Versie 1.0
16-02-2018
VRA

Gemeente Amsterdam

Verkorte Risicoanalyse Informatiebeveiliging en Privacy

GGD Amsterdam

Datum :10-11-2018
Projectnummer :
Projectleider 5.1, 2, e 5.1, 2, e
Opdrachtgever :
Versie :1.0
Auteur 5.1, 2, e
Functie:TSO

Versiebeheer

Versies

Versie	Datum	Auteurs	Samenvatting van de wijzigingen
0.5	12-02-2018	5.1, 2, e	Eerste opzet.
1.0	16-02-2018	5.1, 2, e	Uitwerking VRA

Goedkeuring

Versie	Datum	Naam

Ter informatie aan

Versie	Datum	Naam

.

Managementsamenvatting

Het volgende advies wordt gegeven n.a.v. de ingevulde VRA:
De maatregelen uit de Baseline zijn *niet* voldoende voor de beveiliging van het proces: Er moet een Uitgebreide Risico Analyse worden uitgevoerd, waarbij het accent dient te liggen op Integriteit, Vertrouwelijkheid en beschikbaarheid. In het verleden is er een URA ingevuld maar deze is niet volledig. Wel kunnen bepaalde gegevens overgenomen worden. De PIA is reeds uitgevoerd.

Inhoud

Managementsamenvatting **3**

1 Inleiding **5**
1.1 Belang proces 7
1.2 Project 9

2 Vragenlijst belang processen **10**

3 Vragenlijst BIV **12**
3.1 Vragenlijst Beschikbaarheid 12
3.2 Integriteit 13
3.3 Vertrouwelijkheid 14

4 Vragenlijst persoonsgegevens **15**

5 Analyse en advies **17**
5.1 Analyse BIV 17
5.2 Analyse Persoonsgegevens 18
5.3 Advies 19

1 Inleiding

Steeds vaker is informatie als een van de kritieke ingrediënten voor succesvolle bedrijfsvoering te beschouwen. Het ontberen van informatie, verminking of uitlekken van informatie aan onbevoegden, kan ernstige negatieve effecten hebben op bijna alle zakelijke processen.

