Gemeente Diemen

Informatie van het college

Onderwerp : ***Voortgang implementatie informatieveiligheid – mei 2020***
Datum : 15 mei 2020
Portefeuillehouder : E. Boog
Afdeling : Duo+ / Directie
Stellers : F. Vianen / K. Deutekom

Wat is de voorgeschiedenis en de concrete aanleiding van de informatie?
In de raadsvergadering van januari 2018 zijn de uitgangspunten en doelen omtrent informatieveiligheid en privacy door de raad vastgesteld. De raad heeft gevraagd over de voortgang hiervan geïnformeerd te worden. Op 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) in werking getreden. In april 2018 heeft de raad een informatiememo van het college ontvangen over het vastgestelde privacybeleid en privacyreglement. De implementatie van de AVG is onderdeel van het informatieveiligheidsbeleid.
Als gevolg van de het lokale rekenkameronderzoek is de raad in mei 2018 geïnformeerd over het privacy beleid binnen het sociaal domein. Na een eerder informatiememo over de voortgang in september 2018 en juni 2019, ontvangt u nu opnieuw een update met de laatste stand van zaken. Voorstel is deze wijze van informeren te stoppen. In de Paragraaf Bedrijfsvoering van de reguliere planning- en controlproducten is een apart onderdeel ‘Informatiebeveiliging’ opgenomen.

Aanpassing van Baseline van BIG naar BIO
In het vorige memo kondigden we al aan dat per 1 januari 2020 de huidige Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), het normenkader voor informatieveiligheid, is overgegaan naar een nieuwe gezamenlijke Baseline voor Overheidsinstellingen, de BIO. De achterliggende reden is om de informatiebeveiliging verder optimaal te professionaliseren voor de gehele overheid. De BIO is gebaseerd op de internationaal erkende en actuele ISO-normatiek.
Het uiteindelijke doel hiervan is te komen tot een veilige digitale overheid.

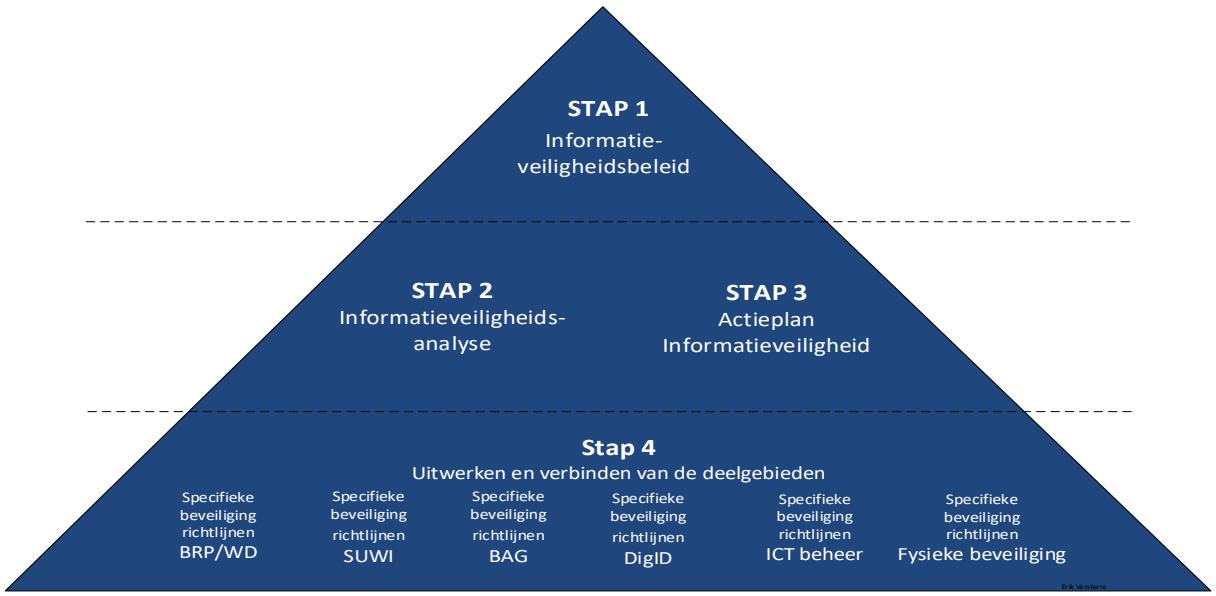
Welke gevolgen heeft dit?
De BIO is een doorontwikkeling, ofwel een ‘update’ van de BIG. De verandering van het normenkader betekent dat er een aanpassing van het gehele informatieveiligheid beleid moet worden doorgevoerd. En de stappen uit het model opnieuw moeten worden doorlopen. Concreet betekent dit dat het strategisch en tactisch informatieveiligheidsbeleid opnieuw door de DUO-organisaties (gemeenten Diemen, Ouder-Amstel, Uithoorn en Duo+) moet worden vastgesteld.
- zie stap 1 in de Figuur 1. -

