Gemeente Deurne

Rapportage Informatiebeveiliging Deurne 2019

Inhoudsopgave

Inleiding

Dit rapport geeft de uitkomsten weer van de gemeente brede (horizontaal) uitgevoerde ENSIA-zelfevaluatie informatieveiligheid over het jaar 2019. Deze zelfevaluatie is gebaseerd op de Baseline Informatieveiligheid Gemeenten (BIG). De BIG is sinds 2013 het gemeentelijk basisnormenkader voor informatieveiligheid. ENSIA staat voor Eenduidig Normatiek Single Information Audit.

De resultaten van de ENSIA-zelfevaluatie worden gebruikt voor twee doelen. Namelijk voor de verantwoording door het college van B&W aan de raad (horizontale verantwoording) en om verantwoording af te leggen aan stelselhouders. Dit wordt de verticale verantwoording genoemd. De verantwoording aan stelselhouders gaat over:

- De Basisregistratie Personen (BRP) en Paspoort en Nederlandse Identiteitskaart (PNIK);
- De Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en Basisregistratie Ondergrond (BRO);
- Digitale persoonsidentificatie (DigiD) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet);

Overgang naar de Baseline Informatiebeveiliging Overheid (BIO)

De zelfevaluatie over 2019 is nog uitgevoerd volgens de Baseline Informatiebeveiliging Gemeenten, de BIG. Vanaf 2020 werken wij als overheid op basis van de Baseline Informatiebeveiliging Overheid, de BIO. Vier belangrijke kenmerken van de BIO zijn:

1. Belangrijke informatiesystemen moeten het best beschermd worden

Onder de BIG waren voor ieder informatiesysteem alle maatregelen verplicht. De gemeente moest een uitleg geven voor iedere maatregel die de gemeente niet kon of wilde nemen. Onder de BIO werkt dit anders. Ieder informatiesysteem krijgt een basisbeveiligingsniveau (BBN). Hoe belangrijker het informatiesysteem is, hoe hoger het BBN-niveau. En hoe hoger het BBN-niveau, hoe meer maatregelen verplicht zijn. De verplichte maatregelen worden overheidsmaatregelen genoemd. In totaal heeft de BIO minder verplichte maatregelen dan de BIG.

Wat doet Deurne

De gemeente stelt een lijst op van alle informatiesystemen die gebruikt worden en bepaalt de BBN-niveaus. Zo wordt voor ieder informatiesysteem duidelijk welke maatregelen verplicht zijn. Deze lijst helpt ook om beter te plannen en sturen op informatievoorziening. Ook voor het kunnen naleven van privacywetgeving (de AVG) is dit inzicht nodig.

2. Risicomanagement door de eigenaar van een informatiesysteem

Het inschalen van informatiesystemen naar BBN-niveau is een eenvoudige vorm van risicomanagement. Een gedetailleerde risicoanalyse kan nog extra

maatregelen opleveren die nodig zijn om een informatiesysteem te beschermen. De "eigenaar" van een informatiesysteem neemt beslissingen over risico's en zorgt voor middelen om maatregelen te nemen.

Wat doet Deurne
De gemeente Deurne stelt voor ieder informatiesysteem vast wie de eigenaar is. Dit zorgt voor duidelijkheid over wie waarop aanspreekbaar is. Verder brengen we de belangrijkste risico's in kaart en nemen we hier beslissingen over.

3. Eindverantwoordelijkheid beleggen voor maatregelen
Ook beveiligingsmaatregelen moeten een eigenaar hebben die zorgt dat ze worden uitgevoerd. De BIO onderscheidt drie hoofdrollen: de secretaris of algemeen directeur, een proceseigenaar en een dienstverlener.

Wat doet Deurne
Het belang van informatiebeveiliging wordt steeds groter. We gaan meer digitaal werken. Cybercriminaliteit neemt snel toe. En de toezichthouder voor privacy ziet de digitale overheid als belangrijk aandachtsgebied. Om daar met schaarse tijd en geld mee om te gaan zijn goede sturing en borging en heldere keuzes van de leiding nodig. We richten de organisatie in om hiervoor te kunnen zorgen.

4. Planning & Control cyclus op basis van de ISO 27001
Met de overgang van BIG naar BIO is ons overheidsnormenkader verbonden aan de norm ISO 27001. Dit is wereldwijd de belangrijkste leidraad voor het inrichten van een planning & control cyclus (of managementsysteem) voor het besturen van informatiebeveiliging in organisaties.

