Bijlage 3 bij besluit met kenmerk 2018-0000187654

Documenten 19 - 28

I. Basisinformatie: type persoonsgegevens, type verwerking en noodzaak/gegevensminimalisering

1. Wilt u als verantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type?

De missie van B/T is het juist verlenen van Toeslagen aan hen die daar recht op hebben. Informatie die B/T met het oog op deze missie kan ontlenen aan uitingen over of mbt toeslagen op sociale media kan daar aan bijdragen. Naast dienstverlening aan de burger wil de Belastingdienst effectief handhaven. Daarom kunnen zowel trends die te maken hebben met de toeslagen zoals deze door B/T worden uitgevoerd als persoonsgebonden info deel uitmaken van het hulp bieden zowel als aan het informeren.

Een behandelaar zelf zal bij B/T hooguit algemene informatie op het internet zoeken, zoals gegevens over een kinderopvanginstelling via het openbare register of via de site van zo'n instelling. Sinds kort zoekt B/T ook zelf naar trends die invloed kunnen hebben op de onderscheiden toeslagen. Mogelijk kunnen deze handvatten bieden voor gebruik binnen risicoselectie, of om de dienstverlening te verbeteren.

Zie ook ISC: De webdienst maakt gebruik van persoonsgegevens die door de gebruikers van de diverse sociale media in de openbaarheid van het internet zijn geplaatst. Voorbeelden hiervan zijn namen, gebruikersnamen, sociale media adressen en andere gegevens die een gebruiker mogelijk ingevuld heeft op het sociale media profiel/account zoals de biografische tekst, woonplaats, nicknames en geo-locatie. Het is mogelijk dat beeldmateriaal is geplaatst, waardoor bijzondere persoonsgegevens kunnen worden verwerkt.

Daarnaast kunnen medewerkergegevens (voornaam, achternaam, email adres werk, geslacht) worden verwerkt.

- *Bij de uitvoering van een opdracht moet, d.m.v. het gebruik van filters, zoveel mogelijk het gebruik van niet relevante gegevens worden uitgesloten.*
- *Bij de verwerking beeldmateriaal is extra zorgvuldigheid geboden. Het specifiek zoeken op beeldmateriaal dient extra gemotiveerd te worden. De informatieproducten dienen zoveel mogelijk van beeldmateriaal te zijn ontdaan.*
- *Zoveel mogelijk beperken van het gebruik van medewerker gegevens*

2. Andere specifieke persoonsgegevens?

2a. Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting te verwerken?

Zie ook ISC: Het is niet de bedoeling om het recht op toeslagen in kaart te brengen. Wel is het mogelijk dat financiële/economische gegevens opkomen (b.v. over tweede woningen).

2b. Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?

Zie ook ISC: Onder de aanvragers van toeslagen zitten kwetsbare personen. Mochten groepen kwetsbare personen in beeld worden gebracht, in het kader van een opdracht, dan is extra zorgvuldigheid geboden. Daarom zal bij het gebruik van gegevens van kwetsbare personen/groepen een zo kort mogelijke bewaartermijn worden gehanteerd worden. In het intakeformulier wordt hiertoe een extra vraag opgenomen.

2c.Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens te verwerken?

Zie ISC: Het is mogelijk dat gebruikersnamen verwerkt worden: dit is afhankelijk van de keuze van de gebruiker van de netwerksites. De gebruikersnamen zijn de namen waarvan een individu

gebruik maakt op sociale media. Dit kan de echte naam zijn van de betrokkene, of een nickname. Wachtwoorden worden niet verwerkt.

2d. Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?

Nee.

2e. Is het de bedoeling om het BSN-nummer, of een ander persoonsgebonden nummer te verwerken?

Nee.

3. Kan van elk van de onder vraag I.1 en vraag I.2 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn voor het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken persoonsgegeven toe.

Sociale media uitingen markeren sinds enige jaren een nieuwe maatschappelijke ontwikkeling. Omdat B/T in de maatschappij staat is het voor haar noodzakelijk om hiervan met het oog op haar missie kennis te nemen. Zonder deze informatie zal B/T ontwikkelingen missen die van belang kunnen zijn voor haar dienstverlening of haar toezicht.

Zie ook ISC: De webdienst levert een aantal informatieproducten op zoals fenomeen- sentiment en imagoanalyses. Deze informatieproducten worden door B/T ingezet voor het versterken van de kennispositie.

- *Aandacht bij het uitvoeren van de opdracht voor het gebruik van zo min mogelijk persoonsgegevens, per opdracht motiveren welke gegevens noodzakelijk zijn, overige gegevens uitzetten d.m.v. filterfunctie.*
- *De mogelijkheid tot het herleiden naar de bron van de gegevens moet geblokkeerd kunnen worden wanneer de gegevens binnen de Belastingdienstomgeving worden geëxporteerd.*

4. Kan, als het gaat om gevoelige persoonsgegevens hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?

Het gaat om nieuwe gegevens dus het combineren van normale persoonsgegevens levert niets vergelijkbaars op. Het is niet de bedoeling bijzondere persoonsgegevens te verwerken. En zeker geen nieuwe. Persoonsgegevens kunnen wel deel uitmaken van de geaggregeerde sociale metadata. De informatie van de webdienst zelf is niet persoonsgebonden, persoonsgegevens zijn mogelijk te herleiden. Vanwege het feit dat de bronnen waaruit de analyses zijn opgebouwd, nog te herleiden zijn, is er geen sprake van anonimisering. Zie ook II-1.

5. In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene traject? Wordt hierbij gebruikt gemaakt van (nieuwe) technologie of informatiesystemen?

Cfm ISC:

De belastingdienst voert haar taken uit binnen het kader van o.a. de AWR, de AWIR, de heffingswetten en de Wbp.
Op basis van art. 8 onder e Wbp biedt de goede vervulling van de publiekrechtelijke taak (in dit geval de wettelijke taken heffen, innen en uitkeren) grondslag voor de Belastingdienst en

Toeslagen voor het verwerken van persoonsgegevens. Daarbij moet per verwerking worden aangegeven voor welk (sub)doel de gegevens worden verzameld.

- *In intakeformulieren dient expliciet gevraagd te worden naar het doel van de gegevensverzameling*

II. Doelbinding, koppeling, kwaliteit en profilering

Doeleinden/doelbinding en koppeling

1. Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel?

Zie ook ISC: Monitoren draagt bij aan de taken van B/T – het rechtmatig verlenen van Toeslagen aan hen die daar recht op hebben. Voor zowel dienstverlening als toezicht zal het raadplegen van informatie vervat in openbare bronnen (sociale media) de kennispositie versterken en bijdragen aan het verrichten van verder onderzoek bij deze taak. Analyses van data van sociale media bieden een mogelijkheid om een beter beeld te krijgen van trends, fenomenen, imago, sentiment, subjecten, objecten en om inzichten te verkrijgen in de reacties van burgers en organisaties op maatschappelijke veranderingen.

Het monitoren van sociale media levert een bijdrage aan de uitvoering van de taken van B/T. Data uit sociale media hebben een duidelijke toegevoegde waarde op data van bijvoorbeeld algemene websites of andere reeds beschikbare interne of externe data. Deze toegevoegde waarde zit in de soort berichtgeving die je vindt op sociale media: sociale media kenmerken zich door een puur, rauw beeld te geven van wat er speelt in de buitenwereld. Er wordt dus geput uit de behoefte van mensen om hun mening online te ventileren. Dit levert informatie op die je op andere plekken niet vindt. In een tijdperk waarin burgers zich steeds meer online begeven voor o.a. het voeren van discussies, het uiten van klachten en het doorspelen van informatie, kan de Belastingdienst niet achterblijven in het analyseren van deze specifieke vorm van informatie. Daarnaast is het een extreem actuele bron van informatie, wat ertoe leidt dat sociale media analyse de mogelijkheid biedt om snel de gewenste informatie te verkrijgen en hier desgewenst op te acteren.

De webdienst wordt alleen ingezet op basis van opdrachten. In deze opdrachten staat het specifieke doel vermeld voor het uitvoeren van een sociale media analyse met als achterliggend doel het ondersteunen van de processen van de Belastingdienst op basis van de wettelijke taken moeten worden uitgevoerd.

Bij het gebruik van de informatie uit sociale media dient er aandacht te zijn voor de kwaliteit van de gegevens en de interpretatie ervan, om onoordeelkundig gebruik van de informatie te voorkomen.

- *De webdienst wordt alleen aan geschoolde en bevoegde medewerkers ter beschikking gesteld. De webdienst mag door deze medewerkers alleen worden gebruikt conform een nog te ontwikkelen instructie.*

2 en 3. Gaat het bij het project/systeem om gebruik van nieuwe persoonsgegevens voor een bestaand doel, of bestaande doelen binnen al bestaande systemen? (scenario toevoeging nieuwe persoonsgegevens). Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden). Zo ja, hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?

Zie ISC: De persoonsgegevens die worden gebruikt zijn nieuw. Deze gegevens zijn niet gekoppeld aan andere systemen binnen de Belastingdienst. Het gebruik van gegevens voor de genoemde doelen (kennisverwerving bijv. T.b.v. toezichtbeleid) geschiedt op een geaggregeerd niveau. Door de webdienst worden persoonsgegevens verwerkt om te komen tot deze geaggregeerde gegevens. Het gaat om een bestaand doel: namelijk het versterken van de kennispositie van B/T. Dit doel vloeit rechtstreeks voort uit de publiekrechtelijke taken van B/T.

Bij de analyses op sociale media is het doel van B/T in principe niet om persoonsgegevens te verzamelen. Het gaat om de geaggregeerde data, waaruit analyses kunnen worden gemaakt m.b.t trends, sentiment, imago etc. Daar waar specifieke berichten worden getoond, functioneren deze als ondersteuning van dergelijke analyses. Het is B/T bij het gebruik van sociale media data niet te doen om te achterhalen wie persoon X is die iets zegt over onderwerp Y.

4. Indien u positief hebt geantwoord op vragen II.2 of II.3, hoe wordt een dergelijk voorgenomen gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) gemeld aan: (a) de functionaris voor de gegevensbescherming, of (b) het Cbp indien er geen FG is?

Geen gebruik van nieuwe persoonsgegevens in bestaande systemen. Geen bestaande persoonsgegevens voor nieuwe doeleinden.

5. Indien u positief geantwoord hebt op vragen II.2 of II.3, welke (nadere) controles op een dergelijk gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) zijn voorzien?

Zie ISC: Maatregelen voor zorgvuldig gebruik van de webdienst zijn eerder genoemd in dit stuk.

- *Deze maatregelen zullen via ic's worden gecontroleerd.*

Kwaliteit

6. Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de in het beleidsvoorstel, wetsvoorstel op overheidsICT-systeem verwerkte persoonsgegevens na te gaan?

Zie ISC: De deskundigheid van de medewerkers die de webdienst mogen gebruiken, borgen een zorgvuldige duiding van de gebruikte gegevens.

Profilering

7. Zullen de verzamelde/verwerkte persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen? Zijn de betrokkenen daarvan op de hoogte? Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld?

Zie ISC: Profilering houdt in het verzamelen, analyseren en combineren van (persoons)gegevens met als doel iemand in te delen in een bepaalde categorie. Het gebruik van de webdienst kan het gebruik van profielen met zich meebrengen. Er worden informatieproducten gegenereerd om vermoedelijk relevante informatie in kaart te brengen. Deze producten worden gemaakt m.b.v. de webdienst na invoeren van zoektermen door de belastingdienst, gebaseerd op een opdracht. De resultaten van deze producten kunnen worden gebruikt bij het versterken van de kennispositie van de belastingdienst. Ze worden niet gebruikt voor besluiten ten aanzien van individuele personen. Daarnaast worden er geen geautomatiseerde beslissingen genomen; een deskundig medewerker beoordeeld altijd de gegenereerde informatie voordat deze verder wordt verstrekt aan de opdrachtgever.

- *Informeren betrokkenen over het gebruik van de webdienst en meer specifiek het profileren (zie ook inleiding)*

8. Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)? Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?

Zie ISC: Een webdienst verzamelt grote hoeveelheden sociale media data beschikbaar op het internet. Op deze data worden algoritmes toegepast die diverse informatieproducten opleveren, zoals trend, fenomeen- en imagoanalyses.
Zonder tussenkomst van een menselijke beoordeling wordt er geen actie ondernomen. De gegevens zullen niet worden gebruikt voor besluiten ten aanzien van individuele personen.

- *Een gespecialiseerde medewerker van de belastingdienst zorgt voor duiding van de resultaten.*

III. Betrokken instanties/systemen en verantwoordelijkheid

1. Welke interne en externe instantie(s) en/of systemen is/zijn betrokken bij de voorziene verwerking in elk van de onder I.5 onderscheiden fasen? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?

Zie ISC: De webdienst betreft een webbased toegankelijke dienstverlening. Deze dienstverlening wordt door een externe partij verleend. De dienstverlening van deze externe partij wordt eveneens aan andere geïnteresseerde marktpartijen aangeboden. Het is dus niet zo dat de dienstverlener enkel in opdracht van de Belastingdienst een opdracht uitvoert.

Het gebruik van de e-dienst geschiedt ook door B/T.

2. Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens? Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?

Zie ook ISC: Verantwoordelijke voor het leveren van de webdienst: externe te contracteren partij. De minister van Financiën en namens hem de DG Belastingdienst is verantwoordelijk voor de verwerking van de gegevens binnen de Belastingdienst.
Binnen B/T wordt de dienst alleen ingezet door een selecte groep gekwalificeerde en bevoegde medewerkers. De webdienst zal niet algemeen ter beschikking worden gesteld.

- *PIA's moeten regelmatig worden uitgevoerd om bewust scherp te blijven op rechtmatige verwerkingen van persoonsgegevens.*
- *Er zal een instructie worden opgesteld voor de gebruikers van de webdienst.*

3. Wie binnen uw organisatie, en elk van de andere betrokken organisaties, krijgen precies toegang tot de persoonsgegevens?

Zie ISC: Een selecte groep speciaal opgeleide en geautoriseerde medewerkers.

4. Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen (in verband met functie/wet)?

Zie ook ISC: Art 2:5 Awb en Art 7 van de Wet Politiegegevens zijn van toepassing, evenals artikel 12 DWU juncto artikel 1:33 ADW.

- *Er wordt een geheimhoudingsplicht opgelegd aan de dienstverlener.*

5. Zijn alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?

Zie ISC: B/T gebruikt de webdienst voor het genereren van diverse analyses. Deze analyses worden verstrekt aan de diverse interne opdrachtgevers.

6. Zijn er beleid en procedures voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken? Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?

Zie ISC: Er is een instructie in de maak over het gebruik van informatie beschikbaar op het internet door de Belastingdienst. Op basis van deze instructie zal een specifiek protocol over het gebruik van de webbased dienst worden geschreven.

- *Opstellen protocol(binnen het kader van bovengenoemde instructie) voor het gebruik van de webdienst*

7. Is er sprake van overdracht van persoonsgegevens naar een (overhelds)instantie buiten de EU/EER? Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de Minister van Veiligheid en Justitie? Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven?

Zie ISC:

- *Contractueel vastleggen dat gegevens binnen de EU worden opgeslagen.*
- *Toezien op het feit dat bovenstaande eis wordt nageleefd door de leverancier.*

IV. Beveiliging en bewaring/vernietiging [1]

Beveiliging

1. Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde? Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan? Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging?

2. Indien (een deel van) de verwerking bij een bewerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die bewerker?
Nader te bespreken, vormgeven in bewerkersovereenkomst plus toezicht op naleving van de gestelde voorwaarden.

3. Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a) gegevens die in een geautomatiseerd format staan (bv. wachtwoord-bescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend bv. sloten op kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen?

4. Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften, en voor het detecteren ervan? Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen?

Gezamenlijke beantwoording vraag 1t/m 4, zie ISC

Aan de leverancier van de webdienst zullen de volgende eisen worden gesteld.

De Dienst dient aan de beveiligingseisen van de Overheid te voldoen zoals beschreven in de volgende bijlagen.

- *bijlage 'ICT-Beveiligingsrichtlijnen voor web applicaties- Verdieping leesversie (NCSC, september 2015)'; NCSC staat voor National Cyber Security Centrum. Dit document beschrijft richtlijnen over eisen aan web applicaties, waaraan de inschrijver moet voldoen. Bron: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html*
  - *'Baseline Informatiebeveiliging Rijksdienst' (BIR 2012 Tactisch Normenkader; bron http://content.rp.rijksweb.nl/cis/content/media/rijksportaal/dgobr/tab_kerntaken/domeinen/informatisering_1/BIR_TNK_1_0_definitief.pdf)*
  - *Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007' (VIR 2007; bron http://wetten.overheid.nl/BWBR0022141/2007-07-01*
  - *Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013' (VIRBI 2013; bron http://wetten.overheid.nl/BWBR0033507/2013-06-01*

Risico is dat data, waaronder persoonsgegevens, zich buiten de gesloten en beveiligde infrastructuur van de Belastingdienst bevindt. Dit brengt het risico met zich mee dat onbevoegden mogelijk toegang kunnen verkrijgen tot deze data. Zodra een selectie is uitgevoerd, vallen deze data onder de bedrijfsdata van de belastingdienst en worden derhalve als vertrouwelijk aangemerkt.

Overzicht van de data, waaronder persoonsgegevens, die buiten de dienst worden geplaatst: inlogfrequenties, namen van projecten, belastingdienst- emailadressen gebruikers webdienst, de zoektermen die worden gebruikt voor een zoekopdracht, de dashboards die voortvloeien uit een zoekopdracht, lijsten van gebruikte internetbronnen.

---

[1] Voorde details betreffende de beveiliging wordt verwezen naar de 'Beschrijving functionele eisen en wens en onderzoeken sociale media' en de 'Demandspecificatie Internet- en Mediaonderzoek 2016'.

Bedrijfsdata mogen slechts worden verwerkt en opgeslagen binnen de Europese Unie.

De webdienst is alleen toegankelijk voor gebruikers van wie het account is geverifieerd. Alleen geautoriseerde Belastingdienstmedewerkers hebben toegang tot de webdienst.

Medewerkers van de inschrijver of onderaannemers van de inschrijver hebben geen toegang tot Bedrijfsdata. Een uitzondering wordt gemaakt voor medewerker(s) van de inschrijver die door de inschrijver zijn aangewezen om de dienstverlening te beheren. Toegang tot Bedrijfsdata door medewerkers van de inschrijver moet worden beveiligd. De volgende maatregelen zijn voor medewerkers van de inschrijver van toepassing:

- *Er dient een geheimhoudingsverklaring te worden ondertekend door de medewerkers van de dienstverlener die specifiek betrokken zijn bij de uitvoering van de werkzaamheden voor de Belastingdienst,*
- *De minimale screeningseis is een Verklaring Omtrent Gedrag o.b.v. algemeen screeningsprofiel functieaspecten 11, 12 en 13 (zie www.justis.nl).*

De Dienst is verplicht om Belastingdienst Projecten af te schermen van andere klanten van de inschrijver (chinese walls).

De Dienst voorziet in autorisatie op Projecten die alleen door een geautoriseerde gebruiker kunnen worden uitgevoerd (bijvoorbeeld het opvoeren, wijzigen of verwijderen van gegevens)

Beheer van autorisaties kan plaatsvinden op basis van rollen (Role Based Acces Control)

De Dienst kan hierbij aansluiten op een voorziening waarin de rechten (permissies) van medewerkers zijn vastgelegd. Zie ook Wens TW1.

De geautoriseerde autorisatiebeheerder van de Belastingdienst wil zelf rollen, rechten en gebruikersbeheer op de niveaus van Bedrijfsonderdelen en daarbinnen per Project in de Dienst uitvoeren.

De Belastingdienst moet periodiek een overzicht kunnen genereren van actieve gebruikers met welke rollen en rechten zij hebben in de Dienst, zodat licentiebeheer en integriteitsonderzoek kan plaatsvinden.

Hiervoor wordt bij voorkeur aangesloten op het Identity Management systeem met Single Sign on van de Belastingdienst, zodat inloggegevens niet bij de inschrijver komen.

10.1.c en 10.2.g

Ten behoeve van verantwoording afleggen moeten rapportages voor een audit trail kunnen worden gemaakt door de Belastingdienst.

Op basis van de logging van activiteiten moet verantwoording over het gebruik worden afgelegd en onderzoek kunnen worden gedaan naar wie wat wanneer welk subject in onderzoek had c.q. welk Project onderhanden was. Loggegevens van medewerkers moeten minimaal twee jaar na ontstaan daarvan beschikbaar blijven voor interne controle binnen de Belastingdienst. De Belastingdienst moet over de loggegevens kunnen beschikken om integraal met andere Belastingdienstactiviteiten verantwoording aan het management af te leggen. Het vereiste formaat is 'Cleartekst'. Bovenstaande geldt ook voor beheerderactiviteiten op alle niveaus

Aanvullende specifieke eisen zijn:

- *wanneer en door wie een onderzoek in een Project is aangemaakt,*

- *Wie wanneer welke zoekopdracht (voor een Project) heeft uitgevoerd,*
- *Wie wanneer welke resultaatgegevens heeft veilig gesteld (bewaard t.b.v. Project),*
- *Wie wanneer gebruik heeft gemaakt van de gegevens (raadplegen),*
- *Wie wanneer resultaatgegevens heeft gewijzigd, aangevuld of verwijderd.*

10.1.c en 10.2.g

De inschrijver moet de Belastingdienst actief informeren bij alle incidenten en calamiteiten. De inschrijver informeert de Belastingdienst onmiddellijk in het kader van de wet Meldplicht datalekken

De inschrijver dient actief beleid op beveiliging uit te voeren. Zodra er beveiligingslekken voor data zijn geconstateerd, dan dient er z.s.m. een beveiligings-update van de Dienst plaats te vinden. Conform richtsnoeren beveiligingsniveau CBP en interen richtlijnen belastingdienst.

