Voorstel BVO VRT

ONDERWERP	Plan van Aanpak Informatieveiligheid		
DATUM	3 november 2016		
OPENBAAR	[ja/nee]	BEHANDELD DOOR	
REGISTRATIENUMMER	[Registratienummer]	TELEFOONNUMMER	
		PARAAF LEIDINGGEVENDE	
PORTEFEUILLEHOUDER	Strategie & Ondersteuning		

Besluit instemming:

- Er wordt de leden van het BVO gevraagd in te stemmen met het plan van aanpak Informatieveiligheid Veiligheidsregio Twente
- Er wordt de leden van het BVO gevraagd in te stemmen met de samenstelling van het projectteam Informatieveiligheid

---

Inhoudsopgave

Plan van aanpak Informatieveiligheid Veiligheidsregio Twente

1 Inleiding

1.1 Aanleiding

Internet en ICT zijn niet meer weg te denken in onze samenleving. In bijna alle maatschappelijke sectoren is de digitale technologie het belangrijkste middel om informatie te verwerken, te verzenden of het primaire bedrijfsproces aan te sturen. Nederland heeft zich ontwikkeld tot één van de meest gedigitaliseerde landen ter wereld, waarbij ons land het grootste internetknooppunt (Amsterdam Internet Exchange) huisvest. Dat maakt Nederland bij uitstek aantrekkelijk voor cybercriminaliteit. Nederlandse overheidsinstellingen blijken structureel doelwit van digitale spionage. Aanvallen worden ingezet om planmatig hoogwaardige kennis en bedrijfsinformatie te stelen. Naast criminaliteit en spionage vormt sabotage ook een groot risico. De moedwillige verstoring van vitale sectoren kan tot grote maatschappelijke en economische ontwrichting leiden.

Naast aanvallen van buitenaf vormen de medewerkers binnen de organisatie ook een risico. Processen kunnen strak ingeregeld zijn en systemen goed beveiligd, maar als medewerkers op een verkeerde link in een e-mail klikken of een ‘foute’ website openen, heeft de organisatie niets meer aan deze beveiliging. Bewustwording over het veilig verwerken van persoonsgegevens en informatie in het algemeen is daarmee van cruciaal belang.

1.2 Europese wetgeving

Nederland kende sinds 6 juli 2000 de wet Bescherming persoonsgegevens (Wbp[1]) die per 1 januari 2016 is aangescherpt. Echter, in mei 2016 is de Europese Algemene Verordening Gegevensbescherming (AVG) aangenomen die de Nederlandse wet in twee jaar tijd overschrijft. Deze nieuwe wetgeving moet zorgen voor harmonisatie van de huidige privacyregelgeving in Europa en verbetering van de privacy(bescherming) van burgers. De oude privacyregelgeving uit 1995 werd vastgesteld toen internet nog in de kinderschoenen stond. Bij de nieuwe regelgeving gaat het daarom vooral om het beschermen van persoonsgegevens in de digitale wereld. De Europese Unie wil met de AVG het vertrouwen bij burgers en consumenten in de verwerking van persoonsgegevens door overheid en bedrijven vergroten. In de komende twee jaar dient de AVG in onder andere alle overheidsorganisaties binnen de Europese Unie gerealiseerd te worden, zo ook binnen Veiligheidsregio Twente.

1.3 Toepassing Veiligheidsregio Twente

Op 10 december 2015 is door middel van een memo, besproken in het BVO en MT Brandweer, een start gemaakt met het onderwerp bescherming van persoonsgegevens. Onderliggend plan van aanpak is een uitwerking van deze memo, waarin de Europese wetgeving als leidraad is genomen.

Binnen Veiligheidsregio Twente (VRT) wordt niet alleen met persoonsgegevens gewerkt, maar

[1] In bijlage 4 is een bijlage met gebruikte afkortingen toegevoegd.

ook met andersoortige gevoelige informatie, zoals aanbestedingsgegevens, operationele en financiële informatie. De VRT wil zorgvuldig met al deze gegevens omgaan, omdat deze gevoelige informatie grote impact kan hebben op werknemers, bestuurders en burgers. Daarbij heeft VRT als overheidsorganisatie een voorbeeldfunctie en dus een imago hoog te houden. De VRT richt zich daarom op *informatieveiligheid*.