Wat doet Deurne
Het opzetten van een goed werkende planning & control cyclus was een belangrijke doelstelling voor informatiebeveiliging en privacy in 2019. In 2020 wordt het werk hieraan voortgezet.

Prestaties 2019

Voor informatiebeveiliging en privacy is in 2019 het volgende bereikt:

- Informatiebeveiliging en privacy zijn verder ingebed in bedrijfsprocessen en managementtaken.
- Er zijn diverse bewustwordingsacties uitgevoerd voor medewerkers.
- Er is een projectplan gemaakt om autorisatiemanagement (wie mag wat, in welk systeem?) beter te organiseren.
- Het beoordelen op privacy en informatieveiligheid is nu vast onderdeel van het proces bij voorstellen voor veranderingen in de ICT-omgeving.
- Deurne heeft samen met ruim 300 andere gemeentes deelgenomen in een aanbesteding voor een dienst om doorlopend beveiligingsdreigingen te signaleren. De implementatie gebeurt in 2020.
- De gemeente heeft het inloggen in systemen veiliger gemaakt met een extra controle via een melding op de mobiele telefoon.

- Een ethische-hacker heeft een penetratietest uitgevoerd om zwakke plekken in de ICT-infrastructuur te ontdekken zodat we die kunnen oplossen. De komende jaren wordt deze test vaker uitgevoerd en ook verder uitgebouwd.
- Voor een aantal nieuwe processen en applicaties zijn de risico's op informatieveiligheid en privacy in kaart gebracht, zo ook voor het nieuwe zaaksysteem.
- De samenwerking en kennisdeling met gemeenten in de regio is geïntensiveerd.

De overgang van de BIG naar BIO (beschreven in het vorige hoofdstuk) is nog niet voltooid.

Resultaat ENSIA-zelfevaluatie 2019

Hieronder volgen de resultaten van de ENSIA-zelfevaluatie 2019.

Zelfevaluatie informatieveiligheid ENSIA 2019

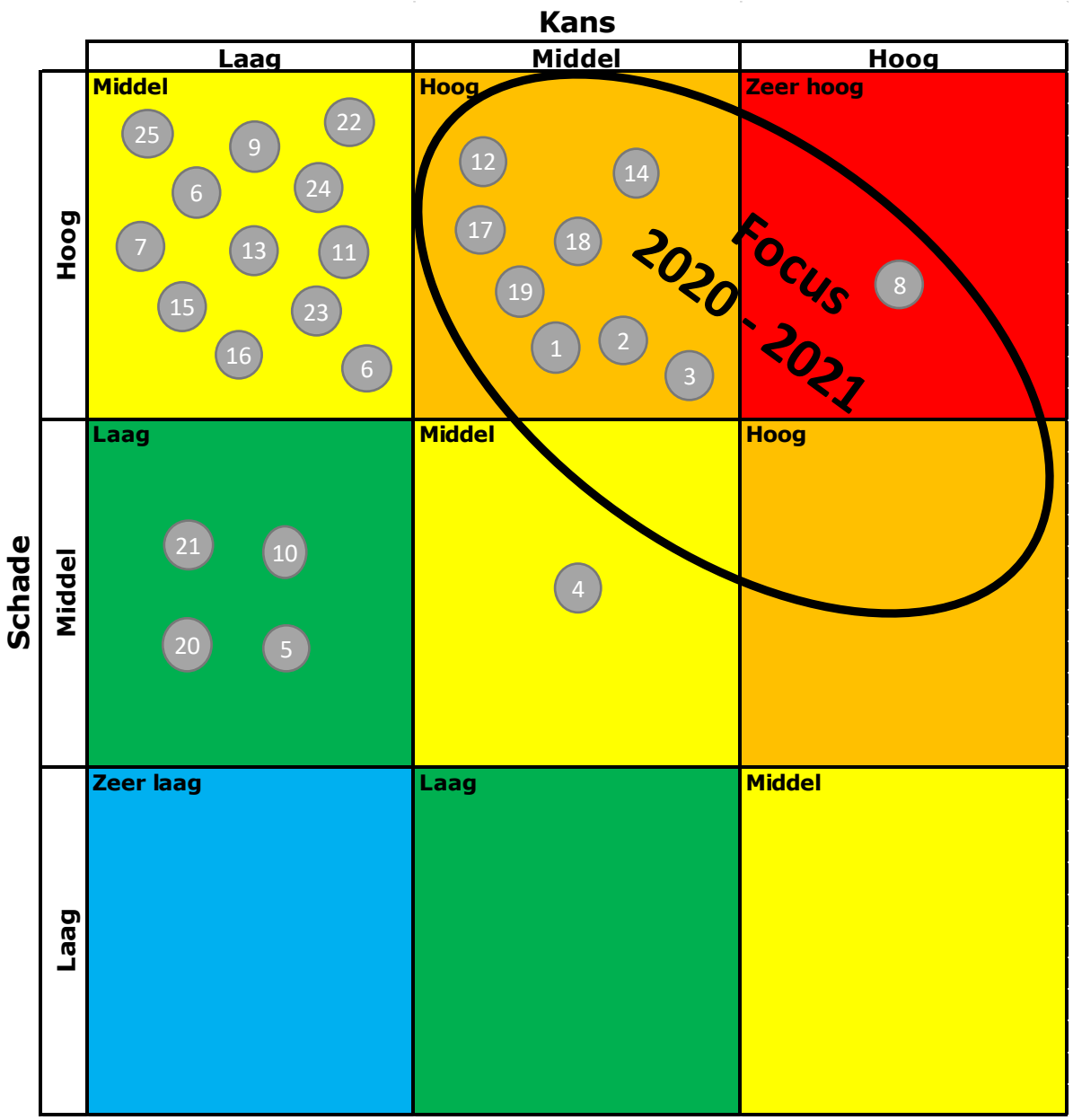
De gemeente Deurne voldoet op zeer veel punten aan de eisen van de Baseline Informatiebeveiliging Gemeenten (BIG). Er zijn ook punten waarop de gemeente niet voldoet. Een samenvatting van de belangrijkste onderdelen van de BIG waarop de gemeente niet voldoet staat hieronder in Tabel 1.

