Aanpak herijking processen en uitvoering quickscans en BIO-analyses

5.1.2e

5.1.2e

5.1.2e

Inhoudsopgave

Inleiding

In 2017 zijn de bedrijfsprocessen binnen de directies van het VWS Kerndepartement geïnventariseerd, maar daarin zijn de Te Beschermen Belangen niet meegenomen en is onvoldoende gekeken naar de verwerking van persoonsgegevens.

Inmiddels is er veel veranderd binnen de directies en programmadirecties. Om te zorgen dat alle processen en ondersteunende systemen in beeld zijn bij het nemen van beveiligingsmaatregelen, is het belangrijk dat de bedrijfsprocessen binnen de directies opnieuw worden geïnventariseerd.

Aanpak

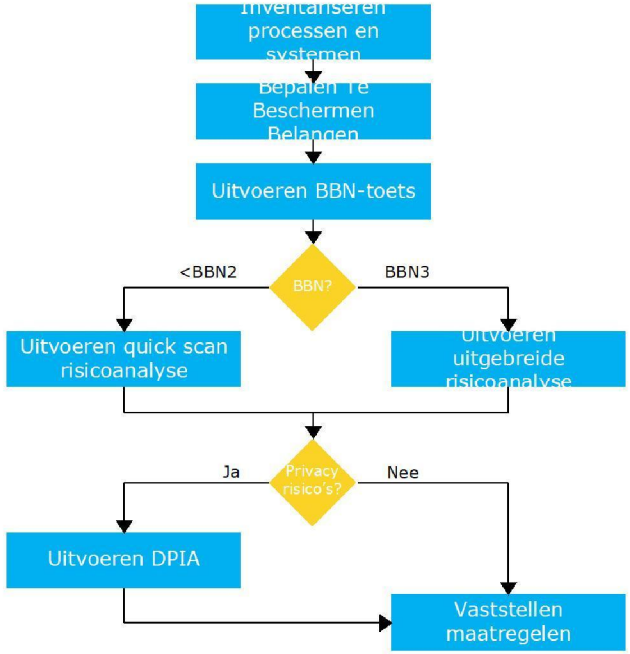
Als eerst wordt een inventarisatie gemaakt van de processen, ondersteunende systemen, en Te Beschermen Belangen binnen de directies.

Vervolgens wordt een BBN-toets uitgevoerd voor de geïnventariseerde processen om een beeld te krijgen van de belangrijkste dreigingen. Op basis daarvan wordt bepaald of een quick scan of uitgebreide risicoanalyse noodzakelijk is.

Hierbij wordt tevens gecontroleerd of een eventuele verwerking van persoonsgegevens correct in het AVG-register staat geregistreerd en of er eventuele privacyrisico's zijn. In dat geval wordt een aanvullende DPIA ingepland.

Tot slot worden de nodige maatregelen geformuleerd om de gevonden risico's te mitigeren.

Aanpak (vervolg)



Betrokken stakeholders

Stap	Activiteit	Facilitator	Betrokkenen
1	Inventariseren processen en systemen	Adviseur informatiebeveiliging & privacy (CIO Office & IM en/of I-Team)	Proceseigenaar, IB&P-coördinator
2	Bepalen Te Beschermen Belangen	Adviseur informatiebeveiliging & privacy (CIO Office & IM en/of I-Team)	Proceseigenaar, IB&P-coördinator
3	Uitvoeren BBN-toets	Adviseur informatiebeveiliging & privacy (CIO Office & IM en/of I-Team)	Proceseigenaar, IB&P-coördinator
4	Uitvoeren quick scan risicoanalyse	Adviseur informatiebeveiliging & privacy (CIO Office & IM en/of I-Team)	Proceseigenaar, IB&P-coördinator
5	Uitvoeren uitgebreide risicoanalyse	Adviseur informatiebeveiliging & privacy (CIO Office & IM en/of I-Team)	Proceseigenaar, IB&P-coördinator
6	Uitvoeren DPIA	Adviseur informatiebeveiliging & privacy (CIO Office & IM en/of I-Team)	Proceseigenaar, IB&P-coördinator
7	Vaststellen maatregelen	Adviseur informatiebeveiliging & privacy (CIO Office & IM en/of I-Team)	Proceseigenaar, IB&P-coördinator

Inventarisatie processen en systemen

De ICV vormt hiervoor het uitgangspunt. Hierin zijn de processen en systemen opgegeven.