- *De autorisatieprofielen zullen regelmatig moeten worden gecontroleerd op actualiteit en de AdR zal de naleving van het beleid hieromtrent moeten toetsen. Dit is onderdeel van de controle op de beveiliging van de verwerking.*

Afhankelijkheid van het publieke internet is hier een factor.

- *Alleen gebruik maken van beveiligde browsers en verbindingen en vanaf werkplekken in beveiligde netwerken binnen de belastingdienst omgeving conform ICT-Beveiligingsrichtlijn voor web- applicaties NCSC.*

Bewaring/vernietiging

5. Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring?

Zie ISC:
De rapportages en analyses worden door B/T verstrekt aan de interne opdrachtgever. Die draagt verder zorg voor een passende bewaartermijn.

- *In de (nader te ontwikkelen) interne instructie procedure rondom vernietiging van gegevens opnemen*

6. Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?
Zie ISC – verwijst naar 5

7. Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen? Worden alle persoonsgegevens, inclusief log-gegevens, vernietigd? Is er controle op de vernietiging, en door wie?
Zie ISC: Monitoren en loggen van het gebruik, inclusief beheerdersactiviteiten. De dienst is alleen toegankelijk voor gebruikers wiens identiteit is geverifieerd. Het beheer wordt centraal belegd bij het ISC en wordt uitgevoerd door een data-informatiespecialist Online (Social) Media Monitoring.

- *Maak een plan van aanpak (of afsprakendocument) met duidelijke proces- en beheersafspraken.*

V. Transparantie en rechten van betrokkenen

Transparantie

1. Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend gemaakt worden? Wat is de procedure om betrokkenen indien nodig te informeren over het doel van de verwerking van hun persoonsgegevens?

Zie ISC:

- *In aanvulling op wat nu op de website staat; informatie over gebruik van de dienst/gebruik sociale media door Belastingdienst op website publiceren uit oogpunt van transparantie.*
- *Melding bij FG*

2. Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?

- *Zie ISC: Informeren via www.belastingdienst.nl*

3. Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking?

- *Zie ISC: Overweging om gebruik van de dienst/ gebruik sociale media door belastingdienst op website te publiceren uit oogpunt van transparantie.*

Rechten van betrokkenen

4. Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? Bij een weigering toestemming te geven, of bij een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?

Zie ISC: nvt;

5. Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?

Zie ISC: Informatie over de verwerking van persoonsgegevens door de Belastingdienst en het uitoefenen van het recht op inzage of correctie is te vinden op www.rijksoverheid.nl en www.belastingdienst.nl.[2]

6. Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?

Zie ISC: Informatie over de behandeling van een verzoek tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens door de Belastingdienst is te vinden op www.rijksoverheid.nl en op www.belastingdienst.nl.[3]

-

- 0 -

[2] http://download.belastingdienst.nl/belastingdienst/docs/belastingdienst_wet_bescherming_persoonsgegevens_al5331z2pl.pdf
[3] http://www.rijksoverheid.nl/ministeries/fin/organisatie/meldingenregister

20

PIA FIOD

FIOD
Belastingdienst

Ische
opsporingsinformatie
Utrecht

Bernadottelaan 13-15

3527GA Utrecht

Contactpersonen

Datum
06-09- 2016

Versienummer
1

memo

FIOD Privacy Impact Assessment
gebruik dienst voor social media monitoring & analyse

Aanleiding

Social media maken inmiddels een onlosmakelijk deel uit van de informatiestromen in de Nederlandse samenleving. De FIOD wil effectief kunnen blijven handhaven. De politiek speelt zeer dynamisch in op maatschappelijke ontwikkelingen, van de FIOD wordt verwacht dat zij als organisatie deze ontwikkelingen eveneens kan volgen en erop kan anticiperen. Hiervoor is het essentieel dat men een goed beeld heeft van wat zich afspeelt op de diverse (social) media.

Voor de FIOD is het van belang om trends en fenomenen te signaleren die informatie kunnen verschaffen over relevante ontwikkelingen in de samenleving. Data uit social media worden gebruikt voor het maken van trend, fenomeen- en imagoanalyses maar ook in het kader van de opsporing. De inzichten die deze analyses opleveren zijn relevant voor de inzet in diverse projecten en taken van de opsporing en hebben een strategisch en tactisch karakter.
De keuze voor de onderwerpen die worden gemonitord komt voort uit de keuzes binnen de handhavingsagenda. Het gebruik van de diverse sociale media zal naar verwachting de komende jaren alleen maar toenemen. Inzicht en kennis in deze media zullen derhalve een belangrijke bron van informatie voor de FIOD opleveren.

Het volume aan berichten op de diverse sociale netwerk-sites, blogs, fora, nieuwssites, etc. is enorm en bevat ook veel niet-relevante informatie. Het is onmogelijk om uit deze hoeveelheid berichten handmatig de informatie te destilleren die voor de FIOD relevant is. Daarom is een social media monitoring & analyse (ssm&a) dienst voor het monitoren van sociale media onmisbaar geworden. Dergelijke dienst maakt de data doorzoekbaar, en biedt daarnaast diverse analyses. Met behulp van deze analyses wordt de kwaliteit van de intelligence die de FIOD tot haar beschikking heeft sterk verbeterd en kan het werk sneller en efficiënter worden gedaan. De reeds geboekte resultaten zijn bemoedigend en de vraag naar deze informatie vanuit de diverse FIOD teams groeit.

Sinds 2010 wordt gewerkt met een social media dienst die wordt aangeboden door een externe partij. Het gebruik van smm&a dienst is vast onderdeel geworden van diverse werkprocessen waardoor een afhankelijkheid is ontstaan van deze dienst. Specifiek aan social media dienst is het feit dat de dienst webbased toegankelijk is. Er wordt derhalve geen dienst aangekocht die vervolgens wordt geïnstalleerd binnen de belastingdienstomgeving.

Het contract met de huidige aanbieder loopt einde 2016 af. De smm&a dienst zal openbaar worden aanbesteed.

I. Basisinformatie: type persoonsgegevens, type verwerking en noodzaak/gegevensminimalisering

1. Wilt u als verantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type?

Ja. Door het gebruik van de dienst zullen ook persoonsgegevens verwerkt worden. Hierbij kan gedacht worden aan namen en informatie van sociale media accounts. Het zou kunnen zijn dat er ook bijzondere persoonsgegevens worden verwerkt (aangezien foto's vaak onderdeel zijn van social media accounts). FIOD mag bijzondere persoonsgegevens slechts verwerken als dat noodzakelijk is voor de uitvoering van de taak.

2. Andere specifieke persoonsgegevens?

2a. Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting te verwerken?

Ja, indien er aanleiding toe is zullen er gegevens over de financiële of economische situatie van betrokkenen worden verwerkt. Echter deze gegevens zullen niet gebruikt worden voor stigmatisering dan wel uitsluiting

2b. Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?

De verwerking zal daar niet primair op gericht zijn, maar kunnen onderdeel zijn van de gegevens verzameling. Dit zal samenhangen met het doel waarvoor de gegevens verzameld worden.

2c.Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens te verwerken?

Gebruikersnamen die in het openbaar gebruikt worden(bijv. @jjansen op Twitter) zullen mogelijk verwerkt kunnen worden. Wachtwoorden en andere inloggegevens niet.

2d. Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?

Nee

2e. Is het de bedoeling om het BSN-nummer, of een ander persoonsgebonden nummer te verwerken?

Bij het verwerken van de gegevens die door de smm&a dienst worden gehanteerd, wordt geen BSN-nummer gebruikt.
Het is mogelijk om meer persoonsgericht informatie die uit de dienst komt, te koppelen aan een BSN-nummer. Dat is een beslissing, die in principe los staat van het gebruik van de smm&a dienst. Het koppelen van een BSN-nummer is echter niet iets wat door de smm&a dienst wordt uitgevoerd. Het is een handeling die door een medewerker van de FIOD zal worden uitgevoerd, binnen de infrastructuur van de FIOD.

3. Kan van elk van de onder vraag I.1 en vraag I.2 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn voor het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken persoonsgegeven toe.

1. De FIOD zal de gegevens niet gebruiken voor het bereiken van beleidsdoelstellingen maar in het kader van de uitoefening van de wettelijke taak. Zoals verwoordt staat in art 3 van de wet op de Bijzondere Opsporingsdiensten. De aard en de hoeveelheid van de data die gebruikt gaat worden is afhankelijk van de individuele casus. Per casus zal bekeken moeten worden welke data benodigd is en zal een proportionaliteit afweging gemaakt dienen te worden.

4. Kan, als het gaat om gevoelige persoonsgegevens hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?

De verwerking van gevoelige persoonsgegevens vindt slechts plaats in aanvulling op de verwerking van andere persoonsgegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is.

5. In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene traject? Wordt hierbij gebruikt gemaakt van (nieuwe) technologie of informatiesystemen?

De FIOD voert haar bevoegdheden (strafrecht en strafvordering) uit binnen het kader van de WPG. Om de opsporingstaken uit kunnen voeren kan het noodzakelijk zijn om over informatie te beschikken vanuit sociale media

II. Doelbinding, koppeling, kwaliteit en profilering

Doeleinden/doelbinding en koppeling

2. Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel?

Op basis van art. 3 van de Wet op de bijzondere opsporingsdiensten biedt de uitvoering van de strafrechtelijke taak in het algemeen de grondslag voor de bijzondere opsporingsdiensten voor het verwerken van persoonsgegevens. Daarbij moet per verwerking worden aangeven met welk doel de gegevens worden verzameld. Daarnaast kan social media informatie gebruikt worden om een algemeen beeld te krijgen van bepaalde trends en fenomenen en om de berichtgeving over de FIOD te monitoren.

2 en 3. Gaat het bij het project/systeem om gebruik van nieuwe persoonsgegevens voor een bestaand doel, of bestaande doelen binnen al bestaande systemen? (scenario toevoeging nieuwe persoonsgegevens). Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden). Zo ja, hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?

2&3 Nee. Het gaat niet om nieuwe persoonsgegevens en het gaat ook niet om nieuwe aanvullende doeleinden.

4. Indien u positief hebt geantwoord op vragen II.2 of II.3, hoe wordt een dergelijk voorgenomen gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) gemeld aan: (a) de functionaris voor de gegevensbescherming, of (b) het Cbp indien er geen FG is?

Nee

5. Indien u positief geantwoord hebt op vragen II.2 of II.3, welke (nadere) controles op een dergelijk gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) zijn voorzien?

Nee

Kwaliteit

6. Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de in het beleidsvoorstel, wetsvoorstel op overheidsICT-systeem verwerkte persoonsgegevens na te gaan?

Dit punt dient contractueel gewaarborgd te worden.

Profilering

7. Zullen de verzamelde/verwerkte persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen? Zijn de betrokkenen daarvan op de hoogte? Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld?

Nee. Indien wordt overwogen tot profilering over te gaan, dient allereerst opnieuw een PIA te worden uitgevoerd.

8. Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)? Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?

Nee, niet van toepassing

III. Betrokken instanties/systemen en verantwoordelijkheid

1. Welke interne en externe instantie(s) en/of systemen is/zijn betrokken bij de voorziene verwerking in elk van de onder I.5 onderscheiden fasen? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?

2. Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens? Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?

Verantwoordelijke voor het bouwen van de tool: externe te contracteren partij
De minister van Financiën is verantwoordelijk voor de verwerking van de gegevens binnen de FIOD. Binnen de FIOD dient de dienst alleen te worden ingezet door een selecte groep gekwalificeerde en bevoegde medewerkers. De dienst zal niet algemeen ter beschikking worden gesteld.
PIA's dienen regelmatig te worden uitgevoerd om bewust scherp te blijven op rechtmatige verwerkingen van persoonsgegevens.

3. Wie binnen uw organisatie, en elk van de andere betrokken organisaties, krijgen precies toegang tot de persoonsgegevens?

Verschillende gebruikersgroepen: data-analisten, rechercheurs, OSINT en IRN-medewerkers in het kader van de uitvoering van de strafrechtelijke taak.
Criminologen, communicatiemedewerkers en adviseurs om een algemeen beeld te krijgen van bepaalde trends en fenomenen en om de berichtgeving over de FIOD te monitoren.

4.Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen (in verband met functie/wet)?

Art 7 van de Wet Politiegegevens is van toepassing

5. Zijn alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?

Binnen het strafdossier dienen alle handelingen verantwoord te worden, waaronder ook het gebruik van social media informatie

6. Zijn er beleid en procedures voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken? Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?

Op het moment dat de social media data gebruikt worden voor de opsporing gelden de kaders die uitgewerkt staan in de Leidraad & Matrix Gebruik info van internet tbv de opsporing

7. Is er sprake van overdracht van persoonsgegevens naar een (overheids)instantie buiten de EU/EER? Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld

door een besluit van de Europese Commissie of de Minister van Veiligheid en Justitie? Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven?

Contractueel vastleggen waar gegevens worden opgeslagen. De gegevens moeten binnen EU worden opgeslagen. Daarnaast geleden de regels van de FIOD voor de interne verwerkingen.

IV. Beveiliging en bewaring/vernietiging [1]

Beveiliging

1. Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde? Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan? Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging?

Aanbeveling: opdracht geven tot passende maatregelen.

2. Indien (een deel van) de verwerking bij een bewerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die bewerker?
Nader te bespreken, vormgeven in bewerkersovereenkomst plus toezicht op naleving van de gestelde voorwaarden.

Punt van aandacht is dat data die de FIOD gebruikt voor haar processen zich buiten de gesloten en beveiligde infrastructuur van de FIOD bevindt. Dit brengt het risico met zich mee dat onbevoegden mogelijk toegang kunnen verkrijgen tot deze, mogelijk vertrouwelijke data. Zodra een selectie is uitgevoerd, vallen deze data onder de bedrijfsdata van de belastingdienst en worden derhalve als vertrouwelijk aangemerkt. Beveiligingseisen At/m E (zie beschrijving functionele en technische eisen en wensen)zijn van toepassing.

3. Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a) gegevens die in een geautomatiseerd format staan (bv. wachtwoord-bescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend bv. sloten op kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen?

Conform richtsnoeren beveiligingsniveau CBP en interne richtlijnen FIOD.

4. Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften, en voor het detecteren ervan? Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen?

Opnemen in bewerkersovereenkomst.
Afhankelijkheid van het publieke internet is hier een factor.
Alleen gebruik maken van beveiligde browsers en verbindingen en vanaf werkplekken in beveiligde netwerken binnen de FIOD omgeving conform ICT-Beveiligingsrichtlijn voor web-applicaties NCSC.

---

[1] Voorde details betreffende de beveiliging wordt verwezen naar de 'Beschrijving functionele eisen en wens en onderzoeken sociale media' en de 'Demandspecificatie Internet- en Mediaonderzoek 2016'.

Aanbeveling: De webbased dienst moet aan de beveiligingseisen van de Belastingdienst/ FIOD voldoen.

Bewaring/vernietiging

5. Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring?

Als de gegevens worden gebruikt voor de strafrechtelijke vervolging is de bewaartermijn 5 jaar na uitspraak van het hoger beroep. Als gegevens worden gebruikt voor andere doeleinden (bijvoorbeeld themaontwikkeling) dienen ze na gebruik te worden vernietigd. Voor het project stellen we voor om een termijn van 5 jaar aan te houden.

6. Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?

Zie 5.

7. Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen? Worden alle persoonsgegevens, inclusief log-gegevens, vernietigd? Is er controle op de vernietiging, en door wie?

De FIOD voert eigen beheer op de gegevens, in 10.2.c *wordt registratie geautomatiseerd bijgehouden en vernietigd.*

V. Transparantie en rechten van betrokkenen

Transparantie

1. Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend gemaakt worden? Wat is de procedure om betrokkenen indien nodig te informeren over het doel van de verwerking van hun persoonsgegevens?

Door de FIOD zal niet actief worden geïnformeerd, de betrokkenen kunnen wel een verzoek tot kennisneming indienen, conform Art 25 WPG

2. Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?

Niet aan de orde.

3. Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking?

Niet aan de orde.

Rechten van betrokkenen

4. Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? Bij een weigering toestemming te geven, of bij een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?

Niet van toepassing.

5. Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?

Verzoeken van betrokkenen op grond van art. 25 worden gedaan aan de gemandateerde verantwoordelijke (de verantwoordelijke is de Minister van Financiën) i.c. de directeur FIOD. Deze heeft de afhandeling gemandateerd aan de Privacyfunctionaris van de FIOD (PF).

6. Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?

Verzoeken van betrokkenen op grond van art. 28 Wpg worden gedaan aan de gemandateerde verantwoordelijke i.c. de directeur FIOD. Deze heeft de afhandeling gemandateerd aan de Privacyfunctionaris van de FIOD (PF)

21

Agenda stuurgroep Aanbesteding Publishing en Engagement (P&E) en Social Media Monitoring en Analyse (SMMA).

Datum: 24 november 2016 10:00 – 12:00 uur
Locatie: Diverse via VC.
Voorzitter: , IM/Toezicht.

Agenda.

1. **Adviezen voorlopige Gunning**. De afgelopen weken hebben twee beoordelingsteams de aanbiedingen beoordeeld. Inkoop heeft een economische en juridische toetsing gedaan. Uitkomst hiervan is een advies voor voorlopige gunning voor elk perceel. Na de voorlopige gunning volgt nog een periode waarin de afgewezen partij(en) in bezwaar kunnen gaan. Na afloop hiervan kunnen de contracten definitief gemaakt worden. Een eventueel bezwaar heeft een stuitende werking.
    a. Gunningsadvies perceel Publishing en Engagement.
    b. Gunningsadvies perceel Social Media Monitoring en Analyse.
2. **Inrichten beheersituatie en implementatie.** Het is de bedoeling om het beheer zoveel mogelijk over te brengen van ISC en DV naar BCAO en BCIE. De afgelopen periode is intensief samengewerkt met alle betrokken, zowel gebruikers als beheerpartijen als B/cao en B/CIE. De uitkomst daarvan is vastgelegd in bijgevoegde memo. Bij de inrichting is zoveel als mogelijk is rekening gehouden met enerzijds de behoefte aan flexibiliteit en direct contacten met de aanbieders en anderzijds de formele verantwoordelijkheden die voortvloeien uit de contracten met externe leveranciers. (memo wordt separaat verzonden). De implementatie-inspanning is afhankelijk van de te gunnen contracten en zal mondeling worden toegelicht.
3. **Afronden PIA's.** De afgelopen periode zijn de concept PIA's beoordeeld en zijn de bevindingen teruggekoppeld aan de opstellers. Planning voor de afronding van dit traject zal separaat worden verzonden en mondeling worden toegelicht.
4. **Afsluiting.**

22

Leidraad bevoegdheden informatievergaring op internet

Laatste update: 17 november 2016

Tags : informatievergaring, internetrecherche, leidraad bevoegdheden informatievergaring op internet

Uitgangspunten leidraad bevoegdheden informatievergaring / opsporing binnen internet

De leidraad opsporing binnen internet (bestaande uit een matrix
met een leeswijzer
) is geen formele richtlijn of instructie van het OM, maar een kaderstellend document dat richtinggevend is voor opsporing en vervolging. De documenten zijn vastgesteld door de landelijke vergadering van Recherche-officieren wat inhoudt dat zij niet geheel vrijblijvend zijn, maar gelden als leidend en als vertrekpunt in de uitvoering.

De doelstelling van de leidraad is om behulpzaam te zijn en een handvat te bieden bij het afwegingen die op de werkvloer plaatsvinden. Met andere woorden: waar houdt de reikwijdte van het algemeen taakstellend artikel (artikel 3 wet BOD) op en wanneer is er sprake van een bijzondere opsporingsbevoegdheid waarvoor het OM geconsulteerd dient te worden?

Ter bepaling van de mate van inbreuk op de privacy (en de consequenties daarvan) spelen verschillende factoren een rol. Deze factoren, zoals stelselmatig uitvoeren van handelen, worden uitgebreider besproken in de toelichting bij de matrix.

Hieronder worden de belangrijkste uitgangspunten kort opgesomd:
Het toetsingskader van de matrix ziet op de mate van inbreuk op de privacy voor de burger (verregaand of beperkt). Dit uitgangspunt uit artikel 8 EVRM geldt onverkort voor alle informatievergaring op internet. Overigens gelden privacyafwegingen bij alle inbreukmakende opsporingsbevoegdheden (zoals stelselmatige observatie, tappen etc.)
Opsporing op internet verschilt niet wezenlijk van de "gewone" opsporing. Derhalve is de manier van samenwerken tussen politie en OM ook bij opsporing op internet het uitgangspunt.
De matrix ziet op fase van opsporing zoals genoemd in artikel 132a Sv. Ook de sturing -en wegingsinformatie (inclusief de preweeg) valt hieronder. Er hoeft dus nog geen sprake te zijn van een verdenking van een strafbaar feit.