Tabel 1: Samenvatting van de belangrijkste tekortkomingen per onderdeel van de BIG.

Nr.	BIG-onderdeel	Tekortkoming gaat over …
1	3.1 Benoem verantwoordelijkheden	Geen effectieve P&C-cyclus
2	6.1. Interne organisatie	Verantwoordelijkheid leiding uitvoeren
3	6.2. Externe partijen	Eisen en maatregelen bij uitbesteding
4	7.1. Beheer van bedrijfsmiddelen	Overzicht van bedrijfsprocessen, applicaties & gegevensverwerkingen
5	7.1. Beheer van bedrijfsmiddelen	Eigenaarschap bedrijfsmiddelen
6	8.3. Beëindiging of wijziging van het dienstverband	Intrekken autorisaties bij uitdienst
7	10.1. Bedieningsprocedures en -verantwoordelijkheden	Beheersen van technische wijzigingen in ICT omgeving
8	10.1. Bedieningsprocedures en -verantwoordelijkheden	Testen van wijzigingen in informatiesystemen
9	10.2. Exploitatie door een derde partij	Beoordelen naleving door derde partijen
10	10.3. Systeemplanning en –acceptatie	Accepteren van wijzigingen
11	10.8. Uitwisseling van informatie	Beveiligingsmaatregelen in Office365
12	10.10. Controle	Monitoren en Reageren op dreigingen en inbreuken
13	11.2. Beheer van toegangsrechten van gebruikers	Accounts met bijzondere privileges
14	11.2. Beheer van toegangsrechten van gebruikers	Autorisatiebeheer
15	11.2. Beheer van toegangsrechten van gebruikers	Tweefactor authenticatie
16	11.7. Draagbare computers en telewerken	Richtlijnen gebruik thuis- en telewerken

17	11.7. Draagbare computers en tele-werken	Technische beveiliging thuis- en tele-werken.
18	12.1. Beveiligingseisen voor informa-tiesystemen	Eisen bij aanschaf van nieuwe informa-tiesystemen
19	12.1. Beveiligingseisen voor informa-tiesystemen	DPIA's: privacy effectanalyses
20	12.4. Beveiliging van systeem-bestanden	Persoonsgegevens in testomgevingen
21	12.5. Beveiliging bij ontwikkeling en ondersteuningsprocessen	Beheersen van (functionele) wijzigingen in informatiesystemen
22	13.1. Rapportage van informatie-beveiligingsgebeurtenissen en zwakke plekken	Procedures incidenten en datalekken
23	14.1: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	Continuïteitsplanning
24	15.2. Naleving	Borging en controle van maatregelen
25	7.2. Classificatie van informatie	Classificatie en labelen van informatie

