KPMG Advisory
Postbus 74500
1070 DB Amsterdam

Laan van Langerhuize 1
1186 DS Amstelveen
Telefoon (020) 656 7890
Fax (020) 656 7700

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Operatie BRP
Postbus 20011
2500 EA DEN HAAG

Onze ref 15 I001444 D5.2 Evaluatie inzage broncode BRP

Contact

Amstelveen, 2 september 2015

Betreft: Evaluatie inzage broncode BRP

Op uw verzoek hebben bij conform onze opdrachtbevestiging met referentie 15 I001444 een evaluatie uitgevoerd naar de inzage in de broncode van operatie BRP (hierna: oBRP). Het is ons een genoegen u hierbij de resultaten van deze evaluatie aan te bieden.

Managementsamenvatting

Deze rapportage bevat de antwoorden op de gestelde onderzoeksvragen. Het onderzoek is bedoeld om vanuit een onafhankelijke positie te bezien of de inzage is verlopen zoals bedoeld, aan de doelstellingen heeft beantwoord en of naar de toekomst toe wijzigingen aanbevelenswaardig zijn.

In het kader van de inzage van de broncode zijn een plan van aanpak en een overeenkomst voor responsible disclosure opgesteld. Uit onze evaluatie komt naar voren dat:

- oBRP in het kader van een interne evaluatie een duidelijk feitenrelaas heeft opgesteld van de voorbereiding, de uitvoering en afronding van de inzage;
- de overeenkomst voor responsible disclosure goed heeft gefunctioneerd, conform de 'Leidraad Responsible Disclosure' van het Nationaal Cyber Security Centrum (NCSC);
- de inzageronde ten aanzien van de doelstelling 'gratis kwaliteitscontrole' nuttig is gebleken. De gedane bevindingen zijn, hoewel in aantal beperkt, relevant. De bevindingen waren al bekend uit eerdere software kwaliteitschecks. De bevindingen blijven nuttig omdat hiermee aanvullende zekerheid is verkregen dat er geen aanvullende kwetsbaarheden in de code geconstateerd zijn en
- de inzage ook ten aanzien van de doelstelling 'transparant zijn over de voortgang' waarde heeft: werkende stukken software kunnen worden ingezien en worden beschouwd in relatie tot de stapsgewijze ontwikkeling zoals vastgelegd in het opleverplan van de BRP.

Onze conclusie is dat het voor de hand ligt om volgende inzageronden te organiseren. Onze suggestie daarvoor is om inzage mogelijk te maken na afronding van iedere BOP-stap waarin een werkende versie van de software wordt opgeleverd. Ook adviseren wij om na afronding

van de ontwikkeling van de BRP de afweging te maken of, en zo ja welk deel van, de broncode van de BRP openbaar gemaakt kan worden en onder welke voorwaarden dat kan geschieden. Op dat moment dient tevens de afweging worden gemaakt of de broncode, en zo ja welk deel daarvan, als open source software beschikbaar wordt gesteld. Tot slot adviseren wij het plan van aanpak aan te scherpen om enerzijds de verwachtingen van geïnteresseerde partijen in lijn te brengen met de doelstelling van de inzage en om anderzijds meer belangstelling en feedback te verkrijgen.

Achtergrond

Binnen het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) ontwikkelt het programma oBRP de Basis Registratie Personen (verder BRP). De minister van BZK (hierna: de minister) heeft de Tweede Kamer toegezegd de broncode van de BRP binnen kaders voor inzage beschikbaar te maken. Het doel daarbij is tweeledig, te weten enerzijds inzicht geven in de voortgang en anderzijds organiseren van 'gratis kwaliteitscontrole' waarbij externe partijen kwetsbaarheden kunnen melden. Inmiddels is aan enkele belangstellenden inzage in de broncode geboden, overeenkomstig de toezegging van de minister. Het programma oBRP heeft een interne evaluatie uitgevoerd. In aanvulling daarop is behoefte aan evaluatie door een externe partij.