Niet alle directies of programmadirecties hebben een ICV opgeleverd. Bij die directies zullen we een afspraak inplannen met de IB&P-coördinator om de processen en systemen in kaart te brengen.

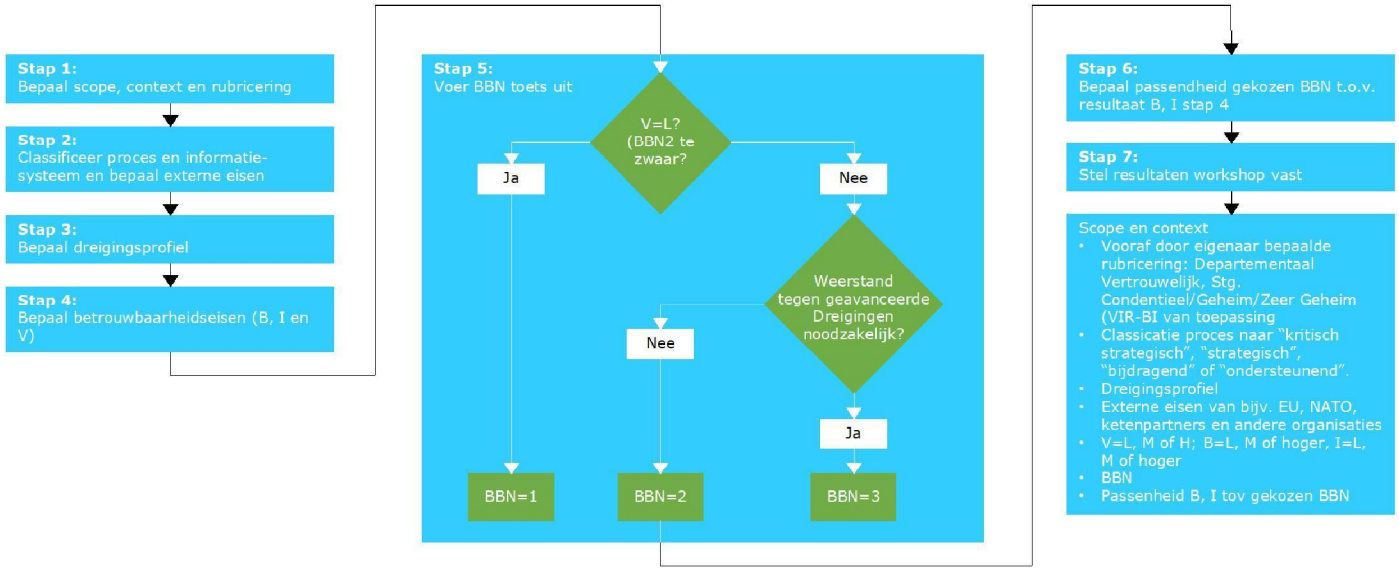
Hierbij wordt ook een check gedaan op het AVG-verwerkingsregister om te controleren of alle verwerkingen van persoonsgegevens geregistreerd staan.

Bepalen Te Beschermen Belangen

De volgende stap is om te beoordelen of er binnen de geïnventariseerde processen belangen bestaan waarbij in geval van (de mogelijkheid van) compromittering nadelige gevolgen kunnen ontstaan voor de betrouwbaarheid en continuïteit van de primaire processen van VWS.

De Te Beschermen Belangen zijn in 2019 door de Concern CISO in kaart gebracht. Deze inventarisatie vormt het uitgangspunt voor deze stap.