De fase van toezicht, controle, handhaving, hulpverlening vallen echter buiten de scope van de matrix. Derhalve geeft de matrix geen antwoord op vragen waarbij een keuzemogelijkheid bestaat tussen toezicht en opsporing.
De matrix ziet op het verkrijgen van informatie, niet zozeer de verwerking van die informatie
Rode draad bij de beoordeling is de stelselmatigheid van handelen: de stelselmatigheid ziet op het verkrijgen van een min of meer volledig beeld van het privéleven van een persoon. Echter ook de combinatie van het verrichten van verschillende handelingen kan leiden tot stelselmatigheid (bijvoorbeeld: geautomatiseerd bekijken + bij herhaling bekijken, of meermalen bevragen + opslaan van gegevens).
Een beoordeling aan de hand van de matrix geldt ook bij het verkrijgen van gegevens van derden (dus niet: de derde partij dient dan de afweging te maken).
Openbaar internet bestaat niet! Het is niet zo dat als iets op internet staat (ook al heeft iemand dat er zelf op gezet) dat het daarmee openbaar is en dat je ermee kunt doen wat je wilt. Het feit dat iets "gewoon via google" te verkrijgen is, is niet relevant.
Het feit dat derden informatie over een datasubject op internet hebben geplaatst, maakt niet dat deze informatie voor de privacy afweging openbaar is.
Een site/app kan verschillende deelgebieden (onderdelen) hebben. Voor de verschillende handelingen binnen die deelgebieden dient tekens opnieuw een aparte afweging te worden gemaakt.
De verbaliseerplicht geldt altijd: vastleggen in het kader van verantwoording. Ook bij onderzoek op internet waarna wordt beslist niets met de gegevens te doen: ook dan geldt een verbaliseerplicht. "Uit onderzoek op internet is wel/niet gebleken dat" is onvoldoende. Wel juist is: met betrekking tot datasubject X zijn de twitter berichten van periode x t/m y nagetrokken. Daarbij is gebleken dat etc. (de opsporing dient achteraf verantwoording te kunnen afleggen wat de handeling was en wat het heeft opgeleverd). Het mag niet "te vaag" blijven welke handelingen de opsporing op internet heeft uitgevoerd.

Stelselmatig inwinnen

In november 2016 is de 'Brancherichtlijn SI op het internet
' vastgesteld. Deze brancherichtlijn is een leidraad voor de uitvoering van de bijzondere opsporingsbevoegdheid van het stelselmatig inwinnen van informatie op internet. Deze brancherichtlijn schrijft voor dat de opsporingsambtenaren die betrokken zijn bij de uitvoering van SI op het internet door de opsporingsdienst daartoe aangewezen en gecertificeerd zijn.

Status: gevalideerd (17-11-2016)
Bijgewerkt op: 17 november 2016

Belastingdienst

Inleiding
Momenteel loopt de aanbesteding voor Social media Monitoring en Analyse (SMMA) en Publishing & Engagement (P&E). De nieuwe contracten voor deze webdiensten worden 19 december a.s. afgesloten. De afgelopen periode hebben medewerkers van IM, B/CA, B/CAO, B/CIE en de business tijdens verschillende meetings gesproken over het beheerproces, die hebben geresulteerd in dit voorstel.

Hieronder gaan we verder in op de activiteiten die bij het beheer horen en doen een voorstel voor de inrichting. De volgende activiteiten komen aan de orde:

- Gebruikersbeheer
- Incidentproces
- Contractmanagement
- Technische gebruikers wensen

Huidige situatie beheer
Voor SMMA gebruikt de Belastingdienst op dit moment Coosto. Het beheer van Coosto wordt uitgevoerd door enkele medewerkers van het ISC. Vervolgens is het aan de supergebruikers van de verschillende organisatieonderdelen om dit voor hun eigen gebied verder in te richten. De FIOD werkt in een afgescheiden omgeving. Zij zijn verantwoordelijk voor hun eigen beheer.

Voor P&E zet de Belastingdienst de webdienst OBI4wan in. De enige gebruiker van OBI4wan is het webcareteam van de BelastingTelefoon. Zij zijn verantwoordelijk voor hun eigen beheer.

Nieuwe situatie beheer
Bij het inrichten van het nieuwe beheerproces is rekening gehouden met de volgende voorwaarden:

- Het beheer van de webdiensten SMMA en P&E wordt overgedragen aan B/CAO team MCC.
- Omdat de FIOD in een afgeschermde omgeving werkt, voeren zij het beheer voor SMMA zelf uit.

We hebben het hierboven voornamelijk over het beheer op het hoogste admin niveau. Op dit niveau kunnen supergebruikers worden aangewezen die voor hun eigen organisatieonderdeel rollen en accounts toekennen. Daarnaast voeren zij zelf de projecten op. Hierbij moeten er goede afspraken worden gemaakt over de te verdelen accounts per organisatieonderdeel.

Met het team MCC van B/CAO is afgesproken dat zij het beheer uitvoeren (hoogste niveau admin). Zij kunnen supergebruikers toekennen, die vervolgens beheerrechten krijgen voor hun eigen omgeving. Het toekennen van nieuwe supergebruikers zal in overleg plaatsvinden met de huidige groep supergebruikers. Op korte termijn worden overleggen gepland tussen het MCC en het ISC (en andere supergebruikers) om over de beheerwerkzaamheden spreken.

IM FIOD heeft aangegeven dat zij verantwoordelijk willen zijn voor hun eigen functioneel beheer.

Incidentproces
Voor de huidige webdiensten SMMA en P&E is geen intern incidentproces ingericht bij B/CIE. De externe leveranciers (Coosto en OBI4wan) bieden nu de mogelijkheid aan om de gebruiker direct (via de website) te laten communiceren over een verstoring. Dit werkt snel en is praktisch.

Het is de bedoeling om deze werkwijze in stand te houden. Daarnaast heeft de gebruiker ook de mogelijkheid om bij een verstoring met [redacted] contact op te nemen. Met B/CIE zijn hierover goede afspraken gemaakt. Incidenten van gebruikers worden na analyse bij [redacted] direct doorgezet naar de externe leverancier.

De leverancier is verantwoordelijk voor de rapportage over vragen/incidenten. De contractmanager (Vendormanagement) maakt hierover afspraken met de externe leverancier.

Contractmanagement, licentiebeheer en changemanagement
Afspraken en wijzigingen in het contract worden uitgevoerd door de contractmanager van B/CAO. De contractmanager (Vendormanagement) voert i.s.m. B/CFD Inkoop gesprekken hierover met de externe dienstenleveraar.

Wijzigingen die het contract raken of waarbij budget een rol speelt worden via het gebruikelijke impulsenproces opgepakt, waarbij IM Toezicht een lead rol heeft.

Technische gebruikerswensen
Het is goed om hier twee vlakken te onderscheiden: operationeel en tactisch. Operationeel vlak: de supergebruiker voert gesprekken met de leverancier over onderwerpen die passen binnen het contract. Om dit te bewaken zal met de leverancier moeten worden afgesproken dat de contractmanager wordt ingelicht als het contract wordt geraakt.

Tactisch vlak: gesprekken over onderwerpen die het contract raken (bijvoorbeeld nieuwe functionaliteiten/modules) worden namens de Belastingdienst gevoerd door de contractmanager i.s.m. B/CFD Inkoop. Naast IM Toezicht en de opdrachtmanager zullen ook de supergebruikers (inhoudsdeskundigen) hierbij worden betrokken.

Ter verduidelijking zijn de verschillende processen in beeld gebracht. Zie daarvoor bij de bijlage.

24

Overeenkomst inzake

IUC16-017

Perceel 1: Sociale Media Monitoring & Analyse
Perceel 2: Sociale Media Engagement & Interactie

Contractnummer: 5600006661

De ondergetekenden:

1.De Staat der Nederlanden, gevestigd te Den Haag, te dezen vertegenwoordigd door de *Staatssecretaris van Financiën, voor deze, de Belastingdienst/Centrum voor Facilitaire* Dienstverlening (B/CFD), Directeur IUC Belastingdienst,

hierna te noemen: Opdrachtgever,

en

2.Coosto B.V., (statutair) gevestigd te Eindhoven, te dezen vertegenwoordigd door Directeur,

hierna te noemen: Wederpartij,

Overwegende dat:

Organisatie en doelstelling van Opdrachtgever

a. Opdrachtgever verantwoordelijk is voor heffen en innen van belastingen en premies, alsook de uitkering van inkomensafhankelijke toeslagen, het opsporen van fiscale, economische en financiële fraude, het houden van toezicht op de invoer, uitvoer en doorvoer van goederen en het toezicht houden op de naleving van fiscale wetten en regels.

b. Perceel 1: Om effectief te kunnen handhaven (Belastingen/ Toeslagen/ Douane) en opsporen (FIOD) is het essentieel dat men doelgroepen zoals belastingplichtigen, toeslaggerechtigden (subjecten) en goederen (objecten) en diens omgeving goed in beeld heeft en houdt. Data uit sociale media wordt gebruikt voor het maken van trend-, fenomeen- en imagoanalyses. Al deze inzichten en analyses zijn van essentieel belang en worden ingezet in de diverse projecten en taken van handhaving, toezicht en opsporing.

   Perceel 2: Webcare is ook een belangrijke taak waarbij social media wordt gebruikt. Met Webcare antwoordt een organisatie op vragen, verstrekt ze informatie en lost ze klachten op. Dat doet de organisatie zowel reactief als op eigen initiatief. Opgedane inzichten over producten, diensten en/of serviceverlening worden intern teruggekoppeld aan relevante personen en/of afdelingen.

c. Opdrachtgever in verband met hetgeen hiervoor onder a en b is overwogen, tot aanbesteding van levering van diensten bestaande uit een webbased oplossing, die minimaal moet voorzien in de functionaliteiten met betrekking tot Sociale Media en die in samenhang functioneren, inclusief aanverwante dienstverlening als gespecificeerd in het

Paraaf Opdra

Paraaf Wederpartij

Beschrijvend document, ten behoeve van de Belastingdienst door middel van een Europese openbare aanbestedingsprocedure, is overgegaan;

d. In Bijlage A van het Beschrijvend Document - de omschrijving van de Opdracht – staat uitgebreid omschreven wat onder Social Media Monitoring & Analyse en Social Media Engagement & Interactie moet worden verstaan.

e. op 23 september 2016 door of namens Opdrachtgever een aankondiging naar het Supplement op het Publicatieblad van de Europese Unie (hierna: Publicatieblad) is verzonden en dat deze aankondiging is gepubliceerd onder nummer IUC16-017 en *2016/S 187-336553*;

f. Opdrachtgever de doelstellingen en omgeving, waarbinnen de Dienst gaat en moet functioneren, heeft vastgelegd in het de het Beschrijvend Document (ook wel Bestek genoemd) met kenmerk IUC16-017.

g. Wederpartij de economisch meest voordelige aanbieding op 3 november 2016 heeft ingediend, zodat de opdracht aan hem is gegund bij brief van 25 november 2016, met kenmerk IUC/94/16/810/BS.

h. Opdrachtgever geen bezwaar heeft ontvangen tegen de gunning aan Wederpartij.

i. Naar aanleiding hiervan Opdrachtgever de opdracht definitief heeft gegund aan Wederpartij en zijn Partijen deze Overeenkomst aangegaan voor het uitvoeren van bovengenoemde werkzaamheden.

j. Opdrachtgever thans de onderhavige Overeenkomst met Wederpartij wenst te sluiten om de wederzijdse rechten en verplichtingen vast te leggen van de onder de hierboven genoemde dienstverlening.

k. Deze Overeenkomst tot stand is gekomen op basis van de Modelovereenkomst ARBIT 2016.

Paraaf Opdrac

Paraaf Wederpartij

INHOUDSOPGAVE

Paraaf Opdra

Paraaf Wederpartij

26

Komen overeen:

Artikel 1. Begrippen

1.1 In de Overeenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan is gegeven in de Voorwaarden.

1.2 In aanvulling op, of in afwijking van, de begrippen als omschreven in artikel 1 van de Voorwaarden, hanteert Opdrachtgever begrippen nader omschreven in Bijlage 1 van het Beschrijvend Document. Deze begrippen maken eveneens onderdeel uit van deze Overeenkomst.

1.3 Voor zover de gehanteerde begrippen met elkaar in tegenspraak zijn gelden de begrippen in Bijlage 1.

1.4 Het begrip Prestatie wordt gebruikt in deze Overeenkomst onder verwijzing naar de betekenis die het toekomt aan de hieraan gegeven Voorwaarden. Voor de duidelijkheid: Onder het begrip Prestatie dient het begrip Diensten en Oplossing in Bijlage 1 van het Beschrijvend Document te worden verstaan.

1.5 Het begrip Beschrijvend Document (met kenmerk IUC16-017) wordt gebruikt in deze Overeenkomst in plaats van het begrip Bestek. De begrippen hebben qua strekking en inhoud dezelfde betekenis.

Artikel 2. Voorwerp van de Overeenkomst

2.1 Partijen sluiten hierbij een Overeenkomst waarbij Wederpartij zich verbindt tegen de in artikel 12 bedoelde Vergoeding tot het verrichten van de Prestatie zoals beschreven in het Beschrijvend Document en de daarbij behorende Bijlagen (met name Bijlage A), behorend bij deze Overeenkomst.

2.2 De Prestatie bestaat in hoofdlijnen uit de levering van Diensten waaronder in ieder geval moet worden verstaan het krachtens deze Overeenkomst ten behoeve van de Opdrachtgever te verrichten werkzaamheden, waaronder mede wordt verstaand de resultaten van de Dienst, waaronder in ieder geval wordt verstaan:

- een SaaS (Software as a service) oplossing, die minimaal voorziet in de functionaliteiten met betrekking tot de Sociale Media Dienst (Hierna te noemen: de Oplossing)
- Ondersteuning bij Implementatie en Migratie
- Beheer en Onderhoud
- Opleiding (inclusief het leveren van lesmateriaal ten behoeve van de Implementatie en migratie
- Verbetervoorstellen op verzoek van de Belastingdienst
- Additionele diensten, waaronder in ieder geval, maar niet limitatief, consultancy, opleidingen en changes tijdens de operationele fase van Overeenkomst.

2.3 De omvang van de Oplossing staat omschreven in het Beschrijvend document. Het betreft qua Gebruikersgroepen:
- Perceel 1: Handhavings –en opsporingsmedewerkers
- Perceel 2: webcare medewerkers
één en ander teneinde Opdrachtgever in staat te stellen daarvan het overeengekomen gebruik te maken.

2.4 De navolgende stukken vormen gezamenlijk de Overeenkomst. Voor zover deze stukken met elkaar in tegenspraak zijn, prevaleert het eerder genoemde stuk boven het later genoemde:

1) dit document, met inbegrip van Bijlage A bij het Beschrijvend Document;
2) de Voorwaarden (BIJLAGE Voorwaarden);

Paraaf Opdr

Paraaf Wederpartij

3) het Beschrijvend Document, inclusief Bijlagen (BIJLAGE BESCHRIJVEND DOCUMENT);
4) de overige Bijlagen

2.5 de door Wederpartij aan Opdrachtgever uitgebrachte offerte van 3 november 2016.

Indien echter op grond van een lager gerangschikt stuk expliciet hogere eisen worden gesteld aan de Prestatie, dan gelden steeds die hogere eisen, tenzij in het hoger gerangschikt document is aangegeven dat, en ten aanzien van welk specifiek onderdeel, van het lager gerangschikte document wordt afgeweken.

Artikel 3. Additionele Diensten

3.1 Partijen kunnen gedurende de looptijd van deze Overeenkomst overeenkomen dat Additionele Diensten bij Wederpartij worden afgenomen.

3.2 De Additionele Diensten als bedoeld in artikel 3.1 dienen gerelateerd te zijn aan het onderwerp van deze Overeenkomst en de hieraan ten grondslag liggende aanbesteding.

3.3 De Additionele Diensten worden slechts uitgevoerd na schriftelijke uitvraag door Opdrachtgever, op basis van een door Opdrachtgever geaccepteerde offerte en/of op basis van een door de Wederpartij geaccepteerd projectplan conform de bepalingen in artikel 12 en 13 van deze Overeenkomst.

3.4 De bepalingen neergelegd in deze Overeenkomst zijn mede van toepassing op de overeenkomst(en) voor Additionele Diensten, tenzij één of meerdere bepalingen uit deze Overeenkomst in de overeenkomst(en) voor Additionele Dienstverlening uitdrukkelijk niet van toepassing zijn verklaard.

Artikel 4. Contactpersonen en rapportage

4.1 De personen die de contacten over de uitvoering van de Overeenkomst onderhouden zijn opgesomd in de BIJLAGE Contactpersonen.

4.2 Wederpartij rapporteert over de wijze van uitvoering van de Overeenkomst als bepaald in het Beschrijvend Document en nader uitgewerkt in het implementatieplan en de nader overeen te komen SLA gebaseerd op Service Levels zoals zijn opgenomen in Bijlage A van het Beschrijvend Document.

4.3 Partijen zullen in goed onderling overleg de inhoud en omvang van de rapportage bepalen.

Artikel 5. Inwerkingtreding en duur van de Overeenkomst

5.1 De Overeenkomst treedt in werking op 1 januari 2017, heeft een looptijd van 2 jaar en eindigt van rechtswege op 31 december 2018.

5.2 Opdrachtgever kan de Overeenkomst onder gelijkblijvende voorwaarden zes (6) keer voor een periode van één (1) jaar verlengen, waarbij Opdrachtgever tevens de mogelijkheid heeft om deze Overeenkomst niet in zijn geheel, maar slechts voor bepaalde Sociale Media aandachtsgebieden te verlengen.

De verleningsopties kunnen tevens flexibel afgenomen worden.

Indien Opdrachtgever van dit recht tot verlenging gebruik wenst te maken doet hij hiervan uiterlijk twee maanden voor het einde van de in artikel 5.1 bedoelde looptijd schriftelijk mededeling aan Wederpartij.

Paraaf Op

Paraaf Wederpartij

5.3 Opdrachtgever kan de Overeenkomst te allen tijde opzeggen met een opzegtermijn van 3 maanden. Hierbij is de tussen Partijen overeengekomen Retransitie bepaling en eventuele vergoeding van toepassing.

Artikel 6. Oplevering

6.1 Wederpartij draagt zorg voor Oplevering van de Prestatie conform het bepaalde in het Beschrijvend Document, inclusief Bijlagen.

Artikel 7. Acceptatie

7.1 Opdrachtgever is gerechtigd de Prestatie voorafgaand aan Acceptatie te testen,conform een nader te overeenkomen testplan en het door partijen overeengekomen implementatieplan en SLA. Wederpartij is verplicht zijn medewerking hieraan te verlenen.

Artikel 8. Eigendom van de gegevens

8.1 In aanvulling op artikel 18 van de Voorwaarden geldt dat alle gegevens, waaronder persoonsgegevens als bedoeld in de Wbp, die Opdrachtgever in het kader van de uitvoering van deze Overeenkomst ter beschikking stelt van Wederpartij eigendom blijven van Opdrachtgever.

8.2 Wederpartij is verplicht tot geheimhouding van de gegevens, waaronder persoonsgegevens, die hem in het kader van de uitvoering van deze Overeenkomst ter beschikking worden gesteld.

8.3 In aanvulling op het in artikel 32 Exitclausule van de Voorwaarden bepaalde, rust op Wederpartij bij beëindiging van de Overeenkomst de verplichting zorg te dragen voor de digitale teruglevering van de gegevens (inclusief metadata) aan Opdrachtgever binnen 24 klokuren. Het formaat van deze digitaal teruggeleverde gegevens voldoet aan Open Standaarden.

8.4 Na ontvangst, verificatie en goedkeuring van de verstrekte gegevens in dit format door Opdrachtgever, dient Wederpartij alle gegevens (inclusief metadata) van Opdrachtgever die nog in kopie op zijn systemen staan, binnen 24 klok uren onherstelbaar te vernietigen en, indien door Opdrachtgever gewenst, een gecertificeerde verklaring van vernietiging aan Opdrachtgever te verstrekken.

