Colofon

Titel	Review risico-analyse PoC AcceptEmail
Auteur(s)	
Datum	17 november 2015
Bijlagen	2
Inlichtingen	**Auditdienst Rijk**
Status	Definitief
Kenmerk	ADR/2015/1421 M

Inhoud

1 Samenvatting

Op verzoek van de COO van de Belastingdienst heeft de ADR een review uitgevoerd op het proces van totstandkoming van de risico-analyse voor de Proof of Concept (PoC) AcceptEmail en de uitkomsten van dit proces: de geïnventariseerde risico's en beheersingsmaatregelen. Uit ons onderzoek komen op hoofdlijnen de volgende bevindingen naar voren.

Risicoanalyse uitgevoerd en aantal compenserende maatregelen beschreven
Een aantal risico's die bij de PoC AcceptEmail belangrijk zijn zoals phishing en opslag van data in de Microsoft cloud zijn onderkend en een aantal compenserende maatregelen is geformuleerd. Over de mate waarin door de maatregelen het phishing risico is afgedekt is discussie tussen IV Voortbrenging enerzijds en B/CIE SOC anderzijds. B/CIE / SOC acht het restrisico in relatie tot de maatregelen fors te hoog.

Risico phishing zeer groot
B/CIE/ SOC raadt –vanuit hun praktijkervaring met cybercriminaliteit - uitvoering van de PoC ten zeerste af gegeven het phishing risico. Op dit moment worden uit naam van de Belastingdienst al grootschalig phishing mails verstuurd door cybercriminelen. Nadere informatie hierover is bij het SOC op te vragen.
Als bekend wordt dat de Belastingdienst zelf ook e-mail gebruikt voor het versturen van links voor betalingen, is het de verwachting van SOC dat cybercriminelen hier misbruik van gaan maken. Doelgroep van phishing zijn hierbij niet zozeer de personen die in het kader van het PoC door de Belastingdienst worden benaderd, maar juist de gehele populatie Nederlandse belastingplichtigen. Het SOC schat in dat de criminelen binnen enkele dagen na de start van de PoC in de stijl van de AcceptEmails van de Belastingdienst phishing emails gaan versturen, eventueel gecombineerd met het eerst bellen van personen. Dit is ook de verwachting van het fraudeteam van Logius, dat wij in het kader van het onderzoek hebben geïnterviewd.

Gebruik AcceptEmail niet in overeenstemming met beleid Belastingdienst
Het gebruik van AcceptEmail met een betaallink is niet overeenkomstig het vigerende beleid van de Belastingdienst en wijkt af van hetgeen de Belastingdienst communiceert in het email verkeer met belastingplichtigen. Het gebruik van een betaallink in een mail is ook in tegenspraak met de boodschap in de bewustwordingscampagnes voor het maatschappelijk verkeer zoals 'Hang op, klik weg, bel uw bank' van de Nederlandse Vereniging van Banken.

Wegvallen Safe Harbor afspraken voor privacy als basis voor gebruik cloud
AcceptEmail wordt geleverd door een commerciële partij die gebruik maakt van opslag in de cloud bij Microsoft. Gevolg is dat bij uitvoering van de PoC gegevens van de Belastingdienst over belastingplichtigen tijdelijk op Microsoft servers worden opgeslagen. Dit is strijdig met het specifieke beleid van de Rijksoverheid op dit punt. Tevens is met de uitspraak van het Europees hof over het Safe Harbor-besluit een belangrijke algemene juridische basis voor het onderbrengen van privacy gevoelige data bij Amerikaanse cloud providers weggevallen.

Veiliger alternatieven genoemd
Bij ons onderzoek is door B/CIE/SOC gewezen op een veiliger manier van gebruik van moderne technieken. Dit betreft bijvoorbeeld het toepassen van een berichtenbox of het ontwikkelen van betalingsmogelijkheden in de portalen van de Belastingdienst. Naar vernomen worden deze mogelijkheden door de Belastingdienst nader onderzocht.

