nationale ombudsman

# Inhoud

# 1 Inleiding

Voor u ligt een document met technische eisen van de Nationale ombudsman (de No) als onderdeel van de eisen en wensen voor de aanbesteding van een nieuw Zaaksysteem en een nieuw Document Management Systeem (DMS). Met deze technische eisen heeft de No een set van niet-functionele eisen tot haar beschikking, die worden toegepast bij de selectie in beheer name van de eerder genoemde systemen.

## 1.1 Waarom technische eisen?

Dit document bevat een set van niet-functionele eisen waaraan het nieuwe Zaaksysteem en het DMS dienen te voldoen.

Deze technische eisen gelden niet enkel bij het selecteren van de informatie systemen en de overdracht hiervan naar beheer, maar ook gedurende de exploitatieperiode in geval van wijzigingen en/of vernieuwing.

Met behulp van deze technische eisen wordt er voor gezorgd dat de gegevens in en van de nieuwe systemen op een efficiënte, effectieve, communicatieve en voor de gebruikers eenduidige wijze ontsloten worden.

Als zodanig zijn de geselecteerde technische eisen een onderdeel van de acceptatiecriteria, waaraan het geselecteerde Zaaksysteem en DMS worden getoetst.

Het kan ook zijn dat een eis zoals beschreven niet exact van toepassing is omdat die maatregel bijvoorbeeld betrekking heeft op een product en de leverancier een dienst levert. In dat geval volstaat een korte uitleg waarom de maatregel niet van toepassing is. Ook kan het zijn dat de maatregel zoals beschreven niet zoals beschreven aanwezig is, maar dat er een andere maatregel is getroffen die vergelijkbaar of zelfs beter is. Ook dan volstaat een korte uitleg.

## 1.2 Afstemming binnen de overheid

Deze set No specifieke technische eisen verwijst naar rijksbrede (aansluit)voorwaarden en richtlijnen. Hiermee borgt de No dat zij nu en in de toekomst gebruik kan maken en aan kan (blijven) sluiten op overheidsbrede voorzieningen.

## 1.3 Scope

De scope van dit document omvat de technische eisen die aan een nieuw zaaksysteem en DMS worden gesteld.

## 1.4 Pas toe of Leg uit

Het doel van deze technische eisen is om nu en in de toekomst de gewenste functionaliteit en dienstverlening te kunnen bieden op een efficiënte en effectieve wijze. Het niet voldoen aan de geselecteerde technische eisen kan gevolgen hebben voor de No ICT Infrastructuur in het algemeen en het betreffende informatiesysteem in het bijzonder. Dit kan leiden tot meerkosten en/of het niet kunnen afgeven van garanties over de beheer(s)baarheid, beschikbaarheid, robuustheid en performance van het informatiesysteem.

Anderzijds kunnen er natuurlijk gegronde redenen zijn voor het afwijken van een of meerdere eisen. Bijvoorbeeld omdat er een andere techniek of betere oplossing geboden wordt. Het verdient dan ook de aanbeveling voor de leverancier om te allen tijde afwijkingen van de eisen te onderbouwen en deze af te stemmen met en te laten accorderen door de eigenaar van het Programma van Eisen. Deze handelswijze wordt aangeduid met Pas toe of Leg uit, ook bekend als ‘Comply or Explain’.
Informatiemanagement en architectuur ondersteunen de eigenaar van het Programma van Eisen bij het beoordelen van de onderbouwing. Hierbij zijn de Nationale ombudsman Enterprise Principes leidend[1].

[1] Zie bijlage 1 Enterprise Principes Nationale ombudsman

## 1.5 Risicoafweging en Informatie beveiliging

Door de No is een BIO scan uitgevoerd en hiermee is vastgesteld dat de eisen binnen de BIO afdoende beveiliging bieden.
De overheid kent enkele kaders met betrekking tot informatiebeveiliging waaraan informatiesystemen moeten voldoen. Dat zijn:

- Baseline Informatiebeveiliging Overheid (BIO)
- Algemene Verordening Gegevensbescherming (AVG)

Om de interpretatie verschillen te voorkomen hebben de Functionaris Gegevensbescherming en de Chief Information Security Officer relevante eisen van de BIO en de AVG geselecteerd. Deze eisen zijn voor het nieuwe Zaaksysteem en het nieuwe DMS van de Nationale ombudsman van toepassing en in het programma van eisen opgenomen als los document: "Privacy & Security eisen nieuwe zaaksysteem en DMS" Let wel, ook voor deze eisen geldt voor de leveranciers Pas toe of Leg uit, zie paragraaf 1.4