Niet voldoen aan punten van de BIG betekent dat de gemeente een risico loopt. De kans dat het fout gaat en de schade die dat kan opleveren bepalen samen hoe hoog het risico is. Een kans loopt van onwaarschijnlijk (Laag) tot bijna zeker (Hoog). Schade voor de gemeente varieert van hinderlijk maar eenvoudig op te lossen (Laag) tot bijvoorbeeld maatschappelijke onrust en het moeten aftreden van een bestuurder (Hoog). Er kan ook schade zijn voor een inwoner waarvan de gemeente persoonsgegevens verwerkt. De risicomatrix in Figuur 1 geeft weer hoe ernstig ieder samengevatte punt van tekortkoming is. De nummers in de risicomatrix verwijzen naar de eerste kolom van Tabel 1.



Figuur 1: Hoogte van het risico per BIG-onderdeel waarop de gemeente een tekortkoming heeft.

Meer uitgebreide beschrijvingen van de tekortkomingen en risico's zijn te vinden in Bijlage 2. Het hoofdstuk Benodigde verbeteringen gaat in op de keuzes van de gemeente om risico's door tekortkomingen aan te pakken.

Basisregistratie Personen (BRP) en Paspoort en Nederlandse Identiteits-kaarten (PNIK)

De scores voor de Basisregistratie Personen (BRP) en de Paspoort en Nederlandse Identiteitskaarten (PNIK) zijn samengesteld uit de zelfevaluatie vanuit ENSIA en uit specifieke vragenlijsten voor BRP en PNIK. Samengevat voldoet de gemeente aan de norm die door het ministerie wordt gesteld.

De inhoudelijke kwaliteit van de BRP-persoonslijsten is goed. Dit betekent dat het beheer en het verwerken van de persoonsgegevens volgens de wet gebeurt en de kwaliteit goed is.

De scores bij de zelfevaluatie van de processen liggen boven de norm:

Domein	Score domein	Score ENSIA	Norm
BRP	98,6%	95,1%	90%
PNIK	99,5%	98%	90%

Om de scores tot 100% te verbeteren kunnen maatregelen genomen worden op:

- Autorisatiemanagement;
- Het voeren van regie bij de inzet van SaaS-oplossingen.

In het informatiebeveiligingsplan 2020-2021 bepaalt de gemeente of dit wordt aangepakt.

Digitale persoonsidentificatie (DigiD) en Structuur uitvoerings-organisatie Werk en Inkomen (Suwinet)

Voor DigiD voldoet de gemeente aan alle normeneisen
DigiD staat voor Digitale iDentiteit. Hiermee kunnen inwoners inloggen op de websites van de overheid en in de zorg.

Voor Suwinet voldoet Senzer (en daarmee ook de gemeente) aan alle normeneisen
Suwinet is het systeem van informatie-uitwisseling in de keten van werk en inkomen. Suwinet wordt gebruikt door Senzer, een gemeenschappelijke regeling die de Participatiewet uitvoert voor o.a. Deurne. De gemeente zelf maakt geen gebruik van Suwinet maar is wel verantwoordelijk voor het gebruik door Senzer.

Collegeverklaring in de bijlage
De verantwoording over Suwinet en DigiD aan de stelselhouders (Ministerie van SZW en Logius/BZK) doet de gemeente met een collegeverklaring die door een auditor wordt gewaarmerkt. De Collegeverklaring ENSIA 2019 is te vinden in de bijlage van dit rapport zodat ook de raad deze kan lezen.

Basisregistraties Adressen en Gebouwen (BAG), Grootschalige Topografie (BGT) en Ondergrond (BRO)

Alle gemeenten zijn verantwoordelijk voor het opnemen van gegevens in drie registraties over de ruimtelijke ordening van Nederland en voor de kwaliteit en het beheer van (het eigen deel van) die gegevens. Het gaat daarbij om:

- Gegevens over adressen en gebouwen binnen de gemeentegrenzen (BAG);
- Een gedetailleerde digitale kaart met onder andere gebouwen, wegen, water, spoorlijnen en groen (BGT);
- Gegevens over de geologische en bodemkundige opbouw van de Nederlandse ondergrond (BRO).