Besluitvorming over PoC AcceptEmail noodzakelijk op hoogste niveau
De bestuurlijke lijn is dat het kernteam Roadmap Inning de OBC met een advies tot al dan niet uitvoering van de POC voorlegt aan de RvB.
De ADR acht het wenselijk om vanwege enerzijds de gesignaleerde risico's, door het afwijken van vigerende beleid en afwijken van de aan het maatschappelijk verkeer gecommuniceerde gewenste gedragslijn, maar ook de mogelijke impact van de beslissing op de modernisering van het berichtenverkeer met burgers en bedrijven (een onderdeel Investeringsagenda), een beslissing over het al of niet uitvoering PoC AE, op basis van een gedegen risico-analyse voor te leggen aan de eindverantwoordelijke functionaris van de Belastingdienst, de DG.

2 Inleiding

In voorliggende onderzoeksrapportage zijn de bevindingen van het onderzoek "Review risico-analyse PoC AcceptEmail" weergegeven. Dit onderzoek betreft een deelopdracht van de audit "*Realisatie van de visie op inning".* Opdrachtgever voor de Risico-analyse Proof of Conceopt (PoC) AcceptEmail is de COO, dhr. Blokpoel. Gedelegeerd opdrachtgever uit het kernteam Roadmap Inning is . Vanwege de verantwoordelijkheid voor en belang van de PoC AcceptEmail voor het LIC en B/CA Betalingsverkeer, zijn en (LIC) en mw. ook betrokken.

Een tussentijdse afstemming van de bevindingen op hoofdlijnen met de gedelegeerd opdrachtgeefster en auditmanager heeft op 15 oktober plaatsgevonden. Op 27 oktober is een eerste versie van de rapportage uitgebracht en op 29 oktober besproken met medewerkers van IM/B. Op 29 oktober is het concept van de rapportage uitgebracht aan gedelegeerd opdrachtgever en betrokkenen. Vervolgens is na verwerking van opmerkingen op 16 november de definitieve versie van het rapport uitgebracht.

Na de samenvatting en de inleiding is in hoofdstuk 3 de opdracht aan de ADR beschreven. In hoofdstuk 4 treft u de uitkomsten van ons onderzoek aan. In bijlage 1 is een beschrijving opgenomen van de ontwikkelingen telefonische incasso Belastingdienst. In bijlage 2 treft u het overzicht In BuCA PoC AE uitgewerkte risico's en beheersmaatregelen aan.

3 Opdracht

3.1 Doel van het onderzoek en opdracht ADR

Doel
Doel van het onderzoek is om de opdrachtgever inzicht te verschaffen in de kwaliteit van de door de Belastingdienst zelf uitgevoerde risico-analyse AcceptEmail en de uitkomsten te gebruiken ter ondersteuning van een advies tot al dan niet uitvoering van de PoC aan de RvB.

Opdracht ADR
De ADR voert een review uit op het proces van totstandkoming van de risico-analyse AcceptEmail en de uitkomsten van dit proces: de geïnventariseerde risico's en beheersingsmaatregelen. Hierbij wordt nagegaan of de opgesomde risico's en beheersmaatregelen volledig en juist overeenstemmen met onderliggende dossiervorming. De ADR signaleert bevindingen in de vorm van een onderzoeksrapport. De ADR geeft geen zekerheid over de volledigheid van de gesignaleerde risico's. Ook geeft de ADR geen overall conclusie of de implementatie van AcceptEmail verantwoord is. Dit valt onder de verantwoordelijkheid van het management van de Belastingdienst.

3.2 Dossiervorming en beroepsstandaarden

Deze onderzoeksopdracht wordt uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing en conform het vakinhoudelijk beleid van de ADR. Het door ADR voor deze opdracht aangelegde dossier voldoet aan de richtlijnen van het vakinhoudelijk beleid van ADR. Het dossier is eigendom van ADR en wordt conform de wettelijke termijn door ADR bewaard. Indien sprake is van verkregen vertrouwelijke informatie dan zal deze alleen voor de vervulling van deze opdracht worden gebruikt. Voor eventuele overige aspecten hierover wordt verwezen naar de 'Mantel opdracht'.