## 1.6 Leeswijzer

Het document is als volgt opgebouwd:

- Hoofdstuk 2 beschrijft de eisen welke gehanteerd worden bij de selectie van informatiesystemen;
- Indien een geselecteerd, dan wel ontwikkeld, informatiesysteem een webapplicatie betreft of biedt zijn de eisen zoals opgenomen in hoofdstuk 3 additioneel van toepassing;
- Hoofdstuk 4 beschrijft de voorwaarden voor het in beheer nemen en de exploitatie van informatiesystemen;
- Hoofdstuk 5 beschrijft enkele cloud specifieke eisen.

## 1.7 Referenties en begrippen

In dit document wordt, onder vermelding van de tussen blokhaken geplaatste afkorting, verwezen naar de volgende documenten en publicaties

| Referentie | Document/Bron |
|---|---|
| BIO | Baseline Informatiebeveiliging Overheid |
| AVG | Algemene Verordening Gegevensbescherming |
| FS | Forum Standaardisatie |
| DigiK | Digikoppeling Standaard voor gegevensuitwisseling |
| NoEP | Nationale ombudsman Enterprise Principes |

# 2 Selectie eisen

Dit hoofdstuk beschrijft niet-functionele eisen die gehanteerd worden bij de selectie van informatiesystemen. Bij de aanbesteding gelden deze als aanvulling op de functionele en toepassing specifieke eisen.
Niet relevante eisen zijn uit deze lijst gehaald, daardoor zal de nummering op sommige plaatsen niet doorlopen.

## 2.1 Gebruikersinterface

| Nr. | Eis | |
|---|---|---|
| 2.020 | De gebruikersinterface van het informatiesysteem is een webinterface en wordt ontsloten in de browser. | |
| 2.040 | De ontsluiting van de applicatie, de gebruikersinterface (UI), mag geen belemmeringen opleveren voor het plaats en tijd onafhankelijk werken | |
| 2.050 | Middelen die nodig zijn voor het uitvoeren van de werkzaamheden met behulp van het informatiesysteem. (b.v. printers) zijn door de gebruiker eenvoudig te selecteren | |
| 2.060 | De gebruikersinterface, handleidingen en helpbestanden voor de eindgebruikers zijn in het Nederlands opgesteld. Gebruikersinterfaces en helpbestanden voor beheerders mogen Engelstalig zijn. | |
| 2.070 | De gebruikersinterface dient in zijn volledigheid getoond te worden bij de standaard schermresolutie (1920x1080) van de door de No verstrekte gangbare mobiele werkplekken (laptops). | |
| 2.071 | De beeldschermen op het kantoor van de No ondersteunen een resolutie van 3440x1440, automatisch schalen naar deze resolutie is een mooie toevoeging, geen eis. | |
| 2.080 | Er is voor de gebruiker duidelijk onderscheid of de gebruiker gegevens bekijkt (bijv. communicatie op intranet en een adresgids) of gegevens bewerkt. | |
| 2.090 | De getoonde gegevens en toepassingen zijn gepersonaliseerd. De getoonde gegevens zijn relevant voor de gebruiker, er worden alleen toepassingen en/of functionaliteiten getoond waarvoor de gebruiker geautoriseerd is. | |

## 2.2 Applicatie Architectuur

| Nr. | Eis | |
|---|---|---|
| 2.100 | Voor gegevensuitwisseling met een informatiesysteem in de No Infrastructuur kan gebruik gemaakt worden van een Enterprise Service Bus (ESB) voorziening. Deze wordt in de toekomst geïntegreerd. Informatie ontsluiting via API's of webservices is beschikbaar in het nieuwe zaaksysteem en het nieuwe DMS. | |
| 2.110 | Gegevensuitwisseling met andere overheidsinstanties gebeurt op basis van de standaarden van Digikoppeling [DigiK]. | |
| 2.120 | Zowel inkomend als uitgaand berichtenverkeer tussen systemen van de No en systemen daarbuiten kan in de toekomst plaatsvinden via een ESB. | |