Missie: "Veiligheidsregio Twente gaat zorgvuldig om met alle gegevens"

In deze memo worden een aantal begrippen verduidelijkt en de Algemene Verordening Gegevensbescherming toegelicht. Daarna volgt de stand van zaken van Veiligheidsregio Twente en wordt het plan van aanpak voor de komende twee jaar voorgesteld.

2 Begrippen

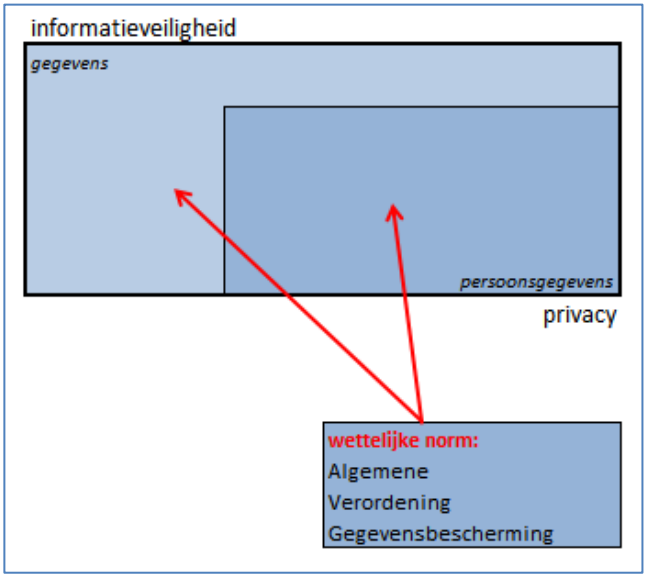
Het onderwerp informatieveiligheid bevat een aantal begrippen die met elkaar samenhangen. Om duidelijkheid te geven, worden ze hieronder nader toegelicht.

Informatieveiligheid is het geheel aan maatregelen, procedures en processen die de beschikbaarheid, integriteit en vertrouwelijkheid van alle vormen van informatie binnen een organisatie of een maatschappij garanderen. Het doel van deze maatregelen, processen en procedures is het waarborgen van continuïteit van informatie en informatievoorziening en eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau, te beperken.

Persoonsgegevens zijn alle gegevens over een geïdentificeerde of identificeerbare natuurlijk persoon. Dat houdt in dat het gegeven direct over een persoon gaat of naar die persoon te herleiden valt. Een bijzondere categorie is het bijzondere persoonsgegeven, wat betekent dat het gevoelige informatie betreft zoals ras, gezondheid en godsdienst. Ook het BSN is een bijzonder persoonsgegeven, omdat dit een uniek persoonsgebonden nummer is.

Privacy is een afweerrecht dat de persoonlijke levenssfeer beschermt. Hierbij gaat het niet alleen om fysieke bescherming, maar ook bescherming van persoonsgegevens en het recht om vertrouwelijk te communiceren via brief, telefoon of e-mail.

Bovenstaande begrippen hebben veel met elkaar te maken en kunnen eigenlijk niet afzonderlijk van elkaar bekeken worden. Het volgende figuur laat dat ook zien.



3 Europese en landelijke ontwikkelingen

Zoals eerder beschreven is in mei 2016 de Europese verordening goedgekeurd door de Europese Commissie en dient deze in twee jaar tijd, dus voor 25 mei 2018, binnen organisaties geïmplementeerd te worden. De belangrijkste punten uit de nieuwe wetgeving worden hieronder toegelicht. Ook binnen Nederland zijn er ontwikkelingen gaande, die hieronder eveneens worden toegelicht.

3.1 Europese Algemene Verordening Gegevensbescherming

De AVG schrijft een heel aantal verantwoordelijkheden en verplichtingen voor die voor een overheidsorganisatie als Veiligheidsregio Twente gelden. Deze zijn in een overzicht in bijlage 1 weergegeven. De belangrijkste verplichtingen die de AVG voorschrijft zijn:

- Aantoonbaar op orde hebben van informatieveiligheid en daarover verantwoording kunnen afleggen;
- Melden van datalekken;
- Het faciliteren van de rechten van betrokkenen;
- Aanstellen van een Functionaris Gegevensbescherming (FG).

