In dit document treft u de vragen die de pilotgemeenten stelden naar aanleiding van de BIO pilot ENSIA

Documentversie: 7 mei 2019

Wat is de scope van de verantwoording op basis van de BIO?	De scope van de BIO bestaat uit de bedrijfsvoeringsprocessen van de ambtelijke organisatie. (Grofweg alles waar de gemeentesecretaris eindverantwoordelijk voor is). Een gemeente bepaalt op basis van een eigen risicoafweging de reikwijdte van de verantwoording over de gemeentelijk processen. De gemeente dient ten minimale de primaire processen waar persoonsgegevens in verwerkt te worden binnen de scope van de BIO (en de horizontale verantwoording) te plaatsen. Dit betreft een combinatie van verantwoordelijke, processen en maatregelen.
Worden de verplichte maatregelen minder dan in de BIG nu risicomanagement een grotere rol gaat spelen?	Het aantal verplichte maatregelen is in absolute zin minder, echter dit zegt niet alles over het totaal aantal te treffen maatregelen. Dit is afhankelijk van de resultaten van het door de gemeente uitgevoerde risicomanagement. Met de BIO voert de gemeente voorafgaand aan de implementatie een risico-analyse uit en niet achteraf zoals met de BIG het geval was. Bij de BIG wordt gewerkt met het 'pas toe of leg uit principe'. Vanuit de BIO wordt op voorhand bepaald welke controls van toepassing zijn (controls kunnen niet van toepassing worden verklaard). Vervolgens implementeert u de benodigde maatregelen en de maatregelen die mogelijk aanvullend zijn opgesteld naar aanleiding van de uitgevoerde risicoanalyse.
Ik zie dat controls ook een BBN niveau toebedeeld hebben gekregen. De maatregelen hebben ook een niveau toebedeeld gekregen. Hoe verhoudt zich dit tot elkaar?	Dat klopt. De werkgroep normatiek heeft controls uit de ISO geselecteerd en opgenomen in de BIO. Dit vormt de baseline. De controls hebben een niveau van een te beschermen belang toebedeeld gekregen van 1 of 2. Om de risico's te mitigeren zijn passende maatregelen nodig. De maatregelen in de BIO zijn eveneens van niveau 1 of 2. Het niveau van de control is altijd gelijk of van een hoger niveau dan de maatregel(en). U ziet wel een control op BBN1, met maatregelen op BBN1 en mogelijk BBN2 niveau. Een maatregel is nooit van een lager niveau dan de control. Op basis van de risico inschatting van het proces (BIV-classificatie) wordt het benodigde niveau van de maatregel bepaald. Wanneer het proces wordt vastgesteld op BBN2 dan implementeert u zowel de maatregelen van BBN1 als van BBN2 bij een control. Een voorbeeld: de control (BBN1) is veilig wonen in een huis. Op BBN1 niveau kan de maatregel zijn dat er een deur in het huis aanwezig dient te zijn met een slot. Echter wanneer er grote te beschermen belangen zijn (al uw juwelen), dan dient u een stevigere maatregel in te zetten om de belangen te beschermen, namelijk een alarmsysteem (BBN2).

	Een hoger te beschermen belang in enige situatie kan zwaardere maatregelen vereisen. Het niveau van de control wijzigt hierdoor niet.
Hoe kan een control op een BBN1 staan en de maatregelen op BBN2 zijn gedefinieerd in de BIO?	Vanuit de baselinetoets kan een proces op BBN2 uitkomen. Wanneer een **control** op 1 in de BIO is vastgesteld en maatregelen kent op zowel BBN1 en BBN2 dan implementeert u de maatregelen van zowel BBN1 als van BBN2. Wanneer aanvullende maatregelen nodig zijn om het risico te mitigeren, dan stelt u deze aanvullend op.
Bij een control zie ik maatregelen met BBN1 en BBN2. Zijn alle maatregelen verplicht?	Maatregelen zijn altijd gekoppeld aan een proces. Wanneer vanuit de baselinetoets het proces wordt ingeschat op BBN1, dan implementeert u alle maatregelen met BBN1. Is uw proces ingeschaald op BBB2 niveau dan implementeert u zowel de maatregelen op BBN1 als op BBN2 niveau.
Bij een control zie ik alleen maar BBN1 niveau staan. Kan ik daar zelf maatregelen voor opstellen en de geformuleerde maatregelen op BBN1 laten voor wat het is?	De maatregelen uit de BIO zijn verplicht zolang de control waarbij deze zijn opgenomen voor uw organisatie van toepassing zijn.
Op welke wijze zijn de pilot gemeente voor de ENSIA pilot BIO gestart met de implementatie van de BIO?	De pilot gemeenten zijn gestart met de GAP analyse van de IBD. Voor de pilot hebben deze gemeenten geen baseline toets uitgevoerd, voor alle processen wordt uitgegaan van BBN2.

Wilt u meer weten over de pilot ENSIA op basis van de BIO, neem dan contact op met het ENSIA team. Bellen kan ook via 070 2502400.