Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 16292 2500 BG Den Haag

Ministerie van Justitie en Veiligheid
T.a.v. de minister, mevrouw D. Yeşilgöz-Zegerius
Postbus 20301
2500 EH Den Haag

Adviescollege ICT-toetsing

Muzenstraat 95
Den Haag
Postbus 16292
2500 BG Den Haag
Nederland

www.adviescollegeicttoetsing.nl

Contactpersoon

info@adviescollegeicttoetsing.nl

Kenmerk
2022-0000105814

Uw kenmerk
3234608

Bijlage(n)
1 Definitief BIT-Advies

Datum	28 februari 2022
Betreft	BIT-advies project Realisatie JBZ-systemen

Geachte mevrouw Yeşilgöz-Zegerius,

Uw voorganger, de heer Grapperhaus, heeft het Adviescollege ICT-toetsing, verzocht een toets uit te voeren op het project Realisatie JBZ-systemen.
Het Adviescollege heeft haar onderzoek naar dit project afgerond. Bijgaand treft u het definitieve advies aan.

Uw ambtenaren zijn geïnformeerd over de strekking van het advies. Voor de volledigheid maak ik u erop attent dat nu de periode van vier weken ingaat waarbinnen het advies met de bestuurlijke reactie naar de Tweede Kamer dient te worden gestuurd.

Met de meeste hoogachting,
namens het Adviescollege ICT-toetsing,

w.g.

prof. dr. J.P.J. Verkruijsse RE RA
Voorzitter

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 16292 2500 BG Den Haag

Ministerie van Justitie en Veiligheid
T.a.v. de minister, mevrouw D. Yeşilgöz-Zegerius
Postbus 20301
2500 EH Den Haag

Adviescollege ICT-toetsing

Muzenstraat 95
Den Haag
Postbus 16292
2500 BG Den Haag
Nederland
www.adviescollegeicttoetsing.nl

Contactpersoon
[redacted]

Kenmerk
2022-0000105823

Uw kenmerk
3234608

Datum 28 februari 2022
Betreft Definitief BIT-advies project Realisatie JBZ-systemen

Geachte mevrouw Yeşilgöz-Zegerius,

Uw voorganger, de heer Grapperhaus, heeft het Adviescollege ICT-toetsing verzocht een toets uit te voeren op het project Realisatie JBZ[1]-systemen (JBZ). De opdrachtgever van dit project is de directeur Regie Migratieketen. Het advies kan als volgt worden samengevat:

Het project JBZ realiseert het Europaloket voor berichtenverkeer met lidstaten over terugkeerbesluiten en inreisgegevens van derdelanders. Het projectbudget is geraamd op 10 miljoen euro.

Conclusie
Er bestaat een reëel risico dat Nederland niet tijdig voldoet aan EU-eisen voor beveiliging en privacybescherming aan het Europaloket. Daarvoor zijn drie redenen:
A. Aansluiteisen en governancestructuur voor de ketenpartners binnen Grenzen en Veiligheid zijn onvoldoende uitgewerkt.
B. Eisen voor het Europaloket zijn onvoldoende uitgewerkt.
C. Een tijdige afronding is onzeker, ondanks uitstel invoeringsdatum.

Advies
Wij adviseren u maatregelen te nemen om tijdige en veilige uitwisseling van gegevens tussen Nederland en de EU mogelijk te maken:
1. Richt binnen de keten Grenzen en Veiligheid een eenduidige en transparante governance voor beveiliging en privacybescherming in.
2. Scherp de eisen voor het Europaloket aan.
3. Neem maatregelen om het risico op verdere uitloop te beperken.

Hieronder vindt u een korte beschrijving van het project en de gekozen reikwijdte van ons onderzoek. Daarna werken we bovenstaande analyse en adviezen uit. Wij concentreren ons hierbij op de belangrijkste risico's. In de bijlage staan de details van het project.