Artikel 9. Garantie

In aanvulling op artikel 12 van de Voorwaarden garandeert Wederpartij tenminste gedurende de looptijd van deze Overeenkomst, inclusief eventuele verlengingen en tijdens de benodigde migratieperiode dat:

9.1 de gegevens, waaronder begrepen persoonsgegevens, slechts mogen worden verwerkt binnen de Europese Economische Ruimte (EER);

9.2 het transport van gegevens, waaronder persoonsgegevens, te allen tijde versleuteld plaatsvindt, waarbij de versleuteling, voor zover niet reeds specifiek voorgeschreven door Opdrachtgever, tenminste voldoet aan de stand der techniek die in de relevante markt gebruikelijk is;

9.3 bij de Prestatie gebruik wordt gemaakt van een oplossing waarbij een doorlopende back-up wordt gegarandeerd van alle gegevens en persoonsgegevens die deel uitmaken van de Prestatie;

9.4 hij, in aanvullling op het gestelde in artikel 18.2 van de Voorwaarden, bij elk datalek, als bedoeld in de Wet bescherming persoonsgegevens (Wbp),

Paraaf O

Paraaf Wederpartij

Opdrachtgever informeert en tevens passende organisatorische en technische maatregelen treft om verdere lekken te voorkomen en de schade als gevolg van het opgetreden lek te beperken;

9.5 Wederpartij de verstrekte gegevens,waaronder persoonsgegevens, niet verwerkt buiten de Europese Economische Ruimte (EER), noch de gegevensverwerking aan een derde partij uitbesteedt, zonder voorafgaande schriftelijke toestemming van Opdrachtgever, waarbij Opdrachtgever gerechtigd is om aanvullende maatregelen te eisen. Deze aanvullende maatregelen zijn in het belang van de bescherming van de persoonlijke levenssfeer van de betrokken personen wier gegevens worden verwerkt, hetzij in het belang van Opdrachtgever als rechthebbende en verantwoordelijke ten aanzien van de Gegevens, waaronder persoonsgegevens.Wederpartij verschaft op eerste verzoek inzicht in de locatie(s) waar de gegevensbewerking plaatsvindt of heeft plaatsgevonden. Voorzover Opdrachtgever instemt met de inschakeling van subbewerkers, geldt in ieder geval dat deze derden onverkort gehouden zijn aan de in dit artikel opgenomen verplichtingen.

9.6 Wederpartij garandeert de gegevens van Opdrachtgever worden opgeslagen in een "dedicated database" ten behoeve van Opdrachtgever.

Artikel 10. Procedure gegevensvordering

10.1 Indien Wederpartij benaderd wordt door buitenlandse overheidsdienst(en) met het verzoek Gegevens of persoonsgegevens over te dragen waarover hij in het kader van deze Overeenkomst beschikt, volgt hij onderstaande procedure.

10.2 Wederpartij informeert Opdrachtgever onverwijld door middel van een schriftelijke kennisgeving indien hij een verzoek, als bedoeld in artikel 10.1, heeft ontvangen. Wederpartij verklaart zich bereid om de behandeling van het verzoek over te laten aan Opdrachtgever en desgevraagd de redelijkerwijs benodigde medewerking aan Opdrachtgever te verlenen, het verstrekken van volmachten daarbij begrepen om het verweer voor zover nodig in naam van Wederpartij te voeren.

10.3 Voor zover het Wederpartij niet is toegestaan Opdrachtgever te infomeren over het verzoek, geldt dat Wederpartij verplicht is;

a. het verzoek van de buitenlandse overheidsdienst(en) juridisch inhoudelijk te (laten) toetsen teneinde te verifiëren of het verzoek conform alle wettelijke vereisten bevoegdelijk is afgegeven;

b. te onderzoeken of het verzoek betrekking heeft op de afgifte van persoonsgegevens in de zin van de Wbp;

c. na te gaan op welke betrokkene het verzoek betrekking heeft;

d. te beoordelen of het land waarnaar de persoonsgegevens doorgegeven dienen te worden een passend beschermingsniveau waarborgt als bedoeld in de Wbp. Voor zover dit niet het geval is, dienst Wederpartij na te gaan of sprake is van een grondslag in de Wbp op basis waarvan doorgifte toch is toegestaan;

e. met de buitenlandse overheidsdienst(en) in overleg te treden, indien geen sprake lijkt te zijn van een rechtmatige grondslag voor de doorgifte van persoonsgegevens. Het overleg moet erop gericht zijn om alternatieve mogelijkheden te verkennen teneinde te allen tijde in overeenstemming met de Wbp te handelen en de omvang van de te verstrekken persoonsgegevens zo beperkt mogelijk te houden. Waar mogelijk zal Wederpartij zich voor advies wenden tot de Autoriteit Persoonsgegevens;

f. (in rechte) bezwaar te maken tegen het verzoek, alsmede tegen het verbod om Opdrachtgever hierover te informeren.

Paraaf Opd

Paraaf Wederpartij

10.4 Indien Wederpartij besluit gehoor te geven aan een verzoek tot verstrekking van persoonsgegevens door een buitenlandse overheidsdienst, zal Wederpartij in elk geval;

- de Gegevens zo veel als mogelijk ontdoen van (direct en indirect) identificerende kenmerken en deze gegevens slechts op geaggregeerd niveau aanbieden;
- geen bijzondere persoonsgegevens in de zin van de Wbp verstrekken;
- slechts de hoogstnodige Gegevens verstrekken ter voldoening aan het verzoek;
- voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van betrokkenen wier gegevens worden verwerkt niet onevenredig wordt geschaad;
- Opdrachtgever onmiddellijk informeren zodra dit is toegestaan.

10.5 In alle gevallen geldt dat Wederpartij onder geen beding mag afzien van verweer en evenmin met betrekking tot het verzoek een schikking aangaat, zonder voorafgaande schriftelijke toestemming van Opdrachtgever. Het informeren van betrokkenen vindt uitsluitend plaats via Opdrachtgever.

Artikel 11. Informatiebeveiliging

11.1 In aanvulling op het bepaalde in artikel 19 van de Voorwaarden geldt dat de wijze van werken bij Opdrachtgever met betrekking tot de vertrouwelijkheid van gegevens en het waarborgen van integriteit onder andere is vastgelegd in de brochure Business etiquette van de Belastingdienst. Wederpartij verplicht zich te houden aan de inhoud van dit document en draagt er tevens zorg voor dat het beveiligingsniveau van de Prestatie als beschreven in het Bestek niet wordt aangetast.

11.2 De naleving van de beveiligingseisen is tevens onderworpen aan internationale standaarden waarbij Wederpartij voldoet aan ISO/IEC 27001 en 27002 Informatiebeveiliging of gelijkwaardig. Wederpartij verbindt zich voorts om de beheersmaatregelen op te volgen.

Artikel 12. Vergoeding

12.1 Partijen komen de navolgende Vergoeding overeen. Alle met de Prestatie gemoeide kosten zijn verwerkt in de Vergoedingen, tenzij anders vermeld.

12.2 De door Wederpartij geoffreerde Vergoedingen met betrekking tot de Implementatie zijn vast. Slechts Meerwerk komt voor extra Vergoeding in aanmerking. Meerwerk wordt verrekend op basis van het door Wederpartij geoffreerde Implementatie tarief en geschiedt op nacalculatie van daadwerkelijk bestede uren.

12.3 De door Wederpartij geoffreerde Vergoedingen met betrekking tot de Oplossing en de Additionele diensten zijn vast gedurende de initiële looptijd (2 jaar) van de Overeenkomst, exclusief eventuele verlengingen.

12.4 De geoffreerde Vergoedingen met betrekking tot de Oplossing en de Additionele Diensten kunnen tijdens de verlenging van de Overeenkomst jaarlijks per 1 januari geïndexeerd worden op basis van de indexering "Zakelijke dienstverlening; omzetontwikkeling, index 2010 = 100". Uitgangspunt voor de tariefstijging is de ontwikkeling van deze index gedurende de periode november n-1 t/m oktober jaar n voorafgaand aan de genoemde datum van 1 januari voor prijsindexering. Het percentage voor de prijsstijging wordt afgerond op één decimaal achter de komma.

Prijsstijging per	Ontwikkeling index
10.1.c en 10.2.b	

Paraaf Opd

Paraaf Wederpartij

31

10.1.c en 10.2.b

12.5 De Opdrachtnemer dient voor 1 december voorafgaande aan de genoemde momenten van prijsindexering een schriftelijk verzoek, met bijbehorende onderbouwing, in om voor indexering in aanmerking te komen.

12.6 Kosten die niet in de inschrijving genoemd worden en niet verdisconteerd zijn in de prijssstelling, maar toch noodzakelijk blijken te zijn voor het goed functioneren van de Diensten conform de in het Bestek gestelde eisen en de in de Inschrijving opgenomen beantwoording van de wensen, zijn voor rekening van Wederpartij. Indien Opdrachtgever kosten moet maken die noodzakelijk blijken te zijn voor een goed functioneren van de Diensten, zijn deze voor rekening van Wederpartij.

Artikel 13. Facturering, verschuldigdheid en betaling

13.1 In aanvulling op de artikelen 14 tot en met 16 van de Voorwaarden geldt dat Wederpartij verplicht is om elektronisch te factureren. De facturen dienen voorzien te zijn van de gegevens als bedoeld in artikel 13.2 en ingediend te worden conform de eisen als vermeld in het Bestek.

13.2 De factuur wordt door Wederpartij voorzien van datum, het overeenkomst nummer, het nummer van de inkoopopdracht (voor zover van toepassing), hoogte van de Vergoeding en andere door Opdrachtgever schriftelijk aan Wederpartij kenbaar gemaakte gegevens. Bij niet-, of niet correcte,vermelding van één of meer gegevens wordt de betalingsverplichting opgeschort totdat de bedoelde gegevens correct zijn vermeld. Facturen die niet voldoen aan de hiervoor gestelde eisen neemt Opdrachtgever niet in behandeling. In zo'n geval wordt de factuur per omgaande retour gezonden met het verzoek een nieuwe en verbeterde versie te sturen, waarbij de factuurdatum wordt aangepast aan de datum van verzending van de factuur. Wederpartij accepteert een betalingstermijn van 30 dagen na ontvangst van een correcte factuur .

13.3 De in artikel 13.2 bedoelde opschorting van de betaling, alsook de opschorting in geval van betwisting van de factuur, geeft Wederpartij niet het recht zijn Prestatie op te schorten.

13.4 De facturering van eenmalige Vergoedingen (Implementatie en Additionele Diensten) vindt plaats na Acceptatie van de Prestatie.

13.5 De facturering van periodieke Vergoedingen (abonnement, Beheer en Onderhoud) vindt plaats per jaar, voorafgaand aan de levering van deze periodieke Prestatie.

De peildatum voor deze Prestatie is de datum waarop het aantal Gebruikers of medewerkers van de Belastingdienst door de Belastingdienst vastgesteld wordt. Als peildatum wordt aangehouden 1 januari van het jaar waarop de Vergoeding betrekking heeft.

Artikel 14. Algemene en bijzondere voorwaarden

14.1 De toepasselijkheid van algemene en bijzondere voorwaarden van Wederpartij dan wel van door Wederpartij bij het verrichten van de Prestatie te betrekken derden, is uitgesloten.

Paraaf Opd

Paraaf Wederpartij

14.2 In afwijking van artikel 14.1 en onverminderd het bepaalde in artikel 2, zijn tevens de licentievoorwaarden van Wederpartij dan wel van door Wederpartij bij het verrichten van de Prestatie te betrekken derden van toepassing indien en voor zover:
- de toepasselijkheid daarvan niet in het Beschrijvend Document is uitgesloten;
- Wederpartij (a) de toepasselijkheid daarvan expliciet heeft bedongen (b) een exemplaar van de betreffende voorwaarden bij de Offerte is gevoegd en (c) deze daarvan expliciet onderdeel uitmaken, en;
- het Overeengekomen gebruik daardoor niet wordt uitgesloten of beperkt en;
- Wederpartij kan aantonen dat de rechten van Opdrachtgever uit hoofde van de Overeenkomst daardoor niet worden verminderd dan wel diens uit de Overeenkomst voortvloeiende verplichtingen daardoor niet onredelijk worden verzwaard.

14.3 De voor het gebruik van de Prestatie vereiste acceptatie van algemene of bijzondere voorwaarden, zoals bijvoorbeeld bij "shrink-wrap"- en "click-wrap" licenties, bindt Opdrachtgever niet. Wederpartij vrijwaart Opdrachtgever dat dergelijke acceptaties niet leiden tot enige beperking op het Overeengekomen gebruik.

14.4 Een exemplaar van de Voorwaarden is bij de Overeenkomst gevoegd.

Artikel 15. Overige bepalingen

15.1 In afwijking van artikel 26, tweede lid van de Voorwaarden, geldt voor de hoogte van het aldaar genoemde bedrag, dat dit (neerwaarts) wordt bijgesteld tot een bedrag van 10.1.c en 10.2.b per gebeurtenis.

15.2 In afwijking van artikel 29, tweede lid van de Voorwaarden geldt dat het aldaar genoemde bedrag (neerwaarts) wordt bijgesteld tot een bedrag van 10.1.c 10.2.b - per aanspraak.

15.3 Aan artikel 11.4 van de Voorwaarden wordt de volgende zinsnede toegevoegd: "De nadere termijn als bedoeld in artikel 11.4 stelt Opdrachtgever in beginsel op 10 Werkdagen, tenzij partijen onderling een langere termijn zijn overeengekomen."

15.4 Aan artikel 17.4 van de Voorwaarden wordt de volgende zinsnede toegevoegd: "Voor zover Wederpartij t.a.v. deze gegevens een wettelijke bewaarplicht heeft, zal hij alle gegevens die het betreft, na ommekomst van deze wettelijke termijn, onverwijld aan Opdrachtgever ter beschikking stellen."

15.5 Aan artikel 22.1 van de Voorwaarden wordt de volgende zinsnede toegevoegd:"Wederpartij vervangt Personeel alleen na voorafgaande melding aan Opdrachtgever, mits, voor zover van toepassing, de vervanging voldoet aan de bij de Opdracht gestelde eisen. Inwerkkosten en andere kosten samenhangend met deze vervanging, zijn voor rekening van Wederpartij.

15.6 Aan artikel 30.1van de Voorwaarden wordt de volgende zinsnede toegevoegd: "Ontbinding in de zin van dit artikel werkt ex nunc, d.w.z. de ontbinding geldt alleen voor toekomstige verplichtingen."

15.7 De artikelen 56 tot en met 59 van de Voorwaarden (Ontwikkelingen Maatwerkprogrammatuur) zijn niet van toepassing.

15.8 De artikelen 60 tot en met 66 van de Voorwaarden (Detachering) zijn niet van toepassing.

15.9 De artikelen 43 lid 2 sub b, 43 lid 3 en 45 van de Voorwaarden zijn niet van toepassing.

15.10 In aanvulling op artikel 47 van de Voorwaarden geldt het volgende:

Paraaf Op

Paraaf Wederpartij

Indien de rechten van de uiteindelijke producten van de (Standaard)Programmatuur zich verzetten tegen het deponeren van de broncode, dan zal Wederpartij er in ieder geval voor zorgen dat:
· Maatwerkprogrammatuur en eventuele op maat gemaakte koppelingen wel in escrow kan worden gegeven;
· Wederpartij proactief zal meedenken met een oplossing waardoor de continuïteit voor de Opdrachtgever zoveel mogelijk gewaarborgd wordt, ook met betrekking tot Standaardprogrammatuur van derden.

Aldus overeengekomen op 23 december 2016 en ondertekend in tweevoud door:

OPDRACHTGEVER	WEDERPARTIJ
Naam:	Naam:
Functie: Directeur IUC	Functie: Directeur
Handtekening:	Handtekening:
Datum: 23 december 2016	Datum: 23 december 2016

Paraaf O

Paraaf Wederpartij

BIJLAGE Beschrijvend Document

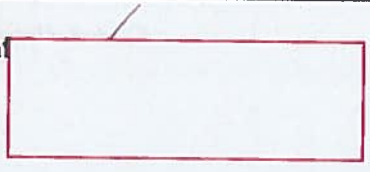
Is openbaar gemaakt in het kader van de tender. Zie:
https://www.tenderned.nl/tenderned-tap/aankondigingen/90885

BIJLAGE Contactpersonen

Opdrachtgever
De <*functie*>, thans <*naam*> is bevoegd Opdrachtgever te binden voor zover het betreft de uitvoering van de Overeenkomst.

Wederpartij
De <*functie*>, thans <*naam*> is bevoegd Wederpartij te binden voor zover het betreft de uitvoering van de Overeenkomst.

Paraaf



Paraaf Wederpartij

BIJLAGE Voorwaarden
<Voorwaarden invoegen>

BIJLAGE SERVICE LEVEL AGREEMENT

Coosto BV

www.coosto.com

Service Level Agreement Coosto B.V., Eindhoven, Nederland

Versie 1

Inhoud

KvK nr. 58 88 07 71
BTW nr. NL 8532 21 510 B01
IBAN NL34ABNA0599133058

COOSTO

1. **Beschrijving Dienst**

Coosto is een Social Media Monitoring web-oplossing (SaaS) waarmee de Afnemer toezicht kan houden op hun merk en reputatie, waarmee gereageerd kan worden op vragen en leads en waarmee Social Media content gepubliceerd kan worden.

2. **Beschrijving Service Level Agreement (SLA)**

Gedurende de looptijd (Serviceperiode) van de toepasselijke overeenkomst ("Gebruikersovereenkomst") van de Dienstverlener is de Dienst tenminste gedurende 10.1.c, 10.2.g (Beschikbaarheidspercentage) van een kalendermaand (24 uur per dag / 7 dagen per week) operationeel en beschikbaar voor de Afnemer.

De Dienst dient snel en flexibel een grote hoeveelheid (meer dan één miljoen Berichten met hun reacties per dag) social media data te kunnen bevragen. Het aantal Nederlandstalige en op Nederland gerichte bronnen waaruit deze data afkomstige zijn, omvat minimaal 350.000 bronnen. Voor het aantal internationale bronnen is de minimale eis meer dan één miljoen. Bronnen moeten uit, minimaal, de volgende brontypen afkomstig zijn: Twitter, Facebook, YouTube, LinkedIn, Pinterest, Instagram, Google+, media (RTV), nieuws, blogs en fora.

Wanneer de Dienstverlener niet voldoet aan deze SLA en wanneer de Afnemer voldoet aan de verplichtingen van deze SLA, komt de Afnemer in aanmerking voor de hieronder beschreven Servicetegoeden. Deze SLA beschrijft de enige vorm van genoegdoening voor de Afnemer wanneer de Dienst verlener op enig moment niet voldoet aan deze SLA.

3. **Beschikbaarheid**

Het Beschikbaarheidspercentage wordt per maand als volgt berekend, met daarbij alle tijden in minuten:

10.1.c, 10.2.g

4. Gepland Onderhoud

1. Onder Gepland Onderhoud wordt al het werk verstaan dat volgens planning van de Dienstverlener plaatsvindt en een onderbreking van de Service tot gevolg heeft.

2. Dienstverlener zal Gepland Onderhoud uitvoeren tussen 10.1.c, 10.2.g CET).

3. Gepland Onderhoud zal 10.1.c, 10.2.g voorafgaand aan het onderhoud aan Afnemer kenbaar gemaakt worden. Noodonderhoud is hierop een uitzondering en kan op kortere termijn uitgevoerd en gecommuniceerd worden.

5. Snelheid Dienst

Het gaat hier om de reactietijd van de geleverde Dienst. Vertragingen die volledig zijn toe te wijzen aan netwerkcommunicatie tellen hierin niet mee.

1. Reactietijden

De Dienst kan zodanig ingericht worden dat, bij hierboven genoemd aantal gebruikers, onderstaande performance-eisen gerealiseerd kunnen worden:

- In 99 % van de gevallen is de handeling van een gebruiker in de Dienst binnen 2 seconden afgerond.
- Het uitvoeren van een zoekopdracht (= filteren) kost in 99 % van de gevallen maximaal 10 seconden, de overige 1 % mag niet langer dan 20 seconden duren.
- Het exporteren van tekst kost in 99% van de gevallen maximaal 10 seconden, de overige 1% mag niet langer dan 20 seconden duren.
- Het exporteren van video en/of afbeeldingen kost in 99% van de gevallen in maximaal 60seconden, de overige 1 % mag niet langer dan 180 seconden duren.
- Het opstellen van de rapportage kost in 99% van de gevallen maximaal 10 seconden, de overige 1 % mag niet langer dan 20 seconden duren.
- Bij bewerkingen die langer dan 2 seconde duren wordt een wacht- of voorgangsindicator getoond, zodat het voor de gebruiker duidelijk is dat de Dienst bezig is.

6. Efficiency

1. Er mag maximaal 1 minuut tijdsvertraging zitten tussen het online plaatsen van een origineel bericht op een Belastingdienst account en het moment waarop dit bericht voor de behandelaar zichtbaar is.

2. Er mag maximaal 1 minuut tijdsvertraging bestaan tussen het online plaatsen van een origineel bericht op een bron en het moment waarop dit bericht verschijnt in een zoekopdracht.

3. Er mag maximaal 1 minuut tijdsvertraging bestaan tussen het versturen door de Belastingdienst van een bericht of antwoord en plaatsing op de originele bron.

4. Er kunnen minimaal 100 gebruikers gelijktijdig ingelogd zijn.

5. Op jaarbasis kunnen minimaal 200.000 berichten verwerkt worden.

6. Op jaarbasis kunnen minimaal 5.000 proactieve berichten worden verstuurd.

7. Op dagbasis kunnen minimaal 1.000 berichten verstuurd worden en kunnen minimaal 10.000 berichten ontvangen worden.

8. In 99 % van de gevallen is de handeling van een gebruiker in de webdienst binnen 2 seconden afgerond.

9. Status- en voortgangsinformatie van berichten is inzichtelijk en ook wie, wanneer, wat, welk bericht, heeft behandeld.

