overheidsorganisaties. Het CIP is opgericht door vier grote uitvoeringsorganisaties en ZBO's die uitkeringen doen aan burgers: Belastingdienst, DUO, SVB en UWV, waarbij de laatste als trekker optreedt. Kennis die bij de overheidsorganisaties aanwezig is op het vlak van informatiebeveiliging en privacybescherming, wordt binnen de samenwerking in het CIP gebundeld en toegankelijk gemaakt.

Good practices

CIP heeft vier categorieën geformuleerd waarmee de reikwijdte van good practices wordt aangegeven:

1. Individuele praktijk: een toepassing bij een van de organisaties die werkt, als handreiking voor hergebruik binnen geïnteresseerde organisaties. Een individuele praktijk is al bruikbaar nadat een individuele organisatie die aanreikt.
2. Becommentarieerde praktijk: een door meerdere professionals veralgemeniseerde praktijk als handreiking voor hergebruik binnen geïnteresseerde organisaties. Een becommentarieerde praktijk ondergaat eerst een reviewslag binnen een CIP-domeingroep en/of door de CIP-Leesgroep.
3. Gecommitteerde praktijk: een namens meerdere in CIP samenwerkende organisaties onderschreven praktijk, als sterk advies voor hergebruik bij alle organisaties binnen de uitvoerende overheid. Een praktijk is pas gecommitteerd als bestuurders daarvoor hebben gekozen.
4. Verplichtende praktijk: een praktijk die door de in CIP samenwerkende organisaties is bekrachtigd als basis voor zelfregulering binnen deze kring en met een sterk advies om dat

¹⁰⁶ <http://www.taskforcebid.nl/producten/het-spoor-leren/>

¹⁰⁷ <https://informatieveiligheidstest.nl>

¹⁰⁸ <http://www.taskforcebid.nl>

¹⁰⁹ <https://informatieveiligheid.pleio.nl/>

¹¹⁰ <http://www.cip-overheid.nl/>

voor de gehele overheidslaag van de uitvoering toe te passen. Een praktijk is pas verplichtend als bestuurders daarvoor hebben gekozen.

De volgende producten zijn in de reeks “uit de praktijk” door CIP gepubliceerd:

Grip op Secure Software Development: Organisaties hebben nog onvoldoende vat op security, getuige de explosieve groei van incidenten. In de praktijk blijkt dat 75% van die incidenten hun oorzaak vinden in softwarefouten.

- De methode “Grip op secure software development (SSD)” beschrijft hoe een opdrachtgever grip krijgt op het ontwikkelen van goed beveiligde software. De drie pijlers daarbij zijn 1) standaard beveiligingseisen, 2) contactmomenten en 3) inrichten van SSD processen.
- De beveiligingseisen die de opdrachtgever kan hanteren als eisen aan de op te leveren software, zijn vervat in het tweede document.

Borging awareness informatiebeveiliging: Dit product bestaat uit een presentatie en bijbehorende verdiepingsmateriaal. “Borging” duidt hier op het proces van voortdurende inspanning om de organisatie bij de les te krijgen en houden op het gebied van informatiebeveiligingsbewustzijn.

Responsible Disclosure - handreiking voor implementatie: ‘Responsible Disclosure’ betreft het op verantwoorde wijze melden van ICT-kwetsbaarheden, op basis van een protocol dat de organisatie en de ontdekker van de kwetsbaarheid duidelijkheid biedt. CIP biedt hiervoor een template voor het beleid en een checklist van acties die nodig zijn om dat te realiseren.

Meldplicht Datalekken en meldplicht Inbreuken op elektronische systemen: Er is wet- en regelgeving in de maak die organisaties verplicht inbreuken op ICT-systemen – en verlies van persoonsgegevens in het bijzonder – onverwijld te melden bij respectievelijk het ministerie van Veiligheid en Justitie, annex het Nationaal Cyber Security Centrum (NCSC) en het College Bescherming Persoonsgegevens annex de getroffen burgers. Nalatigheid kan hoge boetes opleveren. Op Europese schaal is soortgelijke wet- en regelgeving op handen, die er qua consequenties nog een flinke schep bovenop doet. Hoe verhouden deze zaken zich tot elkaar en wat u zoal moet organiseren om aan de nieuwe verplichtingen te kunnen voldoen?