Informatieveiligheid aantoonbaar op orde
Er dienen passende technische en organisatorische maatregelen te worden getroffen die de gegevensverwerking beperken tot strikt noodzakelijk. Er moet actief beleid gevoerd en maatregelen getroffen worden voor naleving van de AVG. Daarnaast geldt dat bij nieuwe verwerkingen van persoonsgegevens een Privacy Impact Analyse (PIA) uitgevoerd dient te worden om te kunnen beoordelen of persoonsgegevens op verantwoorde manier worden verwerkt.

Meldplicht datalekken
Zowel de wet Bescherming Persoonsgegevens (huidige wetgeving) als de AVG schrijven voor dat wanneer er inbreuk is geweest op de beschikbaarheid, integriteit of vertrouwelijkheid van persoonsgegevens, dit wordt gezien als een datalek. Hierbij moet zowel aan het verliezen van een iPad met gevoelige informatie als aan een hack of virus worden gedacht. Een datalek dient

binnen 72 uur aan de Autoriteit Persoonsgegevens gemeld te worden.

Rechten betrokkenen
De persoon van wie de gegevens worden verwerkt, heeft recht op inzage, correctie, in bepaalde gevallen het wissen en het beperken van verwerking van zijn of haar persoonsgegevens.

Aanstellen Functionaris Gegevensbescherming
In de Nederlandse wet Bescherming Persoonsgegevens werd een dergelijke functionaris al voorgesteld. Met de invoering van de AVG is het voor overheidsinstanties een verplichting geworden. De Functionaris Gegevensbescherming ziet toe op naleving van de Europese verordening in de breedste zin van het woord, geeft desgevraagd advies over Privacy Impact Analyses (PIA's) en is de contactpersoon voor de Autoriteit Persoonsgegevens.

De Autoriteit Persoonsgegevens ziet toe op realisatie van de AVG en onderzoekt of organisaties voldoende maatregelen hebben genomen voor bescherming van persoonsgegevens, in het bijzonder in het geval van datalekken. Datalekken zijn onmogelijk 100% te voorkomen, maar organisaties moeten wel aantoonbaar acties en maatregelen hebben ondernomen om de risico's zo klein mogelijk te maken en houden.

Risico niet nakomen AVG
Wanneer de Autoriteit Persoonsgegevens onderzoek heeft gedaan (onder andere bij een datalek) en constateert dat een organisatie in gebreke is gebleken, dan kan de maximale boete die aan de organisatie wordt opgelegd *20 miljoen euro* bedragen.

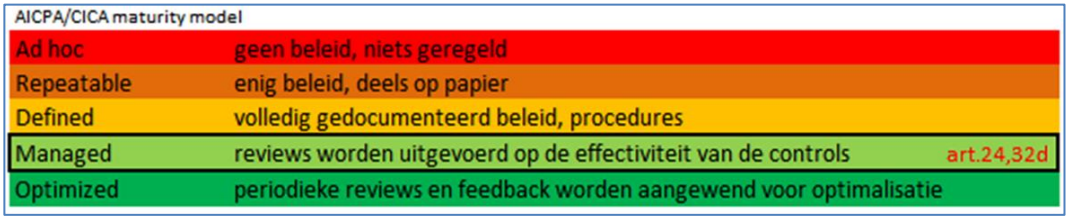
3.2 Landelijk: Vakgroep Informatiemanagement

Een van de doelstellingen van de Wet Veiligheidsregio's is het positioneren en professionaliseren van informatiemanagement. In het Veiligheidsberaad is daarvoor het Programma Informatievoorziening Veiligheidsregio's 2015-2020 vastgesteld. Binnen dit programma wordt het thema informatieveiligheid als speerpunt vormgegeven door de daarvoor opgerichte Vakgroep Informatieveiligheid. De vakgroep heeft de Baseline Informatieveiligheid Gemeenten (BIG) geadopteerd als normatief kader voor de inrichting van informatieveiligheid. In lijn met de AVG wordt bij de implementatie van de BIG de volgende aanpak gehanteerd:

- Risicogericht (de grootste risico's het eerst aanpakken)
- Passend (de maatregelen zijn proportioneel in de context van het risico)
- Uitvoerbaar (praktisch en financieel)

De leden van de Vakgroep Informatieveiligheid hebben elk in hun eigen Veiligheidsregio een quickscan uitgevoerd naar het huidige volwassenheidsniveau van informatieveiligheid. Daaruit is gebleken dat het gemiddelde niveau in de Veiligheidsregio's tussen niveau 1 (ad-hoc) en niveau 2 (repeatable) ligt.