| Nr. | Eis | |
|---|---|---|
| 2.130 | De applicatie maakt gebruik van een bij het desbetreffende toepassingsgebied vermelde verplichte open standaard, zoals vastgesteld door het Forum Standaardisatie [FS]. | |
| 2.150 | Applicatielogica en -data dienen gescheiden te worden opgeslagen. | |
| 2.160 | Het informatiesysteem maakt onderscheid tussen gebruikersinformatie (bv. gebruikersinstellingen) en (globale) applicatie-informatie. De eerste wordt opgeslagen op een gebruikerslocatie of in een gebruikersprofiel, de tweede op een locatie welke toegankelijk is voor alle instanties / sessies van de applicatie(componenten). | |
| 2.180 | Het informatiesysteem ondersteunt Single Sign On (SSO) voor authenticatie van gebruikers in functie met een No-account gebruikmakend van een AD koppeling en in de toekomst van een IDM koppeling. Zie ook hoofdstuk 5.3 Eén Identiteit. | |
| 2.200 | Functioneel beheer op het informatiesysteem wordt uitgevoerd door gebruikers met aanvullende rechten op het informatiesysteem en zonder administrator rechten op het onderliggende besturingssysteem. Dit is een webgebaseerde gebruikers-interface voor beheerders. In de documentatie van het informatiesysteem (zie ook 5.1) worden de rechten en de objecten/componenten waarop de rechten betrekking hebben, beschreven. | |
| 2.210 | Informatiesystemen moeten separaat en flexibel (per gebruiker) configureerbaar zijn en geen vaste verwijzingen te bevatten naar:<br>• Databasenamen;<br>• Driveletters;<br>• Werkfolders;<br>• Tijdelijke folders;<br>• IP adressen;<br>• Directory systemen (LDAP);<br>• Domeinnamen;<br>• Licentie gegevens, c.q. bestand(en);<br>• (Service) accounts;<br>• Omgevingsspecifieke (OTAPP) variabelen;<br>• Configureerbare applicatie instellingen.<br>Deze lijst moet aanpasbaar zijn en niet hardcoded in de applicatie zitten | |
| 2.230 | Het informatiesysteem maakt geen gebruik van hardware (dongles) voor licentiebeheer. | |
| 2.240 | Het informatiesysteem maakt geen gebruik van parallelle poorten (fysiek). | |
| 2.250 | Informatiesystemen welke gebruik maken van een klok, geven de juiste tijd aan volgens GMT+1, rekening houdend met zomer- en wintertijd. | |

| Nr. | Eis | |
|---|---|---|
| 2.260 | Indien een informatiesysteem uit meerdere componenten bestaat, een relatie heeft of een integratie kent met andere systemen en/of applicaties (bijvoorbeeld de MS Office componenten), wordt aangegeven welke functionaliteit wordt gebruikt, welke datastromen (transport en opslag) worden onderkend en welke eisen worden gesteld aan de gerelateerde systemen en applicatie(s) c.q. componenten van applicatie(s). | |

## 2.3 Beheer en Beveiliging

| Nr. | Eis | |
|---|---|---|
| 2.280 | Het informatiesysteem voldoet aan de relevante kaders zoals opgegeven door de security officer bij aanvang van het project, zie paragraaf 1.5 en de AVG en BIO eisen (los document, onderdeel van het programma van eisen) | |
| 2.290 | Als het informatiesysteem persoonsgegevens verwerkt voldoet het informatie systeem aan de Algemene Verordening Gegevensbescherming (AVG), zie paragraaf 1.5 en de AVG en BIO eisen (los document, onderdeel van het programma van eisen) | |
| 2.300 | Indien er systeemprocessen bewaakt moeten worden (bijvoorbeeld monitoring van services of batchverwerking), is het informatiesysteem geschikt voor opname in de system management tooling van de beheerder van de No Infrastructuur. | |
| 2.350 | Het gebruik van MS Access als databaseplatform is niet toegestaan | |
| 2.370 | Het informatiesysteem mag geen eisen stellen aan de omgeving die conflicterend zijn met andere systemen en/of applicaties (gebruik conflicterende DLL's, etc.). | |
| 2.380 | Voor de juiste werking van het informatiesysteem zijn geen aanpassingen aan (de instellingen van) bestaande informatiesystemen in de No infrastructuur, of delen daarvan, noodzakelijk. | |
| 2.400 | Het informatiesysteem maakt geen gebruik van scripts (vbs, bat, cmd) en command line interpreters (zoals de Windows command prompt, cmd.exe). | |
| 2.410 | Van het informatiesysteem is het volgende bekend en beschikbaar:<br>1) Change log met wijzigingen t.o.v. de voorgaande versie;<br>2) Verwerkingswijze van transacties en/of handelingen: batch of (near) realtime;<br>3) Afhankelijkheden met andere informatiesystemen en/of applicaties in de vorm van specificaties van software die door het informatiesysteem gebruikt wordt zoals database, databaseversie, benodigde licenties, etc.;<br>4) Op welke wijze de authenticatie beveiligd is, bijvoorbeeld m.b.v. gebruikersnaam/wachtwoord en/of 2-factor authenticatie;<br>5) Welke autorisaties vereist zijn; | |