Testen met persoonsgegevens: Het doel van dit document is om beveiligingsgerelateerde richtlijnen te geven voor het gebruik van persoonsgegevens in testsituaties buiten de productieomgeving. Het document is in lijn met de gangbare algemene baselines, normenkaders en best practices, met name de ISO 27xxx normen, de Code voor Informatiebeveiliging, en het tactisch normenkader van de Baseline Informatiebeveiliging Rijksdienst (BIR-TNK) voor zover van toepassing.

Beveiligingsbeleid clouddiensten: Het bespreekt de relatie van verschillende cloudtypes met de diverse aspecten van informatiebeveiligingsbeleid. Het resultaat is een checklist van opletpunten (vereisten zo je wilt) bij het inzetten van clouddiensten.

Privacy impact assessment: De eerdere publicatie op deze plek moesten wij terugtrekken. Nieuwe, praktijkgerichte documentatie rond het thema PIA van de hand van onze kennispartner Considerati wordt op korte termijn op deze plaats beschikbaar gesteld.

De documentatie is beschikbaar op zowel de (publieke) website¹¹¹ als de (besloten) Pleio site¹¹² van het CIP.

5.5 College bescherming persoonsgegevens

¹¹¹ <http://www.cip-overheid.nl/>

¹¹² <http://www.cip-pleio.nl/>

Het College bescherming persoonsgegevens (CBP) ¹¹³ houdt toezicht op de naleving van de wettelijke regels die zien op de bescherming van persoonsgegevens, zo nodig met behulp van sancties. Daarnaast adviseert het CBP de regering over voorgenomen wet- en regelgeving die betrekking heeft op de verwerking van persoonsgegevens. Bij het uitvoeren en verantwoorden van zijn werkzaamheden heeft het CBP oog voor de maatschappelijke context van de aan hem voorgelegde vragen, problemen of klachten.

De volgende producten zijn door de CBP gepubliceerd:

Privacy by Design: Organisaties willen zorgvuldig omgaan met de gegevens die hen ter beschikking staan en die hun vaak in vertrouwen zijn verstrekt. Door al tijdens de ontwikkeling van informatiesystemen aandacht te schenken aan privacyverhogende maatregelen (Privacy Enhancing Technologies of PET) kan op een effectieve manier zorgvuldige en verantwoorde omgang met persoonsgegevens technisch worden afgedwongen. Privacy by Design speelt niet alleen een belangrijke rol bij de ontwikkeling van grote ICT-projecten, maar kan ook een rol van betekenis spelen bij de invoering van RFID, het Burgerservicenummer of mobiel betalen.

Richtsnoeren beveiliging van persoonsgegevens: De richtsnoeren leggen uit hoe het CBP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens de beveiligingsnormen uit de Wet bescherming persoonsgegevens (Wbp) toepast. De richtsnoeren vormen de verbindende schakel tussen het juridisch domein, met daarbinnen de eisen uit de Wbp, en het domein van de informatiebeveiliging, waarin de noodzakelijke kennis en kunde aanwezig is om daadwerkelijk aan die eisen te voldoen.

Compliance-instrumenten: De bescherming van persoonsgegevens is een verantwoordelijkheid voor alle organisaties die met persoonsgegevens omgaan. Het CBP stimuleert daarom zelfregulering van overheid en bedrijfsleven voor een adequate privacybescherming. Het CBP heeft in samenwerking met diverse marktpartijen de afgelopen jaren een viertal compliance-instrumenten ontwikkeld. De samenhang tussen deze instrumenten en het algemene begrippenkader wordt uiteengezet in 'Overzicht van de Zelfreguleringsproducten'.

Medische gegevens: Mensen moeten erop kunnen vertrouwen dat met de medische gegevens die zij toevertrouwen aan een arts, zorgvuldig wordt omgegaan. Medische gegevens zijn per definitie gevoelige gegevens, ook in de zin van de wet. Dit betekent dat ze met de hoogst mogelijke zorgvuldigheid moeten worden verwerkt. Patiënten moeten er absoluut zeker van kunnen zijn dat hun gegevens goed beveiligd zijn en dat onbevoegden geen toegang krijgen tot de gegevens.

