Belastingdienst

VERTROUWELIJK

MT MKB

Naam dienstonderdeel
MKB, landelijkde coördinatie Fraude/EOS

Contactpersoon
naam persoon

Datum
17 april 2018

Versienummer
1.0

Datum vaststelling
30 april 2018

Opdrachtgever
naam persoon

Auteurs
naam persoon

Kopie aan
naam persoon

Bijlagen
Rapport: Gegevensbeschermingseffect-beoordeling (PIA) Rijksdienst Fraude-EOS Informatieloketten met bijlage

memo

Gegevensbeschermingseffectbeoordeling Fraude-EOS Informatieloketten: Aanbevelingen en vervolg.

1. Inleiding

Op 25 mei 2018 wordt de Algemene Verordening Gegevensbescherming (AVG) van kracht. Op dat moment dient elke organisatie die onder deze verordening valt haar gegevensverwerkingen te hebben opgenomen in een register. Daarnaast moeten risico's, issues en maatregelen rondom adequate bescherming van de privacy behorende bij deze gegevensverwerkingen in kaart zijn gebracht.

De informatieloketten Fraude/EOS zijn gepositioneerd binnen de specialteams Fraude/EOS (SFO). De gegevensverwerkingen binnen de loketten betreffen (vaak gevoelige) informatie verkregen uit zowel in-als externe bronnen. Naast de aangekondigde AVG was de relatie met de externe samenwerking aanleiding om al in een vroeg stadium (meer) aandacht te besteden aan privacyaspecten binnen deze loketten.
Het MT MKB heeft daarom al voor inwerkingtreding van het programma AVG opdracht gegeven een Privacy Impact Assessment (PIA) uit de voeren op de informatieloketten Fraude/EOS.

De rapportage is inmiddels gereed en als bijlage bij dit stuk gevoegd.
Dit memo fungeert als leeswijzer en geeft adviezen omtrent vervolgstappen op basis van de geconstateerde risico's en aanbevelingen uit het rapport.
In termen van de AVG spreken we niet meer (of dan toch op dit moment) over een PIA maar een GEB: een Gegevensbeschermingseffectbeoordeling.

2. De basis is goed

Doel van een GEB is het detecteren van risico's en issues omtrent privacy en het aanreiken van risico verminderende maatregelen. Omdat het al bestaande verwerkingen betreft bevat deze GEB ook elementen van een audit.

De scope ligt op de verwerking van gegevensaanvragen en daaruit voortkomende verstrekkingen en de verwerking van inkomende signalen.

Belangrijke constatering is dat de basis van de gegevensverwerking in de informatieloketten goed is.
De noodzaak gegevens te verwerken is voldoende aangetoond.
Er wordt in het algemeen zorgvuldig gewerkt, met expliciete aandacht voor de wettelijke grondslagen, doelbinding, proportionaliteit en subsidiariteit.

3. De risico's

In het rapport worden in onderdeel 16 de geconstateerde risico's opgesomd.
Deze liggen met name op het vlak van informatiebeveiliging.
Het gaat dan om zaken als (wijze van) verzenden, bewaren en vernietigen van gegevens. Bijzondere aspecten zijn de afscherming van vertrouwelijke informatie op de werkplek van de SFO's (huisvesting) en het proces rondom tips en kliks.
Tot slot vergt het gebruik van RIEC-IS aandacht van alle betrokken partners.

4. De maatregelen

Onderdeel 17 bevat de risico-reducerende of opheffende maatregelen.
Een aantal, zoals bijvoorbeeld terugdraaien van te vergaande mandatering, zijn eenvoudig te implementeren. Andere vereisen nadere uitwerking.

Een belangrijke algemene constatering is dat verdere uniformering en meer landelijke centrale aansturing veel van de risico's kan reduceren en/of opheffen.
Een aantal andere aspecten verdienen daarnaast apart aandacht.

Huisvesting
MKB is afhankelijk van de uitwerking van de landelijke beleidslijnen.
Het (open) AGH concept kan gezien worden als een risico wat betreft geheimhouding en privacy t.a.v. de binnen de SFO's aanwezige informatie.

Tips en Kliks/Brede Informatiestromen
Het proces met betrekking tot tips en kliks staat in verbinding het vraagstuk van de brede informatiestromen (zie punt 5). Betrokken dienstonderdelen moeten een oplossing uitwerken die leidt tot eenduidig beleggen en verwerken van segment en/of dienstonderdeel overstijgende informatiestromen.

Tooling
Op 24 mei 2017 heeft het MT MKB gekozen voor FSV als centrale tool om signalen en verstrekkingen binnen MKB vast te leggen. Tijdens de GEB zijn wat FSV betreft vragen opgekomen. Het gaat met name om aard en omvang van autorisaties.
Daarom wordt er op FSV apart een toets uitgevoerd. Eerst in de vorm van een quick-scan, indien nodig gevolgd door het zwaardere instrument (GEB/PIA).
Van belang is dat FSV niet alleen wordt gebruikt door MKB, maar ook door andere segmenten en dienstonderdelen. Mochten uit de privacy toets op FSV voorstellen voortvloeien die ook andere dienstonderdelen gaan raken, is afstemming (en wellicht besluitvorming hoger in de organisatie) noodzakelijk.