De Vakgroep Informatieveiligheid heeft vastgesteld dat op grond van de AVG, voor de onderdelen met een groot risico, de BIG als pakket van risico-reducerende maatregelen geïmplementeerd zal moeten worden op niveau 4 (managed).



Het identificeren van risico's, het implementeren van de BIG en het behalen en handhaven van het vereiste volwassenheidsniveau, samengevat informatieveiligheid, is een verantwoordelijkheid van Veiligheidsregio's zelf.

3.3 Landelijk: VNG

Op 12 juli 2016 heeft de VNG een ledenbrief gepubliceerd waarin het in werking treden van de AVG is aangekondigd. In vergelijkbare lijn met de Vakgroep Informatieveiligheid wordt een voorzet gedaan om de verplichtingen vanuit de AVG te implementeren. Voor het plan van aanpak voor informatieveiligheid binnen Veiligheidsregio Twente wordt dezelfde aanpak gehanteerd.

4 Stand van zaken Veiligheidsregio Twente

Voor Veiligheidsregio Twente is op basis van de quickscan geconstateerd dat het niveau van informatieveiligheid ligt tussen niveau 1 (ad hoc) en niveau 2 (repeatable). Dit is mede gebaseerd op het feit dat Veiligheidsregio Twente een aantal dingen goed doet, zoals:

- Actief eigen beheer van de VRT ICT-omgeving met enige aandacht voor informatieveiligheid;
- Monitoren op beschikbaarheid van netwerkverbindingen;
- Incidentmanagement ICT door Servicedesk.

Daarnaast kan er een aantal zaken verbeterd worden, zoals:

- Het vastleggen van beleidsafspraken over beveiliging en gebruik van informatie en middelen;
- Het documenteren en beheren van autorisaties in gebruik van systemen, de termijn voor het opslaan van gegevens en het behouden van rechten in systemen bij wisseling van functie;
- Passende maatregelen voor het gebruik van bronnen en gegevensdragers als Dropbox, WeTransfer en USB-sticks;
- Procedures en middelen voor het structureel monitoren van informatieveiligheid.

5 Plan van aanpak Veiligheidsregio Twente

Zoals in bijlage 1 zichtbaar schrijft de AVG vele verplichtingen voor die in twee jaar tijd gerealiseerd dienen te worden. Al deze voorschriften kunnen echter niet in een keer uitgevoerd worden en verschillen ook in belang en zwaarte.

Zoals in de memo van 10 december 2015 aangegeven, kan informatieveiligheid alleen op orde komen en gehouden worden als op 3 terreinen acties worden ondernomen, namelijk: gedrag & cultuur, processen en techniek. De organisatie kan allerlei technische maatregelen nemen om de veiligheid van informatie te borgen, maar als een medewerker alsnog inloggegevens op een post-it onder het toetsenbord laat liggen, hebben deze technische maatregelen weinig effect.

In lijn met het plan van aanpak van de landelijke vakgroep Informatieveiligheid, wordt de komende periode op de volgende zaken ingezet:

a. Op orde krijgen van beveiligen van informatie (processen & techniek);
b. Bewustwording voor informatieveiligheid creëren bij medewerkers (cultuur & gedrag);
c. Organisatie inrichten op informatieveiligheid

a. Informatieveiligheid systemen (processen & techniek)