[1] Justitie Binnenlandse Zaken

KORTE OMSCHRIJVING VAN PROJECT EN BEREIK TOETS

Het project JBZ is gedefinieerd door het programma Grenzen en Veiligheid (GenV) en vervolgens belegd bij de directeur Regie Migratieketen binnen het ministerie van JenV. Het ondersteunt de implementatie van twee Europese verordeningen die Nederland verplichten om reizigers uit derde landen te registreren in het Entry Exit Systeem (EES) en terugkeerbesluiten vast te leggen in het Schengen Informatie Systeem (SIS-TKB). Dit berichtenverkeer tussen de lidstaten dient bij te dragen aan minder illegale immigratie, grotere veiligheid en soepeler verlopende grensprocessen. De betrokken ketenpartners zijn de IND, KMar en de Nationale Politie.

Het beoogde resultaat van het project JBZ is:

- de ingebruikname van de door eu-LISA – het ICT-agentschap van de EU – geleverde National Uniform Interface (NUI);
- de realisatie van het Europaloket, dat fungeert als koppelvlak tussen de NUI en de systemen van de Nederlandse ketenpartners;
- een governancestructuur waardoor aangetoond kan worden dat Nederland voldoet aan de eisen ten aanzien van beveiliging en privacybescherming die Europa stelt bij het koppelen van het Europaloket aan de NUI.

Ons onderzoek richt zich op de totstandkoming van het Europaloket en bijbehorende governancestructuur omdat de NUI bij aanvang van ons onderzoek reeds in gebruik was genomen. Bij de analyse van de governancestructuur is uitgegaan van het door het project geformuleerde doel dat Nederland aantoonbaar "in control en audit-proof" moet zijn ten aanzien van de verplichte eisen aan beveiliging en privacybescherming uit de beide verordeningen. Dit betekent niet dat het project JBZ verantwoordelijkheid draagt voor de implementatie van deze eisen bij de ketenpartners. Ketenpartners hebben eigen organisatorische en ICT-implementatietrajecten ingericht om de beide verordeningen te kunnen uitvoeren. Deze vallen buiten de scope van het project JBZ en van dit onderzoek.

Dit onderzoek is uitgevoerd tussen 6 juli en 1 november 2021.

CONCLUSIE: RISICO DAT NEDERLAND NIET TIJDIG VOLDOET AAN EU-EISEN

Er bestaat een reëel risico dat Nederland niet tijdig een Europaloket operationeel heeft dat aantoonbaar voldoet aan de hoge EU-eisen voor beveiliging en privacybescherming. Enerzijds ligt dat aan de uitwerking van die eisen op twee gebieden: de keten (A) en het Europaloket zelf (B). Anderzijds bestaat het risico dat het Europaloket zelf niet tijdig werkend kan worden opgeleverd (C). Hieronder werken we deze drie punten verder uit.

A. Uitwerking aansluiteisen en governancestructuur keten onvoldoende

De EES- en de SIS-TKB-verordeningen stellen hoge eisen aan de beveiliging en de privacybescherming. We vinden de manier waarop het project deze eisen heeft uitgewerkt naar de aansluitvoorwaarden voor de ketenpartners onvoldoende. Dat geldt ook voor de uitwerking van de governancestructuur waarbinnen ketenpartners moeten aantonen dat ze aan deze eisen voldoen. Wel waarderen we dat het project het inrichten van zo'n governancestructuur tot zijn taak rekent, in de wetenschap dat er op dit moment geen bevoegde instantie is die de ketenpartners formeel kan opleggen aan de gestelde eisen te voldoen.

De belangrijkste tekortkomingen zijn:

- De voorgestelde governancestructuur kent hiaten. Zo is de verantwoordelijkheid voor de compliance van de keten als geheel onvoldoende belegd. Ook ontbreekt op het niveau van de keten een proces van pas-toe-of-leg-uit, en is onduidelijk wie bevoegd en verantwoordelijk is voor het accepteren van afwijkingen ten opzichte van de gestelde eisen.
- De aansluitvoorwaarden voor ketenpartijen bevatten nog onduidelijkheden en openstaande punten zijn daardoor onvoldoende normatief. Van de veertig beveiligingseisen uit de EU-documentatie zijn er slechts twaalf verwerkt in de specificaties, zonder dat gemotiveerd is waarom de andere EU-eisen niet van toepassing zijn.
- Een geïntegreerd bedrijfscontinuïteits- en uitwijkplan voor de gehele keten – zoals vereist in de beide verordeningen – ontbreekt.
- In de lijst met beveiligingseisen en -maatregelen zijn geen eisen opgenomen ten aanzien van de beschikbaarheid en de performance van zowel het Europaloket als de aansluitingen van ketenpartijen daarop.
- Wij hebben geen uitwerking gezien van de in-controlverklaringen[2] van de ketenpartijen, noch wat betreft het proces, noch inhoudelijk. De toetsing van de verklaringen wordt bovendien niet door een onafhankelijke derde partij uitgevoerd, maar via een peerreview.