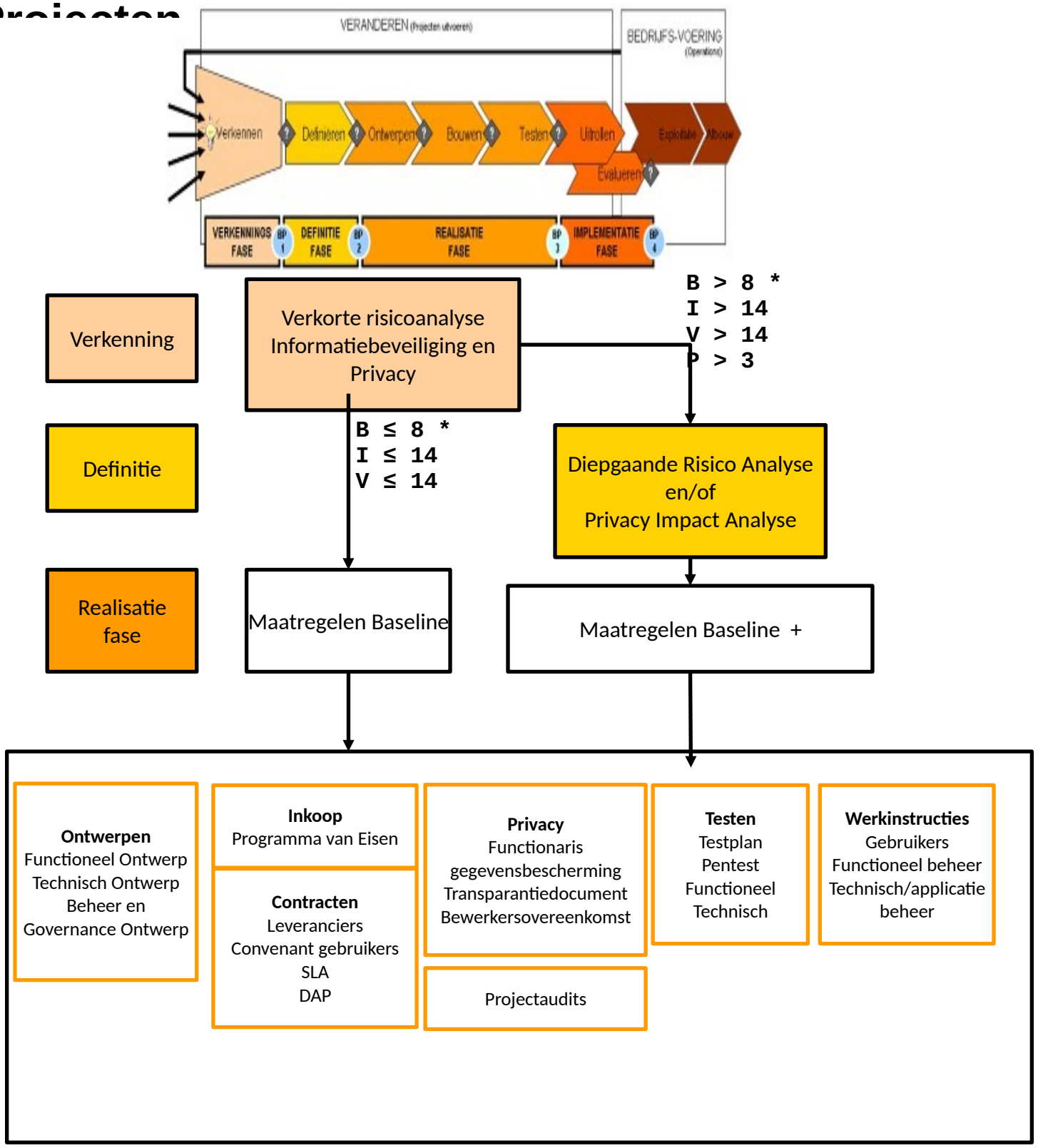
Het resultaat van deze verkorte risicoanalyse[1] (VRA) is bedoeld voor lijn- en procesmanagers die resultaatverantwoordelijkheid dragen. Deze managers hebben belang bij de juiste kwaliteit c.q betrouwbaarheid van het proces, hun product en de bijbehorende informatie. Daarbij hebben ze ook belang bij zo min mogelijk verstoring van het proces en zoveel mogelijk zekerheid over het verloop van het proces en de kwaliteit van het product en de informatie.

De VRA 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 (baseline) voldoende is, of dat er een aanvullend onderzoek nodig is (uitgebreide risico analyse/PIA).
De bedoeling is om aan de hand van de scores waar mogelijk maatregelen te benoemen die het risico verminderen. Organisatorische maatregelen kunnen vaak een middel zijn om hoge risico's te verminderen en te komen tot een acceptabel restrisico. Juist het benoemen van de organisatorische maatregelen is een business aangelegenheid en geen ICT aangelegenheid. Dit is ook de reden waarom de ICT BIV waarden niet overeen komen met de BIV waarden die uit deze vragenlijst naar voren komen

[1] Deze verkorte risicoanalyse is onder meer afgeleid van het assessmenttool dat IQUIP bij het voormalige Ministerie van Verkeer en Waterstaat in het verleden heeft gebruikt voor het vaststellen van betrouwbaarheidsniveau van informatiesystemen.