| Nr. | Eis | |
|---|---|---|
| | 6) Databeheer: bewaartermijn(en), databehoefte (verwachte hoeveelheid opslag), belangrijke normwaarden en beschrijving hoe te handelen in geval van een verstoring;<br>7) Informatie over netwerkconnectiviteit:<br>a) welke protocollen gebruikt het informatiesysteem in communicatie met andere lagen (tiers) of andere systemen en/of applicaties;<br>b) welke (firewall)poorten gebruikt het informatiesysteem in communicatie met andere lagen (tiers) of andere systemen en/of applicaties;<br>c) ondersteunt de communicatie routering en Network-Addres Translation (NAT) over IP;<br>d) bandbreedtegebruik voor verschillende vormen van functionaliteit (bijv. queries uitvoeren, printen, etc.);<br>e) robuustheid van de netwerkcommunicatie bij lage bandbreedte:<br>- hoge latency;<br>- wat gebeurt er bij uitval van een verbinding / wat zijn de gevolgen voor de gebruiker. | |

# 3 Eisen voor webapplicaties

De volgende richtlijnen zijn van toepassing wanneer de applicatie als webapplicatie wordt aangeboden.

| Nr. | Eis | |
|---|---|---|
| 4.010 | Voor webapplicaties welke ook van buiten de No infrastructuur toegankelijk moeten zijn, geldt dat dit met een internetverbinding mogelijk moet zijn. | |
| 4.020 | De leverancier levert een document aan waaruit blijkt dat de webapplicatie met goed gevolg gevalideerd is met de W3C Markup Validation Service [2] | |
| 4.030 | Een webbased applicatie maakt ***geen*** gebruik van proprietary applicatie-componenten, zoals plug-ins en applets. Deze kunnen namelijk niet door de gebruiker worden geïnstalleerd. | |
| 4.040 | Webapplicaties welke ook buiten de No infrastructuur toegankelijk moeten zijn, zijn geschikt voor gebruik met alle browserversies die een marktaandeel van meer dan 5% hebben. Zie bijvoorbeeld de website van Netmarketshare[3] voor de gebruiksstatistieken per browserversie (Desktop Share by Version). De leverancier geeft een verklaring af dat aan deze voorwaarde is voldaan. Dit geld bijvoorbeeld voor de persoonlijke internet pagina (zie functionele eisen) | |
| 4.050 | Webapplicatie voor gebruik vanaf de No infrastructuur (interne web applicaties) zijn geschikt voor gebruik op de No standaard werkplekken geleverde browsers; te weten Google Chrome en Microsoft Edge (beide versie 87.x en hoger) | |
| 4.060 | Webapplicaties die ook buiten de No infrastructuur toegankelijk moeten zijn werken correct op de stockbrowser van elke mobile OS versie (Android, iOS) met een marktaandeel van meer dan 5%. Zie de website van Netmarketshare voor de gebruiksstatistieken per browserversie op een mobiel apparaat (Mobile Share by Version). De leverancier geeft een verklaring af dat aan deze voorwaarde is voldaan. Dit geld bijvoorbeeld voor de persoonlijke internet pagina (zie functionele eisen) | |
| 4.070 | De gebruikersinterface moet voldoen aan de No huisstijl. De leverancier geeft een verklaring af dat aan deze voorwaarden is voldaan. | |
| 4.080 | De webapplicatie voldoet ten minste aan de voor (semi-)overheid verplichte toegankelijkheidseisen voor websites en mobiele applicaties, zie DigiToegankelijk[4]. De leverancier geeft een verklaring af dat aan deze voorwaarde is voldaan. | |
| 4.090 | De leverancier van de webapplicatie overhandigt een rapport waaruit blijkt dat de webapplicatie met goed gevolg een security scan op ten | |