3.3 Uitgevoerde werkzaamheden

De ADR is aan de hand van een overzicht van de projectleider PoC AcceptEmail nagegaan wie betrokken zijn geweest bij de uitvoering van de risico-analyse. Na overleg met de projectleider zijn medewerkers van de Belastingdienst benaderd voor het afnemen van een interview. Betreffende medewerkers komen uit verschillende bij de PoC AcceptEmail betrokken onderdelen van de Belastingdienst. Voorts hebben wij een interview afgenomen met medewerkers van het fraudeteam van Logius. Van elk interview is een verslag opgesteld dat is geaccordeerd door betrokkenen.
De ADR is nagegaan welke regelgeving en normenkaders zijn gehanteerd bij de uitvoering van de risico-analyse. Vervolgens is de wijze onderzocht waarop betrokkenen partijen gezamenlijke zekerheid hebben verkregen over de volledigheid en juistheid van de geïnventariseerde risico's en beheersmaatregelen. Wij hebben geen onderzoek uitgevoerd naar de effectieve werking van de beheersmaatregelen.

3.4 Verspreidingskring rapportage

Onze rapportage is uitsluitend bedoeld voor gebruik binnen de doelstelling van het onderzoek door de opdrachtgever binnen de Belastingdienst. Verspreiding buiten de directe kring van betrokkenen bij de Belastingdienst is slechts toegestaan na uitdrukkelijke toestemming van de ADR.
De rapportage heeft niet het karakter van een assurance rapportage.

3.5 Ondertekening

Auditmanager ADR

Plaats en datum

4 Onderzoek

4.1 Beschrijving ADR van het totstandkomingsproces, door Belastingdienst gesignaleerde risico's en voorgenomen beheersmaatregelen bij gebruik AcceptEmail

Medio 2014 is aan B/CA Betalingsverkeer opdracht gegeven om de impact van AE op de processen die Betalingsverkeer raken te onderzoeken en advies uit te brengen aan het MT incassoketen over het gebruik van AE. De opdracht heeft geleid tot het rapport Vooronderzoek Toepasbaarheid en Implementatie AcceptEmail (16 december 2014). In dit rapport wordt in de samenvatting onderstaande conclusie en belangrijkste aandachtspunten inzake het gebruik van AE opgesomd:
"Gezien de doelstelling van het mogelijke gebruik van AE binnen de Belastingdienst, de invordering, is de conclusie van het onderzoek dat Betalingsverkeer, vanuit betalingsverkeer perspectief, de inzet van AE middels een pilot (of POC) bij het LIC van harte ondersteunt. Betalingsverkeer adviseert daarbij het gebruik van de Direct Contact Module van AcceptEmail B.V. (hierna: AEBV) en het betalen middels uitsluitend iDeal. Producten van andere aanbieders lijken inferieur en minder toepasbaar. Gebaseerd op de ervaringen van andere gebruikers lijken goede resultaten (lagere kosten en hogere ontvangsten) voor gebruik van AE bij de Belastingdienst zeer goed mogelijk. Bij Reaal Verzekeringen wordt reeds enige tijd met de Direct Contact module gewerkt. Zo'n 55% van de achterstallige betalingen wordt daar op deze manier alsnog betaald. Implementatie kan snel omdat de applicatie draait bij AEBV en niet op de IT-omgeving van de Belastingdienst behoeft te worden geïnstalleerd.

De belangrijkste aandachtspunten inzake het gebruik van AE betreffen:

a) de beveiliging: tot op heden heeft AEBV met haar product alle beveiligingstesten doorstaan, maar ook de Belastingdienst en de ADR (voorwaarde Agentschap) zullen hun oordeel moeten vormen. Ook speelt hier de fundamentele vraag of de Belastingdienst met belastingplichtigen per e-mail wenst te corresponderen.
b) de sourcing: gegevens van de Belastingdienst worden op de IT-omgeving van AEBV geplaatst. Vraag is of M0 daarmee akkoord kan gaan;
c) de inkooptechnische aspecten: een Proof of Concept in plaats van een Pilot is ook een mogelijkheid en bij de wens tot definitieve aanschaf van een dergelijk product zal Europees moeten worden aanbesteed, hetgeen vereist dat bij de Offerteaanvraag volledige openheid van zaken met betrekking tot de pilot moet worden gegeven."