De gemeente doet het beter dan de door het ministerie gestelde norm
Dit geldt voor de drie stelsels. Het overzicht hieronder bevat de scores uit de ENSIA-zelfevaluatie in punten en percentage. Merk op dat het stelsel BRO pas sinds 2018 bestaat. Dit verklaart de lage score in het eerste jaar.

Basisregistratie	**2018**	**2019**	**Norm**
BAG	95,1%	90%	75%
BGT	96,7%	100%	75%
BRO	37,5%	87,5%	60%

Voor de BAG is door een eenmalige verstoring de maximale score niet behaald. Er worden daarom in 2020 geen structurele verbetermaatregelen genomen. Voor de BGT wordt in 2020 geïnvesteerd in het optimaliseren en beschrijven van de processen voor de aansluiting tussen BGT en BAG en tussen BGT en BRO. Voor de BRO ten slotte zijn in 2019 grote stappen gezet om op niveau te komen in dit nieuwe stelsel. In 2020 zullen de processen verder worden beschreven om ze te kunnen borgen.

Beveiligingsincidenten en datalekken

Zowel wereldwijd als in Nederland zagen we in 2019 een sterke toename van het aantal beveiligingsincidenten met ernstige gevolgen voor organisaties. De gemeente Deurne heeft gelukkig in 2019 op dit gebied weinig onheil mee-gemaakt. Hieronder volgt een overzicht van geregistreerde beveiligings-incidenten met persoonsgegevens (zogenaamde datalekken). Voor de kleine toename is geen duidelijke reden aan te wijzen. Wellicht laat het zien dat door actief te communiceren over privacy, fouten vaker worden gemeld.

	2018	**2019**
Intern geregistreerde datalekken	8	10
Gemeld aan Autoriteit Persoonsgegevens	3	5
Gemeld aan betrokkenen (bij hoog risico voor hen)	0	0

In twee gevallen werden persoonsgegevens bij vergunningsaanvragen onterecht op de website gepubliceerd. In 2020 is de procedure aangepast zodat het niet meer fout kan gaan. Het testen en opleiden van medewerkers voor het nieuwe zaaksysteem gebeurde met gegevens uit het BRP. Dit mocht niet op deze manier gedaan worden. De overige incidenten waren incidentele menselijke fouten.

Volgende stappen

Eerder is al beschreven wat de gemeente Deurne gaat doen om de BIO verder in te voeren. Daarnaast wijst de risicoanalyse die eerder is afgebeeld aan wat voor 2020–2021 de belangrijke onderwerpen zijn:

- Eisen aan derde partijen bij uitbesteding (risico 3)
- Eisen bij aanschaf van nieuwe informatiesystemen (risico 18)

- Autorisatiebeheer samen met in- en uitdienstproces P&O (risico's 6, 14)
- Testen van wijzigingen in informatiesystemen (risico 8)
- Beveiligingsmaatregelen in Office365 en mobiele apparaten (risico 11, 17)
- Monitoren en Reageren op dreigingen en inbreuken (risico 12)
- DPIA's: effectanalyse over het verwerken van persoonsgegevens (risico 19)
- Overzicht van processen, applicaties & gegevensverwerkingen (risico 4)

De meeste onderwerpen hierboven vragen een flinke inspanning en betrokkenheid van personen in meerdere onderdelen en lagen van de organisatie. Daarom worden ze als projecten aangepakt.

Laaghangend fruit en aansluiten op actualiteiten
De gemeente kijkt ook welke verbeteringen met weinig inspanning veel resultaat kunnen opleveren. Verder wordt aangesloten op de actualiteit in de organisatie. Zo kunnen verbeteringen worden meegenomen in initiatieven die met een ander doel worden gestart. In deze categorieën vallen:

- Richtlijnen thuis- en telewerken (risico 16)
- Beheersen van veranderingen in de ICT-omgeving (risico 7)
- Procedures voor incidenten en datalekken (risico 22)
- Fysieke beveiliging en gedrag in het Huis voor de Samenleving

Conclusie

De gemeente Deurne doet het ruim beter dan de norm voor alle stelsels waarover de gemeente zich moet verantwoorden aan het Rijk. Het invoeren van de BIO is nog niet gereed. Met de beperkte capaciteit en kennis binnen Informatiemanagement & Automatisering was in 2019 echter niet meer voortgang mogelijk. De zelfevaluatie informatieveiligheid ENSIA 2019 laat zien dat er nog een aantal risicovolle tekortkomingen zijn. Volledige veiligheid is een illusie. De lat te hoog leggen maakt het onbetaalbaar en kan het werken onmogelijk maken. Kijken naar waar de grootste risico's liggen helpt om de juiste balans te zoeken. Juist in een tijd van grote veranderingen en toenemende cyberdreiging verdient dit voortdurend onze aandacht.