[2] https://validator.w3.org/
[3] https://netmarketshare.com/
[4] https://www.digitoegankelijk.nl/

| | | |
|---|---|---|
| | minste de top 10 kwetsbaarheden, zoals opgenomen in de meest actuele versie van het OWASP Top Ten Project[5], heeft doorstaan. | |

[5] https://owasp.org/www-project-top-ten/

# 4 Eisen voor in gebruik name en exploitatie

Voordat een informatiesysteem in beheer wordt genomen dient aan een aantal voorwaarden te zijn voldaan. Deze voorwaarden blijven van kracht gedurende de lifecycle van het informatiesysteem, Wanneer niet aan deze voorwaarden is voldaan, wordt het informatiesysteem niet in beheer genomen of worden er geen garanties afgegeven voor beschikbaarheid en performance.

| Nr. | Eis | |
|---|---|---|
| 5.020 | De aanvullende maatregelen, als resultaat van de risicoanalyse zijn getroffen | |
| 5.030 | Indien, op basis van beveiligingseisen van toepassing (volgt uit risicoanalyse), dient het functioneel ontwerp te vermelden:<br>• Hoe gegevens die worden ingevoerd in informatiesystemen, worden gevalideerd op juistheid en volledigheid door de uitvoering van integriteitcontroles;<br>• Hoe de controles op het juiste verloop van de geautomatiseerde gegevensverwerking worden uitgevoerd. | |
| 5.040 | Het informatiesysteem is gereed bevonden (geaccepteerd) door de proceseigenaar alvorens deze in gebruik genomen kan worden. Aan de basis van deze acceptatie ligt een advies van de functioneel beheerder, gebaseerd op met de gebruikersgroep afgestemde acceptatiecriteria waaronder testrapporten. | |
| 5.050 | De functioneel beheerders zijn opgeleid om het informatiesysteem te kunnen beheren. | |
| 5.070 | Er is een dienstverleningsovereenkomst (DVO) tussen de proceseigenaar en dienstverlener afgesloten. | |
| 5.080 | Beheercontracten, SLA's (Service Level Agreement), DAP (Dossier Afspraken en Procedures) NOK (Nadere Overeenkomst) en licenties zijn beschikbaar wanneer van toepassing. | |

# 5 Cloudbeleid en cloud-specifieke eisen

## 5.1 Rollen met betrekking tot clouddienstverlening

Een belangrijke voorwaarde voor succesvol afnemen van cloud oplossingen is de governance van clouddienstverlening. Zonder volledig te zijn en uitputtend te zijn is het toch van belang om enkele belangrijke zaken uit lichten.

Governance zoals hier bedoeld gaat over wie welke rol heeft, wie waarvoor verantwoordelijk is, binnen welk verzorgingsgebied, welke mandaten er zijn, hoe processen rondom financiering, beheer en ontwikkeling georganiseerd zijn, wie adviseert wie en wie controleert wie, etc.
De NIST heeft een governancemodel ontwikkeld als onderdeel van de (door de NIST) opgestelde Referentie Architectuur voor Cloudcomputing[6]. Deze referentiearchitectuur wordt vanuit BZK gezien als de beoogde standaard voor de Nederlandse Rijksoverheid (programma RijksCloud) en binnen NORA wordt deze referentie architectuur ook aangehaald.

- Cloud consumer
  Een persoon of organisatie die een zakelijke relatie onderhoudt met en diensten gebruikt van een cloud provider.
- Cloud provider
  leverancier van cloud services aan geïnteresseerde partijen en consumenten.
- Cloud auditor
  Een persoon of organisatie die een onafhankelijk assessment kan doen van geleverde cloud services, operatie, prestaties en beveiliging van de cloud voorzieningen
- Cloud carrier
  Een intermediair die de connectiviteit verzorgt en de transport van cloud services van cloud provider naar cloud consument.