Om de functionele wens van het Landelijk Incasso Centrum om direct betalen bij het telefonische incasso proces mogelijk te maken, is in vervolg op bovengenoemd vooronderzoek vanaf 2015 een Proof of Concept met AcceptEmail voorbereid onder leiding van IM/B. Dit heeft geleid tot een outline business case PoC AcceptEmail bij

telefonische incasso (0.8 na 25-08-2015). In deze OBC is onderstaand advies opgenomen:
" *Aan het Kernteam Inning wordt gevraagd om gezien de beheersbaarheid van de geïnventariseerde risico's en de kleinschaligheid van de proef accoord te gaan met het uitvoeren van een Proof of Concept met AcceptEmail."*

Ten aanzien van de risico's en beheersmaatregelen is in de OBC onderstaand opgenomen:

"In het kader van (technische) beveiliging van persoonsgegevens, het risico op phishing en extern hosten worden bij het uitvoeren van de Proof of Concept de volgende 6 beheersmaatregelen in acht genomen:

1. *Alleen contact naar aanleiding van een ontvangen aanmaning*
2. *Onder water meesturen gegevens in de mail*
3. *Vijf verificatiepunten*
4. *Gegevens cloud maandelijks gewist*
5. *Communicatie Website en template*
6. *Beperkt en beheersbare groep voor de proef periode*

Deze risico's en beheersmaatregelen zijn in hoofdstuk 10 Risico's en beheersmaatregelen van de OBC uitgewerkt en is als bijlage bij dit rapport opgenomen.

4.2 Bevindingen

4.2.1 Totstandkomingsproces vooronderzoek toepasbaarheid en implementatie AE

Bij de totstandkoming van het rapport Vooronderzoek Toepasbaarheid en Implementatie AcceptEmail zijn zowel medewerkers van de Belastingdienst (IM/B, B/CA, B/CFD en LIC) als medewerkers buiten de Belastingdienst (UWV, Reaal, Tacstone en AcceptEmail) ondervraagd.

4.2.2 Totstandkomingsproces BuCa PoC AE bij telefonische incasso

Bij de totstandkoming van de BuCa PoC AcceptEmail telefonische incasso zijn diverse Belastingdienstmedewerkers van IM/B, de gebruikersorganisatie (B/CA en LIC), B/CAO, B/CIE, B/CFD, B/CKC en DGBel betrokken geweest. Hieronder bevinden zich beveiligingsexperts van de Belastingdienst. Ook is in de periode januari 2015 – augustus 2015 contact geweest met vertegenwoordigers van AcceptEmail, Tacstone, het Agentschap GT, Cannock Chase, Microsoft en UWV.
De ADR heeft na overleg met de projectleider een aantal bij de totstandkoming betrokken medewerkers van de Belastingdienst geïnterviewd. Door alle geïnterviewde betrokkenen wordt aangegeven dat de gesignaleerde risico's goed zijn beschreven in de OBC PoC AcceptEmail.

4.2.3 Risico's

4.2.3.1 Risico van Phishing

Het gebruik van AcceptEmail met een betaallink is niet overeenkomstig vigerende beleid van de Belastingdienst.

Het gebruik van een betaallink in een mail is ook in tegenspraak met de boodschap in de bewustwordingscampagnes voor het maatschappelijk verkeer als hang op, klik weg, bel uw bank.

Het SOC heeft op 24-08-2015 een security bulletin over AcceptEmail (classificatie : Vertrouwelijk) uitgebracht. De Lead Security Operations Center/Security Officer geeft aan dat de strekking van het bulletin in onvoldoende mate terugkomt in de BuCa PoC AE.
Metingen bij het SOC laten een stijging zien in de gevallen waar sprake is van phishingmailing runs waarbij de naam van de Belastingdienst wordt ingezet om misbruik te maken. Deze gevallen halen regelmatig de krant. Nadere informatie over de metingen zoals aantallen ed, dienen bij het SOC te worden opgevraagd. Voorbeelden van phishing bij gebruik AcceptEmail zijn op internet te vinden (Ziggo).

Door de inzet van AcceptEmail wordt afgeweken van hetgeen door het maatschappelijk verkeer wordt verwacht. Hierdoor is de kans groot dat er onduidelijkheid ontstaat bij het maatschappelijk verkeer over wat wel te vertrouwen is en wat niet en hoe te handelen. Kwaadwillenden kunnen hier misbruik van maken.