Uitvoeren BBN-toets

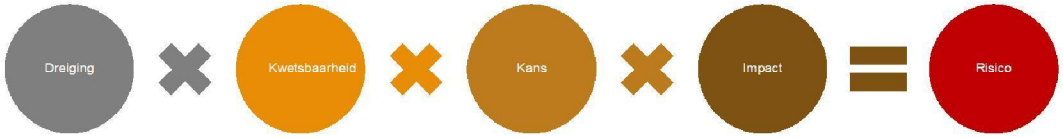


Uitvoeren (quick scans) risicoanalyses

Voor processen en systemen waarvoor een BBN van 1 of 2 geldt wordt een quick scan risicoanalyse uitgevoerd. Dit is een verkorte risicoanalyse op basis van de BIO en bedoeld om een snel beeld te krijgen van eventuele risico's.

Voor processen en systemen waarvoor een BBN van 3 geldt wordt een uitgebreide risicoanalyse op basis van de BIO uitgevoerd.

De uitkomsten van de risicoanalyses worden verwerkt in een verslag. Risico's worden in een risicoregister geregistreerd.



Uitvoeren DPIA

Wanneer tijdens de risicoanalyses privacyrisico's naar voren komen, worden voor betreffende processen, systemen en/of verwerkingen een DPIA uitgevoerd.

De DPIA borduurt voort op de reeds uitgevoerde risicoanalyses, maar gaat nader in op de risico's voor de privacy van betrokkenen.

De uitkomsten van de DPIA's worden verwerkt in een verslag. Risico's worden in een risicoregister geregistreerd.

Vaststellen maatregelen

Tot slot worden maatregelen geformuleerd en vastgesteld in overeenstemming met de proceseigenaren, om de geïdentificeerde risico's te mitigeren.

Vervolgens is het zaak om uitvoering te geven aan de gedefinieerde risico-beperkende maatregelen.

Hiervoor bestaat verschillende strategieën:

- Vermijden van een risico
- Reduceren van een risico
- Overdragen van een risico
- Accepteren van een risico

Vragen stap 1 – inventariseren processen

Inventarisatie processen/informatie/systemen

#,	Proces	Opmerking	Informatie	Gerubriceerde informatie	Informatie-systeem	Persoons-gegevens	BBN	TBB	PIA	Risico's	Quick scan risicoanalyse
1	Financiële processen	Zoals de financiële processen bij alle directies van het kerndepartement	Financiële administratie	Nee	SA/GMI	Ja, namelijk 5.1.2e kun je hier voorbeelden van persoonsgegevens invullen binnen de financiële processen]	Nee	Nee	Nee	5.1.2e zijn er bij jou risico's op het gebied van informatie-beveiliging of privacy bekend in deze processen?	Nee
2	Beantwoording burgerbrieven	Proces zoals bij alle directies binnen het kerndepartement	Persoonsgegevens van de schrijvers van burgerbrieven 5.1.2e hoe lang blijven burgerbrieven bewaard?	Nee	Algemene bedrijfsvoerings-applicaties van VWS	Ja, namelijk 5.1.2e kun je hier voorbeelden van persoonsgegevens invullen binnen dit proces]	Nee	Nee	Nee?	5.1.2e zijn er bij jou risico's op het gebied van informatie-beveiliging of privacy bekend in dit proces?	Nee

5.1.2e websites zien wij ook als informatiesysteem. Zijn er in bovengenoemde processen websites waarvoor PDC-19 verantwoordelijk is?