B. Uitwerking eisen voor het Europaloket onvoldoende

Het project heeft de eisen op het gebied van beveiliging en privacybescherming uit de EU-verordeningen en nationale wet- en regelgeving vertaald en geconcretiseerd in eisen voor de ontwikkeling van het Europaloket door ICTU en het beheer door D-ICT. Wij plaatsen daarbij de volgende kanttekeningen:

- De uitgevoerde analyse is onvolledig. Het project baseert zich op twee documenten van eu-LISA met daarin slechts een deel van de uitwerking van de beveiligingseisen uit de verordeningen. Bovendien zijn de beveiligings-onderwerpen niet altijd met dezelfde detaillering uitgewerkt als in de verordeningen. Voorbeelden van eisen die niet zijn meegenomen zijn:

[2] In een 'in-controlverklaring' legt een organisatie verantwoording af over de werking van de beheersingsmaatregelen gericht op het voldoen aan gestelde eisen.

  - eisen met betrekking tot het nationale beveiligingsplan en bedrijfscontinuïteits- en uitwijkplannen;
  - eisen rond de aansprakelijkheid voor en de afhandeling van beveiligingsincidenten;
  - trainingsverplichtingen voor medewerkers van ketenpartijen die toegang krijgen tot EES-gegevens.
- Het project heeft vastgesteld dat voor de gegevensuitwisseling via het Europaloket het Basisbeveiligingsniveau 3 (BBN3) geldt. Bij dat beveiligingsniveau is een specifieke analyse van de risico's als gevolg van statelijke actoren noodzakelijk. Die heeft niet plaatsgevonden. Wel is een dreigingsanalyse (PLATO–sessie) uitgevoerd met NCSC en de ketenpartners. Daarbij is echter niet specifiek gekeken is naar kwetsbaarheden in het Europaloket. Bovendien blijkt uit de aangeleverde goedgekeurde lijst met beveiligingsmaatregelen dat aanvullende maatregelen die wel uit deze dreigingsanalyse naar voren zijn gekomen nog niet zijn uitgewerkt en gepland.
- Hoewel het realisatietraject al ver gevorderd is, bevat de hiervoor genoemde lijst met beveiligingseisen en -maatregelen nog onduidelijkheden en openstaande punten. De lijst is daarom op die punten onvoldoende normatief voor ICTU en D-ICT en bovendien niet controleerbaar. Ook bestaat het risico dat zaken achteraf moeten worden aangepast. Voorbeelden van openstaande punten hebben we tijdens ons onderzoek met het project gedeeld.
- In de door JBZ opgestelde aansluitvoorwaarden voor de ketenpartners is de eis opgenomen dat in de berichten een uniek identificerend nummer mee wordt gestuurd van de medewerker die de actie uitvoert. In de berichtspecificaties van het Europaloket is die eis afgezwakt tot herleidbaarheid tot een systeem.
- We hebben niet kunnen vaststellen hoe het project toetst dat ICTU en D-ICT voldoen aan de eisen op het gebied van beveiliging en privacy, en invulling geven aan de bijbehorende maatregelen. Tijdens onze toets hebben wij drie significante kwetsbaarheden geconstateerd die niet bekend waren bij het project. We hebben deze om veiligheidsredenen separaat gerapporteerd aan het project.

C. Tijdige afronding onzeker ondanks uitstel invoeringsdatum

Doordat het realisatietraject voor het Europaloket pas laat is gestart, was de planning vanaf het begin al erg krap. Door veranderende specificaties bij de ontwikkeling van het loket en verlate oplevering van de testomgeving bleek in oktober 2021 dat de resterende tijd tot de invoering van de beide verordeningen onvoldoende was voor het uitvoeren van de noodzakelijke keten- en andere testen. Kort daarna werd duidelijk dat de EU van plan is om de invoering van de beide verordeningen vier maanden op te schuiven. Hierdoor ontstaat weliswaar enige ruimte voor het project, maar de planning blijft krap.