Vraagstelling

U heeft aan ons gevraagd om, vanuit een onafhankelijke positie, invulling te geven aan een beknopt onderzoek. Tijdens dit onderzoek hebben wij ons gericht op de volgende vijf onderzoeksvragen:

1. Is de interne evaluatie volledig en is deze duidelijk?
2. Heeft de responsible disclosure goed gefunctioneerd en is er aanleiding deze aan te passen?
3. Heeft de inzage een bijdrage geleverd aan de doelstellingen en was deze nuttig?
    a) Ten aanzien van doelstelling 'gratis kwaliteitscontrole': waren de gedane bevindingen relevant en nuttig?
    b) Ten aanzien van de doelstelling 'transparant zijn over de voortgang': heeft de inzage een bijdrage geleverd aan deze doelstelling en was deze nuttig?
4. Voldoet het huidige proces in het licht van de toezegging van de minister en zijn discussies hierover met de Tweede Kamer?
5. Heeft u suggesties voor aanpassing van het huidige proces, rekening houdend met het aantal belangstellenden, de toezegging van de minister en zijn discussies hierover met de Tweede Kamer en met (beveiligings) risico's?

Scope

Het onderzoek is uitgevoerd op basis van aan KPMG Advisory N.V. beschikbaar gestelde informatie en publiek toegankelijke informatie.

Aanpak

Na afstemming met de opdrachtgever en het opleveren van de benodigde documentatie, zijn de volgende werkzaamheden uitgevoerd:

- bestuderen documentatie;
- interview met projectleider inzage van het programma oBRP;
- controle van de PC die voor inzage is gebruikt en
- afstemmen van de bevindingen met opdrachtgever.

Beantwoording van de 5 onderzoeksvragen

1) Is de interne evaluatie volledig en is deze duidelijk?

Op 3 augustus jl. is het interne evaluatiedocument van de inzageronde aan de gedelegeerd opdrachtgever BRP aangeboden. Het interne evaluatiedocument is opgesteld door de projectleider van de inzageronde. Het document betreft een feitelijk verslag van de stappen uitgevoerd in het proces.

Bij het interne evaluatiedocument hebben wij de volgende observaties:

- de voorbereiding en uitvoering van de inzage en afronding daarvan worden gestructureerd en duidelijk omschreven. Ten eerste is beschreven hoe het proces van aankondiging van de inzageronde en de aanmelding is verlopen. Vervolgens is beschreven welke stappen er zijn genomen na aanmelding van geïnteresseerde partijen. Hierbij is opgemerkt dat twee partijen die zich na de deadline van 15 mei 2015 hebben aangemeld alsnog de mogelijkheid tot inzage hebben gekregen. Dit is conform de opmerking van de minister in het Algemeen Overleg van 20 mei 2015. Van de dag van inzage zelf is voor elk van de twee reviewende partijen een verslag van het gevolgde proces opgenomen. Hierbij is vastgesteld dat enkele procedures zoals beschreven in het plan van aanpak niet strikt zijn gevolgd. Zo is, anders dan de procedure voorschrijft, het maken van foto's en gebruik van de eigen laptops van de reviewers wel toegelaten. Ten slotte bevat het document een samenvatting van de bevindingen en evaluaties van de deelnemers.
- de interne evaluatie is niet opgesteld als een evaluatie van het plan van aanpak en de doelstelling van de inzage waardoor onderdelen als de kosten, geleerde lessen, mate waarin de doelstelling is gerealiseerd niet zijn opgenomen. Overigens zijn de kosten van deze inzage wel door het oBRP geïnventariseerd.

2) Heeft de responsible disclosure goed gefunctioneerd en is er aanleiding deze aan te passen?

Centraal bij het werken met responsible disclosure staat het verhelpen van kwetsbaarheden en het verhogen van de veiligheid van het informatiesysteem. Het op verantwoorde wijze melden van kwetsbaarheden kan in belangrijke mate bijdragen aan het verhogen van de veiligheid van deze systemen. Vanuit dit idee heeft oBRP, als gedelegeerd opdrachtgever, een responsible disclosure opgezet welke is gebaseerd op de leidraad voor Responsible Disclosure zoals opgesteld door het Nationaal Cyber Security Centrum (NCSC) en de hierin benoemde bouwstenen. Het ministerie heeft op de volgende wijze invulling gegeven aan deze bouwstenen:

- oBRP heeft een beleid rondom responsible disclosure vastgesteld en dit publiekelijk toegankelijk kenbaar gemaakt. Dit heeft plaatsgevonden door de aankondiging en het plan van aanpak op de website van oBRP te plaatsen;
- oBRP heeft deelname aan de inzage laagdrempelig gemaakt. Dit is kenbaar gemaakt in het plan van aanpak zoals gepubliceerd op de website van oBRP. Elke geïnteresseerde partij kon zich aanmelden zonder verdere selectie hetgeen ook als zodanig heeft plaatsgevonden;
- oBRP heeft capaciteit gereserveerd om adequaat op meldingen te kunnen reageren. oBRP heeft blijkens onder andere het interne plan van aanpak capaciteit gereserveerd voor de inzageronde. Alle meldingen gemaakt door reviewers als resultaat van de inzage zijn, blijkens de vastleggingen van het inzage proces, serieus geanalyseerd en teruggekoppeld aan de reviewer. Hierbij heeft oBRP op enkele punten om opheldering gevraagd aan de reviewer;
- oBRP heeft in de overeenkomst met de reviewende partijen de termijn voor het bekendmaken van meldingen bepaald op 60 dagen. Van deze termijn kan worden afgeweken. Dit is kenbaar gemaakt in het plan van aanpak zoals gepubliceerd op de website van oBRP en
- oBRP heeft in de overeenkomst tevens toegezegd geen juridische stappen te ondernemen tegen reviewers die conform de overeenkomst handelen.

Hiermee is geconstateerd dat de responsible disclosure met betrekking tot de broncode van de BRP goed heeft gefunctioneerd, conform de 'Leidraad Responsible Disclosure' van het NCSC. De aard van de gedane meldingen is niet dusdanig dat sprake is van een kwetsbaarheid die ook in andere applicaties aanwezig is. oBRP heeft ons inziens dan ook terecht het NCSC niet over de gedane meldingen geïnformeerd. Verder hebben alle partijen (oBRP en de twee reviewende partijen) zich gehouden aan de afspraken in de overeenkomst inzake responsible disclosure. Hierbij dient te worden opgemerkt dat door een reviewende partij foto's zijn gemaakt en getweet. Op een gepubliceerde foto zijn ook oBRP-medewerkers te herkennen. Volgens de responsible disclosure was dit niet verboden. Eventueel had via het portretrecht hierop actie kunnen worden ondernomen. Hiervoor is niet gekozen. Wij adviseren de responsible disclosure hier ook niet op aan te passen. Het zonder toestemming van betrokkene

publiceren van foto's blijft niet fatsoenlijk daar hoeven wat ons betreft geen afspraken over worden vastgelegd.

Daarnaast kan het zinvol zijn om de term 'documentatie' in het plan van aanpak expliciet te definiëren , waarbij wij opmerken dat de ter beschikking gestelde documentatie moet passen bij de doelstelling van de inzage. In onze optiek passen daar vanuit het perspectief van het geven van inzicht in de voortgang en het organiseren van "gratis kwaliteitscontrole" uitsluitend documenten bij die inzicht geven in de opzet en de structuur van de broncode.

3) Heeft de inzage een bijdrage geleverd aan de doelstellingen en was deze nuttig?

   a) Ten aanzien van doelstelling 'gratis kwaliteitscontrole': waren de gedane bevindingen relevant en nuttig?

      In de brief van de minister d.d. 3 maart 2014 wordt als een van de doelstellingen van de responsible disclosure een 'gratis kwaliteitscontrole' genoemd. Externe partijen krijgen daarbij de mogelijkheid om kwetsbaarheden in de broncode te detecteren en te melden aan oBRP. oBRP definieert kwetsbaarheden als *'een zwakke plek in de broncode die een bedreiging kan vormen voor het correct en ongestoord functioneren van de BRP dan wel voor de beveiliging van de gegevens in de BRP'.*

      In de overeenkomst met de deelnemers aan de responsible disclosure is opgenomen dat oBRP van de deelnemer verwacht dat zij kwetsbaarheden zo snel mogelijk zullen melden en kennis over kwetsbaarheden niet met partijen buiten oBRP zullen delen.