In de vakgroep Informatieveiligheid is een plan van aanpak in ontwikkeling, waarin voor het op orde krijgen van informatieveiligheid voor een risicogerichte invalshoek is gekozen. Dat houdt in dat de systemen waarbij de organisatie het meeste risico loopt in het kader van datalekken (kans of effect), als eerste geanalyseerd dienen te worden. Er moet daarbij gedacht worden aan het personeelssysteem, systemen voor geoefendheid en operationele systemen. Voor Veiligheidsregio Twente zijn alle systemen in kaart gebracht aan de hand van VERA (Veiligheidsregio ReferentieArchitectuur) (bijlage 2). Op basis van deze twee overzichten, gaat de komende periode de informatieveiligheid van de volgende primaire systemen geanalyseerd worden:

Systeem	**Aard gegevens**
Beaufort	belangrijkste bron van personeelsgegevens, o.a. BSN
Veiligheidspaspoort	Personeelsgegevens i.r.t. geoefendheid en medische keuringsgegevens
LCMS	operationele gegevens
VNET/Sharepoint	bevat alle mogelijke soorten gegevens, breed toegankelijk
GMS	operationele gegevens
AFAS	financiële gegevens

De genoemde systemen zullen worden onderzocht op:

- Welke taken worden uitgevoerd en onder wiens verantwoordelijkheid?
- Hoe is de toegang tot het systeem geregeld?
- Hoe zijn autorisaties in het systeem geregeld?
- Welke (categorieën van persoons)gegevens worden in dit systeem verwerkt?
- Wat is het doel van de verwerking?
- Hoe is in de werkprocessen geborgd dat uitsluitend noodzakelijke gegevens verwerkt worden?
- Hoe lang worden de (persoons)gegevens bewaard?
- Welke relaties (koppelingen/afhankelijkheden) zijn er met andere systemen?
- Hoe is de systeembeveiliging geregeld?
- Welke informatie wordt door het systeem opgeslagen in logbestanden?

De resultaten van dit onderzoek dienen vervolgens als input voor PIA's, aan de hand waarvan maatregelen worden voorgesteld, uitgevoerd en gemonitord. Na afronding van bovenstaande zes primaire systemen, zal voor alle andere systemen van VRT ook een analyse worden uitgevoerd, evenals het treffen van maatregelen.

Tools

Er bestaan informatiemanagementsystemen die overzicht bieden waar in de organisatie welke informatie wordt opgeslagen. Een dergelijk systeem beheert ook de maatregelen die in het kader van informatieveiligheid uitgevoerd moeten worden en geeft signalen wanneer dit niet gebeurt. Ook zijn systemen beschikbaar die gericht zijn op het achterhalen van virussen en lekken op mobiele telefoons (nieuwe trend) en het bijhouden van digitale acties, waardoor bij hacks,

virussen en datalekken kan worden achterhaald wat er is misgegaan. Dit maakt de oplossing vaak makkelijker en er wordt ervaring en kennis opgedaan voor de toekomst (bv. verscherpte beveiliging of detectie). Het projectteam Informatieveiligheid (onder punt c verder toegelicht) gaat in Q3 en Q4 2016 uitzoeken of en welke systeem/systemen nodig zijn voor VRT.

b. Bewustwording organisatie (cultuur & gedrag)

Data-incidenten kunnen niet alleen door technische aspecten tot een minimum beperkt worden, daarvoor is ook bewustwording onder medewerkers van belang. Alle medewerkers (inclusief vrijwilligers, gedetacheerden, stagiaires, externen, et cetera) moeten geïnformeerd, bewust gemaakt én gehouden worden over het veilig omgaan met gegevens. Hierbij moet niet alleen worden gedacht aan het beveiligen van een laptop, I-pad en mobiele telefoons, maar ook aan het delen van informatie via e-mail en het bijhouden van gegevens in Excel. Daarnaast dient er extra aandacht te zijn voor collega's die werken met systemen waar gevoelige informatie (bv. persoonsgegevens) wordt bewerkt.
Het projectteam gaat uitzoeken op welke manier alle medewerkers bewust gemaakt en gehouden kunnen worden. Voor beeldmateriaal en ideeën kan aangehaakt worden bij bijvoorbeeld SSNT, andere Veiligheidsregio's of landelijk.