Informatiebeveiliging en Privacy in IV Projecten



(*) is het aantal punten uit de VRA op basis waarvan het vervolgtraject besloten wordt. Als de BIV (beschikbaarheid, integriteit en vertrouwelijkheid) waarden worden overschreden dient een diepgaande risicoanalyse uitgevoerd te worden. Bovenstaande plaat geeft de samenhang weer als de PIA in een project wordt toegepast. In de verkenningsfase wordt de VRA uitgevoerd. Het resultaat van de VRA geeft uitslag over het feit of de BIG voldoende maatregelen bevat of niet.

In het laatste geval moet een diepgaande risicoanalyse uitgevoerd worden. De maatregelen uit de diepgaande risicoanalyse dienen te worden toegevoegd aan de BIG maatregelen voor zover deze nog niet in de BIG staan. Ook zegt de baselinetoets in de verkenningsfase van een project of een PIA uitgevoerd moet worden. Als er veel onduidelijk is in de verkenningsfase kan de baselinetoets herhaald worden in de definitiefase. Als het proces en de informatievoorziening grote wijzigingen ondergaan in de productfase dient opnieuw een baselinetoets te worden uitgevoerd.

Deze vragenlijst dient in de verkenningsfase te worden opgesteld en te worden ingevuld door de business. Bij het invullen kan de Privacy-coördinator en/of de IBC van de dienst of het cluster worden ingeschakeld. De vragenlijst vormt input voor de eventueel te nemen beveiligingsmaatregelen welke in de definitiefase nader worden bepaalt al dan niet aan de hand van een uitgebreide risico analyse.

De VRA maakt onverkort deel uit van de producten die tijdens de verkenningsfase moeten worden opgeleverd en dient te allen tijde in kopie te worden verzonden aan de secretaris van de CPA.
Door het CBP kan worden getoetst of de risicoanalyse is uitgevoerd.

1.1 Belang proces

Het bepalen van het belang van het proces (en de ondersteunende systemen) gebeurt door na te gaan hoe groot de schade is die kan ontstaan als het betreffende betrouwbaarheidsaspect niet in orde is. Het toekennen van waarden (per betrouwbaarheidsaspect) is specifiek voor de dienst/stadsdeel of het betreffende verantwoordelijkheidsgebied. Deze dient in de argumentatie bij de vragenlijsten tot uitdrukking te komen en is subjectief. Het is een inschatting die gemaakt wordt om eventuele risico's vroegtijdig te onderkennen.

Invalshoeken om tot een waardebepaling te komen zijn bijvoorbeeld:

- Persoonlijke veiligheid

Bijvoorbeeld: Wordt de veiligheid van personen bedreigd als gegevens niet beschikbaar zijn, een systeem uitvalt, of als er verkeerde informatie wordt verstrekt? Zo ja, hoe ernstig zijn de gevolgen?

- Persoonsgegevens

Bijvoorbeeld: Wordt de persoonlijke levenssfeer van een persoon of een groep personen aangetast of wordt inbreuk gemaakt op een wet of regelgeving als gegevens over personen in handen vallen van ongeautoriseerde personen? Hoe ernstig is de mate van ongemak voor een persoon of een groep personen?

- Wettelijke en reglementaire verplichtingen

Bijvoorbeeld: Kan er strafrechtelijk vervolgd worden of worden civiele procedures aangespannen resulterend in het moeten betalen van boetes of schadevergoedingen als niet voldaan wordt aan wettelijke of reglementaire verplichtingen doordat informatie of een systeem niet beschikbaar is? Hoe groot zijn de boetes of schadevergoedingen?

- Rechtshandhaving

Bijvoorbeeld: Worden overtredingen of misdaden vergemakkelijkt als een systeem uitvalt of als door een systeem onjuiste of verouderde informatie wordt verstrekt? Hoe ernstig zijn de consequenties?

- Economische belangen

Bijvoorbeeld: Worden commerciële of economische belangen van de dient/stadsdeel of van derden geschaad als vertrouwelijke informatie bij ongeautoriseerde personen terecht komt? Hoe groot is de schade die kan ontstaan?