Handleiding Wet bescherming persoonsgegevens: Om personen, organisaties, ondernemingen en overheidsinstellingen die persoonsgegevens verwerken of gaan verwerken, behulpzaam te zijn bij het nemen van maatregelen om aan de Wet bescherming persoonsgegevens te voldoen, geeft het ministerie van Justitie deze handleiding uit. Deze handleiding richt zich dus niet tot de burger wiens persoonsgegevens worden verwerkt, maar is bestemd voor de personen, organisaties, ondernemingen en overheidsinstellingen die persoonsgegevens verwerken.

Anonimiseer gegevens bij gebruik big data: Via big data worden op geavanceerde wijze enorme hoeveelheden (persoons)gegevens verwerkt. Het College bescherming persoonsgegevens (CBP) waarschuwt voor de risico's van dit soort gigantische databases en de bijbehorende geautomatiseerde verwerking van persoonsgegevens. Voor veel doelen waarvoor big data wordt ingezet, zijn tot de persoon herleidbare gegevens helemaal niet nodig. De gegevens moeten dan onomkeerbaar worden geanonimiseerd. Als organisaties voor hun doel

¹¹³ <http://www.cbppweb.nl/Pages/home.aspx>

wél herleidbare gegevens verwerken, moeten zij aan alle eisen van de Wet bescherming persoonsgegevens (Wbp) voldoen.

De documentatie is beschikbaar op de (publieke) website van het CBP.¹¹⁴

5.6 Overige organisaties

Overige organisaties die een rol spelen bij informatieveiligheid zijn de Nederlandse Orde van Register EDP-Auditors (NOREA)¹¹⁵, het National Institute of Standards and Technology (NIST)¹¹⁶, de International Organization for Standardization (ISO)¹¹⁷ / de NEN (Nederlandse Norm)¹¹⁸ en Logius¹¹⁹.

5.7 Ondersteunde documenten

De onderwerpen uit paragraaf 5.1 zijn in tabel 1 verder uitgewerkt. Dit houdt in dat er een koppeling is gelegd tussen de onderwerpen en relevante documenten van diverse organisaties zoals in voorgaande paragrafen beschreven. In deze paragrafen wordt ook een korte omschrijving gegeven van de producten waar in tabel 1 aan wordt gerefereerd.

De onderwerpen die op dit moment worden onderkend zijn:

- Inrichten Informatiebeveiliging
- Privacy impact assessment
- Risicoanalyse (inclusief GAP-analyse)
- Dataclassificatie
- Beheer ICT-componenten
- Awareness informatiebeveiliging
- Meldplicht Datalekken en meldplicht Inbreuken op elektronische informatiesystemen
- Responsible Disclosure
- Authenticatie en Autorisatie (inclusief wachtwoorden)
- Inkopen / aanbesteding
- Secure Software Development
- Persoonsgegevens
- Medische gegevens
- Testen met persoonsgegevens
- Mobiele apparaten waaronder Bring Your Own Device (BYOD)
- Communicatie & Opslag
- Telewerken
- Cloudcomputing
- Big Data

¹¹⁴ <http://www.cbppweb.nl>

¹¹⁵ <http://www.norea.nl/Norea/Home/default.aspx>

¹¹⁶ <http://www.nist.gov/>

¹¹⁷ <http://www.iso.org/iso/home.html>

¹¹⁸ <http://www.nen.nl/>

¹¹⁹ <https://www.logius.nl/>

Onderwerp	CIP	BIG-OP	Overig
Inrichten informatiebeveiliging		• Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten mei 2013 versie 1.0 IBD • Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten mei 2013 versie 1.0 IBD • Bijlage hoofdstuk 15.1.1 Identificatie toepasselijke wetgeving • Implementatie BIG • Handreiking implementatie BIG voor kleine gemeenten (in ontwikkeling) • ISMS P&C cyclus implementatie op basis van de Operationele Baseline (in ontwikkeling) • Handreiking CISO functieprofiel • Voorbeeld Informatiebeveiligingsbeleid Gemeenten	•
Privacy impact assessment	Privacy impact assessment bij de Belastingdienst (cip.pleio.nl)	• Toelichting bij het Privacy Impact Assessment (PIA) • PIA – Vragenlijst • PIA - Verslag	• Norea - Handreiking Privacy Impact Assessment • Rijksdienst - Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst
Risicoanalyse (inclusief GAP-analyse)		• Baselinetoets BIG • Baselinetoets BIG voorbeeld • Diepgaande risicoanalyse methode (in ontwikkeling) • GAP-analyse: ○ colofon ○ resultaat ○ vragenlijst ○ uitleg	•
Dataclassificatie		• Handreiking dataclassificatie	•