c. Organisatie informatieveiligheid

Projectteam Informatieveiligheid / Taakveld
Tot nu toe is door Jeroen Brouwer (Privacy-specialist + lid landelijke vakgroep Informatieveiligheid) en Chaka Geerdink (projectleider) tijd geïnvesteerd om tot dit plan van aanpak te komen. Bij de uitvoering daarvan is meer capaciteit nodig om slagvaardig te worden. Daarom wordt voorgesteld om voor de uitvoering van het plan van aanpak een projectteam te vormen voor de komende 2 jaar. In het projectteam zitten naast Jeroen en Chaka de volgende medewerkers:

- Controller
- Informatiemanager
- Teamleider Operationele Informatievoorziening
- Specialist Communicatie

In het begin zal met name capaciteit nodig zijn om informatieveiligheid op te zetten door de zes belangrijke systemen te analyseren en bewustwording te creëren. Dit zal in de loop van de tijd verschuiven naar 'beheren' en 'monitoren'. Het projectteam denkt na over de projectkosten en structurele kosten in de toekomst en komt hiervoor nog met een uitwerking.
Naast uitvoering van dit plan van aanpak dient ook breder kennis opgebouwd te worden, zodat het projectteam een gedeelde basiskennis van informatieveiligheid heeft. De rol van FG wordt (voorlopig) ingevuld door één van de leden van het projectteam. Wie deze rol krijgt wordt nog nader bekeken door het projectteam.

Loket
Als bewustwording gecreëerd gaat worden moet aan medewerkers ook een handelingsperspectief geboden worden als zij vragen hebben dan wel verdachte situaties tegen komen. Er wordt voorgesteld om dit binnen de Servicedesk re organiseren. Hier kunnen medewerkers met vragen, verzoeken tot inzage en meldingen terecht en vanuit dit loket kunnen ook acties gericht op bewustwording ingezet worden. Dit is ook de plek om informatie, kennis en ervaring uit te wisselen en te clusteren. Het projectteam gaat dit idee verder uitwerken, waarbij ook het melden van incidenten buiten kantooruren wordt meegenomen.

Crisisteam
Inmiddels heeft een eerste incident plaatsgevonden op de Meldkamer, waarbij VRT in actie moest komen. Dit heeft veel informatie opgeleverd over de nog te nemen acties voor het goed

kunnen afhandelen van een data-incident. Hierbij moet gedacht worden aan goede beeldvorming, de inzetbaarheid van bepaalde personen, bereikbaarheid van personen buiten kantooruren en verantwoordelijkheid in het nemen van beslissingen. De komende periode wordt benut om deze onduidelijkheden op te helderen, een protocol op te stellen en een crisisteam aan te wijzen die de data-incidenten kan afhandelen.

5.1 Tijdsplanning

	2016		2017				2018	
	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
6 primaire systemen								
- Analyse	X	X	X					
- Risicobeoordeling			X	X				
- Maatregelen voorstellen/voorbereiden				X	X	X		
- Maatregelen uitvoeren					X	X	X	X
- Monitoren					X	X	X	X
Onderzoek benodigde tools	X	X						
Bewustwording medewerkers								
- Sleutelfiguren	X	X			X	X		
- Gebruikers	X	X			X	X		
Loket informatieveiligheid								
- Onderzoek loket	X							
- Voorstel (inclusief DPO)	X							
- Implementeren + aanstellen DPO	X	X	X	X	X	X	X	X
- Kennis vergaren	X	X		X				X
Crisisteam en protocol								
- Voorstel crisisteam en protocol data-incidenten	X	X						
- Implementatie crisisteam en protocol	X	X	X	X	X	X	X	X

Financiële consequenties:
Financiële consequenties, zowel voor het project als structureel, worden door het projectteam nader uitgewerkt.

Personele consequenties:
Personele consequenties worden nader uitgewerkt in een voorstel.