- Financieel verlies/verstoring van activiteiten

Bijvoorbeeld: Lijdt de organisatie directe of indirecte financiële schade als een informatie niet beschikbaar is of een systeem uitvalt? Hoe groot bedraagt de schade?

- Openbare orde

Bijvoorbeeld: Veroorzaakt het niet goed functioneren van een systeem protesten, demonstraties of acties? Blijft dit beperkt tot lokaal protest of komt de openbare orde door demonstraties in gevaar?

- Beleid en werking van de openbare dienstverlening

Bijvoorbeeld: Wordt de openbare dienstverlening belemmerd als een systeem uitvalt? Hoe ernstig is dit?

- Imagoschade

Bijvoorbeeld: Kan door het uitvallen van systemen of in de openbaarheid komen van informatie leiden tot negatieve publiciteit waardoor de betrekkingen met het publiek of andere organisaties schade lijden? Hoe ernstig is dit voor de organisatie?

1.2 Project

Doel van Jij en je gezondheid is dat jongeren op tijd de juiste zorg ontvangen. Daarbij wordt aangesloten bij het concept positieve gezondheid.
Bij de inzet van Jij en je gezondheid vullen leerlingen voorafgaande aan het contactmoment met de jeugdarts of jeugdverpleegkundige een digitale vragenlijst in bestaande uit valide en betrouwbare screeningslijsten. Na het invullen van de vragenlijst ontvangen zij op basis van hun antwoorden direct een gezondheidsprofiel met adviezen over hun gezondheid en leefsituatie. Dit plaatst de jongeren in de eigen kracht, geeft hen de mogelijkheid om ook autonoom aan de slag te gaan en draagt bij aan partnerschap tussen jongeren en JGZ professionals.
De jeugdarts of jeugdverpleegkundige bekijkt eveneens de uitslagen van de vragenlijst en ziet door het stoplichtsysteem (rood-oranje-groen) in één oogopslag wat de sterke kanten zijn van de jongere en waar eventueel ondersteuning gewenst is. Indien nodig wordt de jongere uitgenodigd voor een gezondheidsconsult. Als er nog vragen zijn over de aard of de ernst van problemen kan de jeugdarts of jeugdverpleegkundige digitale instrumenten inzetten voor nader onderzoek. Dit nader onderzoek kan bestaan uit een extra vragenlijst of een klinisch interview en zorgt ervoor dat de juiste jongeren bij de juiste zorg terecht komen. Indien nodig kan een jongere worden besproken in het zorgadviesteam. De digitale zorgwijzers helpen bij het zoeken naar passende programma’s.
Naast de individuele profielen, levert Jij en je gezondheid schoolgezondheidsprofielen op basis van geanonimiseerde groepsgegevens. Dit biedt scholen richting bij een planmatige gezondheidsbevordering met als doel gezonde leerlingen in een fysiek, sociaal en emotioneel gezond schoolklimaat.

2 Vragenlijst belang processen

Naam en functie geïnterviewde
5.1, 2, e 5.1, 2, e *Groepssessie* 5.1, 2, e5.1, 2, e 5.1, 2, e 5.1, 2, e

Naam en functie proces
Het betreft de JGZ contactmomenten op het Voortgezet Onderwijs. Doel is om jongeren met (een verhoogd risico op) psychosociale of sociaal-medische gezondheidsproblemen tijdig te signaleren en waar nodig passende ondersteuning te bieden.

Geef een bondige beschrijving van het proces/processen en benoem de proceseigenaar.
Zie project. Proceseigenaar is hoofd jeugdgezondheidszorg van de GGD Amsterdam.

Maakt het proces/de processen deel uit van een keten/meerdere ketens? Zo ja beschrijf de keten/ketens
Zie project. Jij en je gezondheid maakt onderdeel uit van het JGZcontactmoment.

Welke eventuele sub-processen zijn te onderscheiden? Welke hoofdactiviteiten worden binnen het proces uitgevoerd en wie doen dat?