10. Eveneens wordt gelogd wie wanneer wat heeft gewijzigd voor interne instellingen, zoals het instellen van zoekopdrachten en het toekennen van autorisaties.

7. Incidentmanagement en Helpdesk Contact

1. Dienstverlener onderscheidt de volgende incidentclassificaties en wijze van contact:

Urgentie	Impact	Contact
10.1.c, 10.2.g		

10.1.c, 10.2.g

2. Reactie- en Oplostijden

Reactietijd: de tijd tussen het melden van een incident door de Afnemer en het bevestigen aan de Afnemer dat de melding binnengekomen is.

Oplostijd: de maximale tijd tussen het vaststellen van een incident en het oplossen van het incident.

Dienstverlener hanteert de volgende reactie- en oplostijden:

Urgentie	Reactietijd	Maximale Oplostijd
10.1.c en 10.2.g		

10.1.c en 10.2.g

8. **Performance**

Dienstverlener draagt zorg voor marktconforme prestaties van de Dienst, waaronder wordt verstaan:

1. Nieuw gepubliceerde Social Media berichten zullen binnen 10.1.c en 10.2.g in de Dienst zichtbaar zijn.

2. De Dienstverlener zal de hierboven beschreven performance waarborgen tot 10.1.c en 10.2.g
10.1.c en 10.2.g

3. Dienstverlener is niet aansprakelijk voor verminderde prestaties bij vertragingen en/of ontbrekende data als gevolg van het disfunctioneren van de service van derde partijen.

9. **Attack and Penetration**

Attack and Penetrations (A&P) tests worden uitgevoerd.

10. **Service Level Rapportage (SLR)**

De Service Level Rapportage wordt 10.1.c 10.2.g toegestuurd. De rapportage omvat:

10.1.c en 10.2.g

11. **Servicetegoed**

10.1.c, 10.2.b en 10.2.g

1. Serviceverlener hanteert de volgende Servicetegoeden:

10.1.c, 10.2.b en 10.2.g

10.1.c, 10.2.b en 10.2.g

2. 10.1.c, 10.2.b en 10.2.g

3.

12. **Beveiliging**

De Opdrachtnemer en de Dienst voldoen aan beveiligingseisen zoals beschreven in ISO27001 en 27002 of gelijkwaardig en daarnaast gedurende de gehele looptijd van de overeenkomst te voldoen aan de laatste versies aan de beveiligingseisen zoals beschreven in de volgende bijlage:

Bijlage 'ICT-Beveiligingsrichtlijnen voor Webapplicaties- Richtlijnen - leesversie-3'.pdf (NCSC richtlijnen, september 2015); NCSC staat voor National Cyber Security Centrum.

13. **Contract management**

De Opdrachtgever is voornemens om contractmanagement in te richten inzake de beoogde Overeenkomst. Contractmanagement wordt omschreven als het op tactisch en operationeel niveau managen van alle contractueel vastgelegde verantwoordelijkheden, verplichtingen, procedures, afspraken, voorwaarden en tarieven rond een bepaalde overeenkomst plus het managen van alle onduidelijkheden. De Opdrachtgever heeft haar ambitie op het gebied van contractmanagement vertaald in de navolgende activiteiten:

1. Het proactief managen van alle afspraken, verplichtingen, voorwaarden, aannames, verwachtingen en doelstellingen met betrekking tot het contractueel bepaalde tussen Opdrachtgever en Opdrachtnemer.

2. Het elimineren van gebreken, hiaten, onduidelijkheden en verschil van interpretatie in de onder 1 genoemde aspecten.

3. Het volgens afspraak of op verzoek tijdig (laten) verschaffen van zo correct mogelijke informatie met betrekking tot status, voortgang, financiën, risico's, besluiten, acties en openstaande issues tussen Inschrijver aan Opdrachtgever.

4. Het organiseren, voeren en administreren van het noodzakelijke overleg tussen Opdrachtgever en Opdrachtnemer.

5. Het managen van niet contractueel vastgelegde, maar voor partijen wel belangrijke aspecten of nevendoelstellingen.

6. Contractmanagement kan pas tot goede resultaten leiden als betrokken partijen op een proactieve en transparante wijze invulling geven, respectievelijk bijdragen, aan deze activiteiten.

7. Coosto onderschrijft bovengenoemde contractmanagementactiviteiten en zal zich gedurende de contractperiode verbinden aan de samen vastgestelde uitkomsten van bovengenoemde activiteiten. Coosto stelt zich daarbij meedenkend op.

Belastingdienst

26

PIA SOC

Privacy Impact Assessment

Social Media Monitoring

Colofon

Titel	Privacy Impact Assessment Social Media Monitoring
Projectnummer / Release / Programma	0.9
Versienummer	Zie documenthistorie
Documentlocati	
Contactpersoon	

Inleiding

Doel van dit document

De Privacy Impact Assessment (PIA) legt in eerste plaats de risico's bloot van projecten die mogelijk inbreuk maken op het recht op informationele privacy en draagt bij aan het vermijden of verminderen van deze privacy risico's. Op basis van de antwoorden van de PIA wordt op systematische wijze inzichtelijk gemaakt of er een kans is dat inbreuk wordt gemaakt op het recht op informationele privacy van betrokkene, hoe groot deze inbreuk is en op welke gebieden dit is.

De PIA doet dit door op gestructureerde wijze:

- de mogelijk (negatieve) gevolgen van het gebruik van persoonsgegevens voor de betrokken personen en organisaties in kaart te brengen; en
- de risico's voor de betrokken personen en organisaties zo veel mogelijk te lokaliseren.

Op basis van de uitkomsten van de PIA kunnen er gerichte acties worden ondernomen om deze risico's te verminderen.

Documenteigenschappen

Historie

Versie	Datum	Veranderingen (Concept/Definitief)	Auteur(s)	Wijzigingen
0.4	2016-11-15	Concept		Eerste opzet
0.8	2016-12-27	Concept		Eerste hoofdstukken vervangen door standaard stukken vanuit het project.
0.9	2017-01-12	Concept		Inleiding vervangen

Goedkeuring

Dit document heeft de volgende goedkeuringen nodig.
Getekende goedkeuringsformulieren worden opgeslagen in de Managementsectie van het projectarchief.

Naam	Rol	Akkoord J/N	Datum document	Versie
	Manager SOC			

Distributie

De volgende personen hebben een exemplaar ontvangen.

Naam	Rol	Organisatie	Datum document	Versie
	Functionaris Gegevensbescherming	Ministerie van Financiën		
	Security Officer	Belastingdienst		
	Product Manager	Belastingdienst		

Aanleiding

Nederland is één van de meest gedigitaliseerde landen ter wereld. Digitalisering levert grote voordelen op en is een drijvende kracht achter onze welvaart. De keerzijde van digitalisering is echter dat wij ook kwetsbaar worden voor cyberdreigingen. Uit onderzoek van onder meer het Nationaal Cyber Security Centrum (NCSC), de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) blijkt dat de dreiging die uitgaat van digitale aanvallen blijft toenemen. Ook de complexiteit van deze aanvallen neemt toe. De potentiële maatschappelijke en economische impact van een aanval kan groot zijn.

De weerbaarheid van Nederland tegen deze dreigingen heeft geen gelijke tred gehouden met de digitalisering.

Sinds 2010 gebruikt de Belastingdienst webdiensten (hierna Webdienst). Deze Webdienst wordt ingezet voor Sociale Media Monitoring en Analyse (SMMA) en voor Publishing en Engagement (P en E). SMMA is gericht op het bijhouden en analyseren van uitingen in de sociale media en biedt de mogelijkheid tot trend-, fenomeen- en sentimentanalyses. P en E behelst kort gezegd het verzenden van en reageren op berichten in sociale media en het uitvoeren van campagnes m.b.v. sociale media.

De huidige contracten van de webdiensten lopen per 31 december 2016 af. Om de continuïteit van het werk te kunnen waarborgen is een openbaar aanbestedingstraject opgestart. Deze aanbesteding is gesplitst in twee percelen: SMMA en P en E. Deze PIA bevat per perceel, en verder per gebruikersgroep, een separaat ingevulde vragenlijst.

Binnen de Belastingdienst wordt door verschillende groepen medewerkers gebruik gemaakt van een sociale media Webdienst.

- P en E: Dienstverlening, team webcare
- SMMA: Security Operations Centre (SOC), B/CKC, ISC/Belastingdienst/Toeslagen, Douane, FIOD, Mobile Competence Centre.

De PIA die in het kader van het gebruik van de webdiensten is uitgevoerd, beoogt de risico's met betrekking tot het verwerken van persoonsgegevens in kaart te brengen en voorstellen te doen voor risico-mitigerende maatregelen. Deze voorstellen kunnen als voorwaarden worden meegenomen bij de implementatie en het gebruik van de Webdienst.

Welke gegevens gebruikt de Webdienst?

Sociale media is een verzamelbegrip voor online platformen waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. Hoofdkenmerken zijn interactie en dialoog tussen de gebruikers. Onder de noemer sociale media worden onder andere weblogs, microblogs, social bookmarking, videosites als YouTube en Vimeo, fora, op samenwerking gebaseerde projecten als Wikipedia, en sociale netwerken als Facebook en Google+ geschaard. Via deze media delen mensen verhalen, kennis en ervaringen. Dit doen zij door berichten te publiceren of door gebruik te maken van ingebouwde reactiemogelijkheden.[1]
Een Webdienst verzamelt grote hoeveelheden sociale media data die algemeen beschikbaar zijn op het internet. Op deze data worden algoritmes losgelaten die diverse informatieproducten opleveren (trend-, fenomeen- en imagoanalyses).

Zoals gezegd gaat het om de verzameling en verdere verwerking van actuele en historische data uit alle publiek toegankelijke, openbare sociale media. Informatie die is beschermd d.m.v. privacy settings valt hier expliciet niet onder. Het gaat uitsluitend om gegevens die in eerste instantie door de betrokkene zelf geplaatst zijn op sociale media. Daarnaast dient te worden opgemerkt dat veilingsites, zoals bijvoorbeeld Marktplaats, geen onderdeel uitmaken van sociale media en dus niet vallen onder de werking van de Webdienst.

[1] https://nl.wikipedia.org/wiki/Sociale_media

Om de voorspelbare waarde van de informatieproducten tot een kwalitatief hoog niveau te brengen, is het van belang zoveel mogelijk gegevens te verzamelen en een zo groot mogelijke database aan te leggen, zowel qua omvang als historie. Het is praktisch onuitvoerbaar om de informatieproducten handmatig te produceren door de Belastingdienst.

Betreft het persoonsgegevens?

In ieder geval een deel van de verzamelde gegevens valt terug te voeren op een persoon. Voor een deel van verzamelde gegevens zal dit niet het geval zijn. Omdat deze verzamelingen niet te scheiden zijn, wordt er vanuit gegaan dat er voor de gehele verzameling sprake is van verwerken van persoonsgegevens.

Is er door het gebruik van de Webdienst sprake van profilering?

Profilering houdt in het verzamelen, analyseren en combineren van (persoons)gegevens met als doel iemand in te delen in een bepaalde categorie. Met profilering kan een organisatie ook het gedrag van mensen voorspellen of een beslissing over hen nemen. Profilering wil dus zeggen dat iemand aan de hand van een (risico)profiel wordt beoordeeld.
Profilering bestaat uit drie stappen:

- het verzamelen van (persoons)gegevens over (een groep) mensen;
- het analyseren en combineren van deze, en soms ook andere, gegevens om verbanden en patronen te ontdekken;
- het toepassen van de verbanden en patronen (profielen) op (een groep) mensen om hen in te delen in een bepaalde categorie en/of hun gedrag te voorspellen. [2]

Het bovenstaande in acht genomen, omvat het gebruik van de Webdienst voor SMMA in voorkomende gevallen ook profilering.. Voor het Security Operations Center zal dit echter niet het geval zijn.

Wat betekent het gebruik van de Webdienst voor betrokkenen?

De Webdienst wordt ingezet voor het versterken van de informatiepositie en voor dienstverlening. Voor betrokkenen, in dit geval de personen die informatie hebben geplaatst op de diverse sociale media, betekent dit dat er geen directe rechtsgevolgen zijn verbonden aan het gebruik van hun gegevens op sociale media. Indien echter de Webdienst wordt ingezet voor onderzoek naar personen, kan dit mogelijk wel rechtsgevolgen voor betrokkenen impliceren. Het SOC gebruikt de Webdienst voor onderzoek naar dreigingen en dreigers. Dreigers kunnen zowel personen zijn als organisaties als statelijke actoren.

Maatregelen

In grote lijnen richten de te treffen maatregelen zich op de volgende onderwerpen:

- Communicatie: betrokkenen moeten worden geïnformeerd over het feit dat de Belastingdienst gebruik maakt van sociale media, onder meer door het gebruik van een Webdienst. Hierbij moet worden aangegeven welke gegevens worden gebruikt, met welk doel en hoe lang de gegevens worden bewaard.
- Aan de leverancier van de Webdienst worden technische eisen en wensen worden gesteld, die een zorgvuldige verwerking van gegevens op sociale media ondersteunen (privacy by design).
- Via interne maatregelen wordt een zorgvuldig gebruik van de Webdienst gewaarborgd. Op naleving van de interne richtlijnen wordt toegezien. In de tekst van de deelvragen van de PIA zullen de interne te treffen maatregelen meer geconcretiseerd worden (aangegeven door pijltjessymbool in de tekst).

Noodzaak gebruik van de Webdienst

[2] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/reclame-en-profilering/profilering?qa=Profilering

Sociale media maken inmiddels een onlosmakelijk deel uit van de informatiestromen in de Nederlandse samenleving. Het Security Operations Center van de Belastingdienst gebruikt social media monitoring om het dreigingsbeeld ten aanzien van security gerelateerde thema's in relatie tot de dienstonderdelen Belastingdienst, Toeslagen, Douane en Fiod te kunnen volgen. Deze security gerelateerde thema's kunnen naar aanleiding van een veranderend dreigingsbeeld worden aangepast. Voorbeelden waarop momenteel wordt gemonitord zijn:

10, 2, dg

Werking van de Social Media Infrastructuur

10.1.b, 10.2.c en 10.2.g

Vragen PIA volgens het Toets model Rijksdienst

I. Basisinformatie: type persoonsgegevens, type verwerking en noodzaak/ gegevensminimalisering

I.1. Wilt u als verantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type?

Ja. In het kader van de Wbp is de directeur-generaal Belastingdienst de verantwoordelijke voor de aansluiting van het SOC op de Webdienst; de Belastingdienst/Centrum voor infrastructuur en exploitatie (B/CIE) is de beheerder. Het SOC voert de werkzaamheden feitelijk uit. De betrokkenen van wie de persoonsgegevens worden verwerkt zijn (potentiële) dreigers die doorgaans anoniem willen blijven.

De typen persoonsgegevens die worden verwerkt, zijn variabel. Dit zal hieronder worden toegelicht.

10.1.b, 10.2.c en 10.2.g

I.2. Andere specifieke persoonsgegevens?

I.2a. Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting te verwerken?

Ja, het is mogelijk dat wanneer de cyberdreiging die wordt geuit richting de Belastingdienst kan leiden tot schade aan de potentiele dreiger doordat de aansluiting op de infrastructuur van de Belastingdienst wordt ontnomen.

10.1.b, 10.2.c en 10.2.g

I.2b. Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?

Nee.

I.2c. Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens

te verwerken?

Nee. Wanneer dit onverhoopt toch gebeuren dan zijn er procedures zowel bij het SOC Belastingdienst die er voor zorgen dat deze persoonsgegevens onomkeerbaar worden vernietigd.

I.2d. Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?

Nee. Wanneer dit onverhoopt toch gebeuren dan zijn er procedures zowel bij het SOC Belastingdienst die er voor zorgen dat deze persoonsgegevens onomkeerbaar worden vernietigd.

I.2e. Is het de bedoeling om het BSN-nummer, of een ander persoonsgebonden nummer te verwerken?

Nee. Wanneer dit onverhoopt toch gebeuren dan zijn er procedures zowel bij het SOC Belastingdienst die er voor zorgen dat deze persoonsgegevens onomkeerbaar worden vernietigd.

I.3. Kan van elk van de onder vraag I.1 en vraag I.2 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn voor het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken persoonsgegeven toe.

Ja. De verwerking beperkt zich tot die persoonsgegevens die in het kader van de dreiging technisch noodzakelijk zijn om te komen tot een match met events binnen het SIEM. Zie ook I.1.

I.4. Kan als het gaat om gevoelige persoonsgegevens hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?

(a) Nee. Er is geen sprake van verwerking van gevoelige persoonsgegevens door het SOC.
(b) Nee. Er is geen sprake van verwerking van gevoelige persoonsgegevens door het SOC.

I.5. In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene traject? Wordt hierbij gebruikt gemaakt van (nieuwe) technologie of informatiesystemen?

Het (beleidsmatig) kader op grond waarvan de Belastingdienst verplicht is te beveiligen, is beschreven in het Handboek Beveiliging Belastingdienst. Specifiek ten aanzien van de verwerking van persoonsgegevens door de Belastingdienst geldt artikel 13 van de Wbp, dat regelt dat 'passende technische en organisatorische maatregelen' moeten worden genomen. Deze zijn uitgewerkt in de richtsnoeren van het CBP voor de beveiliging van persoonsgegevens. De Webdienst is dienstbaar aan de beveiliging van de (persoons)gegevens die verwerkt worden bij de Belastingdienst en maakt gebruik van nieuwe technologie om beter weerstand te kunnen bieden aan digitale dreigingen. Zeer frequent worden er nieuwe technieken door dreigers ontwikkeld waarvan het SOC nog geen weet van heeft. Middels de Webdienst wordt inzage verkregen in deze nieuwe hacktechnieken. Verder zijn er dreigingen waarvoor dusdanig veel kosten moeten worden gemaakt om deze permanent de kunnen weerstaan dat het economische meer verantwoord is om inzage te krijgen in deze dreiging en wanneer de dreiging opportuun wordt pas de mitigerende maatregelen in te zetten. Denk hier bij aan DDoS aanvallen. Permanente mitigatie is zeer kostbaar.

II. Doelbinding, koppeling, kwaliteit en profilering

II.1. Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel?

Ja, dit is gebeurd. Het Security Operations Center van de Belastingdienst gebruikt de Webdienst om het dreigingsbeeld ten aanzien van security gerelateerde thema's in relatie tot alle dienstonderdelen van de Belastingdienst te kunnen volgen. Deze security gerelateerde thema's kunnen naar aanleiding van een veranderend dreigingsbeeld worden aangepast. 10.1.b, 10.2.c en 10.2.g

10.1.b, 10.2.c en 10.2.g

Nederland is één van de meest gedigitaliseerde landen ter wereld. Digitalisering levert grote voordelen op en is een drijvende kracht achter onze welvaart. De keerzijde van digitalisering is echter dat wij ook kwetsbaar worden voor cyberdreigingen. Uit onderzoek van onder meer het Nationaal Cyber Security Centrum (NCSC), de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) blijkt dat de dreiging die uitgaat van digitale aanvallen blijft toenemen. Ook de complexiteit van deze aanvallen neemt toe. De potentiële maatschappelijke en economische impact van een aanval kan groot zijn. Dit valt onder andere te lezen in het Cyber Security Beeld Nederland 2016 . Deze is op 5 september 2016 door het NCSC uitgegeven in samenwerking met onder ander de Belastingdienst.

Om de opdracht van artikel 13 WBP uit te kunnen voeren moet het SOC de dreigingsinformatie voor een ander doel (namelijk het beschermen van de voorzieningen tegen inbreuken) gebruiken. Op basis van artikel 43 WBP kan (onder voorwaarden) artikel 9 WBP buiten toepassing gelaten worden als dit noodzakelijk is voor de bescherming van de betrokkene of van de rechten en vrijheden van anderen (art. 9 lid e WBP), maar ook voor het voorkomen van strafbare feiten (art. 9 lid b WBP).

De verwerking van de dreigingsinformatie is bedoeld om, strafbare, inbreuken op de voorzieningen van de belastingdienst te voorkomen of, in ieder geval, te minimaliseren. Daarmee wordt voldaan aan de gestelde voorwaarde in lid b van het artikel. Daarnaast is het echter voor de burger van groot belang dat hij ongestoord gebruik kan maken van de voorzieningen. Immers, de beschikbaarheid van de voorzieningen kan van belang zijn voor het tijdig doen van aangifte. Tijdige aangifte voorkomt boetes voor de burger en kan ook de aanleiding zijn tot een snellere afwerking van deze aangifte en tot het eerder uitbetalen van een teruggave door de Belastingdienst. De ongestoorde toegang is daarmee direct van belang voor de bescherming van de belangen en de rechten van de burger. Deze verwerking is noodzakelijk om de ongestoorde toegang tot de voorzieningen te garanderen en daarmee noodzakelijk om de rechten van de burger te kunnen garanderen. Hiermee wordt voldaan aan de voorwaarde in lid e van artikel 43 WBP. De doelbinding uit artikel 9 lid 1 WBP kan voor deze verwerking buiten toepassing gelaten worden..

II.2. Gaat het bij het project/systeem om gebruik van nieuwe persoonsgegevens voor een bestaand doel, of bestaande doelen binnen al bestaande systemen? (scenario toevoeging nieuwe persoonsgegevens).