Inventarisatie processen/informatie/systemen

#	Proces	Opmerking	Informatie	Gerubriceerde informatie	Informatie-systeem	Persoons-gegevens	BBN	TBB	PIA	Risico's	Quick scan risicoanalyse
3	Bedrijfsvoering en secretariële ondersteuning	Personeelsgegevens staan op beveiligde schijf	Op personeelsgegevens na geen gevoelige informatie	Nee	Algemene bedrijfsvoerings-applicaties van VWS: - Kantoorautomatisering - Marjolein - P-Direkt	Ja, namelijk personeelsgegevens van medewerkers van PDC-19	Nee	Nee	Nee?	5.1.2e zijn er bij jou risico's op het gebied van informatie-beveiliging of privacy bekend in dit proces?	Nee
4	Testen en traceren	1. Beleidvorming voor uitvoering van testen bij GGD's en toegangstesten (Stichting Open Nederland, bijv. voor FieldLab pilots). 2. Aanbieden van twee zelftests 3. Melden van besmettingen door ziekenhuizen en zorginstellingen 4. Inkoop en subsidie voor uitvoeren van het beleid testen en traceren 5. Dashboard gegevens verwerken via Dienst testen 6. Inzetten van ICT end data oplossingen ter ondersteuning van de GGD's en GGD Ghor 7. Inzetten van Coronamelder en Coronacheck (via IRDO)	1.Beleidsinformatie en inkoopgegevens (o.a.prijsafspraken, afspraken met partijen die de uitvoering doen 2. Adresgegevens 3. Gegevens van personeel en van patiënten 4. Contactpersonen bij organisaties 5. Gegevens van doelgroepen die herleidbaar kunnen worden	5.1.2e zou je dit willen navragen? Ik kan me voorstellen dat prijsafspraken Departementaal Vertrouwelijk zijn?	Algemene bedrijfsvoerings-applicaties van VWS: - Kantoorautomatisering - Marjolein - 3F (inkoop)	Nee	Nee	Nee	N.v.t.	Nee	Nee

5.1.2e websites zien wij ook als informatiesysteem. Zijn er in bovengenoemde processen websites waarvoor PDC-19 verantwoordelijk is?

Inventarisatie processen/informatie/systemen

#	Proces	Opmerking	Informatie	Gerubriceerde informatie	Informatie-systeem	Persoons-gegevens	BBN	TBB	PIA	Risico's	Quick scan risicoanalyse
5	Bron- en contactonderzoek	Beleidsvorming rondom bron- en contactonderzoek, afstemming met GGD's, informeren van de Tweede Kamer	Beleidsinformatie, informatie vanuit de GGD's over uitgevoerd bron- en contactonderzoek	Nee 5.1.2e zou je voor de zekerheid willen navragen of er in dit proces gevoelige en/of gerubriceerde informatie wordt verwerkt?	Algemene bedrijfsvoerings-applicaties van VWS: - Kantoorautomatisering - Marjolein	Nee	Nee	Nee	N.v.t.	Nee	Nee
6	Coördinatieproces Covid-19	Er is een coördinatieteam dat de afstemming van interdepartementale overleggen tussen NCTV en VWS coördineert.	Beleidsinformatie, verslagen van technische briefing dat voorafgaat aan debat, persoonsgegevens van deelnemers aan overleggen (vaak openbare informatie),	5.1.2e zou je willen navragen of hier gerubriceerde informatie verwerkt wordt, bijvoorbeeld in de afstemming met NCTV?	Algemene bedrijfsvoerings-applicaties van VWS: - Kantoorautomatisering - Marjolein	Ja namelijk contactgegevens	Nee	Nee	N.v.t.	Nee	Nee

5.1.2e websites zien wij ook als informatiesysteem. Zijn er in bovengenoemde processen websites waarvoor PDC-19 verantwoordelijk is?

Inventarisatie processen/informatie/systemen

#	Proces	Opmerking	Informatie	Gerubriceerde informatie	Informatie-systeem	Persoons-gegevens	BBN	TBB	PIA	Risico's	Quick scan risicoanalyse
7	Parlementaire processen PDC-19	Het coördineren van de moties en toezeggingen aan de Tweede Kamer, beantwoording van Kamervragen, voorbereiding van debatten	Beleidsinformatie zoals 5.1.2e kun je hier een aantal voorbeelden van noemen voor dit proces?]	Nee	Algemene bedrijfsvoerings-applicaties van VWS: - Kantoorautomatisering - Marjolein - Delphi	Nee	Nee	Nee	N.v.t.	Nee	Nee
8	Innovatieve behandelingen Covid-19	Samenwerking met GMT rondom behandeling van Covid-19. Check waar de scheiding tussen GMT en PDC-19 ligt.	Beleidsinformatie zoals 5.1.2e kun je hier een aantal voorbeelden van noemen voor dit proces?]	Navragen, mogelijk info over beursgenoteerde bedrijven?	Algemene bedrijfsvoerings-applicaties van VWS: - Kantoorautomatisering - Marjolein	Nee	Nee	Nee	N.v.t.	Hangt af van rubricering	Nee

5.1.2e websites zien wij ook als informatiesysteem. Zijn er in bovengenoemde processen websites waarvoor PDC-19 verantwoordelijk is?