Beschrijf welke afnemers het proces heeft. Welke producten nemen zij af en welke kwaliteitseisen stellen zij aan deze producten?
JGZ professionals zijn de hoofdgebruikers van dit product. Zij gebruiken Jij en je gezondheid als input voor de toepassing van triage of als input voor een gezondheidsconsult. Ook de leerlingen gebruiken het product. Zij krijgen persoonlijke gezondheidsadviezen op basis van de gegeven antwoorden.

Beschrijf welke leveranciers het proces heeft. Welke producten leveren zij aan en welke stellen zij aan de verwerking in het te onderzoeken proces?
Kidos

Welke wet- en regelgeving is van toepassing op dit proces en welke specifieke eisen komen hieruit naar voren?
Op dit informatiesysteem is de onderstaande wet- en regelgeving op het gebied van Informatiebeveiliging en Privacy van toepassing[1][1]: Wet bescherming persoonsgegevens (WBP) Wet basisregistratie personen (BRP) Archiefwet Wet Big WBGO WPG

Door welke informatievoorziening wordt het proces ondersteund?
<alleen invullen indien bekend>

(beoogd) Eigenaar informatiesysteem
JGZ/afdelingshoofd

[1]

3 Vragenlijst BIV

3.1 Vragenlijst Beschikbaarheid

Gevolgen van het niet beschikbaar hebben van de benodigde Informatie of gegevens. *(in het ergste geval)*		**Waardering**				**Argumentatie** *(verplicht invullen)*
		1 uur	1 dag	1 week	1 mnd	
B1	**Managementbeslissingen:** Hoe lang duurt het, voordat het nemen van beslissingen nadelig beïnvloedt wordt door het ontbreken van informatie ?	3	**2**	1	0	
B2	**imagoverlies** Hoe lang duurt het voordat er sprake is van imagoverlies wanneer informatie niet voorhanden is?	3	**2**	1	0	
B3	**Hapering dienstverlening** Hoe lang kan de applicatie of informatie niet beschikbaar zijn voordat er daadwerkelijk hapering in de dienstverlening aan burgers/bedrijven/ketenpartners ontstaat?	3	**2**	1	0	
B4	**Wettelijke aansprakelijkheid**: Hoe lang kan de applicatie of informatie niet beschikbaar zijn voordat er wettelijke of contractuele verplichtingen niet kunnen worden nagekomen?	3	**2**	1	0	
B5	**Additionele kosten**: Na welke periode zijn additionele kosten voor de organisatie te verwachten bij het niet beschikbaar zijn van de applicatie of informatie?	3	**2**	1	0	
B6	**Moreel van de medewerkers**: Na welke periode is er sprake van een duidelijk negatieve invloed op het moreel en de motivatie van medewerkers wanneer de informatievoorziening hapert?	**3**	2	1	0	
B7	**Herstel:** Hoe lang duurt het om te herstellen na een langdurige onbeschikbaarheid van een applicatie of informatie?	0	1	2	**3**	
	Subtotalen B1-B7	3	10		3	
Totaal Beschikbaarheid:		**16**				

3 = zeer ernstige schade: de dienstverlening aan de burger/bedrijven/ketenpartners komt in gevaar, raadsvragen, reactie wethouder vereist, berichten in de krant, professionaliteit van het concern, de gemeentelijke dienst ter discussie.

2 = ernstige schade: krantenkoppen, vragen van belangrijke partners / klanten, budgettaire problemen.

1 = acceptabele schade, binnen marges: incident met direct betrokkenen snel recht te zetten.

0 = verwaarloosbare schade of niet van toepassing.