      Tijdens de inzageronde is de deelnemers een formulier ter beschikking gesteld om gedane bevindingen in te registreren ten behoeve van oBRP. De interne evaluatie vermeldt dat de reviewende partij A het formulier heeft ingevuld (formulier Partij A) met vier bevindingen en dat het formulier door een medewerker van oBRP met de reviewende partij is doorgenomen. Van de vier bevindingen van Partij A zijn er drie geclassificeerd met de ernstcategorie 'laag' en een als 'middelmatig'. Daarnaast zijn de bevindingen door een oBRP-medewerker geclassificeerd als twee vragen en twee constateringen (bevindingenformulier Partij A). oBRP heeft deze bevindingen geanalyseerd en op 21 juli jl. een inhoudelijke reactie gestuurd aan Partij A. De twee bevindingen welke een vraag betroffen zijn hierbij beantwoord, de twee bevindingen welke een constatering betroffen zijn door oBRP als te adresseren issue verwerkt.

      Reviewende partij B, heeft geen bevindingenformulier ingevuld op de dag van de inzage. Middels een emailbericht is door één van de reviewers namens partij B op 15 juni bevestigd dat er door partij B geen enkele zwakke plek in de code is aangetroffen.

      Op basis van een analyse van de gedane bevindingen concluderen wij dat, hoewel in aantal beperkt, deze relevant zijn. De bevindingen waren daarbij al bekend uit eerdere software kwaliteitschecks. De bevindingen blijven nuttig omdat hiermee aanvullende zekerheid is verkregen dat er geen aanvullende kwetsbaarheden in de code geconstateerd zijn.

b) Ten aanzien van de doelstelling 'transparant zijn over de voortgang': heeft de inzage een bijdrage geleverd aan deze doelstelling en was deze nuttig?

In het informatiedocument dat aan de deelnemers van de responsible disclosure is verstrekt, staan de BOP-stappen genoemd waarvan de broncode gedurende de inzageronde beschikbaar worden gesteld. Dit betreft de volgende objecten:

- *de broncode van de BOP-stappen 2.1 en 2.2;*
- *de broncode voor BOP-stap 3.1, onderdeel leveringen in GBA-formaat en*
- *de "as is"-versie van de broncode voor BOP-stap 3.1, onderdeel leveringen in BRP-formaat.*

Dit zijn alle geplande BOP-stappen tot en met het tweede kwartaal van 2015 conform het programmaplan van de oBRP d.d. 8 november 2014 zoals beschikbaar op de website van oBRP. Beredeneerd vanuit het plan van aanpak is, door inzage te verlenen, transparantie betracht ten aanzien van de voortgang van de BOP-stappen versus de broncode zoals gereed op de periode van inzage.

Hierbij dient te worden opgemerkt dat de code die ter inzage is aangeboden overeenkomt met de broncode die in mei 2015 door ons is onderzocht met dien verstande dat wel extra test- en configuratiebestanden zijn meegeleverd.

De mate waarin inzage in de broncode van afgeronde delen van de software als zodanig nuttig is, is een vraag van een andere orde. Hierbij hebben wij de volgende opmerkingen:

- Meerdere inzageronden bieden de deelnemers de mogelijkheid de voortgang tussen de verschillende inzageronden te vergelijken. Het ligt hierbij in de lijn der verwachting dat geplande BOP-stappen als leidraad voor het tijdstip van inzage aan te houden omdat dan ook functioneel duidelijk is wat ter inzage wordt aangeboden. Door meerdere inzageronden te hanteren wordt de doelstelling om transparantie te betrachten over de voortgang nog beter gediend.
- Inzage in de broncode is slecht één van de maatregelen die de minister heeft aangekondigd om de Tweede kamer op de hoogte te houden van de voortgang van oBRP[1]. Met dit pakket aan maatregelen streeft de minister een relatief grote mate

---

1 De minister heeft in een brief aan de Tweede Kamer op 28 oktober 2013 een aantal maatregelen aangekondigd om de Tweede Kamer op de hoogte te houden van de voortgang van de Operatie BRP, te weten:

- Halfjaarlijkse voortgangsrapportages aan de Tweede Kamer;
- Inrichten onafhankelijke Quality Assurance;
- Instellen productiviteitsmetingen;

van publieke transparantie na. Zo is oBRP van de tien financieel meest omvangrijke ICT-projecten op het Rijks ICT Dashboard, het enige project dat over een eigen website met publieksinformatie beschikt (www.operatiebrp.nl). Op deze website staan niet alleen stukken die logischerwijs openbaar zijn, zoals kamerstukken, maar ook gedetailleerde, interne documenten zoals draaiboeken en stuurgroepstukken. Ook is oBRP het eerste overheidsprogramma in Nederland dat kwaliteitstoetsen via een website openbaar maakt en broncode ter inzage heeft aangeboden.