Goed om te weten is dat diverse onderwerpen die al in de BIG stonden in lijn zijn met wat de BIO vraagt. Met dit verschil, dat de BIO meer nadruk legt op het risicomanagement en strengere eisen stelt aan het nemen van specifieke maatregelen. De rol van de bestuurder en lijnmanager is ten aanzien van risicomanagement explicieter dan de BIG aangaf. Concreet betekent dit dat een analyse moet worden gemaakt op basis van de nieuwe normering. *- zie stap 2 in Figuur 1.* - Gevolgd door een nieuw actieplan in de fase daarop, *- zie stap 3 in Figuur 1* – en doorvertaling naar de afzonderlijke deelgebieden – *zie stap 4 in Figuur 1*- .

Toelichting
Het informatieveiligheid betreft drie onderwerpen, te weten:
1. de Baseline Informatieveiligheid Overheid (BIO)
   – was tot 31/12/2019 de Baseline Informatieveiligheid Nederlandse Gemeenten (BIG) -,
2. de Eenduidige Normatiek Single Information Audit (ENSIA)
   - jaarlijkse verantwoording aan de toezichthouders vanuit het Rijk -
3. en de Algemene verordening gegevensbescherming (AVG 2018),
   - wettelijke verplichting - .

Figuur 1: De informatieveiligheidspiramide

Stap 1 – Informatieveiligheidsbeleid (strategisch) Aanpassing i.v.m. verandering BIG naar BIO.



Stap 3 - Plan van Aanpak (tactisch)

In het nieuwe actieplan komen verbeteracties waaraan de DUO-organisaties het komende jaar prioriteit aan gaan geven. Dit compacte actieplan vormt de praktische leidraad voor het werk van de informatieveiligheids-organisatie.

Stap 4 – Uitwerken en verbinden van de deelgebieden (operationeel)
Vanuit het actieplan is het de bedoeling deelplannen en procedures van de afzonderlijke deelgebieden verder uit te werken en te verbinden, rekening houdend met de wettelijke kaders van de deelgebieden en de organisatie. Deze nadere afstemming is nodig om te komen tot een betere samenhang en moet leiden dat ook de kwaliteit van de toetsing van de afzonderlijke deelgebieden in de jaarlijkse ENSIA-cyclus op het zelfde niveau komt. Zo zal de nieuwe ENSIA-cyclus die start in juli 2020 ook gebaseerd zijn op de BIO-normen.

2. Eenduidige Normatiek Single Information Audit (ENSIA)
Ook al in eerdere versies van het – ‘informatie van het college; voortgang implementatieveiligheid’ – informeerden we u over de ENSIA. ENISA helpt gemeenten in één keer slim verantwoording af te leggen over informatie-veiligheid gebaseerd op de implementatie van het in 2019 nog geldende normenkader, de BIG . De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).

De afzonderlijke, zogenoemde verticale verantwoording, geschied aan landelijke partijen en ministeries die een rol hebben in het toezicht op informatieveiligheid. De afzonderlijke verantwoordingen zijn de basis voor de, zogenoemde horizontale verantwoording, aan de gemeenteraad.

Bij het afleggen van verantwoording wordt het principe van single information single audit toegepast; oftewel alle informatie die noodzakelijk is voor verticale verantwoording is ook onderdeel van het horizontale verantwoordingsproces.
De ENSIA-audit 2019 is uitgevoerd aan de hand van een zelfevaluatie. Deze zelfevaluatie moest vóór 31 december 2019 worden aangeleverd. Dit is alle DUO-gemeenten op tijd gelukt.

Onderdeel van het verantwoordingsproces ENSIA is het afgeven van een Collegeverklaring per gemeente. Deze zogenoemde 'Collegeverklaring' betreft over 2019 het gebruik van DigiD en Suwinet. Besluitvorming hieromtrent valt onder de verantwoordelijkheid van het college van burgemeester en wethouders. Het college is verplicht de raad te informeren, de wijze waarop is vormvrij. Middels deze memo informeert het college u over het resultaat.

- ***Resultaat ENSIA-audit 2019***

De jaarlijkse ENSIA-cyclus heeft in 2019 voor het tweede jaar in de vorm van een zelfevaluatie plaatsgevonden. Ten opzichte van andere gemeenten doet Diemen en de andere DUO-gemeenten het goed. Er is veel werk verricht om de verantwoording tijdig aan te leveren. Ten opzichte van de resultaten over 2018 heeft er een verbetering plaats gevonden. Helaas voldoet de gemeente Diemen nog net niet aan alle voorwaarden. Dit geldt overigens ook voor de gemeenten Uithoorn en Ouder-Amstel.
De normering voor het behalen van de ENSIA-audit worden jaarlijks strenger. Alles moet 100% goed zijn. Eén afwijking leidt dat een niet behalen van de audit.
Het toetsingskader voor de ENSIA-audit bestaat uit maatregelen op het gebied van Beleid, Uitvoering en Controle. In de uitgevoerde zelfevaluatie en de daarop volgende IT-audit naar aanleiding van de bevindingen is gebleken dat er op operationeel niveau in onvoldoende mate afspraken zijn gemaakt, die een volledig voldoen aan gestelde kwaliteitsnormen informatieveiligheid rechtvaardigen. Het resultaat van audit is aanleiding voor vervolgacties en zijn vastgelegd in verbeterplannen.
In afstemming met de auditor is een verbeterplan opgesteld. Het verbeterplan is goedgekeurd door de auditor.