3.2 Integriteit

Gevolgen van fouten in informatie of doelbewuste manipulatie van informatie om te frauderen of fraude te maskeren *(in het ergste geval)*		Waardering				Argumentatie *(verplicht invullen)*
I1	**Managementbeslissingen:** Kan onjuiste informatie leiden tot onjuiste beslissingen? Wat zijn de gevolgen?	**3**	2	1	0	
I2	**Fraude potentie:** Zijn er frauderisico's, en welke gevolgen hebben deze?	3	**2**	1	0	
I3	**Onderbreking van strategische processen:** In hoeverre kunnen de kernprocessen van de organisatie onderbroken worden als gevolg van ongeautoriseerde wijziging van of fouten in informatie?	**3**	2	1	0	
I4	**Vertrouwen van het publiek c.q. klanten:** Kan het vertrouwen van het publiek geschaad worden door onjuiste informatie?	**3**	2	1	0	
I5	**Wettelijke aansprakelijkheid:** Wat kunnen de gevolgen zijn van het niet voldoen aan wettelijke of contractuele verplichtingen die veroorzaakt worden door onjuiste informatie?	3	2	**1**	0	
I6	**Additionele kosten:** In hoeverre kunnen er additionele kosten ontstaan door het toepassen van onjuiste informatie? Bijvoorbeeld door het moeten herstellen van een corrupte database of opnieuw invoeren van gegevens.	**3**	2	1	0	
I7	**Moreel van de medewerkers:** Wat zijn de schadelijke effecten op het moreel van medewerkers als u onjuiste informatie gebruikt?	**3**	2	1	0	
	Subtotalen I1-I7	18	2	1		
Totaal Integriteit:		**21**				

3 = zeer ernstige schade: raadsvragen, reactie wethouder vereist, belangrijke partners / klanten stellen professionaliteit van het concern of de gemeentelijke dienst ter discussie.
2 = ernstige schade: krantenkoppen, vragen van belangrijke partners / klanten , burgers budgettaire problemen.
1 = acceptabele schade, binnen marges: incident met direct betrokkenen snel recht te zetten.
0 = verwaarloosbare schade of niet van toepassing.

3.3 Vertrouwelijkheid

Gevolgen van onbedoelde of ongeautoriseerde verspreiding van gegevens of informatie *(in het ergste geval)*		Waardering				Argumentatie *(verplicht invullen)*
V1	**Vertrouwen van de burger:** Wat zijn de gevolgen voor de gemeente indien de binnen het proces beschikbare informatie te vroeg c.q. niet volgens de regels verspreid wordt?	**3**	2	1	0	
V2	**Vertrouwen van het publiek**: Wat zijn de gevolgen voor het publieke imago van de gemeente als vertrouwelijke informatie van de organisatie onterecht wordt verspreid	**3**	2	1	0	
V3	**Vertrouwen van ketenpartners** Kan de gemeente toegang tot de keten geweigerd worden?	3	2	1	**0**	
V4	**Vertrouwen van ketenpartners** Wat zijn de gevolgen voor de relatie met de ketenpartners als vertrouwelijke informatie onterecht wordt verspreid.	3	2	**1**	0	
V5	**(Wettelijke) Aansprakelijkheid:** Wat zijn de gevolgen voor (wettelijke) aansprakelijkheid bij het onterecht verspreiden van deze informatie?	3	2	**1**	0	
V6	**Additionele kosten:** In hoeverre is er sprake van additionele kosten door onterechte verspreiding van deze informatie?	**3**	2	1	0	
V7	**Moreel van de medewerkers:** In hoeverre kan een duidelijk negatieve invloed op het moreel en de motivatie van medewerkers een gevolg zijn van de onterechte verspreiding van informatie?	**3**	2	1	0	
	Subtotalen V1-V7	12	0	2	0	
Totaal Vertrouwelijkheid:		**14**				

3 = zeer ernstige schade: raadsvragen, reactie wethouder vereist, belangrijke partners / klanten stellen professionaliteit van de gemeentelijke dienst ter discussie.
2 = ernstige schade: krantenkoppen, vragen van belangrijke partners /politiek/burgers afnemers,.
1 = acceptabele schade, binnen marges: incident met direct betrokkenen snel recht te zetten.
0 = verwaarloosbare schade of niet van toepassing.