Bijlage 1: Collegeverklaring ENSIA 2019

Hieronder volgt de collegeverklaring van de gemeente Deurne over de beveiliging van DigiD en Suwinet (zonder bijlagen). Een onafhankelijke auditor heeft deze getoetst.

Collegeverklaring ENSIA 2019 inzake Informatiebeveiliging DigiD en Suwinet

Gemeente Deurne

Doel en achtergrond verklaring

Het college van burgemeester en wethouders geeft met deze verklaring aan in hoeverre de gemeente Deurne voldoet aan de voor DigiD en Suwinet geselecteerde informatiebeveiligingsnormen op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Gemeenten (BIG), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Naast deze verklaring bestaat ENSIA onder meer uit het uitvoeren van de ENSIA-zelfevaluatie, waarmee de genoemde informatiebeveiligingsnormen zijn getoetst onder verantwoordelijkheid van het management.

Reikwijdte en diepgang verklaring

Deze verklaring betreft de onderdelen van de ENSIA-systematiek waarover assurance wordt gevraagd van een onafhankelijke IT-auditor. Het is de verantwoordelijkheid van het college dat het proces voor de totstandkoming van deze collegeverklaring met zorg is uitgevoerd. Dit proces borgt dat de strekking van de collegeverklaring een juiste weergave is van de onderzochte domeinen. Voor gemeente Deurne betreft dit in 2019 DigiD en Suwinet.

De verklaring omvat het op 31 december 2019 voldoen van de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen aan de geselecteerde normen inzake DigiD en Suwinet. De collegeverklaring omvat niet het functioneren (werking) van de maatregelen over 2019.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed aan dienstverlener[s] vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring (bijlage 1 DigiD met kenmerk 1226937/1180832) blijkt welke beheersingsmaatregelen door de gemeente en door de dienstverlener worden uitgevoerd. Over de beheersingsmaatregelen die door de dienstverlener worden uitgevoerd, wordt door de dienstverlener verantwoording afgelegd aan de gemeente. Deze collegeverklaring en de verantwoording van de dienstverlener dekken tezamen de normen inzake DigiD af.

Inzake Suwinet heeft deze collegeverklaring zowel betrekking op de beheersingsmaatregelen van de gemeente als op die van de uitbestede diensten aan Senzer.

Deze collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De verklaring geeft weer in hoeverre de beoogde (opzet) en ingerichte (bestaan) beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet. In de bij deze verklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk 1226937/1180832) en Suwinet (bijlage 2 Suwinet met kenmerk 1226937/1180833) zijn de eventuele afwijkingen van de normen opgenomen.

De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet worden via bij deze collegeverklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk 1226937/1180832) en voor Suwinet (bijlage 2 Suwinet met kenmerk 1226937/1180833) geïnformeerd over de afwijkingen van de normen.

BK BO
BKBO bv 11-3-'20
Voorstraat 20
5251 CP Vlijmen
073 - 211 03 37 drs. M.R.H. Upelaar RE CEH

Verklaring college

Het college verklaart dat bij gemeente Deurne op 31 december 2019 de beoogde en ingerichte beheersingsmaatregelen voldoen aan de geselecteerde normen inzake DigiD en Suwinet.

Samenvattend beeld

Object	Wordt aan alle geselecteerde normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD 1002181	Ja	Neen
Suwinet voor SUWI-taken	Ja	Niet van toepassing
Suwinet voor niet-SUWI-taken	Niet van toepassing	Niet van toepassing

Deurne, 19 februari 2020

College van B en W gemeente Deurne

R.R.M. Halffman
gemeentesecretaris

H.J. Mak
burgemeester

Naam auditfirma:	BKBO
Naam auditor:	drs. M.B.H. IJpelaar RE CEH CISA
Datum: 11 maart 2020	Handtekening of paraaf auditor drs. M.B.H. IJpelaar RE CEH

BKBO bv 11-3-'20
Voorstraat 20
5251 CP Vlijmen
073 - 211 03 37 drs. M.B.H. IJpelaar RE CEH

4

Bijlage 2: Risico's als gevolg van tekortkomingen BIG-maatregelen

Het overzicht hieronder benoemt per hoofdonderwerp van de BIG wat het risico is van de tekortkomingen op dit onderdeel. Om de hoogte van risico's in te schatten is gekeken naar de kans dat het fout gaat door een tekortkoming, en de schade die daardoor kan optreden.