Het gaat om een bestaand doel. Het gebruik van persoonsgegevens afkomstig van het internet vindt reeds plaats door B/CIE/SOC (project Nationaal Detectie Netwerken) en deze verwerking is gemeld bij de functionaris gegevensbescherming

van het ministerie van Financiën. Het verschil is dat de persoonsgegevens nu afkomstig zijn van*uit de Webdienst* en dus niet door het SOC zelf worden verzameld. Er worden geen andere persoonsgegevens verwerkt binnen de Webdienst dan worden verwerkt binnen de standaard Security Operations tooling die nu al wordt gebruikt. Echter de bron van waaruit de persoonsgegevens worden gehaald is *nu de Webdienst in plaats van de Security Operations Tooling en het Nationaal Detectie Netwerk.*

II.3. Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden). Zo ja, hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?

Nee. Er worden geen andere persoonsgegevens verwerkt binnen de Webdienst dan nu al worden verwerkt binnen de standaard Security Operations tooling die nu wordt ingezet binnen het SOC.

II.4. Indien u positief hebt geantwoord op vragen II.2 of II.3, hoe wordt een dergelijk voorgenomen gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) gemeld aan: (a) de functionaris voor de gegevensbescherming, of (b) het Cbp indien er geen FG is?

De verwerking zal worden gemeld bij de Functionaris Gegevensbescherming van het Ministerie van Financiën. Melding moet plaatvinden middels het meldingsformulier en deze kan worden verstuurd aan: wbp@minfin.nl.

II.5. Indien u positief geantwoord hebt op vragen II.2 of II.3, welke (nadere) controles op een dergelijk gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) zijn voorzien?

Er zal periodiek worden gecontroleerd welke gegevens met het NCSC worden uitgewisseld. Het NCSC moet vanuit haar eigen verantwoordelijkheid bewaken en bevorderen dat de persoonsgegevens niet voor andere doeleinden zullen worden gebruikt. Omdat de deelnemers aan het TIP alleen deelnemers zijn aan de Joint SOC samenwerking zal worden onderzocht of er één opdracht namens alle Joint SOC organisaties aan de Auditdienst Rijk (Adr) kan worden verstrekt.

Aanbeveling 1:

11.1

II.6. Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de in het beleidsvoorstel, wetsvoorstel op overheidsICT-systeem verwerkte persoonsgegevens na te gaan?

Er zal periodiek moeten worden gecontroleerd of de eisen van doelbinding worden nageleefd. Hiervoor zal nog een opdracht aan de AdR moeten worden verstrekt. Verder zal er controle op de auditlog van de Webdienst op de SOC housekeepinglijst worden geplaatst. Voor deze controle zal een Standard Operating Procedure (SOP) worden opgesteld.

Aanbeveling 1:

11.1

Aanbeveling 2:

11.1

II.7. Zullen de verzamelde/verwerkte persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen? Zijn de betrokkenen daarvan op de hoogte? Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld?

Nee. Het is niet van te voren te voorspellen welke persoonsgegevens op de Sociale Media worden gedeeld door dreigers of concurrerende dreigers. Verder is het niet gewenst om dreigers van te voren op de hoogte te stellen dat zij mogelijk worden gezien op Sociale Media. Er is echter geen sprake van persoonlijke profilering. Dreigingsprofilering vindt wel plaats. Middels de dreigingsprofilering kan beter in kaart worden gebracht waar een bepaald risico wordt gelopen. Het doel is om de Belastingdienst beter te beschermen tegen dreigingen van buitenaf. Dreigers kunnen personen zijn maar ook groeperingen en statelijke actoren.

Aanbeveling 3:

11.1

II.8. Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)? Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?

Nee. Een match met een vooraf gedefinieerde dreigingsindicator zal nooit zonder tussenkomst van een menselijke beoordeling leiden tot concrete actie. Er zal altijd een handmatige controle zijn door een Security Analist die werkzaam is binnen het SOC plaatsvinden voor dat er een actie wordt uitgezet. Al het SOC personeel heeft minimaal een geldig VOG. Het SOC is bezig om de functie van Security Analist op te waarderen naar een vertrouwensfunctie waarvoor een AIVD screening van Niveau B nodig is. Voor zeer gevoelige zaken zal een aantal Security Analisten worden gescreend op Niveau A.III. Betrokken instanties/systemen en verantwoordelijkheid

III.1. Welke interne en externe instantie(s) en/of systemen is/zijn betrokken bij de voorziene verwerking in elk van de onder I.5 onderscheiden fasen? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?

Het SOC is het organisatieonderdeel van de Belastingdienst die de persoonsgegevens vanuit de Webdienst gaat ontvangen. Het SOC, onderdeel van B/CIE, verwerkt deze informatie op hoofdlijnen in de SOC-rapportage of in incidentinformatie. Voor deze exacte verwerking wordt verwezen naar Werking van de Social Media Infrastructuur.

10.1.b, 10.2.c en 10.2.g

10.1.b, 10.2.c en 10.2.g

III.2. Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de

persoonsgegevens? Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?

Ja, het is duidelijk wie verantwoordelijk is voor de verwerking. Toegang tot de persoonsgegevens is geregeld middels een autorisatiemodel. Het autorisatiemodel ziet er op toe dat er niet mogelijk zonder autorisaties de persoonsgegevens te kunnen benaderen. Binnen de Webdienst zijn voorzieningen voor getroffen. Activiteiten op de Social Media Monitoring website worden vastgelegd in de auditlog. Controle op de auditlog van de Social Media Monitoring website wordt op de SOC housekeepinglijst geplaatst. Voor deze controle zal een Standard Operating Procedure (SOP) worden opgesteld.

Aanbeveling 2:

11.1

III.3. Wie binnen uw organisatie, en elk van de andere betrokken organisaties, krijgen precies toegang tot de persoonsgegevens? Bestaat de kans dat bij het gebruik ervan de gegevens ter beschikking komen van onbevoegden?

De medewerkers van het SOC in de rol van Security Analist, hebben toegang tot de persoonsgegevens. Verder zijn er eisen gesteld aan de beveiliging van de Social Media Monitoring website in de aanbesteding3. De Webdienst moet voldoen aan de beveiligingseisen die de overheid ook stelt aan haar webdiensten.

III.4. Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen (in verband met functie/wet)?

Ja, op grond van artikel 67 van de Algemene wet inzake rijksbelastingen (Awr), artikel 15 van het Communautair douanewetboek (Cdw) en artikel 2:5 van de Algemene wet bestuursrecht (Awb) geldt er een geheimhoudingsplicht voor een ieder die betrokken is bij uitvoering van de belastingwetgeving, douanewetgeving en toeslagenwetgeving. Deze geheimhoudingsplicht kan in een beperkt aantal gevallen worden doorbroken.

Gelet op het feit dat de signaleringen geen fiscale gegevens zullen bevatten (alleen identificerende persoonsgegevens), is toepassing van artikel 43c van de Uitv.reg. Awr niet aan de orde. Er is geen sprake van doorbreking van de geheimhoudingverplichting.

Voor gegevens van toeslagen geldt dat deze ingevolge artikel 2:5 van de Awb mogen worden verstrekt, indien uit de taak van het bestuursorgaan de noodzaak tot mededeling voortvloeit. Hiervan is sprake in het onderhavige geval, waar mededeling nodig is voor het veilig houden van de infrastructuur die van vitaal belang is voor het uitvoeren van de primaire taken van de Belastingdienst.

Ingevolge artikel 1:33 van de Algemene douanewet kan de Douane informatie verstrekken in de daar opgesomde gevallen.

III.5. Zijn alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?

3 Aanbesteding SMME - BIJLAGE A – Specificatie van de opdracht 1.0 hoofdstuk 5.1.3.2 Beveiligbaarheid.

Ja, dit is gebeurd. De stappen van de verwerkingen en de uitwisseling van gegevens zijn in kaart gebracht, maar zullen niet precies worden gedeeld met de betrokkenen. Het SOC (als onderdeel van B/CIE) verwerkt de persoonsgegevens in het kader van de beveiliging van de systemen van de Belastingdienst. Het belang hiervan ligt in de bescherming van de gegevens van de burgers en bedrijven in dit land en de veiligstellen van de middelen die de burgers en bedrijven moeten gebruiken om aan de verplichtingen in het kader van de wet- en regelgeving inzake Belastingen, Toeslagen en Douane te voldoen.

III.6. Zijn er beleid en procedures voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken? Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?

Ja. De AdR zal controleren en er wordt een plan-do-check-act-cyclus doorlopen op basis van het Handboek Beveiliging Belastingdienst (HBB). Er zijn geen bewerkers in de zin van de Wbp.

Aanbeveling 4:

11.1

III.7. Is er sprake van overdracht van persoonsgegevens naar een (overheids)instantie buiten de EU/EER? Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de Minister van Veiligheid en Justitie? Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven?

Nee, in BIJLAGE A – Specificatie van de opdracht 1.0 van de aanbesteding Social Media Monitoring & Engagement is hiervoor een eis opgenomen. Eis 19 lid 3 stelt dat bedrijfsdata alleen binnen de Europese Economische Ruimte (EER) mag worden verwerkt en opgeslagen.

IV. Beveiliging en bewaring/vernietiging

IV.1. Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde? Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan? Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging?

Ja. Verantwoordelijk voor het opstellen van beleid is het directoraat-generaal Belastingdienst. In het Handboek Beveiliging Belastingdienst (HBB) is dit beleid vertaald in concrete acties en stappen om de informatiebeveiliging daadwerkelijk te realiseren. In het HBB deel B staat bijvoorbeeld (B.1.4. Beleid op informatie-uitwisseling) dat maatregelen getroffen moeten worden voor detectie. Hier wordt tevens genoemd dat automatische controle plaatsvindt op virussen, trojans en andere malware. B/CIE past dit beleid toe. Voor implementatie van het beleid is het lijnmanagement verantwoordelijk. De leden van het managementteam van de Belastingdienst in de rol van Chief Financial Officer/Chief Information Security Officer (CFO/CISO) en van Chief Information Officer (CIO) zijn verantwoordelijke voor de naleving van het informatiebeveiligingsbeleid. De Beveiligingssambtenaar (BVA) en de functionaris voor de gegevensbescherming (FG) houden toezicht op de naleving van dit beleid.

IV.2. Indien (een deel van) de verwerking bij een bewerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die bewerker?

Er zijn geen bewerkers.

IV.3. Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter

voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a) gegevens die in een geautomatiseerd format staan (bv. wachtwoord-bescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend bv. sloten op kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen?

In BIJLAGE A – Specificatie van de opdracht 1.0 van de aanbesteding Social Media Monitoring & Engagement is hiervoor een groot aantal eisen opgenomen. Deze eisen zijn terug te vinden in paragraaf 5.1.3.2 Beveiligsbaarheid. Eisen zijn gesteld rond de thema's: Vertrouwelijkheid en authenticiteit, audits, integriteit, autorisatie, gegevensintegreit.

Aanbeveling 2:

11.1

IV.4. Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften, en voor het detecteren ervan? Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen?

In het geval van datalekken geldt de gangbare procedure (standaard incidentproces). Dergelijke meldingen zullen worden gedaan bij het Loket Datalekken.

IV.5. Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring?

De retentieperiode moet gerelateerd worden aan de periode waarover het noodzakelijk is om de persoonsgegevens te blijven bewaren. Het SOC werkt voor dreigingen vanuit de Sociale Media vooral vanuit de actualiteit. Dreigingen worden vaak kort van de te voren aangekondigd en moeten dan worden gevolgd totdat dreiging niet meer opportuun is of is gemitigeerd. Op basis van kennis uit het verleden schat het SOC in dat gegevens en deze gegevens kunnen ook persoonsgegevens bevatten maximaal 30 dagen moeten worden bewaard. De gegevens zullen direct na de genoemde periode van 30 dagen onbenaderbaar moeten worden gemaakt voor SOC medewerkers.

Als er sprake is van een melding, of er binnen 30 dagen een correlatie tussen de verzamelde gegevens en een melding wordt geconstateerd, zijn de verwerkte persoonsgegevens noodzakelijk voor het onderzoek hierna. Dit onderzoek (al dan niet strafrechtelijk) moet eerst zijn afgerond voor de verwerkte gegevens onbereikbaar worden gemaakt. Na beëindiging van het onderzoek, en de eventuele vervolging, hebben de gegevens hun relevantie verloren en moeten deze vernietigd worden.

IV.6. Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?

De termijn van 30 dagen is een initiële waarde. Gedurende het gebruik van de Sociale Media Monitoring website kan deze waarde naar beneden of naar boven worden aangepast na aanleiding van beleidsmatige- en technische gronden. Er zal continue worden bijgehouden wat de juiste waarde is van deze parameter. Wanneer er van de termijn van 30 dagen wordt afgeweken zal er contact worden gezocht met de Functionaris Gegevensbescherming van het Ministerie van Financiën.

IV.7. Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de

bewaartermijn te vernietigen? Worden alle persoonsgegevens, inclusief log-gegevens, vernietigd? Is er controle op de vernietiging, en door wie?

In BIJLAGE A – Specificatie van de opdracht 1.0 van de aanbesteding Social Media Monitoring & Engagement is hiervoor een eis opgenomen. Bij beëindiging van de overeenkomst dient de Opdrachtnemer, lees de leverancier van de Social Media Monitoring website, alle gegevens (incl. metadata en back-up) binnen 24 klokuren onherstelbaar te vernietigen en een gecertificeerde verklaring van vernietiging te overhandigen aan de Belastingdienst.

V. Transparantie en rechten van betrokkene

V.1. Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend gemaakt worden? Wat is de procedure om betrokkenen indien nodig te informeren over het doel van de verwerking van hun persoonsgegevens?

Ja, de Belastingdienst heeft in de 'Gedragscode voor internet' van 16 augustus 2013 in artikel 2.1 bekend gemaakt aan zijn medewerkers dat alle communicatiestromen worden gescand en gelogd. Op www.belastingdienst.nl/security moet een link worden opgenomen naar www.rijksoverheid.nl waarop een melding moet worden geplaatst. Deze specifieke gedragscode voor de Belastingdienst is op 23 juni 2016 vervangen door "Gedragsregeling voor de digitale werkomgeving4". Deze gedragsregeling geldt rijksbreed, dus ook voor de Belastingdienst. In deze gedragsregeling staat vermeld dat de Belastingdienst ambtenaar instemt met dat zijn of haar activiteiten worden gelogd (registeren) en worden gemonitord (bekijken).

Aanbeveling 3:

11.1

V.2. Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?

Niet van toepassing.

V.3. Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking?

Niet van toepassing. Artikel 43 sub a Wbp.

V.4. Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? Bij een weigering toestemming te geven, of bij een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?

Niet van toepassing.

V.5. Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?

4 http://content.rp.rijksweb.nl/cis/content/media/rijksportaal/pdirekt/rijksbreed_4/overigepublicaties_1/gedragscode/Gedragsregeling_voor_de_digitale_werkomgeving_versie_1_0.pdf

Informatie over de verwerking van persoonsgegevens door de Belastingdienst is te vinden op www.rijksoverheid.nl en www.belastingdienst.nl.

Aanbeveling 3:

11.1

V.6. Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?

Informatie over de behandeling van een verzoek tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens door de Belastingdienst is te vinden op www.rijksoverheid.nl en op www.belastingdienst.nl.

Aanbeveling 3:

11.1

Samenvatting van de eerder gesignaleerde risico's en aanbevelingen

In het kader van de aansluiting van de Belastingdienst op TIP is deze Privacy Impact Assessment (PIA) uitgevoerd. Daarbij is de PIA uitgevoerd voor de aansluiting op het Nationaal Detectie Netwerk en de daaruit voortvloeiende risico's als startpunt gebruikt. Er zijn aanbevelingen in de tekst gedaan waar dat nodig is. Deze aanbevelingen zullen zijn gericht op het mitigeren van mogelijke Wbp-risico's. Kortheidshalve wordt hieronder verwezen naar de tekst in de PIA.

Hieronder een overzicht van de aanbevelingen:

Aanbeveling 1:

11.1

Aanbeveling 2:

11.1

Aanbeveling 3:

11.1

Aanbeveling 4:

11.1

PIA Douane

27

PIA Social Media monitoring webdienst en analyse

Colofon

Projectnaam	Aanbesteding Social Media Monitoring webdienst
Projectnummer	nvt.
Versienummer	1.0
Contactpersoon	[redacted] DLK/DLTC
Auteurs	**PIA-algemeen** [redacted] (ISC) **PIA-vragenlijst Douane** [redacted]

Inhoud

Inleiding

Aanleiding uitvoeren PIA

Sinds 2010 gebruikt de Belastingdienst sociale media monitoring webdiensten (hierna webdienst). Deze webdienst wordt ingezet voor Sociale Media Monitoring en Analyse (SMMA) en voor Publishing en Engagement (P en E). SMMA is gericht op het bijhouden en analyseren van uitingen in de sociale media en biedt de mogelijkheid tot trend-, fenomeen- en sentimentanalyses. P en E behelst kort gezegd het verzenden van en reageren op berichten in sociale media en het uitvoeren van campagnes m.b.v. sociale media.

De huidige contracten van de webdiensten lopen per 31 december 2016 af. Om de continuïteit van het werk te kunnen waarborgen is een openbaar aanbestedingstraject opgestart. Deze aanbesteding is gesplitst in twee percelen: SMMA en P en E. Deze PIA bevat per perceel, en verder per gebruikersgroep, een separaat ingevulde vragenlijst.

Binnen de Belastingdienst wordt door verschillende groepen medewerkers gebruik gemaakt van een sociale media webdienst.
P en E: Klantinteractie en –services (webcare)
SMMA: Security Operations Centre (SOC), B/CKC, ISC/Belastingdienst/Toeslagen, Douane, FIOD, Mobile Competence Centre, Klantinteractie en –services (webcare).

De PIA die in het kader van het gebruik van de webdiensten is uitgevoerd, beoogt de risico's met betrekking tot het verwerken van persoonsgegevens in kaart te brengen en voorstellen te doen voor risico-mitigerende maatregelen. Deze voorstellen kunnen als voorwaarden worden meegenomen bij de implementatie en het gebruik van de webdienst.

Welke gegevens gebruikt de sociale media monitoring webdienst?

Sociale media is een verzamelbegrip voor online platformen waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. Hoofdkenmerken zijn interactie en dialoog tussen de gebruikers. Onder de noemer sociale media worden onder andere weblogs, microblogs, social bookmarking, videosites als YouTube en Vimeo, fora, op samenwerking gebaseerde projecten als Wikipedia, en sociale netwerken als Facebook en Google+ geschaard. Via deze media delen mensen verhalen, kennis en ervaringen. Dit doen zij door berichten te publiceren of door gebruik te maken van ingebouwde reactiemogelijkheden.
Een webdienst verzamelt grote hoeveelheden sociale media data die algemeen beschikbaar zijn op het internet. Op deze data worden algoritmes losgelaten die diverse informatieproducten opleveren (o. m. trend-, fenomeen- en imagoanalyses).

Zoals gezegd gaat het om de verzameling en verdere verwerking van actuele en historische data uit alle publiek toegankelijke, openbare sociale media. Informatie die is beschermd d.m.v. privacy settings valt

hier expliciet niet onder. Het gaat uitsluitend om gegevens die in eerste instantie door de betrokkene zelf geplaatst zijn op sociale media. Daarnaast dient te worden opgemerkt dat veilingsites, zoals bijvoorbeeld Marktplaats, geen onderdeel uitmaken van sociale media en dus niet vallen onder de werking van de webdienst.

Om de voorspelbare waarde van de informatieproducten tot een kwalitatief hoog niveau te brengen, is het van belang zoveel mogelijk gegevens te verzamelen en een zo groot mogelijke database aan te leggen, zowel qua omvang als historie. Het is praktisch onuitvoerbaar om de informatieproducten handmatig te produceren door de Belastingdienst.

Betreft het persoonsgegevens?
In ieder geval een deel van de verzamelde gegevens valt terug te voeren op een persoon. Voor een deel van verzamelde gegevens zal dit niet het geval zijn. Omdat deze verzamelingen niet te scheiden zijn, wordt er vanuit gegaan dat er voor de gehele verzameling sprake is van verwerken van persoonsgegevens.

Is er door het gebruik van de webdienst sprake van profilering?
Profilering houdt in het verzamelen, analyseren en combineren van (persoons)gegevens met als doel iemand in te delen in een bepaalde categorie. Met profilering kan een organisatie ook het gedrag van mensen voorspellen of een beslissing over hen nemen. Profilering wil dus zeggen dat iemand aan de hand van een (risico)profiel wordt beoordeeld.
Profilering bestaat uit drie stappen:
1. het verzamelen van (persoons)gegevens over (een groep) mensen;
2. het analyseren en combineren van deze, en soms ook andere, gegevens om verbanden en patronen te ontdekken;
3. het toepassen van de verbanden en patronen (profielen) op (een groep) mensen om hen in te delen in een bepaalde categorie en/of hun gedrag te voorspellen.

Het bovenstaande in acht genomen, omvat het gebruik van de webdienst voor SMMA in voorkomende gevallen ook profilering.