4.2.3.2 Risico bij opslag in de Cloud

Bij inzet van AcceptEmail wordt de hosting verzorgd door een externe partij. Hierbij wordt gebruik gemaakt van opslag in de Cloud van gegevens van de Belastingdienst over belastingplichtigen. Door de patriot act is het mogelijk dat deze informatie over Nederlandse belastingplichtigen bij de Amerikaanse overheid bekend is.
In een brief aan de directeuren van alle Belastingdienstonderdelen van 14 januari 2013 (kenmerk DGB/IV071212), waarschuwt DGBel ter bescherming van de Minister voor het gebruik van de Cloud / Gegevensbescherming binnen de Belastingdienst. In de bijlage van deze brief is het risico van gegevensopslag buiten de infrastructuur (oa Cloud) van de Belastingdienst beschreven. De brief sluit af met het vertrouwen dat binnen het eigen kantoor wordt toegezien op naleving van deze regelgeving.

Recent heeft het Europees Hof van Justitie uitspraak gedaan dat 'internetbedrijven geen data van Europese burgers mogen opslaan op Amerikaanse servers. Dit mocht voorheen wel, op basis van het zogenaamde 'safe harbor'-afspraken ('veilige haven'). In de safe harbor afspraak tussen de Verenigde Staten en Europa, waarin staat dat bedrijven gegevens van gebruikers mogen opslaan op servers op elkaars grondgebied onder de voorwaarde dat de Europese wetgeving wordt gerespecteerd. Door de uitspraak van begin oktober 2015 is het steunen op de Safe Harbor afspraak niet meer mogelijk en dient opnieuw gekeken te worden welke maatregelen/aanvullende afspraken getroffen moeten worden bij gebruik van (Amerikaanse) cloud providers.

4.2.4 Proof of Concept

De Belastingdienst is aan het overwegen om het gebruik van AcceptEmail te testen in een Proof of Concept. Wij vragen ons af in hoeverre het mogelijk is in een internet situatie om een proof of concept in een beschermde/beperkte omgeving uit te voeren?

4.2.5 Mitigering risico's door geformuleerde maatregelen?

Bij beantwoording door geïnterviewden van de vraag of de voorgenomen maatregelen de beschreven risico's in voldoende mate mitigeren, ontstaat er verschil van inzicht. De Business is overwegend voorstander van de inzet van AcceptEmail, mits de risico's goed worden beheerst. B/CIE en SOC raden implementatie ten zeerste af. Dit laatste standpunt wordt ook door Logius

(fraudeteam) gesteund. Het spreekt voor zich dat de leverancier en externe gebruikers van AE behoren tot de voorstanders.

Het lijkt vooral een kwestie van wat het zwaarste wordt gewogen. De benefits die onmiskenbaar aanwezig zijn of de risico's met de al dan niet mitigerende maatregelen?

4.2.6 Veiliger lijkende alternatieven

Bij ons onderzoek is gewezen op enkele suggesties voor een veiliger manier van gebruik maken van moderne technieken. Dit betreft bijvoorbeeld het gebruik van een berichtenbox of ontwikkelen betalingsmogelijkheden in de portalen. Naar vernomen worden deze mogelijkheden door de Belastingdienst nader onderzocht.

4.2.7 Besluitvorming door DG

De bestuurlijke lijn is dat het kernteam Roadmap Inning een positieve beslissing over de PoC voorlegt aan de RvB.
De CIO heeft in een email van 11 juni 2015 gevraagd om "uiteraard te blijven kijken naar de risico's vanuit de wil om eruit te komen, een voorstel te formuleren, al dan niet ter goedkeuring."

De ADR acht het wenselijk om vanwege de gesignaleerde risico's, door het afwijken van het vigerende beleid en afwijken van de aan het maatschappelijk verkeer gecommuniceerde gewenste gedragslijn, maar ook de mogelijke impact van de beslissing op de modernisering van het berichtenverkeer met burgers en bedrijven (een onderdeel Investeringsagenda), een beslissing over het al of niet uitvoering PoC AE, op basis van een gedegen risico-analyse voor te leggen aan de eindverantwoordelijke functionaris van de Belastingdienst, de DG.