Vragenlijst persoonsgegevens Persoonlijke gevolgen van onbedoelde of ongeautoriseerde verspreiding van persoonsgegevens van betrokkene(n) *(in het ernstigste geval)*		Waardering				Argumentatie
P1	**Veiligheid:** Is de veiligheid van personen in het geding indien persoons gegevens uitlekken of onterecht worden verwerkt ?	**3**	2	1	0	
P2	**Chantage:** Kan de betrokkene eventueel gechanteerd worden bij het uitlekken van persoonsgegevens?	**3**	2	1	0	
P3	**Identiteits- en financiële fraude:** Bestaat de mogelijkheid dat door het uitlekken van persoonsgegevens identiteits- of financiële fraude kan plaatsvinden?	3	2	**1**	0	
P4	**Fysieke en geestelijke schade;** Kan de betrokkene schade oplopen indien gegevens over de persoon openbaar worden of onterecht worden verwerkt?	**3**	2	1	0	
P5	**Vertrouwen van de burger:** Wat zijn de gevolgen voor het publieke imago van de gemeente als vertrouwelijke informatie over personen onterecht wordt verspreid/verwerkt?	**3**	2	1	0	
P6	**(Wettelijke) Aansprakelijkheid:** Wat zijn de gevolgen voor (wettelijke) aansprakelijkheid bij het onterecht verspreiden/verwerken van deze persoonlijke informatie?	3	2	**1**	0	
P7	**Additionele kosten:** In hoeverre is er sprake van additionele kosten door onterechte verspreiding/verwerking van deze persoonlijke informatie?	**3**	2	1	0	
P8	**Moreel van de medewerkers:** In hoeverre kan een duidelijk negatieve invloed op het moreel en de motivatie van medewerkers een gevolg zijn van de onterechte verspreiding/verwerking van informatie?	**3**	2	1	0	
	Subtotalen P1-P8	18		2		
Subtotaal Persoonsgegevens (P1-P9):		**20**				

3 = zeer ernstige schade voor de persoon en de gemeentelijke organisatie: raadsvragen, reactie wethouder vereist, belangrijke partners / burgers en derden stellen professionaliteit van de gemeentelijke dienst/stadsdeel ter discussie.
2 = ernstige schade voor de persoon, de gemeentelijke dienst/stadsdeel: krantenkoppen, vragen van partners / burgers ,boete CBP.
1 = acceptabele schade, binnen marges: incident met direct betrokkenen snel recht te zetten.
0 = verwaarloosbare schade of niet van toepassing.

Algemene vragen m.b.t. doeleinden en doelbinding van de verwerking van persoonsgegevens				
		Ja	Nee	Argumentatie
P9	Hebt u het/de specifieke (doel)en waarvoor u de persoonsgegevens gaat verwerken in detail vastgelegd?	**0**	3	Omschrijf het doel
P10	Worden bestaande persoonsgegevens voor nieuwe doeleinden verwerkt in een bestaand of nieuw systeem?	3	**0**	
P11	Gaat het bij het project/systeem om het nastreven van nieuwe aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen koppelen of anderszins verder te verwerken?	3	**0**	
P12	Indien u op P11 ja hebt geantwoord: Hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking **dezelfde** doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang?	0	3	
P13	Indien u op P11 ja hebt geantwoord: Gelden dezelfde doelen voor het gehele proces?	0	3	
P14	Worden de verzamelde/verwerkte persoonsgegevens gebruikt om het gedrag / de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen?	**3**	0	
P15	Indien u op P14 ja hebt geantwoord: Zijn de betrokkenen daarvan op de hoogte?	**0**	3	
P16	Indien u op P14 ja hebt geantwoord: Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld?	3	**0**	
	Subtotalen P9-P16	3	0	
Subtotaal Persoonsgegevens (P9-P16):		**3**		