Als bijlage is de Collegeverklaring toegevoegd. Zowel de bijlagen van de Collegeverklaring als het verbeterplan vallen onder de geheimhouding en zijn daarom niet bijgevoegd. Deze vertrouwelijkheid is gebaseerd op artikel 10 lid 2 sub d van de Wet Openbaarheid Bestuur (WOB). Redenen voor de geheimhouding zijn:
• inzage in de ingevulde zelfevaluatie-tool van ENSIA wordt geweigerd op basis van veiligheidsargumenten;
• er in de Third Party Mededelingen van onze leveranciers expliciete geheimhouding is opgenomen.

3. Algemene Verordening Gegevensbescherming (AVG)
In het informatieveiligheidsbeleid van de DUO-organisaties ligt ook vast dat maatregelen moeten worden getroffen in het kader van verplichtingen uit de Algemene Verordening Gegevensbescherming (AVG). In eerdere versies van dit memo trof u al een update. Hieronder vind u de laatste status.

Stap	Omschrijving	Status per 1 maart 2020
1.	Aanstellen Functionaris voor de Gegevensbescherming (FG)	Er is een Functionaris voor de Gegevensbescherming (FG) aangesteld voor Duo+ en de drie gemeenten.
2.	Convenanten updaten en privacybeleid opstellen	Bij nieuwe convenanten wordt rekening gehouden met de AVG . Dit is een continue proces.
	(model) privacybeleid en -reglement implementeren	Nieuwe AVG zaken die personeel raken worden getoetst. Dit is een continue proces.
3.	Inkoopcontracten en aanbestedingen aan eisen AVG aanpassen	In het aanbestedingsproces wordt rekening gehouden met de AVG . Dit is een continue proces.
4.	Bestaande be-/verwerkers-overeenkomsten updaten en nieuwe aangaan	Overeenkomsten zijn gecontroleerd, indien nodig worden nieuwe verwerkingsovereenkomsten afgesloten. Dit is inmiddels een continue proces geworden
5.	Inzichtelijk maken welke persoonsgegevens door wie worden verwerkt en die vastleggen in een register van verwerkingsactiviteiten	Het register is klaar, maar wordt nog continue verbeterd en actueel gehouden.
6.	Bewustwording en training medewerkers (awareness)	Bewustwording en awareness over informatieveiligheid en belang van de AVG is een continue proces om onder de aandacht te houden.
7	Afvragingsmomenten in werkprocessen op orde brengen (triage)	Door de verandering van de BIG naar de BIO worden strengere eisen aan veel werkprocessen gesteld die bijvoorbeeld in de ENSIA audit worden getoetst. Denk hierbij aan DigiD, Suwi, BAG, AVG en Burgerzaken. Het voldoen aan deze kwaliteitseisen is een continue proces.
8.	Processen rechten burgers inregelen	Het ‘recht op inzage’-proces is openbaar via de privacy verklaring op www.diemen.nl. Daarnaast zijn de medewerkers van het klantcontactcentrum (KCC) en burgerzaken getraind. Ook deze rechten zijn inmiddels opgenomen in de eisen die de BIO stelt, zie punt 7.
9	Communicatie naar burgers over rechten opstellen/aanpassen	Op www.diemen.nl is de privacyverklaring openbaar beschikbaar (is wettelijke verplichting). In overleg met communicatie en de afdelingen is de AVG meer in het proces opgenomen.
10.	Autorisaties aansluiten op werkprocessen	Dit wordt meegenomen in de werkprocessen behorende bij punt 7.

Conclusie
De verandering van het normenkader naar de BIO heeft de nodige impact op het beleid en uitvoering van het informatieveiligheid beleid van de Duo-organisatie en de DUO-gemeenten. Deze verplichte aanscherping van de normering zal ten goede komen aan het doel om voor de inwoners van Diemen een veilige en betrouwbare partner te zijn en te blijven met de vernieuwde eisen die hieraan worden gesteld. Zoals duidelijk blijkt uit bovengenoemde informatie blijkt dat de drie deelonderwerpen van het informatieveiligheid beleid onderdeel zijn van de bedrijfsprocessen. Informatie over deze onderdelen zult u daarom in het vervolg terugvinden in de reguliere jaarrekening en begroting. Indien nodig volgt uiteraard wel een aparte informatiememo.