Bijlage 1 Ontwikkelingen telefonische incasso Belastingdienst

a) Huidige werkwijze Telefonische Incasso particulieren

De Belastingdienst heeft in 2012 een succesvolle pilot uitgevoerd met Telefonische Incasso. Het actief telefonisch benaderen van geselecteerde belastingplichtigen die achterlopen met het voldoen van hun vorderingen blijkt effectief. Daarom is besloten om een regulier proces voor Telefonische Incasso voor particuliere belastingplichtigen in te richten. Het LIC is hiermee belast. De teams telefonische incasso bij het LIC bellen belastingplichtige particulieren die recent een aanmaning hebben gehad om snel een sluitende afspraak te maken voor het voldoen van de schuld. De inzet van telefonische incasso is gericht op persoonlijk contact zodat mensen hun afspraken of verplichtingen nakomen (compliance). Het doel dat in die keten wordt nagestreefd is om te voorkomen dat debiteuren in de intensievere dwanginvordering terecht komen. Op langere termijn wil de Belastingdienst het betaalgedrag van debiteuren positief beïnvloeden: de belastingplichtige betaalt tijdig en weet dat hij anders gebeld kan worden door het team Telefonische incasso. Als tijdens het gesprek de belastingplichtige aangeeft te willen betalen, wordt de betalingstoezegging geregistreerd en wordt het gesprek afgesloten.

b) Verdere effectuering telefonische Incasso particulieren

Een volgende stap om bovenstaand proces effectiever te laten zijn, is om bij het telefonisch contact aan de belastingplichtige te vragen of hij/zij gelijk wil betalen. Als deze daarop positief reageert, dan kan de Belastingdienst direct een email toesturen waarmee directe betaling via iDeal mogelijk wordt gemaakt. Deze werkwijze past goed binnen één van de onderdelen van de Investeringsagenda: "modernisering interactie met burgers en bedrijven".

Bij het proces wordt gebruik gemaakt van de extern ontwikkelde en extern gehoste applicatie "AcceptEmail".

c) Proof of concept AcceptEmail bij Telefonische Incasso particulieren

De Belastingdienst is voornemens om een proof of concept uit te voeren voor het gebruik van AcceptEmail door twee teams van het Landelijk Incasso Centrum te Amsterdam en Groningen.

De Proof of Concept is enerzijds een stap binnen het digitaliseren van het betalingsverkeer om voor het eerst betaling middels iDeal mogelijk te maken. Anderzijds wordt door de inzet van het communicatiekanaal email het aantal papieren dwangbevelen teruggebracht. De start van de proefperiode is begin november 2015 gepland en biedt de Belastingdienst de kans om gedurende een half jaar ervaring op te doen binnen een kleinschalig en beheersbare omgeving met het betalen via e-mail en iDeal. Door middel van een Proof of Concept kan de Belastingdienst verkennen of een dergelijk middel inderdaad het verwachte effect bereikt voordat zij overgaat tot aanschaf of zelfbouw. Het Kernteam Inning wordt gevraagd om in te stemmen met de Proof of Concept met AcceptEmail. Na instemming wordt het voorstel ter goedkeuring aan de COO Belastingdienst voorgelegd.

d) Geïnventariseerde risico's bij gebruik AcceptEmail

B/CA betalingsverkeer heeft in samenwerking met B/CAO, B/CIE, IM/B en AcceptEmail bv de belangrijkste risico's en beheersmaatregelen voor het gebruik van AcceptEmail verkend.