Wat betekent het gebruik van de webdienst voor betrokkenen?
De webdienst wordt ingezet voor het versterken van de informatiepositie en voor dienstverlening. Voor betrokkenen, in dit geval de personen die informatie hebben geplaatst op de diverse sociale media, betekent dit dat er geen directe rechtsgevolgen zijn verbonden aan het gebruik van hun gegevens op sociale media.
Indien echter de webdienst wordt ingezet voor onderzoek naar personen, kan dit mogelijk wel rechtsgevolgen voor betrokkenen impliceren.
Maatregelen
In grote lijnen richten de te treffen maatregelen zich op de volgende onderwerpen:
- Communicatie: betrokkenen moeten worden geïnformeerd over het feit dat de Belastingdienst gebruik maakt van sociale media, onder

meer door het gebruik van een webdienst. Hierbij moet worden aangegeven welke gegevens worden gebruikt, met welk doel en hoe lang de gegevens worden bewaard.
- Aan de leverancier van de webdienst worden technische eisen en wensen worden gesteld, die een zorgvuldige verwerking van gegevens op sociale media ondersteunen (privacy by design).
- Via interne maatregelen wordt een zorgvuldig gebruik van de webdienst gewaarborgd. Op naleving van de interne richtlijnen wordt toegezien. In de tekst van de deelvragen van de PIA zullen de interne te treffen maatregelen meer geconcretiseerd worden (aangegeven door pijltjessymbool in de tekst).

Afbakening PIA Douane
Zoals beschreven in de algemene inleiding kan de webdienst worden gebruikt voor het bijhouden en analyseren van uitingen in de sociale media en biedt de webdienst de mogelijkheid tot trend-, fenomeen- en sentimentanalyses.

De beantwoording van onderstaande vragenlijst is dan ook (deels) gebaseerd op het gebruik van de webdienst voor het bijhouden en analyseren van uitingen in de sociale media. In het geval van de Douane gaat het dan onder meer over het onderkennen van nieuwe trends/sentimenten op het gebied van goederen.

Daarnaast kan de webdienst ook gebruikt worden in het kader van risicogerichte handhaving.
Hierbij moet onder meer gedacht worden aan het monitoren van social-media berichtgeving over verkopen van accijnsgoederen op internet, transportbewegingen, logistieke stromen en berichtgeving over bedrijven, in het kader van risicogericht handhaven, waarbij de mogelijkheid bestaat dat signalen van activiteiten die strijdig zijn met de verboden en beperkingen uit de douanewetgeving, in combinatie met interne gegevens mogelijkerwijs leiden tot toezichtshandelingen.

Een goede monitoring van social media geeft de Douane onder meer de mogelijkheid om:

- Het doen van trend- en fenomeenanalyse. Door bijvoorbeeld vroegtijdig trends te signaleren, die van invloed zijn op de risicogerichte handhaving die de Douane voorstaat. Denk hierbij bijvoorbeeld aan een op social media populair nieuw tabaksproduct, die nog niet eerder in beeld was bij de Douane.
- Het signaleren van activiteiten die strijdig zijn met de verboden en beperkingen uit de douanewetgeving, denk hierbij aan de illegale verkoop van accijnsgoederen of namaakgoederen via social media.
- Damagecontrol en reputatiemanagement. Informatie verzamelen ten behoeve van een goede communicatie met bedrijven en personen (o.a. reizigers) die in de dagelijkse praktijk te maken hebben met de Douane.

De Douane kan inspelen op een gebleken informatiebehoefte, maar ook op klachten over haar dienstverlenings/handhavingstaken.

De PIA-vragenlijst voor de Douane ziet enerzijds op het gebruik van de webdienst voor trend- en analysedoeleinden en anderzijds op het gebruik van de webdienst als een van de hulpmiddelen in het kader van risicogerichte handhaving. In de verdere tekst wordt zoveel mogelijk een onderscheid gemaakt tussen het gebruik van de webdienst voor trend & analyse en als hulpmiddel in het kader van risicogerichte handhaving.
Te meer om duidelijk te verkrijgen vanuit het ministerie van Financiën, die de PIA beoordelen, voor welke doeleinden de webdienst mag worden ingezet. Alleen voor trend- en analysedoeleinden of ook in het kader van risicogerichte handhaving. Waarbij benadrukt dient te worden dat Douane op basis van Europeesrechtelijke verplichtingen (DWU) verplicht is om risico-gericht te werken.

Deze PIA ziet nadrukkelijk niet op het gebruik van de webdienst door de Douane als een van de hulpmiddelen voor communicatie- en dienstverleningsdoeleinden.
Directe communicatie met de klanten en het voeren van campagnes voor de Douane verloopt via team webcare van Belastingdienst online dienstverlening.[1]
De analyse op reacties op/effecten van deze communicatie en campagnes die via social media worden gedeeld, wordt wel verzorgd door team OSINT Douane en wordt dan ook als zodanig besproken in deze PIA.

1 Het gebruik van de social media tooling door Belastingdienst online dienstverlening wordt in een ander PIA beschreven.

PIA

I. Basisinformatie: type persoonsgegevens, type verwerking en noodzaak/gegevensminimalisering

1. **Wilt u als verantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type?**

Verantwoordelijke
Verantwoordelijke voor de gegevens, die zijn verzameld en gebruikt door de Douane, in de zin van artikel 1, onder d, van de Wet bescherming persoonsgegevens (Wbp) is de Minister van Financiën.

Ja. De webdienst maakt gebruik van persoonsgegevens die door de gebruikers van de diverse sociale media in de openbaarheid van het internet zijn geplaatst. Voorbeelden hiervan zijn namen, gebruikersnamen, sociale media adressen, andere gegevens die een gebruiker mogelijk ingevuld heeft op het sociale media profiel/account: de biografische tekst, woonplaats, nicknames en geo-locatie. Deze opsomming is niet compleet. Het is mogelijk dat beeldmateriaal is geplaatst, waardoor bijzondere persoonsgegevens kunnen worden verwerkt.

Daarnaast kunnen medewerkergegevens, voornaam, achternaam, email adres, werk, geslacht worden verwerkt.

Vanwege het felt dat foto's een element zijn van sociale media, is het mogelijk dat daardoor bijzondere persoonsgegevens worden verwerkt. Het betreft (niet in alle gevallen) foto's die door de gebruiker zelf zijn gepost. Niet alle sociale media data zullen identificeerbaar zijn.

Voor wat betreft de Douane zal het vooral gaan om informatie over goederen, het vervoer van goederen en bedrijven.
Denk hierbij aan social-media berichtgeving over verkopen van accijnsgoederen op internet, transportbewegingen, logistieke stromen en over bedrijven.

Maatregelen

- Bij de uitvoering van een opdracht moet, d.m.v. het gebruik van filters, zoveel mogelijk het gebruik van niet relevante gegevens worden uitgesloten.
- Bij de verwerking beeldmateriaal is extra zorgvuldigheid geboden. Het specifiek zoeken op beeldmateriaal dient extra gemotiveerd te worden. De informatieproducten dienen zoveel mogelijk van beeldmateriaal te zijn ontdoen.

- Zoveel mogelijk beperken van het gebruik van medewerker gegevens.

2. Andere specifieke persoonsgegevens?
2a. Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting te verwerken?
2b. Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?
2a+2b.

Nee. Het is niet de bedoeling om gegevens te verwerken die kunnen leiden tot stigmatisering of uitsluiting.

De Douane gebruikt de informatieproducten van de webdienst voor het versterken van haar kennispositie en in het kader van risicogerichte handhaving.
De zoekopdrachten kunnen worden ingegeven door doelgroepanalyse, het ondersteunen van risicoanalyse zoals beschreven in het handhavingsplan, en door verzoeken afkomstig uit samenwerkingsverbanden op nationaal en Europees niveau.

Eveneens is het niet de bedoeling om gegevens over kwetsbare personen of groepen te verwerken. Mochten deze groepen wel in beeld worden gebracht, in het kader van een opdracht, dan is extra zorgvuldigheid geboden.

- Bij het gebruik van gegevens van kwetsbare personen/groepen dient een zo kort mogelijke bewaartermijn gehanteerd te worden. In het intakeformulier wordt hiertoe een extra vraag opgenomen.
- De toegang tot deze gegevens zal extra beveiligd worden en strikt beperkt. (algemene maatregel)

2c.Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens te verwerken?

Het is mogelijk dat gebruikersnamen verwerkt worden: dit is afhankelijk van de keuze van de gebruiker van de netwerksites.
De gebruikersnamen zijn de namen waarvan een individu gebruik maakt op sociale media. Dit kan de echte naam zijn van de betrokkene, of een nickname. Wachtwoorden worden niet verwerkt.

Ten overvloede kan hier gemeld worden dat voor gebruikers (douanemedewerkers) van de webdienst geldt dat handelingen van douanemedewerkers worden opgenomen in een logbestand.
Vastgelegd wordt hoe vaak een medewerker inlogt en in welke projecten de medewerker werkzaam is.

De verwerking van persoonsgegevens van gebruikers voor intern gebruik geschiedt volgens de kaders beschreven in het handboek beveiliging Belastingdienst (HHB).

2d. Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?
Nee.

2e. Is het de bedoeling om het BSN-nummer, of een ander persoonsgebonden nummer te verwerken?
Nee.

Doel: Trend & Analyse
Bij het verwerken van de gegevens die door de webdienst worden gehanteerd, wordt geen BSN-nummer gebruikt.

Doel: in het kader van risicogerichte handhaving

10, 2d

3. Kan van elk van de onder vraag I.1 en vraag I.2 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn voor het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken persoonsgegeven toe.

Doel: Trend & Analyse
De webdienst levert een aantal informatieproducten op zoals fenomeen-sentiment en imagoanalyses. Deze informatieproducten worden door de Douane ingezet voor het versterken van de kennispositie, gezien het feit dat heden ten dage de meeste transacties in het kader van het grensoverschrijdend goederenverkeer langs elektronische weg en door tussenkomst van internet tot stand komen, waaronder via social media.

Daarbij is social media als communicatiemiddel uit de huidige samenleving niet meer weg te denken. Het wordt door miljoenen mensen gebruikt om op verschillende sociale platforms informatie uit te wisselen. Voor de Douane is dit een aanvulling op de bestaande informatiebronnen. Data uit social media omvatten miljoenen berichten per dag en zijn daarom handmatig lastig te verwerken. Daarnaast zou het handmatig zoeken van berichten een enorme capaciteit vragen en zo tijdrovend zijn dat een acceptabele reactietijd niet haalbaar is. Daarom geeft het gebruik van een webdienst de Douane de mogelijkheid om deze data op eenvoudige wijze te ontsluiten.

Doel: in het kader van risicogerichte handhaving
Social media is een van de platforms waarop transacties in het kader van goederenverkeer plaatsvinden. Douane focust zich hierbij op de in - en uitgaande goederenstroom van Niet-Unie goederen, en de handel in accijnsgoederen en onder meer de handel in namaakartikelen, handel in medicijnen, alsmede E-commerce.

Voor het uitvoeren van toezichtstaken is het dan ook noodzakelijk dat de Douane toegang heeft en inzicht kan verkrijgen in deze data in het kader van risicohandhaving.

10.2.c en 10.2.d

vermeld.

Maatregelen

- Aandacht bij het uitvoeren van de opdracht voor het gebruik van zo min mogelijk persoonsgegevens, per opdracht motiveren welke gegevens noodzakelijk zijn, overige gegevens uitzetten d.m.v. filterfunctie.
- De mogelijkheid tot het herleiden naar de bron van de gegevens dient uitgezet te kunnen worden.

4. Kan, als het gaat om gevoelige persoonsgegevens hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?

Doel: Trend & Analyse
Het is niet specifiek te bedoeling bijzondere persoonsgegevens te verwerken. Deze kunnen echter wel deel uitmaken van de verzamelde sociale mediadata, met name foto's. De informatieproducten die de webdienst biedt, zijn niet meer persoonsgebonden. Vanwege het feit dat de bronnen waaruit de analyses zijn opgebouwd, nog te herleiden zijn, is er geen sprake van anonimisering.

Ten behoeve van trend- en analysedoeleinden is het niet noodzakelijk om de (gevoelige) persoonsgegevens te verwerken.
Hier kan volstaan worden met geanonimiseerde gegevens.
Voor de Douane gaat het om het in kaart brengen van bijvoorbeeld goederenbewegingen en trends.

Doel: in het kader van risicogerichte handhaving
In het kader van risicogerichte handhaving is het weliswaar niet specifiek de bedoeling om gericht op (gevoelige) persoonsgegevens te zoeken, maar deze kunnen wel deel uitmaken van de verzamelde data. Deze persoonsgegevens zijn vervolgens van belang in de risicovinding. Denk hierbij aan de situatie wanneer op social media accijnsgoederen worden aangeboden en deze goederen direct te herleiden zijn tot de persoon of het bedrijf dat deze goederen aanbiedt.

Maatregelen

- Beeldmateriaal filteren bij informatieproducten, daarnaast dient de noodzaak tot het gebruik van beeldmateriaal specifiek gemotiveerd te worden (in bijvoorbeeld het intakeformulier).

5. In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene traject? Wordt hierbij gebruikt gemaakt van (nieuwe) technologie of informatiesystemen?

De Douane maakt al enige jaren gebruik van een webdienst.
Op basis van art. 8 onder e Wet bescherming persoonsgegevens biedt de uitvoering van de publiekrechtelijke taak (nl. de wettelijke taken heffen en goederentoezicht) in het algemeen de grondslag voor de Douane voor het verwerken van persoonsgegevens.

De Douane ontleent haar bevoegdheden met betrekking tot controle van goederen en risicobeheer aan artikel 46 DWU.
Het Douanewetboek van de Unie verplicht in artikel 46, lid 2, de douaneautoriteiten om hun controles te baseren op risicoanalyses met gebruikmaking van geautomatiseerde gegevensverwerkingstechnieken. Op deze wijze is de Douane beter in staat om risicogericht te handhaven.

Op basis van art. 1:21 Adw dient de Douane zich bij aanvang van een controle of controleproces te verwittigen van de noodzaak van die maatregel en dient het controleproces aan een proportionaliteits- en subsidiariteitstoets te onderwerpen, zo ook bij het analyseren van social-mediagegevens. Art. 1:26 eerste lid, letter c, Adw biedt vervolgens de kaders voor de omvang van de controle.

Het hanteren van de webdienst voor trend- & analyse en in het kader van risicogerichte handhaving geschiedt binnen de wettelijke kaders en

alleen op basis van een opdracht vanuit handhavingsregie binnen de Douane. Hierbij is het van belang te benoemen dat de opdrachten voor analyses op basis van de webdienst altijd getoetst dienen te worden op proportionaliteit en subsidiariteit alvorens zij worden uitgezet bij team OSINT.

- In intakeformulieren dient expliciet gevraagd te worden naar het doel van de gegevensverzameling.

II. Doelbinding, koppeling, kwaliteit en profilering

Doeleinden/doelbinding en koppeling

1. **Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel?**

De doelen waarvoor de persoonsgegevens worden verwerkt zijn het versterken van de kennispositie van de Douane en risicogerichte handhaving.
De Douane wil effectief toezicht kunnen houden. In dat kader voert de Douane onderzoeken uit, waarbij monitoren van sociale media, selecteren, analyseren en rapporteren een belangrijke rol spelen. Analyses van data van sociale media bieden een mogelijkheid om een beter beeld te krijgen van trends, fenomenen, imago, sentiment, subjecten (personen of bedrijven), objecten (goederen, goederenstromen en vervoermiddelen) en om inzichten te verkrijgen in de reacties van burgers en organisaties op maatschappelijke veranderingen.

Het monitoren van sociale media levert een bijdrage aan de uitvoering van de taken van de Douane. Data uit sociale media heeft een duidelijke toegevoegde waarde op data van bijvoorbeeld algemene websites of andere reeds beschikbare interne of externe data. Deze toegevoegde waarde zit in de soort berichtgeving die je vindt op sociale media: sociale media kenmerken zich door een puur, rauw beeld te geven van wat er speelt in de buitenwereld. Er wordt dus geput uit de behoefte van mensen om hun mening online te ventileren. Dit levert informatie op die je op andere plekken niet vindt. In een tijdperk waarin burgers zich steeds meer online begeven voor o.a. het voeren van discussies, het uiten van klachten en het doorspelen van informatie, kan de Douane niet achterblijven in het analyseren van deze specifieke vorm van informatie. Daarnaast is het een extreem actuele bron van informatie, wat ertoe leidt dat sociale media analyse de mogelijkheid biedt om snel de gewenste informatie te verkrijgen en hier desgewenst op te acteren. Diverse succesvolle resultaten bevestigen het beeld dat deze vorm van analyse niet alleen een waardevolle toevoeging is op de reeds beschikbare informatie, maar ook een noodzakelijke.

10, 2cd

10, 2cd

2 en 3. Gaat het bij het project/systeem om gebruik van nieuwe persoonsgegevens voor een bestaand doel, of bestaande doelen binnen al bestaande systemen?. Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden). Zo ja, hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?

De persoonsgegevens die worden gebruikt zijn nieuw. Deze gegevens zijn niet gekoppeld aan andere systemen binnen de Douane.
Het betreft bestaande doelen (trend & analyse en risicogerichte handhaving) en bestaande systemen (de webdienst).
De gebruikers die betrokken zijn bij de verwerking van de gegevens hebben dezelfde doelstelling. Dezelfde doelen gelden voor het hele proces.

4. Indien u positief hebt geantwoord op vragen II.2 of II.3, hoe wordt een dergelijk voorgenomen gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) gemeld aan: (a) de functionaris voor de gegevensbescherming, of (b) het Cbp indien er geen FG is?

Op basis van artikel 27 Wbp zal de Douane melding maken van het gebruik van de webdienst bij de functionaris voor de gegevensbescherming.
De Directeur Informatiemanagement Douane biedt de PIA aan, aan het Wbp-team van het Ministerie van Financiën.

5. Indien u positief geantwoord hebt op vragen II.2 of II.3, welke (nadere) controles op een dergelijk gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) zijn voorzien?

Nog nader te bepalen.

6. Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de in het beleidsvoorstel, wetsvoorstel op overheidsICT-systeem verwerkte persoonsgegevens na te gaan?

Er zijn algemeen geldende procedures waar door de bevoegde interne en externe instanties op wordt gecontroleerd, conform het handboek beveiliging Belastingdienst.

11.1

Profilering

7. Zullen de verzamelde/verwerkte persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen? Zijn de betrokkenen daarvan op de hoogte? Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld?

Profilering houdt in het verzamelen, analyseren en combineren van (persoons)gegevens met als doel iemand in te delen in een bepaalde categorie. Het gebruik van de webdienst kan het gebruik van profielen met zich meebrengen. Er worden informatieproducten gegenereerd om vermoedelijk relevante informatie in kaart te brengen. Deze producten worden gemaakt m.b.v. de webdienst na invoeren van zoektermen door de Douane gebaseerd op een opdracht. De resultaten van deze producten kunnen worden gebruikt bij het versterken van de kennispositie van de Douane of in het kader van risicogerichte handhaving.

Wanneer er sprake is van een zoekopdracht in het kader van risicogerichte handhaving worden de resultaten te allen tijde beoordeeld om te onderkennen in welke mate er sprake is van handhavingsrisico's met betrekking tot bepaalde goederen of goederenstromen. Bevindingen voortkomend uit social media onderzoek kunnen in combinatie met interne gegevens mogelijkerwijs leiden tot toezichtshandelingen.

Maatregelen

- Informeren betrokkenen over het gebruik van de webdienst en meer specifiek het profileren (algemene maatregel).

8. Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)? Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?

Een webdienst verzamelt grote hoeveelheden sociale media data beschikbaar op het internet. Op deze data worden algoritmes toegepast die diverse informatieproducten opleveren, zoals trend, fenomeen- en imagoanalyses.
Een gespecialiseerde medewerker van de Douane zorgt voor duiding van de resultaten. Zonder tussenkomst van een menselijke beoordeling wordt er geen actie ondernomen.

III. Betrokken instanties/systemen en verantwoordelijkheid
1. Welke interne en externe instantie(s) en/of systemen is/zijn betrokken bij de voorziene verwerking in elk van de onder I.5 onderscheiden fasen? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?

De webdienst betreft een webbased toegankelijke dienstverlening. Deze dienstverlening wordt door een externe partij verleend. De dienstverlening van deze externe partij wordt eveneens aan andere geïnteresseerde marktpartijen aangeboden. Het is dus niet zo dat de webdienst enkel in opdracht van de Belastingdienst (inclusief Douane) opereert.

Het gebruik van de webdienst van de externe partij geschiedt door verschillende partijen binnen de Belastingdienst.
De informatieproducten die zijn gegenereerd worden opgeslagen binnen de Belastingdienstomgeving.

2. Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens? Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?

Verantwoordelijke voor het leveren van de webdienst is een externe te contracteren partij.

Verantwoordelijke voor de gegevens, die zijn verzameld en gebruikt door de Douane, in de zin van artikel 1, onder d, van de Wet bescherming persoonsgegevens (Wbp) is de Minister van Financiën.

Binnen de Douane wordt de dienst alleen gebruikt door een selecte groep gekwalificeerde en bevoegde medewerkers. De webdienst zal niet algemeen ter beschikking worden gesteld.