Inventarisatie processen/informatie/systemen

#	Proces	Opmerking	Informatie	Gerubriceerde informatie	Informatie-systeem	Persoons-gegevens	BBN	TBB	PIA	Risico's	Quick scan risicoanalyse
9	Vaccins Covid-19	Coördinatie van de adviesaanvragen aan de GR, de EMA, inkoop vaccins?	Beleidsinformatie zoals 5.1.2e kun je hier een aantal voorbeelden van noemen voor dit proces?] Informatie over beursgenoteerde bedrijven, in sommige gevallen staatsgeheim	Informatie over vaccins, in sommige gevallen Stg. Geheim 5.1.2e wordt dit alleen intern gebruikt of gedeeld met externe partijen (zoals GGD's)?	Algemene bedrijfsvoerings-applicaties van VWS: - kantoorautomatisering - Marjolein 5.1.2h	Nee	Nee	Nee	N.v.t.	Stg. informatie staat bij 5.1.2e weet niet of de toegang periodiek getoetst wordt	Nee
10	Coronadashboard	Is quick scan van gemaakt en opgenomen in ICV van de directie PG. Moet volgend jaar worden opgenomen bij PDC-19.	Beleidsinformatie zoals 5.1.2e kun je hier een aantal voorbeelden van noemen voor dit proces?] Kengetallen die op het coronadashboard te vinden is	Nee	Algemene bedrijfsvoerings-applicaties van VWS: - kantoorautomatisering - Marjolein Coronadashboard (of het backend) beheerd door IenW?	Nee	Check Quick Scan	Nee	N.v.t.	5.1.2e zou je willen navragen of er m.b.t. coronadashboard nog risico's op het gebied van informatie-beveiliging of privacy voorkomen?	Ja, zie ICV van PG.

5.1.2e websites zien wij ook als informatiesysteem. Zijn er in bovengenoemde processen websites waarvoor PDC-19 verantwoordelijk is? Voor proces 10 is dat in ieder geval coronadashboard.nl lijkt me. Wordt coronamelder.nl ook vanuit jullie gerund?

Inventarisatie processen/informatie/systemen

#	Proces	Opmerking	Informatie	Gerubriceerde informatie	Informatie-systeem	Persoons-gegevens	BBN	TBB	PIA	Risico's	Quick scan risicoanalyse
11	Maatregelen en routekaart Covid-19	Voorbereiden OMT-aanvraag (specifieke vragen van wat er wel of niet kan). Het OMT-advies wordt besproken in het Catshuis. Op basis daarvan wordt de persconferentie voorbereid. Opstellen routekaart	Beleidsinformatie zoals 5.1.2e kun je hier een aantal voorbeelden van noemen voor dit proces?]	OMT-adviezen zijn in eerste instantie vertrouwelijk 5.1.2e worden deze ook gerubriceerd (bijv. als Departementaal Vertrouwelijk (DepV) of Staatsgeheim (Stg)?	Algemene bedrijfsvoerings-applicaties van VWS: - kantoorautomatisering - Marjolein	Nee	Nee	Nee	N.v.t.	5.1.2e zou je willen navragen of er risico's op het gebied van informatie-beveiliging of privacy voorkomen? Bijv. het potentieel risico op lekken OMT-adviezen?	Nee
12	Quarantaine beleid Covid-19	Op basis van OMT-adviezen wordt quarantainebeleid opgesteld.	Beleidsinformatie zoals 5.1.2e kun je hier een aantal voorbeelden van noemen voor dit proces?]	Nee	Algemene bedrijfsvoerings-applicaties van VWS: - kantoorautomatisering - Marjolein	Nee	Nee	Nee	N.v.t.	Nee	Nee

5.1.2e websites zien wij ook als informatiesysteem. Zijn er in bovengenoemde processen websites waarvoor PDC-19 verantwoordelijk is?