Het is van belang dat deze rollen belegd worden. Het moet voor de organisatie (cloud consumer) en haar gebruikers duidelijk zijn hoe ze cloud diensten kunnen afnemen. De organisatie moet weten op welke manier het gebruik van cloud diensten wordt doorbelast. Bijna alle cloud diensten kunnen geautomatiseerd worden afgenomen, zonder menselijke tussenkomst. Echter het moet duidelijk zijn, bij wie of welke organisatie men terecht kan voor customer support en hoe customer support werkt.

Het moet voor de No als organisatie, de cloud consumer,  duidelijk zijn hoe de cloud diensten worden afgenomen. De No moet weten op welke manier het gebruik van cloud diensten wordt doorbelast.

Als het model toegepast wordt op de generieke cloud dienstverlening voor de No, kan je het volgende voorstellen: de No als organisatie is cloud consumer en is afnemer  van SAAS-clouddienst verlening. Het gaat dan om de volgende middelen:

- Een DMS (SAAS/PAAS)
- Een zaakgericht werken systeem  (SAAS).

## 5.2 Integrale werking van de informatievoorziening

Het is van belang dat de integrale werking - inclusief de veranderbaarheid - en de continuïteit van de bedrijfsinformatievoorziening gegarandeerd zijn. Een oplossing die niet on premise is vergroot de complexiteit en daarmee de kans dat de integrale werking van de informatievoorziening nadelig wordt beïnvloed. Om de integrale werking te verzekeren worden de volgende richtlijnen gehanteerd:

[6] https://www.noraonline.nl/images/noraonline/4/4f/NIST_Cloud_Computing_reference_Architecture.pdf

| Richtlijn | Omschrijving |
|---|---|
| | **De integrale werking en continuïteit worden gewaarborgd** |
| RL 6 | Clouddiensten voldoen aan de open overheids- en web standaarden zoals voorgeschreven door het Forum standaardisatie. |
| RL 7 | Communicatie tussen de Private cloud, Public clouds en onpremise applicaties vindt uitsluitend plaats via webservices of API's. Deze koppelingen zijn beveiligd volgens de digikoppeling standaarden |
| RL 9 | Oplossingen die niet on-premise zijn vereisen géén aanpassingen aan de on-premise omgeving, werkplekvoorzieningen daarbij inbegrepen. Het gaat hierbij niet om cofiguratie aanpassingen zoals aan whitelisting, vpn routes, ssl decryption bypasses, firewall access lists e.a. |
| RL 10 | Een leverancier levert zijn diensten als één integraal werkende dienst (geaggregeerde dienst), waardoor geen additionele integratielast bij de organisatie ontstaat. |
| RL 11 | De leverancier moet, ten behoeve van migratie naar een andere oplossing of mogelijke verwerking door een ander systeem, altijd een gegevensdump kunnen leveren van alle in zijn systeem aanwezige organisatiegegevens. |

## 5.3 Eén Identiteit

Clouddiensten dienen gebruik te maken van een LDAP extensie op de Active Directory. Clouddiensten die worden aangeboden, moeten in de toekomst gebruik maken van de centrale, nog in te richten, IDM-omgeving. Dit is mogelijk door middel van (bijvoorbeeld) een veilig gebruik van de protocollen SAML 2.0 en OAUTH.

| Richtlijn | Omschrijving |
|---|---|
| | **Clouddiensten in één integraal IDM-systeem** |
| RL 12 | Voor de gebruiker en het beheer van de digitale identiteit en de toegangsrechten is het niet merkbaar dat een oplossing binnen of buiten de No wordt aangeboden. |
| RL 13 | Bij SaaS-diensten wijkt de digitale identiteit (de user-id) niet af van de werkplekomgeving. Het beheer van toegangsrechten, inclusief de bewaking van functie-scheiding, geschiedt vanuit één (logisch) IDM-systeem. Implementatie bij voorkeur in een Single Sign On systeem met behulp van - bijvoorbeeld - SAML. |
| RL 14 | Alle toegangsrechten worden beheerd vanuit één IDM-systeem. |

RL 13 en RL 14 zijn van toepassing na in gebruik name van een IDM door de No. De geboden cloud oplossing dient wel voorbereid te zijn of binnen een jaar na aanbesteding ondersteuning te bieden aan SSO via een IDM van de No.

# 6 Bijlage 1 Enterprise Principes van de Nationale Ombudsman

De Enterprise Principes zijn als PDF opgenomen in dit document.

Enterprise principes
Nationale ombudsm