Bijlage 2 Overzicht In BuCA PoC AE uitgewerkte risico's en beheersmaatregelen

In de business case "PoC AcceptEmail bij telefonische incasso" (versie 0.7, 26 augustus 2015) zijn in hoofdstuk 10 Risico's en beheersmaatregelen opgenomen

Risico's en beheersmaatregelen

Risico's
In december 2014 heeft B/CA Betalingsverkeer op basis van kritische onderzoeksvragen onderzocht wat de belangrijkste risico's en beheersmaatregelen zijn voor het gebruik van AcceptEmail door de Belastingdienst. De risico's en de daarbij passende beheersmaatregelen zijn verder uitgekristalliseerd door B/CAO, B/CIE, Service Control Security Office, IMB Inning en AcceptEmail BV. De voornaamste risico's die verbonden zijn aan het inzetten van AcceptEmail zijn in twee groepen te verdelen:

1) Beveiliging van persoonsgegevens en het risico op phishing
Een AcceptEmail is een via e-mail verstuurd betaalverzoek of verstuurde rekening. De e-mail die naar de klant wordt verstuurd, bevat de volgende informatie:

- E-mailadres
- Naam van de debiteur
- Bedrag openstaande schuld
- Betalingskenmerk (kan gecodeerd meegestuurd worden, zie beheersmaatregel)

Deze gegevens vallen onder de wet bescherming Persoonsgegevens (Wbp). De Belastingdienst dient zich, als overheidsorganisatie werkend met persoonsgegevens, te houden aan de Wbp. Hetgeen betekent dat de Belastingdienst, als organisatie die persoonsgegevens verwerkt wegens een wettelijke plicht:

- niet meer gegevens mag verwerken dan strikt nodig is voor het uiteindelijke doel;
- de gegevens niet mag gebruiken voor andere doelen dan waarvoor ze zijn verzameld;
- de gegevens niet langer mag bewaren dan nodig is;
- passende technische en organisatorische maatregelen moet treffen om de gegevens te beschermen.

Naast plichten brengt deze inrichting de volgende risico's met zich mee:

- Indien een dergelijke email van de gebruiker wordt gehackt kunnen deze gegevens openbaar worden.
- Behalve dat email accounts gehackt kunnen worden, kunnen e-mails ook nagemaakt worden. De AcceptEmail werkt op basis van een link in een e-mail. Aangezien 'echte' e-mails soms niet van 'namaak' e-mails te onderscheiden zijn bestaat er een kans op phishing: de klant ontvangt een betalingsopdracht via email, maar met een andere begunstigde dan de Belastingdienst.
- Het verzenden van e-mails vanuit de Belastingdienst is nog niet conform het huidige beleid.

2) Extern Hosten
Persoonsgegevens mogen volgens de Wbp alleen worden verwerkt voor het doel waarvoor ze verkregen zijn. Onderzoek van de Nederlandse overheid heeft geleerd dat clouddiensten dit onvoldoende waarborgen (Brief van J.P.H Donner met het

kenmerk: 2011-2000097712 aan de Tweede Kamer, 2011). AcceptEmail B.V. maakt gebruik van de Microsoft-omgeving (Cloud) als dataopslagplaats. Het overheidsbeleid is dat we gebruik maken van eigen, interne cloud diensten. Persoonsgegevens mogen volgens de Wbp alleen naar landen met een zelfde beschermingsniveau worden doorgegeven. Uitzonderingen zijn bedrijven, waaronder Microsoft, die zich hebben aangesloten bij de 'Safe Harbor': een gestroomlijnd proces voor bedrijven in de Verenigde Staten om te voldoen aan Europese richtlijn 95/46/EG over bescherming van persoonsgegevens.

De gegevens van in de proef betrokken belastingplichtigen worden bij het inzetten van AcceptEmail ondergebracht bij een derde partij, te weten AcceptEmail B.V. De data staat op de beveiligde Microsoft-omgeving en wordt maximaal 1 jaar bewaard. Deze manier van gegevensopslag brengt wel risico's met zich mee: in het uitzonderlijke gevallen waarin een persoon verdacht wordt van terroristische activiteiten kan de Amerikaanse overheid de gegevens en database van die persoon rechtstreeks opvragen bij een Amerikaanse Cloud Computing provider als Microsoft.