De in RIEC verband samen met de partners gebruikte tool RIEC-IS verdient ook nadere beschouwing. Zo geven externe partijen op websites aan betrokken te zijn bij RIEC-IS en lijkt het ministerie van J&V ook derde partijen in te zetten.
Hierover is contact opgenomen met het LIEC. Deze zoekt momenteel e.e.a. uit.
Verdere stappen zijn afhankelijk van de bevindingen en duiding door het LIEC.

5. Impact breder dan voldoen aan AVG

De in de GEB geconstateerde risico's en maatregelen zijn niet alleen van belang om in voldoende mate te voldoen aan wet- en regelgeving omtrent privacy.

De aanbevelingen sluiten ook goed aan bij al bestaande ambities voortvloeiende uit de Kapstoknotitie Fraude, zoals verdere professionalisering en uniformering van de werkwijze en vastleggingen binnen de informatieloketten.
Dit betekent dat de resultaten van de vervolgacties ook moeten voldoen aan de uitgangspunten van de door het MT MKB op 24 mei 2017 van besluiten voorziene notitie 'Doorontwikkeling en afbakening Informatieloketten MKB'.[1]

Zo moeten verschillen tussen de SFO/Informatieloketten die zijn ontstaan na het instellingsbesluit moeten worden gereduceerd.
De destijds gehanteerde notie dat de lokale situatie en (wijze en mate van) externe samenwerking de opzet, inrichting en werkwijze mede bepalen blijft een rol spelen, maar komt met de hierboven genoemde ontwikkelingen minder op de voorgrond te staan.

6. Vervolgstappen/beslispunten

Het uitgevoerde onderzoek en rapport heeft geleid tot opname van de gegevens-verwerking in het daartoe bestemde register. Daarmee is aan de eerste eis rondom de invoering van de AVG voldaan.

Met de goedkeuring van het rapport door uw MT wordt de ook de tweede eis ingevuld. De risico's en bijbehorende maatregelen zijn in kaart gebracht.

Er is dan aan de door het programma AVG geformuleerde basispositie voldaan.

Over de procedure met betrekking tot het vervolg na deze registratie van de gegevensverwerking en het in beeld brengen van risico's, issues en maatregelen bestaat nog onduidelijkheid.
De (nieuwe) Functionaris Gegevensbescherming (FG) van het ministerie zal naar verwachting in samenspraak met het programma AVG een procedure gaan vaststellen welke ook deze GEB dan zal doorlopen.
Hoe dan ook is het MT MKB eerstverantwoordelijk voor het feit dat uitwerking en implementatie van de maatregelen vanuit deze GEB worden opgepakt. Hiermee wachten tot de procedure is vastgesteld heeft naar onze mening geen nut. Mede gezien het feit dat met de realisatie van de maatregelen enkele al bestaande ambities van MKB gerealiseerd worden (zie punt 6 hieronder).

Naast uw besluit tot goedkeuring van het rapport, stellen we daarom de volgende -direct ter hand te nemen- besluiten voor.

1. Formeren van een werkgroep met de opdracht de aanbevelingen rondom uniformering en centrale aansturing uit te werken in landelijke werkinstructies en datasets. Hierbij aanwezige expertise vanuit de SFO's en andere dienstonderdelen benutten.
Samenstelling van deze werkgroep: 4 teamleiders SFO + 2 leden van de LC.

[1] Zie besluitenlijst MT MKB 24 mei 2017 en betreffende notitie van 25 april 2017.

2. De kwestie van afgeschermde huisvestiging kan worden aangekaart bij de landelijke projectleiding AGH. Oplossingsrichtingen t.a.v. de in het rapport geconstateerde risico's zijn voorhanden en blijkens het rapport niet zonder precedent. Onderzoek of dergelijke maatregelen op de 11 locaties tot de mogelijkheden behoort.

3. De bevindingen uit de nog uit te voeren toets op FSV op te pakken binnen de al eerder geformeerde werkgroep die werkt aan uniform gebruik en instructies voor FSV naar aanleiding van het besluit van 24 mei 2017 om deze tool binnen MKB te gaan gebruiken als enige registratietool.

4. Het liggende vraagstuk van de brede informatiestromen ter hand nemen conform het op 2 juni 2017 door het toenmalige CDO2 genomen besluit[2].
Dit kan worden opgepakt door het al bestaande Brede Informatiestromen Overleg (BIO) een (nader) vooronderzoek te laten uitvoeren als opstap voor een vervolg in lijn met dit besluit. Deze opstap moet niet alleen rekening houden met de eisen van de AVG, maar ook met de uitgangspunten van de Investeringsagenda, de Topstructuur en de Ontwikkelagenda.

5. LC F/EOS laten bewaken dat RIEC-IS wat inhoud, gebruik en toegang betreft voldoet of gaat voldoen aan de AVG. Bij constatering van risico's dienen maatregelen te worden voorgesteld aan betreffende interne en externe besluitvormende gremia.

[2] CDO2 van 2 juni 2017, met als kern dat er een visie moet komen op de informatiestromen (hoe is het nu; wat willen we en welke -bestaande of nieuwe voorzieningen zijn daarbij nodig?), met als mogelijk uitvloeisel het benoemen van een lead architect op dit thema. Het vraagstuk is in de nieuwe structuur terechtgekomen op de voorraadlijst van het Driehoeksoverleg FJZ UHB. Recent nog aan de orde geweest op het FPO van 29/3/2018.