We zien bovendien een aantal risico's waardoor het tijdpad verder onder druk kan komen te staan:

- Er is een reële kans op nieuwe tegenvallers in het ontwikkeltraject. Ontwerpdocumenten bevatten nog belangrijke hiaten. Vereisten waaraan de

door ICTU ontwikkelde functionaliteit en de beheeromgeving bij D-ICT moeten voldoen, ontbreken deels of zijn niet eenduidig en slechts op hoofdlijnen vastgesteld. De totale omvang van de nog te bouwen functionaliteit is bovendien niet bepaald.
- De Privacy Impactanalyse (PIA) is pas in december 2021 uitgevoerd. Daardoor is er weinig tijd om extra maatregelen die daaruit voortvloeien binnen de vigerende planning in te passen.
- Het maken van afspraken met ketenpartners over het uitvoeren van ketentesten wordt bemoeilijkt doordat planningen steeds opnieuw opschuiven. Zo werd in oktober 2021 duidelijk dat de oplevering van de testomgeving bij D-ICT, die al eerder drie maanden was vertraagd door connectiviteits-problemen, nog verder uitloopt. Verkorten van de doorlooptijd van het testproces is bovendien lastig, omdat de beschikbare testcapaciteit beperkt is.

ADVIES: MAAK TIJDIGE EN VEILIGE UITWISSELING MET EU MOGELIJK

Om ervoor te zorgen dat Nederland bij de invoering van de EES- en de SIS-TKB-verordening kan voldoen aan de eisen van de EU en u uw verantwoordelijkheid kunt nemen voor een veilige en betrouwbare gegevensuitwisseling tussen de ketenpartners en Europa, adviseren we de volgende maatregelen te nemen:

1. Richt een eenduidige en transparante governance in

Het risicoprofiel van het Europaloket en het berichtenverkeer tussen de ketenpartners en Europa als gevolg van de beide verordeningen vereist een governancestructuur met eenduidig belegde verantwoordelijkheden, passende aansluiteisen en een transparante verantwoordingssystematiek. Concreet adviseren we u daarom het volgende:
- Wijs binnen de keten één functionaris – bijvoorbeeld de DG Migratie – aan die verantwoordelijk is voor het vaststellen en bewaken van de compliance van alle partijen èn de keten als geheel. Laat deze met de directie Regie Migratieketen en de ketenpartijen eenduidige afspraken maken over de aansluitvoorwaarden en over de inhoud van en het proces rond de in-controlverklaringen, en de wijze waarop binnen de keten wordt omgegaan met eventuele afwijkingen.
- Laat het project de analyse van vereisten vanuit de EU-verordeningen en de Nederlandse wet- en regelgeving volledig maken en vertalen naar aansluitvoorwaarden voor ketenpartijen.
- Overweeg om een onafhankelijke partij als de Auditdienst Rijk de in-controlverklaringen van de ketenpartners te laten toetsen.

2. Scherp eisen beveiliging en privacy Europaloket aan

Om te voldoen aan de gestelde eisen op het gebied van beveiliging en privacybescherming adviseren wij u het volgende:
- Draag zorg voor een volledige en specifieke risicoanalyse van de dreiging door statelijke actoren (op het niveau BBN3), bijvoorbeeld op basis van de Kwetsbaarheidsanalyse Spionage van de AIVD. Trek daarbij ook lering uit

recente incidenten waarbij statelijke actoren zich wederrechtelijk toegang hebben verschaft tot reisgegevens van personen.
- Vraag het project de eisen op het gebied van beveiliging en privacybescherming voor ICTU en D-ICT aan te scherpen, in lijn met de beide EU-verordeningen en de Nederlandse wet- en regelgeving, en zorg te dragen voor een effectieve toetsing op de naleving.