Onderwerp	CIP	BIG-OP	Overig
Beheer ICT-componenten		• Aanwijzing Logging • Anti-malware beleid • Back-up en Recovery gemeenten • Basis beveiligingsparagraaf SLA (in ontwikkeling) • Handreiking Configuratiebeheer • Handreiking Penetratietesten (in ontwikkeling) • Handreiking Wijzigingsbeheer • Hardening beleid voor gemeenten • ISMS P&C cyclus implementatie op basis van de Operationele Baseline (in ontwikkeling) • Mobiele gegevensdragers • Mobile Device Management • Patch management voor gemeenten • Procedure Afvoer ICT middelen • Procedure nieuwe ICT-voorzieningen • Voorbeeld Incident Management en responsebeleid	•
Awareness informatiebeveiliging	• Borging awareness informatiebeveiliging incl. achtergrondinformatie	• Communicatieplan gemeente (in ontwikkeling) • Presentatie Bewustwording Informatieveiligheid bij gemeenten	•
Meldplicht Datalekken en meldplicht Inbreuken op elektronische systemen	• Meldplicht Datalekken en meldplicht Inbreuken op elektronische systemen	•	•
Responsible Disclosure	• Handreiking implementatie Responsible Disclosure	• Responsible Disclosure	• NCSC - Leidraad om te komen tot een praktijk van Responsible Disclosure
Authenticatie en Autorisatie (inclusief wachtwoorden)		• Aanwijzing Logging • Personeelsbeleid (in ontwikkeling) • Telewerken beleid • Toegangsbeleid • Wachtwoordbeleid	Toegang: • Logius – DigiD • Logius - eHerkenning Gegevensuitwisseling: • Logius - Digikoppeling

Onderwerp	CIP	BIG-OP	Overig
Inkopen / aanbesteding		• Bewerkerovereenkomst • Contractmanagement • Geheimhoudingsverklaringen BIG • Handleiding screening personeel • Inkoopvoorwaarden en informatiebeveiligingseisen	•
Secure Software Development	• Grip op Secure Software Development (zowel de eisen als proces)	•	• NCSC – Paper 'ICT Beveiligingsrichtlijnen voor webapplicaties' • Logius - Beveiliging webapplicaties • CBP - Privacy by Design • NIST - Security and Privacy Controls for Federal Information Systems and Organizations' • ISO/IEC 27034-1 - Information technology -- Security techniques -- Application security (geen gratis document, part 1 published, rest in DRAFT) • ISO/IEC 27034-2 - Organization normative framework (draft) • ISO/IEC 27034-3 - Application security management process (pre-draft) • ISO/IEC 27034-4 - Application security validation (pre-draft) • ISO/IEC 27034-5 - Protocols and application security control data structure (draft) • ISO/IEC 27034-6 - Security guidance for specific applications (draft) • Normenkader Secure Software
Persoonsgegevens		• Bewerkerovereenkomst • Handreiking dataclassificatie	• CBP - Richtsnoeren beveiliging van persoonsgegevens • CBP - Compliance-instrumenten
Medische gegevens		•	• CBP - Medische gegevens
Testen met persoonsgegevens	• Testen met persoonsgegevens buiten de productieomgeving	•	• CBP - Handleiding Wet bescherming persoonsgegevens

Onderwerp	CIP	BIG-OP	Overig
Mobiele apparaten waaronder Bring Your Own Device (BYOD)		• Anti-malware beleid • Encryptiebeleid (PKI) • Hardening beleid voor gemeenten • Mobiele gegevensdragers • Mobile Device Management	• NCSC - Beveiligingsrichtlijnen voor mobiele apparaten • NCSC - Consumerization en security
Communicatie & Opslag		• Encryptiebeleid (PKI)	Gegevensuitwisseling: • Logius - Digikoppeling
Telewerken		• Anti-malware beleid • Encryptiebeleid (PKI) • Hardening beleid voor gemeenten • Telewerken beleid	•
Cloudcomputing	Beveiligingsbeleid clouddiensten, v2.2 (excl. ADR)	• Cloud Computing • Encryptiebeleid (PKI)	• NCSC – Whitepaper ‘Cloudcomputing & Security’
Big Data		•	• CBP- anonimiseer gegevens bij gebruik big data

Tabel 1 Informatiebeveiligingsonderwerpen