Juridische consequenties:
toelichting

Bijlagen
3

Vervolgprocedure

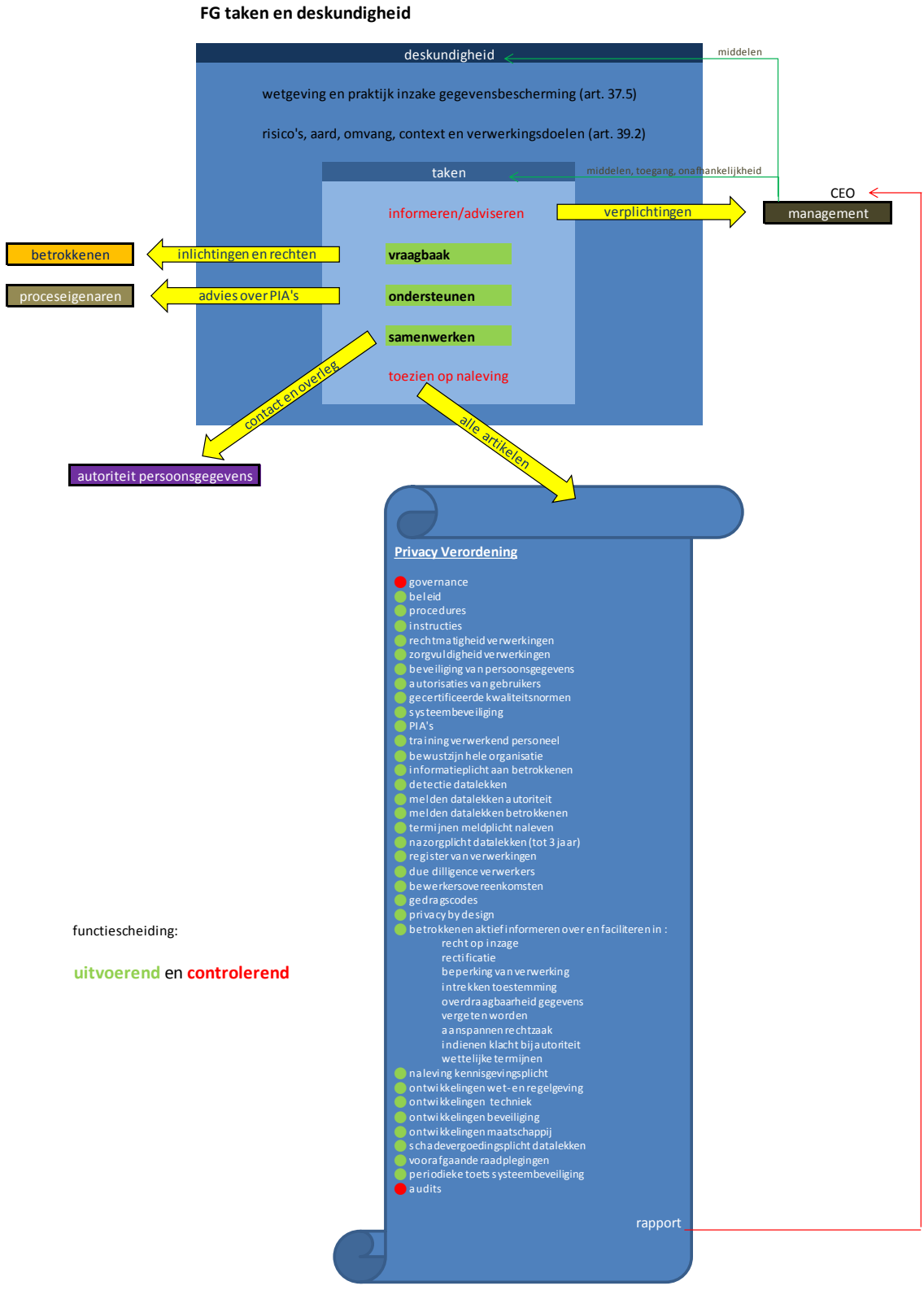
OR	Ja/Nee
GO	Ja/Nee
Algemeen bestuur	Ja/ Nee
Anders	[invulveld]