5 Analyse en advies

5.1 Analyse BIV

	score	Aantal score boven de baseline norm	Focus Risico analyse
Beschikbaarheid (B1-B7)	16	7	Hoger dan 8 focus op beschikbaarheid bij URA
Integriteit (I1-I7)	21	5	Hoger dan 14 focus op vertrouwelijkheid Bij URA
Vertrouwelijkheid (V1-V7)	14	4	Hoger dan 14 focus op Integriteit bij URA
TOTAAL SCORE:	**51**	**17**	

De totale score geeft een globale indicatie voor de beveiligingsbehoefte van het betreffende proces.

Bij Beschikbaarheid aangeven of- en hoe vaak er hoger is gescoord dan een één (2 of hoger).

Bij Integriteit aangeven of- en hoe vaak er hoger is gescoord dan een twee (dat is een 3)

Bij Vertrouwelijkheid aangeven of en hoe vaak er hoger is gescoord dan een twee (dat is een 3)

Het niveau van de Baseline Informatiebeveiliging Nederlandse Gemeenten bevindt zich op de volgende (BIV) waarden[2]:

- Beschikbaarheid: Belangrijk (waarde = 1 in de gehanteerde beschikbaarheidsschaal).
- Integriteit: Hoog (waarde = 2 in de gehanteerde Intergriteitsschaal)
- Vertrouwelijkheid: Vertrouwelijk (waarde =2 in de gehanteerde vertrouwelijksheidsschaal)

Vertaald naar de baselinetoets betekenen de uitkomsten van deze baselinetoets het

[2] Zie handreiking dataclassificatie BIG

volgende:

	Norm
Beschikbaarheid	8 of minder = baseline
Integriteit	14 of minder = baseline
Vertrouwelijkheid	14 of minder = baseline

Let op: Als er één of meerdere keren een twee (2) is gescoord bij Beschikbaarheid (B) en drie (3) gescoord is bij de IV + P rating, dan betekent dat er een verhoogd risico aanwezig is. Op grond hiervan moet, *onafhankelijk* van de rest van de scores, een diepgaande risicoanalyse uitgevoerd worden. De resultaten van deze baselinetoets zijn input voor de diepgaande risicoanalyse. Focus hierbij dan vooral op dat aspect dat een hogere waarde kent.

Focus risico analyse

Indien één of meer van de BIV waarden hoger worden ingeschat dan het niveau van de BIG dan dient bij de vervolganalyse de focus op deze de betreffende BIV aspecten worden gelegd.

5.2 Analyse Persoonsgegevens

	score	Aantal scores 3+
Persoonsgegevens (P1-P9)	20	6
Verwerking Persoonsgegevens (P10-P16)	**3**	**1**
TOTAAL SCORE:	**23**	**7**

De totale score geeft een globale indicatie voor de beveiligingsbehoefte van het betreffende proces.

In de 3+ kolom aangeven of binnen een bepaald aandachtsgebied een 3 is gescoord.

Indien één of meer scores voor wat betreft de verwerking van persoonsgegevens hoger is dan **3** dan dient u een Privacy Impact Analyse (PIA) uit te voeren en contact op te nemen met de CISO of gelijkwaardige functionaris.

5.3 Advies

Het volgende advies wordt gegeven n.a.v. de ingevulde VRA:
De maatregelen uit de Baseline zijn *niet* voldoende voor de beveiliging van het proces: Er moet een Uitgebreide Risico Analyse worden uitgevoerd, waarbij het accent dient te liggen op Integriteit, Vertrouwelijkheid en beschikbaarheid. In het verleden is er een URA ingevuld maar deze is niet volledig. Wel kunnen bepaalde gegevens overgenomen worden. De PIA is reeds uitgevoerd.