Nr.	BIG	Risicobeschrijving	Risico
1	3.1 Benoem verantwoordelijkheden	Informatiebeveiliging en privacy krijgen te weinig aandacht, prioriteit en middelen door het ontbreken van strategische en tactische sturing via de P&C-cyclus.	H
2	6.1. Interne organisatie	Leidinggevenden sturen niet op de aspecten van informatiebeveiliging en privacy waarvoor zij wel verantwoordelijk zijn omdat zij zich niet bewust zijn van hun verantwoordelijkheid.	H
3	6.2. Externe partijen	Goede beveiliging en privacybescherming door samenwerkingspartijen en leveranciers van diensten is niet gegarandeerd. Dat komt omdat bij de start van een samenwerking risico's soms niet in kaart gebracht worden en die niet altijd goed worden aangepakt in contracten, systemen en processen.	H
4	7.1. Beheer van bedrijfs-middelen	De registraties van bedrijfsprocessen, applicaties en verwerkingen van persoonsgegevens zijn geen betrouwbare bron van informatie. De gemeente voldoet voor het verwerkingsregister niet aan de AVG. De belangrijkste oorzaak is dat het onderhoud van de gegevens niet is georganiseerd.	M
5	7.1. Beheer van bedrijfs-middelen	Er wordt niet goed gecontroleerd en gestuurd op naleven van informatiebeveiliging en privacy in informatiesystemen en processen. Dat komt omdat niet altijd duidelijk is wie de eigenaar is en welke verantwoordelijkheid deze heeft.	L
6	8.3. Beëindiging of wijziging van het dienst-verband	Het kan gebeuren dat een (oud-)medewerker toegang houdt tot informatiesystemen nadat hij van functie gewisseld is of zelfs wanneer hij niet meer voor de gemeente werkt. Daardoor kan misbruik gemaakt worden, schade worden toegebracht, fraude worden gepleegd en kunnen persoonsgegevens onrechtmatig worden verwerkt.	M
7	10.1. Bedienings-procedures en -verant-woordelijkheden	Bij het doorvoeren van technische ICT-wijzigingen kunnen beveiligingsmaatregelen worden vergeten of bestaande maatregelen teniet worden gedaan, omdat het proces voor wijzigingen nog beter ingevoerd moet worden.	M

Nr.	BIG	Risicobeschrijving	Risico
8	10.1. Bedienings-procedures en -verant-woordelijkheden	Het aanpassen van (een keten van) applicaties kan ervoor zorgen dat een bedrijfsproces ernstig verstoord wordt of informatie beschadigd raakt. De oorzaak is dat testomgevingen en -procedures voor het testen en accepteren van functionele en technische wijzigingen niet aanwezig zijn of niet goed zijn uitgewerkt.	HH
9	10.2. Exploitatie door een derde partij	Met uitzondering van de partijen waarvoor vanwege de ENSIA-cyclus een verklaring van een onafhankelijke auditor (TPM) door het Rijk wordt gevraagd, worden privacy- en beveiligings-prestaties van ICT- en dienstenleveranciers niet periodiek beoordeeld. Dit is wel verplicht en nodig.	M
10	10.3. Systeemplanning en –acceptatie	Zie testomgevingen en -procedures onder Nr. 8 / BIG 10.1	L
11	10.8. Uitwisseling van informatie	Vertrouwelijke informatie en persoonsgegevens kunnen vanuit Office365 via e-mail, Teams, enzovoorts extern gedeeld worden. De gemeente heeft geen technische maatregelen om dat te controleren, beperken of te voorkomen.	M
12	10.10. Controle	Fouten en inbreuken op beveiligingsmaatregelen worden niet of te laat opgemerkt (een hacker is binnen en we weten het niet). Dat komt omdat logboeken van applicaties en ICT-systemen onvolledig zijn, niet goed worden beschermd en niet actief worden gecontroleerd. De BRP is hierop een positieve uitzondering.	H
13	11.2. Beheer van toegangsrechten van gebruikers	Beheerders hebben soms te veel rechten of gebruiken hun beheeraccount voor uitvoerende taken. Dit geeft kans op fouten en misbruik.	M
14	11.2. Beheer van toegangsrechten van gebruikers	Gebruikers hebben te veel rechten in sommige systemen en applicaties omdat hier weinig beleid, beheer en controle op is. Dit opent een kans op misbruik en toegang tot (persoons)gegevens die niet is toegestaan. Zie ook Nr. 8 / BIG 8.3 voor het intrekken van rechten wanneer een medewerker uitdienst gaat.	H
15	11.2. Beheer van toegangsrechten van gebruikers	Op een klein deel van onze applicaties bestaat nog een verhoogde kans op inbraak vanaf Internet omdat daar geen sterke inlogprocedure met tweefactor-authenticatie is ingevoerd.	M
16	11.7. Draagbare computers en telewerken	De bescherming van informatie en persoonsgegevens kan worden geschonden doordat thuis- en telewerkvoorzieningen	M