Communicatie	Ja/Nee

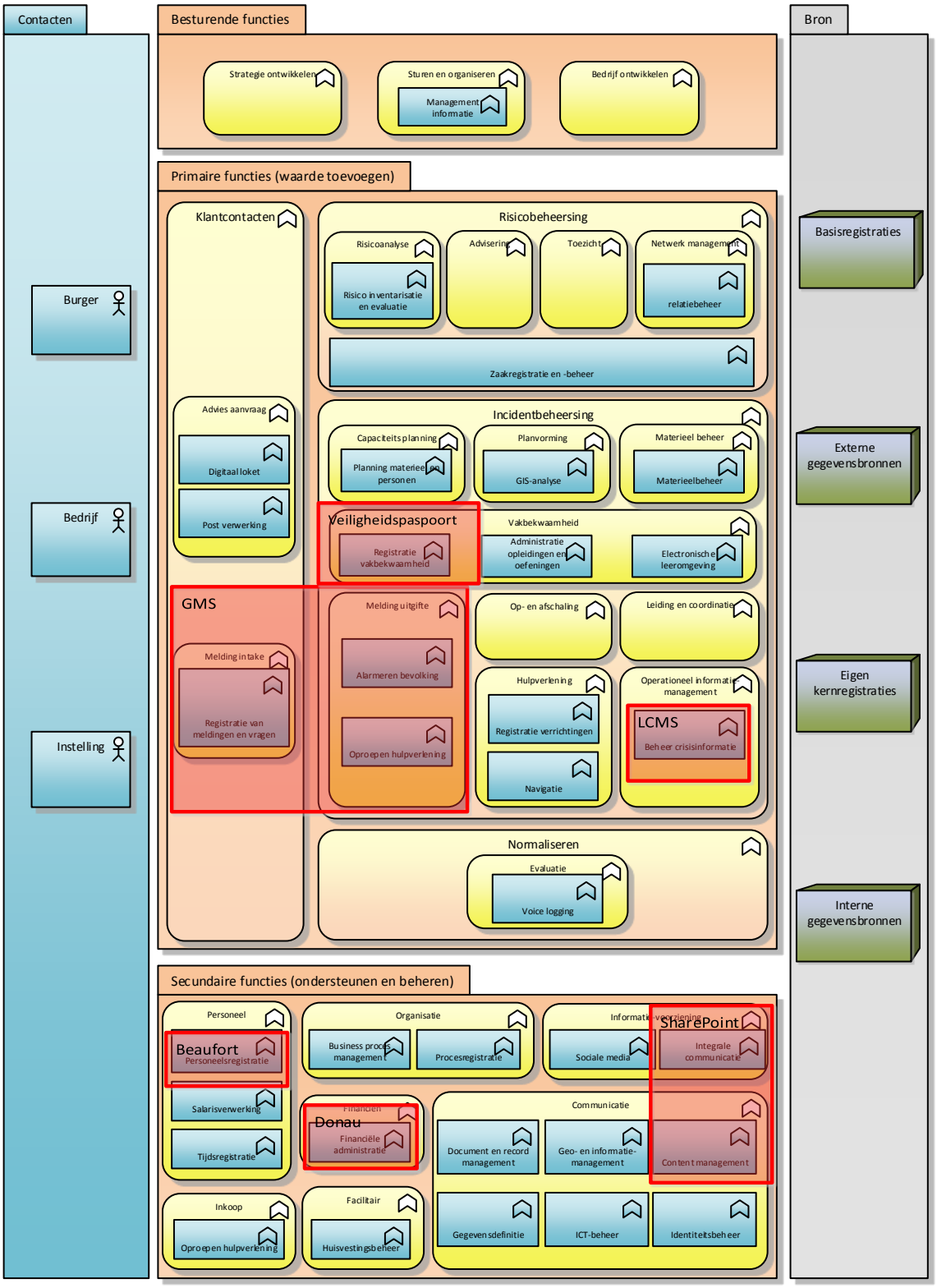
Toelichting:

☐ Persbericht	☐ Website	☐ Overig, nl. [toelichting]
☐ Persgesprek	☐ Advertentie	
☐ Intranet	☐ Digitale nieuwsbrief	

Bijlage 1 Lijst met acties vanuit de Algemene Verordening Gegevensbescherming.



Bijlage 2 Risico identificatie middels VERA



Bijlage 3 Ledenbrief VNG (d.d. 12 juli 2016)

Bijlage 4 Afkortingen

Wbp = Wet Bescherming persoonsgegevens

AVG = Algemene Verordening Gegevensbescherming

FG = Functionaris Gegevensbescherming

PIA = Privacy Impact Analyse

BIG = Baseline Informatieveiligheid Gemeenten

VERA = Veiligheidsregio's Referentie Architectuur