Een korte analyse van (online) nieuws rond de inzageronde maakt duidelijk dat nieuwsberichten kritisch zijn op de mate van transparantie over de voortgang en beschikbaar gestelde documentatie die wordt geboden tijdens de inzageronde (artikelen op computable.nl van 19 juni 2015 en van 24 juni 2015). Opvallend hierbij is dat in alle nieuwsartikelen één van de belangstellenden wordt geciteerd. Hoewel de inzage dus een aanleiding kan geven om met kritische noten de publiciteit te zoeken (en dat zal bij volgende inzageronden weer zo zijn) wordt daarmee de doelstelling van de inzage rond de voortgang juist bevorderd.

Op basis van bovenstaande heeft de inzage nut gehad en is invulling gegeven aan de belofte van minister aan de Tweede Kamer.

4) Voldoet het huidige proces in het licht van de toezegging van de minister en zijn discussies hierover met de Tweede Kamer?

Sinds het derde kwartaal van 2013 is diverse keren in het Algemeen Overleg Overheid en ICT/mGBA (hierna: AO) gesproken over de broncode, waarbij de minister toezeggingen heeft gedaan over de broncode, de wijze van beschikbaarstelling en de randvoorwaarden die hierbij gelden, en de evaluatie van de inzageperiode.

Op basis van het plan van aanpak, zoals gepubliceerd op de website van oBRP en de interne evaluatie van de inzageronde door oBRP en inspectie van de ter inzage aangeboden software kan worden vastgesteld dat het huidige proces voldoet in het licht van de toezegging van de minister op 7 november 2013 en latere discussies over dit onderwerp, zowel per brief van de minister aan de Tweede Kamer als binnen AO's. In aanvulling op de in eerste aanleg geformuleerde doelstelling (nl. gratis kwaliteitscontrole en transparant zijn over de kwaliteit van de software) heeft de minister in het AO van november 2014 toegelicht dat er met de inzage ook transparantie gaat ontstaan over de voortgang. Dit is vervolgens als zodanig ook als doelstelling in het plan van aanpak verwoord.

- Periodieke oplevering werkende versies van de BRP.

Vervolgens heeft de minister in het Algemeen Overleg van 7 november 2013 aan de Tweede Kamer toegezegd om inzage in de broncode mogelijk te maken om de kwaliteit van de software transparant te maken. De minister heeft deze toezegging in zijn brief van 3 maart 2014 aan de Tweede Kamer bevestigd en nader toegelicht.

5) Heeft u suggesties voor aanpassing van het huidige proces, rekening houdend met het aantal belangstellenden, de toezegging van de minister en zijn discussies hierover met de Tweede Kamer en met (beveiligings) risico's?

Rekening houdend met het aantal belangstellenden hebben wij de volgende suggesties:

- *Probeer meer belangstelling te genereren door naast bekendmaking op de website van oBRP ook andere kanalen aan te boren gericht op doelgroepen waarvan het waarschijnlijk is dat er interesse is om kwetsbaarheden in de code op te sporen.*

- *Formuleer specifieke vragen waar feedback op gewenst is in plaats van één open vraag naar kwetsbaarheden. Overweeg hierbij tevens deze vragen te gebruiken om na afloop van de reviewperiode met de reviewer samen te zitten om mondelinge feedback te verzamelen.*

- *Bedenk dat een inzageronde aanleiding kan zijn voor professionals voor vaktechnische discussies; oBRP hoeft aan die discussies niet deel te nemen.*

Het vrijgeven van de broncode voor inzage is een goede manier gebleken om transparant te zijn over de kwaliteit van de software en is een goede manier gebleken on een 'gratis kwaliteitscontrole' te organiseren. Het ligt wat ons betreft daarom voor de hand om volgende inzageronden te organiseren. Rekening houdend met de toezegging van de minister en discussies hierover met de Tweede Kamer hebben wij de volgende suggesties:

- *Stel vast in welke periode een volgende inzage zal plaatsvinden. Wij bevelen hierbij aan om inzage te verlenen na afronding van iedere BOP-stap (cf. programmaplan) die een werkende versie van de software oplevert. Op die wijze kan inzage worden verleend of de BOP-stap ook daadwerkelijk afgerond is wat betreft op te leveren code. Het ligt in de lijn der verwachting dat 'werkende delen' van de software bij overgangen van BOP-stappen ter inzage wordt aangeboden. Meer frequent heeft geen toegevoegde waarde: het ontwikkelteam moet ook enige tijd gegund worden om ook daadwerkelijk aanvullende software te ontwikkelen.*
- *Ook na afronding van de ontwikkeling van het systeem kan openbaar maken van de broncode worden overwogen. Doelstelling kan dan transparantie over de werking en het bevorderen van hergebruik van de software zijn. In een dergelijke situatie zou uitsluitend inzicht in de productieversie afdoende zijn.*
  Bij systemen die, zoals de BRP, een hoge mate van vertrouwelijkheid en integriteit vereisen, kunnen er mogelijk redenen zijn om niet, of niet meteen, de volledige broncode te openbaren. Dit punt wordt ook door de minister aangehaald in zijn brief van 3 maart 2014. Een alternatieve methode voor omgang met deze trade-off tussen openbaarheid en vertrouwelijkheid is een gesloten gemeenschap. Zo heeft Denemarken een systeem waarbij open source software in een centraal register (www.digitaliser.dk) wordt

geplaatst wat toegankelijk is voor alle overheidsorganisaties voor hergebruik en evaluatie, maar niet daarbuiten. Joinup (https://joinup.ec.europa.eu/) is een vergelijkbaar initiatief van de Europese Commissie.

- *Overweeg na afronding van het programma of de broncode en zo ja welk deel daarvan als Open Source software beschikbaar wordt gesteld. Graag attenderen wij hierbij op het volgende:*

  - *Het gebruik van open source software betekent niet dat modificaties die door een gebruiker in de software worden aangebracht ook openbaar moeten worden gemaakt. Zelfs wanneer de software door de gebruiker opnieuw gedistribueerd is, is het afhankelijk van de licentie of er ook een verplichting is om aanvullende modificaties openbaar te maken.*
  - *De keuze om binnen een programma Open Source Software te gebruiken, eventueel als basis voor doorontwikkeling (van een component), wordt regulier bij de start van een ICT-project gemaakt. In dit kader verwijzen wij ook naar de 'Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten' gepubliceerd op 8 november 2008. Hierin is de zogeheten 'comply or explain and commit-regime' opgenomen ten aanzien van het gebruik van open standaarden voor overheidsorganisaties.*
  - *In de brief van 3 maart 2014 van de minister aan de Tweede Kamer is aangegeven dat intellectueel eigendom van de ontwikkelde software bij het Ministerie van Binnenlandse zaken en Koninkrijksrelaties berust.*

  De software van de oBRP is thans geen Open Source Software. Het verlenen van inzage in, of het openbaar maken van, de software van oBRP, met de door de minister aangegeven motivatie, maakt de software niet noodzakelijkerwijs zelf Open Source. Ook het gebruik maken van open source middelen door operatie BRP maakt de ontwikkelde software niet Open Source Software. Uiteraard kan het Open Source maken van de software worden overwogen. Gezien de aard van de functionaliteit is echter niet te verwachten dat er veel behoefte voor hergebruik is; zeer waarschijnlijk zal er ook geen community van ontwikkelaars ontstaan die een bijdrage leveren.

Tot slot

Dit advies is gebaseerd op een beknopt onderzoek en is bedoeld als evaluatie voor de operatie BRP van de inzage van broncode. De evaluatie is niet bedoeld voor andere partijen en het gebruik van de evaluatie door andere partijen is dan ook voor eigen risico. KPMG aanvaardt geen aansprakelijkheid voor het gebruik van deze evaluatie anders dan waarvoor het is opgesteld en aanvaardt geen aansprakelijkheid jegens andere partijen dan het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Wij hebben dit advies zorgvuldig en in afstemming met uw team samengesteld. Wij vertrouwen erop u met deze rapportage inzicht te hebben geboden in het inzageproces. We blijven gaarne bereid om dit advies nader toe te lichten.