Nr.	BIG	Risicobeschrijving	Risico
		vanwege gebrek aan richtlijnen en voorlichting onzorgvuldig worden gebruiken.	
17	11.7. Draagbare computers en telewerken	Vertrouwelijke informatie en persoonsgegevens worden opgeslagen buiten beveiligde systemen, bijvoorbeeld op privé mobiele telefoons en in Clouddiensten. We hebben geen technische maatregelen om dat te controleren, beperken of te voorkomen.	H
18	12.1. Beveiligingseisen voor informatiesystemen	Bij alle investeringen die Deurne de komende jaren gaat doen in informatiesystemen is er een risico dat eisen aan beveiliging en privacy niet of slechts ad-hoc worden meegenomen. Dit kan leiden tot incidenten en hoge kosten voor latere verbetering en herstel.	H
19	12.1. Beveiligingseisen voor informatiesystemen	DPIA's (effectbeoordeling over verwerking van persoonsgegevens) worden zelden uitgevoerd. Er is weinig vaardigheid in het uitvoeren en het is onduidelijk of en hoe resultaten van een DPIA worden opgevolgd door de verantwoordelijke. Deurne voldoet op dit punt niet aan de AVG.	H
20	12.4. Beveiliging van systeembestanden	In sommige testomgevingen worden persoonsgegevens gebruikt. Dit kan onrechtmatig zijn en een overtreding van de AVG. De oorzaak is het ontbreken van afspraken en procedures voor het zorgvuldig en geanonimiseerd gebruik van data in testomgevingen. Zie ook Nr. 8 / BIG 10.1 over testomgevingen en -procedures.	L
21	12.5. Beveiliging bij ontwikkeling en ondersteuningsprocessen	Bij het doorvoeren van functionele wijzigingen in applicaties kunnen beveiligingsmaatregelen worden vergeten of bestaande maatregelen teniet worden gedaan, omdat het proces voor wijzigingen nog beter ingevoerd moet worden. Zie ook wijzigingsbeheer onder Nr. 7 / BIG 10.1.	L
22	13.1. Rapportage van informatiebeveiligings-gebeurtenissen en zwakke plekken	Er is een risico dat een incident, kwetsbaarheid of datalek niet tijdig gemeld wordt en/of onvolledig of met onvoldoende aandacht en spoed wordt behandeld, waardoor de schade kan toenemen. Dit komt omdat procedures rondom incidenten nog beter ingevoerd moeten worden.	M
23	14.1: Informatiebeveiligings-aspecten van bedrijfs-continuïteitsbeheer	Het gevaar voor uitval van dienstverlening neemt toe, naarmate de afhankelijkheid van digitaal werken groter wordt. Met uitzondering van BAG, BRP en PNIK zijn er geen plannen en regelmatig geteste procedures voor het waarborgen van de	M

Nr.	BIG	Risicobeschrijving	Risico
		continuïteit van informatiesystemen in het geval van een calamiteit.	
24	15.2. Naleving	Het falen van informatiebeveiliging en privacybescherming en niet naleven van wettelijke of interne richtlijnen wordt niet opgemerkt. Dat komt omdat er nauwelijks controle op naleving en periodieke rapportage over de juiste werking aan het verantwoordelijk management is.	M
25	7.2. Classificatie van informatie	Het is onzeker of informatie altijd met de juiste (specifieke) beveiligingsmaatregelen wordt behandeld, omdat procedures voor classificatie en labelen van informatie op basis van vertrouwelijkheid ontbreken.	M