3. Neem maatregelen om het risico op verdere uitloop te beperken

Om te zorgen dat het Europaloket tijdig het berichtenverkeer in het kader van de EES- en de SIS-TKB-verordening kan verwerken dient het project de volgende acties uit te voeren:
- Maak zo snel mogelijk de openstaande specificaties van het Europaloket af. Vertaal deze specificaties naar functionele en niet-functionele eisen aan de door ICTU op te leveren functionaliteit en de beheeromgeving van D-ICT en maak de ontwerpdocumenten compleet. Maak op basis daarvan inzichtelijk hoeveel werk nog moet worden verricht.
- Werk met D-ICT een terugvalscenario uit waardoor ten minste een deel van de geplande testen volgens de planning kan worden uitgevoerd.
- Breng met de ketenpartners de consequenties van de bijgestelde planning in beeld. Stel op basis daarvan samen met de ketenpartners een realistische, taakstellende planning op voor het afronden en in beheer nemen van het Europaloket en voor het testen, en maak afspraken over de in te zetten capaciteit.

* * *

Tot slot danken wij alle geïnterviewden voor hun medewerking en openheid bij deze toets. We hopen u met dit advies aanknopingspunten te hebben gegeven voor het tijdig en veilig kunnen inzetten van het Europaloket in het berichtenverkeer met de lidstaten. We zijn graag bereid het project nogmaals gedetailleerd te informeren over onze specifieke bevindingen op het gebied van informatiebeveiliging en privacy.

Met de meeste hoogachting,
namens het Adviescollege ICT-toetsing,

w.g.

prof. dr. J.P.J. Verkruijsse RE RA
Voorzitter

w.g.

drs. S.J. van Amerongen
Secretaris-directeur

Bijlage

Informatie over project Realisatie JBZ-systemen

Nr.	Onderwerp	Toelichting
1.	Projectnaam	Realisatie JBZ-systemen KV
2.	Opdrachtgever	Directeur Regie Migratieketen van het ministerie van Justitie en Veiligheid
3.	Startdatum project	1 januari 2019
4.	Einddatum project	Mei 2022 (nazorgfase)
5.	Type project	Realisatie ICT-voorziening
6.	Fase Project	Realisatiefase
7.	Totaal budget	10,1 miljoen euro
8.	Reeds uitgegeven per datum	5,2 miljoen (per oktober 2021)
9.	Doelstelling	Realisatie van twee nationale ICT-voorzieningen voor informatie-uitwisseling met eu-LISA over terugkeerbesluiten en derde landen-reizigers, inclusief de governance over de voorzieningen
10.	Maatschappelijke/ beleidsdoelstelling	Het bestrijden van illegale immigratie, vergroten van veiligheid binnen het Schengengebied en het faciliteren van het grensproces
11.	Meetbare Baten	Snellere informatie-uitwisseling met andere EU-lidstaten over derde landen reizigers
12.	Huidige technologie/ architectuur	"afstempelen" van reisdocumenten bij in- en uitreis van onderdanen derde landen
13.	Doeltechnologie/- architectuur	Services via API-proxy (nieuw) of BVV Endpoint (bestaand), ebXML-berichten via een standaard product (Axway), in generieke infrastructuur van D-ICT RedHat Enterprise Linux versie 8 OS met aanvullende middleware, DBMS en netwerkdiensten
14.	Omvang systeem	Niet bekend
15.	Aantal gebruikers	Zo'n tienduizend gebruikers maken via de systemen van ketenpartners indirect gebruik van het Europaloket.
16.	Belanghebbenden	Samenwerkingsverband van de ketenpartijen Ketenvoorzieningen (JenV/DGM/KV), IND, KMar, Politie Ontwikkeling: ICTU Beheer: Dienst ICT Politie en eu-LISA
17.	Aanbesteding voorzien	Nee (uitvoering door overheidspartijen)

Informatie over het uitgevoerde onderzoek

Nr.	Onderwerp	Toelichting
1.	Aanmelddatum project	24 maart 2021
2.	Start onderzoek	6 juli 2021
3.	Afronden onderzoek	1 november 2021
4.	Datum concept advies	17 januari 2021
5.	Datum definitief advies	28 februari 2021
6.	Eerder onderzoek	Niet van toepassing
7.	Onderzoeksmethode	Interviews, documentstudie, data-analyse/broncode-onderzoek software ontwikkelomgeving