Maatregelen

- PIA's dienen regelmatig te worden uitgevoerd om bewust scherp te blijven op rechtmatige verwerkingen van persoonsgegevens.
- Er zal een instructie worden opgesteld voor de gebruikers van de webdienst.

3. Wie binnen uw organisatie, en elk van de andere betrokken organisaties, krijgen precies toegang tot de persoonsgegevens?

Nader te bepalen bij implementatietraject van de webdienst binnen de Douane.

10.2.c en 10.2.d

Toegang tot de webdienst is alleen mogelijke via een geregistreerd account en het beheer wordt centraal belegd.

Maatregelen

- Bij het leveren van de rapportages wordt een code of conduct geleverd, waarin staat vermeld dat de opgeleverde informatie niet zelf mag worden gewijzigd of geïnterpreteerd.

4. Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen (in verband met functie/wet)?
Ja, de geheimhoudingsverplichtingen volgen voor wat betreft de Douane uit artikel 12 DWU juncto artikel 1:33 ADW.

Maatregelen

- Er wordt een geheimhoudingsplicht opgelegd aan de dienstverlener. (algemene maatregel)

5. Zijn alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?

De Douane gebruikt de webdienst voor het genereren van diverse analyses. Deze analyses worden verstrekt aan de diverse interne opdrachtgevers.

Maatregelen

- Opstellen stappenplan

6. Zijn er beleid en procedures voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken? Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?

Er is een instructie in de maak over het gebruik van informatie beschikbaar op het internet door de Belastingdienst (De Douane is ook betrokken bij deze instructie). In deze instructie zullen specifieke aanwijzingen over het gebruik van de webbased dienst worden opgenomen.

Maatregelen

- Opstellen specifieke werkaanwijzingen (binnen het kader van bovengenoemde instructie) voor het gebruik van de webdienst.

7. Is er sprake van overdracht van persoonsgegevens naar een (overheids)instantie buiten de EU/EER? Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de Minister van Veiligheid en Justitie? Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven?

Maatregelen

- Contractueel vastleggen dat gegevens binnen de EU worden opgeslagen. (algemene maatregel)
- Toezien op het feit dat bovenstaande eis wordt nageleefd door de leverancier. (algemene maatregel)

IV. Beveiliging en bewaring/vernietiging [2]

Beveiliging

1. Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde? Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan? Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging?

Ja.

Beveiliging is als onderdeel van integraal management en bedrijfsvoering een verantwoordelijkheid van het lijnmanagement op de diverse niveaus in de organisatie. Op het hoogste niveau binnen de Belastingdienst geldt de volgende verdeling van beveiligingsverantwoordelijkheden:

- de eindverantwoordelijkheid ligt bij de Chief Security Officer (CSO), alsook de verantwoordelijkheid voor bedrijfscontinuïteit;
- de verantwoordelijkheid voor personele veiligheid en integriteit bij de Chief Personnel Officer (CPO), het concernpersoneelsbeleid;
- de verantwoordelijkheid voor informatiebeveiliging bij de Chief Information Officer (CIO);
- de verantwoordelijkheid voor fysieke beveiliging bij het verantwoordelijke MT-lid van de Facilitaire Dienst

Verantwoordelijk voor het opstellen van beleid is het directoraat-generaal Belastingdienst. In het Handboek Beveiliging Belastingdienst (HBB) is dit beleid vertaald in concrete acties en stappen om de informatiebeveiliging daadwerkelijk te realiseren. Voor implementatie van het beleid is het lijnmanagement verantwoordelijk. Het management wordt hierbij ondersteund door o.a. een adviseur Informatiebeveiliging.

Het beleid is gericht op het borgen van de gegevensveiligheid.

2. Indien (een deel van) de verwerking bij een bewerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die bewerker?
Nader te bespreken, vormgeven in bewerkersovereenkomst plus toezicht op naleving van de gestelde voorwaarden.

Er is een bewerkersovereenkomst opgesteld waarin we specifiek op de soort verwerkingen de benodigde beheersmaatregelen afstemmen. De bewerker moet aantoonbaar voldoen aan de hiervoor geldende beveiligingseisen en rapporteert hier periodiek over.

3. Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a) gegevens die in een geautomatiseerd format staan (bv.

2 Voor de details betreffende de beveiliging wordt verwezen naar de 'Beschrijving functionele eisen en wens en onderzoeken sociale media' en de 'Demandspecificatie Internet- en Mediaonderzoek 2016'.

wachtwoord-bescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend bv. sloten op kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen?

Risico is dat data, waaronder persoonsgegevens, zich buiten de gesloten en beveiligde infrastructuur van de Belastingdienst bevindt. Dit brengt het risico met zich mee dat onbevoegden mogelijk toegang kunnen verkrijgen tot deze data.

Overzicht van de data, waaronder persoonsgegevens, die buiten de dienst worden geplaatst: inlogfrequenties, namen van projecten, belastingdienst- emailadressen gebruikers webdienst, de zoektermen die worden gebruikt voor een zoekopdracht, de dashboards die voortvloeien uit een zoekopdracht, lijsten van gebruikte internetbronnen.

Bedrijfsdata mogen slechts worden verwerkt en opgeslagen binnen de Europese Unie.

De dienst is alleen toegankelijk voor gebruikers van wie het account is geverifieerd. Alleen geautoriseerde Belastingdienstmedewerkers hebben toegang tot de dienst..

Medewerkers van de inschrijver of onderaannemers van de inschrijver hebben geen toegang tot Bedrijfsdata. Een uitzondering wordt gemaakt voor medewerker(s) van de inschrijver die door de inschrijver zijn aangewezen om de dienstverlening te beheren. Toegang tot Bedrijfsdata door medewerkers van de inschrijver moet worden beveiligd.

De volgende maatregelen zijn voor medewerkers van de inschrijver van toepassing:
- Er dient een geheimhoudingsverklaring te worden ondertekend door de
  medewerkers van de dienstverlener die specifiek betrokken zijn bij de
  uitvoering van de werkzaamheden voor de Belastingdienst,
- De minimale screeningseis is een Verklaring Omtrent Gedrag o.b.v. algemeen
  screeningsprofiel functieaspecten 11, 12 en 13 (zie www.justis.nl).

De Dienst is verplicht om Belastingdienst Projecten af te schermen van andere klanten van de inschrijver (chinese walls).

De Dienst voorziet in autorisatie op Projecten die alleen door een geautoriseerde gebruiker kunnen worden uitgevoerd (bijvoorbeeld het opvoeren, wijzigen of verwijderen van gegevens)

Beheer van autorisaties kan plaatsvinden op basis van rollen (Role Based Acces Control). De Dienst kan hierbij aansluiten op een voorziening (IMS) waarin de rechten (permissies) van medewerkers zijn vastgelegd.

De geautoriseerde autorisatiebeheerder van de Belastingdienst kan zelf rollen, rechten en gebruikersbeheer op de niveaus van Bedrijfsonderdelen en daarbinnen per Project in de Dienst uitvoeren. De Belastingdienst moet een overzicht kunnen genereren van actieve gebruikers met welke rollen en rechten zij hebben in de Dienst, zodat licentiebeheer en integriteitsonderzoek kan plaatsvinden. Hiervoor wordt bij voorkeur aangesloten op het Identity Management systeem met Single Sign on van de Belastingdienst, zodat inloggegevens niet bij de inschrijver komen.

10.1.c en 10.2.g

Ten behoeve van verantwoording afleggen moeten rapportages voor een audit trail kunnen worden gemaakt door de Belastingdienst.

Op basis van de logging van activiteiten moet verantwoording over het gebruik worden afgelegd en onderzoek kunnen worden gedaan naar wie-wat-wanneer-welk subject in onderzoek had c.q. welk Project onderhanden was. Loggegevens van medewerkers moeten minimaal twee jaar na ontstaan daarvan beschikbaar blijven voor interne controle binnen de Belastingdienst. De Belastingdienst moet over de loggegevens beschikken om integraal met andere belastingdienstactiviteiten verantwoording aan het management af te leggen. Het vereiste formaat is 'Cleartekst'. Bovenstaande geldt ook voor beheerderactiviteiten op alle niveaus

Aanvullende specifieke eisen zijn:

- wanneer en door wie een onderzoek in een Project is aangemaakt,
- Wie wanneer welke zoekopdracht (voor een Project) heeft uitgevoerd,
- Wie wanneer welke resultaatgegevens heeft veilig gesteld (bewaard t.b.v. Project),
- Wie wanneer gebruik heeft gemaakt van de gegevens (raadplegen),
- Wie wanneer resultaatgegevens heeft gewijzigd, aangevuld of verwijderd.

10.1.c en 10.2.g

Aandachtspunten:

- De autorisatieprofielen zullen regelmatig moeten worden gecontroleerd op actualiteit en de AdR zal de naleving van het beleid hieromtrent moeten toetsen. Dit is onderdeel van de controle op de beveiliging van de verwerking.
- Afhankelijkheid van het publieke internet is hier een factor.
- Alleen gebruik maken van beveiligde browsers en verbindingen en vanaf werkplekken in beveiligde netwerken binnen de belastingdienst omgeving conform ICT-Beveiligingsrichtlijn voor web- applicaties NCSC.

De Dienst dient aan de beveiligingseisen van de Overheid te voldoen zoals beschreven in de volgende bijlagen.

- bijlage 'ICT-Beveiligingsrichtlijnen voor web applicaties- Verdieping leesversie (NCSC, september 2015)'; NCSC staat voor National Cyber Security Centrum. Dit document beschrijft richtlijnen over eisen aan web applicaties, waaraan de inschrijver moet voldoen. Bron: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html
- 'Baseline Informatiebeveiliging Rijksdienst' (BIR 2012 Tactisch Normenkader; bron

10.2.g

- Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007' (VIR 2007;
  bron http://wetten.overheid.nl/BWBR0022141/2007-07-01
- Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie
  2013' (VIRBI 2013; bron
  http://wetten.overheid.nl/BWBR0033507/2013-06-01

4. Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften, en voor het detecteren ervan? Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen?

De leverancier moet de Belastingdienst actief informeren bij alle incidenten en calamiteiten. De inschrijver informeert de Belastingdienst

onmiddellijk in het kader van de wet Meldplicht datalekken. Binnen de Belastingdienst is specifiek voor datalekken een procedure ingericht.
De Belastingdienst beschikt over een goed georganiseerde calamiteitenorganisatie.
De leverancier dient actief beleid op beveiliging uit te voeren.
Zodra er beveiligingslekken voor data zijn geconstateerd, dan dient er z.s.m. een beveiligings-update van de Dienst plaats te vinden.
Conform richtsnoeren beveiligingsniveau CBP (AP) en interen richtlijnen Belastingdienst.

Bewaring/vernietiging
5. Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring?

Nog nader te bepalen.

Voor het vaststellen van de bewaartermijn van de persoonsgegevens bij de Douane is artikel 10 van de Wbp van belang waarin wordt bepaald dat persoonsgegevens niet langer worden bewaard (in een vorm die het mogelijk maakt de betrokkene te identificeren) dan noodzakelijk is voor het bereiken van de doeleinden waarvoor ze zijn verkregen.

Bewaartermijn binnen de organisatie
Afhankelijk van de opdracht (voor trend & analyse of in het kader van risicogerichte handhaving) wordt gekeken naar de bewaartermijnen, wanneer de gegevens worden opgeslagen. Het bewaren van de informatieproducten geschiedt conform de Wbp, archiefwet en hetgeen bepaald in de ordeningsstructuur (selectielijsten) van de Douane.

Maatregelen

- In de (nader te ontwikkelen) interne instructie procedure rondom vernietiging van gegevens opnemen. Voor zowel geanonimiseerde gegevens als persoonsgegevens.

6. Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?
Zie 5.

7. Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen? Worden alle persoonsgegevens, inclusief log-gegevens, vernietigd? Is er controle op de vernietiging, en door wie?
Monitoren en loggen van het gebruik, inclusief beheerdersactiviteiten.
De dienst is alleen toegankelijk voor gebruikers van wie de identiteit is geverifieerd. Het beheer wordt, naar alle waarschijnlijkheid, centraal belegd bij Team OSINT, afhankelijk van het implementatietraject.

- Maak een plan van aanpak (of afsprakendocument) met duidelijke proces- en beheersafspraken.

V. Transparantie en rechten van betrokkenen

Transparantie

1. Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend gemaakt worden? Wat is de procedure om betrokkenen indien nodig te informeren over het doel van de verwerking van hun persoonsgegevens?

Informatie over de verwerking van persoonsgegevens door de Belastingdienst is te vinden op www.rijksoverheid.nl en www.belastingdienst.nl.[3]

Naast de algemene privacyverklaring die noodzakelijk is voor de verwerking van persoonsgegevens, dienen, in die gevallen dat er sprake is van profilering, de volgende elementen te worden opgenomen in deze verklaring.

- de doelen van profilering;
- de verschillende soorten gegevens die de organisatie daarvoor gebruikt;
- hoe lang de organisatie deze gegevens bewaart;
- de logica die ten grondslag ligt aan het toekennen en toepassen van een profiel vermeld staan.
- hoe de privacy-rechten kunnen worden uitgeoefend(inzage, correctie, verwijdering, verzet)

Maatregelen

- In aanvulling op wat nu op de website staat, informatie over het gebruik van de dienst/ gebruik sociale media door Belastingdienst op website publiceren uit oogpunt van transparantie. (algemene maatregel)
- Melding bij FG

2. Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?
Niet van toepassing.

3. Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking?

Maatregelen

- Overweging om gebruik van de dienst/ gebruik sociale media door de belastingdienst op de website te publiceren uit oogpunt van transparantie. (algemene maatregel)

3 http://download.belastingdienst.nl/belastingdienst/docs/belastingdienst_wet_bescherming_persoonsgegevens_al5331z2pl.pdf

Rechten van betrokkenen

4. Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? Bij een weigering toestemming te geven, of bij een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?

Niet van toepassing.

5. Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?

Informatie over de verwerking van persoonsgegevens door de Belastingdienst en het uitoefenen van het recht op inzage of correctie is te vinden op www.rijksoverheid.nl en www.belastingdienst.nl.[4]

6. Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?

Informatie over de behandeling van een verzoek tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens door de Belastingdienst is te vinden op www.rijksoverheid.nl en op www.belastingdienst.nl.[5]

Maatregelen

- De verplichtingen met betrekking tot de rechten van betrokkenen, zoals verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens, dienen te worden ingebed in de organisatie van de leverancier. (algemene maatregel)

4 http://download.belastingdienst.nl/belastingdienst/docs/belastingdienst_wet_bescherming_persoonsgegevens_al5331z2pl.pdf

5 http://www.rijksoverheid.nl/ministeries/fin/organisatie/meldingenregister

PIA gebruik sociale media monitoring webdiensten

28

Aanleiding uitvoeren PIA
Sinds 2010 gebruikt de Belastingdienst sociale media monitoring webdiensten (hierna webdienst). Deze webdienst wordt ingezet voor Sociale Media Monitoring en Analyse (SMMA) en voor Publishing en Engagement (P en E). SMMA is gericht op het bijhouden en analyseren van uitingen in de sociale media en biedt de mogelijkheid tot trend-, fenomeen- en sentimentanalyses. P en E behelst kort gezegd het verzenden van en reageren op berichten in sociale media en het uitvoeren van campagnes m.b.v. sociale media.

De huidige contracten van de webdiensten lopen per 31 december 2016 af. Om de continuïteit van het werk te kunnen waarborgen is een openbaar aanbestedingstraject opgestart. Deze aanbesteding is gesplitst in twee percelen: SMMA en P en E. Deze PIA bevat per perceel, en verder per gebruikersgroep, een separaat ingevulde vragenlijst.

Binnen de Belastingdienst wordt door verschillende groepen medewerkers gebruik gemaakt van een sociale media webdienst.
P en E: Klantinteractie en –services (webcare)
SMMA: Security Operations Centre (SOC), B/CKC, ISC/Belastingdienst/Toeslagen, Douane, FIOD, Mobile Competence Centre, Klantinteractie en –services (webcare).

De PIA die in het kader van het gebruik van de webdiensten is uitgevoerd, beoogt de risico's met betrekking tot het verwerken van persoonsgegevens in kaart te brengen en voorstellen te doen voor risico-mitigerende maatregelen. Deze voorstellen kunnen als voorwaarden worden meegenomen bij de implementatie en het gebruik van de webdienst.

Welke gegevens gebruikt de sociale media monitoring webdienst?
Sociale media is een verzamelbegrip voor online platformen waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. Hoofdkenmerken zijn interactie en dialoog tussen de gebruikers. Onder de noemer sociale media worden onder andere weblogs, microblogs, social bookmarking, videosites als YouTube en Vimeo, fora, op samenwerking gebaseerde projecten als Wikipedia, en sociale netwerken als Facebook en Google+ geschaard. Via deze media delen mensen verhalen, kennis en ervaringen. Dit doen zij door berichten te publiceren of door gebruik te maken van ingebouwde reactiemogelijkheden.[1]
Een webdienst verzamelt grote hoeveelheden sociale media data die algemeen beschikbaar zijn op het internet. Op deze data worden algoritmes losgelaten die diverse informatieproducten opleveren (trend-, fenomeen- en imagoanalyses).

Zoals gezegd gaat het om de verzameling en verdere verwerking van actuele en historische data uit alle publiek toegankelijke, openbare sociale media. Informatie die is beschermd d.m.v. privacy settings valt hier expliciet niet onder. Het gaat uitsluitend om gegevens die in eerste instantie door de betrokkene zelf geplaatst zijn op sociale media. Daarnaast dient te worden opgemerkt dat veilingsites, zoals bijvoorbeeld Marktplaats, geen onderdeel uitmaken van sociale media en dus niet vallen onder de werking van de webdienst.

Om de voorspelbare waarde van de informatieproducten tot een kwalitatief hoog niveau te brengen, is het van belang zoveel mogelijk gegevens te verzamelen en een zo groot mogelijke database aan te leggen, zowel qua omvang als historie. Het is praktisch onuitvoerbaar om de informatieproducten handmatig te produceren door de Belastingdienst.

[1] https://nl.wikipedia.org/wiki/Sociale_media

Betreft het persoonsgegevens?
In ieder geval een deel van de verzamelde gegevens valt terug te voeren op een persoon. Voor een deel van verzamelde gegevens zal dit niet het geval zijn. Omdat deze verzamelingen niet te scheiden zijn, wordt er vanuit gegaan dat er voor de gehele verzameling sprake is van verwerken van persoonsgegevens.

Is er door het gebruik van de webdienst sprake van profilering?
Profilering houdt in het verzamelen, analyseren en combineren van (persoons)gegevens met als doel iemand in te delen in een bepaalde categorie. Met profilering kan een organisatie ook het gedrag van mensen voorspellen of een beslissing over hen nemen. Profilering wil dus zeggen dat iemand aan de hand van een (risico)profiel wordt beoordeeld.
Profilering bestaat uit drie stappen:
1. het verzamelen van (persoons)gegevens over (een groep) mensen;
2. het analyseren en combineren van deze, en soms ook andere, gegevens om verbanden en patronen te ontdekken;
3. het toepassen van de verbanden en patronen (profielen) op (een groep) mensen om hen in te delen in een bepaalde categorie en/of hun gedrag te voorspellen. [2]

Het bovenstaande in acht genomen, omvat het gebruik van de webdienst voor SMMA in voorkomende gevallen ook profilering.

Wat betekent het gebruik van de webdienst voor betrokkenen?
De webdienst wordt ingezet voor het versterken van de informatiepositie en voor dienstverlening. Voor betrokkenen, in dit geval de personen die informatie hebben geplaatst op de diverse sociale media, betekent dit dat er geen directe rechtsgevolgen zijn verbonden aan het gebruik van hun gegevens op sociale media.
Indien echter de webdienst wordt ingezet voor onderzoek naar personen, kan dit mogelijk wel rechtsgevolgen voor betrokkenen impliceren.

Maatregelen
In grote lijnen richten de te treffen maatregelen zich op de volgende onderwerpen:
- Communicatie: betrokkenen moeten worden geïnformeerd over het feit dat de Belastingdienst gebruik maakt van sociale media, onder meer door het gebruik van een webdienst. Hierbij moet worden aangegeven welke gegevens worden gebruikt, met welk doel en hoe lang de gegevens worden bewaard.
- Aan de leverancier van de webdienst worden technische eisen en wensen worden gesteld, die een zorgvuldige verwerking van gegevens op sociale media ondersteunen (privacy by design).
- Via interne maatregelen wordt een zorgvuldig gebruik van de webdienst gewaarborgd. Op naleving van de interne richtlijnen wordt toegezien. In de tekst van de deelvragen van de PIA zullen de interne te treffen maatregelen meer geconcretiseerd worden (aangegeven door pijltjessymbool in de tekst).

Inhoudsopgave
Perceel Publishing en Engagement
- Klantinteractie &- services, team webcare

Perceel Social Media Monitoring en Analyse
- Belastingdienst/EHi/Internet service Centre
- Toeslagen
- Security Operations Centre
- Fiod
- Douane

[2] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/reclame-en-profilering/profilering?qa=Profilering

- B/CKC
- Mobile Competence Centre
- Klantinteractie &- services, team webcare