Met vriendelijke groet,

KPMG Advisory N.V.

drs. J.M.A. Koedijk CISA CISM
Partner

Bijlage(n):
Geraadpleegde documentatie

Bijlagen

Geraadpleegde documentatie

Voor dit onderzoek is de volgende documentatie van de website van oBRP, gebruikt:

- *Plan van Aanpak inzage broncode BRP maart 2015*
- *Responsible Disclosure BRP*
- *Nieuwsbericht-Inzage broncode Basisregistratie Personen*

Voor dit onderzoek is de volgende documentatie, verkregen uit openbare bronnen, gebruikt:

- OSEPA Policy Recommendation Paper (geraadpleegd op 7 augustus 2015): *http://osepa.eu/pdeliverables/Policy%20Reccomendation%20Paper.pdf*
- Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten (geraadpleegd op 7 augustus 2015): *http://wetten.overheid.nl/BWBR0024717/geldigheidsdatum_07-08-2015*
- Actieplan Nederland Open in Verbinding (geraadpleegd op 7 augustus 2015): *http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2010/07/01/actieplan-nederland-open-in-verbinding.html*
- Rapport Algemene Rekenkamer over Open Standaarden en Open Source software bioj de Rijksoverheid (geraadpleegd op 7 augustus 2015): *http://www.rekenkamer.nl/Publicaties/Onderzoeksrapporten/Introducties/2011/03/Open_standaarden_en_opensourcesoftware_bij_de_rijksoverheid*
- A Practical Guide to Using Free Software in the Public Sector (geraadpleegd op 7 augustus 2015): *https://joinup.ec.europa.eu/community/osor/home/communities/eupl/FAQ-LL-V131-EN.pdf*
- Programmplan Operatie BRP (geraadpleegd op 7 augustus 2015): *http://www.operatiebrp.nl/sites/operatie-brp/files/Programmaplan%20Operatie%20BRP%20publicatie%201.0.pdf*
- Bericht van R. Veldwijk, vertegenwoordiger Ockham Groep (geraadpleegd op 7 augustus 2015): https://twitter.com/ReneJanV/status/613728769224871936
- Verslag van het Algemeen Overleg Overheid en ICT van 7 november 2013 (geraadpleegd op 10 augustus 2015): https://zoek.officielebekendmakingen.nl/kst-26643-303.html
- Leidraad om te komen tot een praktijk van Responsible Disclosure van het Nationaal Cyber Security Centrum (geraadpleegd op 11 augustus 2015): https://www.ncsc.nl/actueel/Responsible+Disclosure+Leidraad

- 11 Best Practices for Peer Code Review van Smartbear (geraadpleegd op 11 augustus 2015): https://smartbear.com/SmartBear/media/pdfs/11_Best_Practices_for_Peer_Code_Review.pdf
- *Brief TK 3 maart 2014 over beschikbaar stellen broncode: https://zoek.officielebekendmakingen.nl/kst-26643-307.html*
- *Brief TK 6 maart 2015: https://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/documenten/kamerstukken/2015/03/06/kamerbrief-tussentijdse-rapportage-operatie-brp*
- *Verslag van een algemeen overleg gehouden op 20 mei 2015 over ICT-aangelegenheden: http://www.tweedekamer.nl/vergaderingen/commissievergaderingen/details?id=2015A01596*
- *Verslag_van_een_algemeen_overleg,_gehouden_op_25_juni_2014,_over_de_Digitale_overheid: http://www.tweedekamer.nl/vergaderingen/commissievergaderingen/details?id=2013A05381Verslag_van_een_algemeen_overleg,_gehouden_op_27_november_2014,_over_Basisr egistratie_personen: http://www.tweedekamer.nl/vergaderingen/commissievergaderingen/details?id=2014A04949*
- *Verslag vragenuurtje 23-06-2015:*

  https://zoek.officielebekendmakingen.nl/h-tk-20142015-99-4.html?zoekcriteria=%3fzkt%3dUitgebreid%26pst%3dParlementaireDocumenten%26vrt%3dBRP%26zkd%3dInDeGeheleText%26dpr%3dAlle%26spd%3d20150901%26epd%3d20150901%26verj%3d2015%26kmr%3dTweedeKamerderStatenGeneraal%26sdt%3dKenmerkendeDatum%26par%3dHandeling%26dst%3dOnopgemaakt%257cOpgemaakt%257cOpgemaakt%2bna%2bonopgemaakt%26isp%3dtrue%26pnr%3d1%26rpp%3d10&resultIndex=0&sorttype=1&sortorder=4