Beheersmaatregelen
In het kader van (technische) beveiliging van persoonsgegevens, het risico op phishing en extern hosten worden bij het uitvoeren van de Proof of Concept de volgende 6 beheersmaatregelen in acht genomen:

1. Alleen contact naar aanleiding van een ontvangen aanmaning:
   Iedere e-mail wordt na bespreking over de openstaande schuld vooraf telefonisch afgesproken en alléén verzonden met toestemming van de belastingplichtige. Omdat de medewerker Telefonische Incasso dan met hem/haar in contact staat, weet deze dat er een betaalverzoek onderweg is, waarbij er feitelijk toestemming is gegeven tot het versturen van een digitale factuur met betaallink. Dus pas na verificatie van (persoons)gegevens zal de medewerker een e-mail versturen, met daarin een link naar iDeal.
2. Onder water meesturen gegevens in de mail:
   In iedere verstuurde AcceptEmail staan het e-mailadres, de naam en de openstaande vordering opgenomen. Het betalingskenmerk waarin met een berekening het BSN nummer is opgenomen, hoeft als zodanig niet te worden opgenomen. Het is namelijk mogelijk om het betalingskenmerk 'onder water' gecodeerd mee te sturen en pas bij ontvangst bij de Belastingdienst te decoderen. Hierdoor zijn de BSN's niet te achterhalen indien de email postbus van de belastingplichtige wordt gehackt.
3. Verificatie:
   Er zijn 5 verifieringspunten voor de belastingplichtige dat er géén sprake is van phishing, hierover zal pro-actief worden gecommuniceerd.
   Allereerst kent de Belastingdienst de naam van de belastingplichtige en wordt deze ook altijd vermeld in de e-mail. Ten tweede bellen we de belastingplichtige en verifiëren dat we dat we met de belastingplichtige spreken en refereren aan een eerder ontvangen aanmaning zodat deze weet dat hij met de Belastingdienst spreekt. Alléén na telefonisch contact wordt een AcceptEmail verstuurd. Ten derde wordt AcceptEmail trusted sender gemaakt waardoor de klant alleen e-mail ontvangt waarvan het e-mailadres eindigt op @belastingdienst.nl. Ten vierde verschijnt in de iDeal-omgeving het betalingskenmerk dat overeen komt met het betalingskenmerk uit de ontvangen Acceptgiro. Tot slot zal voor de Proof of Concept gebruik worden gemaakt van het bekende centrale rekeningnummer (NL86INGB0002445588) van de Belastingdienst. Hierdoor zullen de betrokkenen zeker weten dat zij zaken doen met de Belastingdienst. De betaling met het juiste banknummer en de tenaamstelling staat zowel in de AcceptEmail als in de iDealomgeving al klaar.
   Door deze maatregelen wordt de kans op phishing verkleind.

4. Communicatie Website en template:
   De vijf punten van verificatie worden pro-actief zowel in de template van AcceptEmail als op de site van de Belastingdienst gecommuniceerd. Mochten er vragen komen dan kan de Belastingtelefoon verwijzen naar de speciale webpagina waar kenbaar wordt gemaakt dat voor een aantal processen gebruik wordt gemaakt van AcceptEmail met FAQ.
5. Gegevens cloud maandelijks gewist:
   AcceptEmail B.V. heeft wat de IT beveiliging betreft tot op heden alle testen vanuit andere afnemers doorstaan.
   De gegevens (achternaam, email, schuld en betalingskenmerk) van in de proef betrokken belastingplichtigen worden bij het inzetten van AcceptEmail tijdelijk ondergebracht bij een derde partij, te weten AcceptEmail B.V. De data staat op de beveiligde Microsoft-cloud-omgeving en wordt normaliter maximaal 1 jaar bewaard. Deze manier van gegevensopslag brengt wel een risico met zich mee: in het uitzonderlijke geval waarin een persoon verdacht wordt van terroristische activiteiten kan de Amerikaanse overheid de gegevens en database van die persoon rechtstreeks opvragen bij een Amerikaanse Cloud Computing provider als Microsoft. Om de kans op dit risico te verkleinen is met AcceptEmail B.V. contractueel afgesproken dat de gegevens iedere maand gewist worden en in geen enkel geval langer dan 1 maand in de cloud staan.
6. Beperkt en beheersbare groep voor de proef periode
   Dynamisch monitoren selecteert wekelijks op basis van gegevens de belposten voor het proces van telefonische incasso. Voor de Proof of Concept is het mogelijk om binnen de werkvoorraad een kleine beheersbare groep te selecteren waarbij de direct contact module van Accept Email wordt ingezet.”