Bijlage C - Programma van Eisen

IDP-software

22 juli 2026

Inhoudsopgave

1 Functionele requirements

1.1 Inkomende informatie en formaten

A1 Het systeem moet input van standaard scanners kunnen verwerken.
- a) Zowel pdf- als tiff-formaat moet worden ondersteund.

A2 Het systeem moet input van standaard multi-functionals kunnen verwerken
- a) Zowel pdf- als tiff-formaat moet worden ondersteund.

A3 Het systeem moet e-mails kunnen verwerken.
- a) Het moet mogelijk zijn mailboxen in Exchange te definiëren die automatisch worden uitgelezen.
- b) Bijlagen moeten in formaat pdf, xlsx, docx en jpg kunnen worden verwerkt.
- c) Het moet configureerbaar zijn of de tekst van de mail en de bijlagen in een document worden gecombineerd of als aparte documenten worden geleverd.

A4 Het systeem moet bestanden kunnen ophalen vanaf een via sFTP toegankelijke locatie.
- a) Bestanden moeten in formaat pdf, xlsx, docx en jpg kunnen worden verwerkt.

1.2 Uitgaande informatie en koppelingen

B1 Het systeem moet documenten kunnen aanleveren in PDF/A-formaat.
- a) Het systeem moet andere PDF-formaten automatisch converteren naar PDF/A-formaat.

B2 Het systeem moet documenten met metadata kunnen aanleveren via een API van ons financiële systeem, ProActis.
- a) Naast de originele PDF moet dit ook worden omgezet naar XML UBL2.1. Beide moeten worden doorgestuurd.

B3 Naast het gedigitaliseerde document zelf moeten de volgende metadata worden meegeleverd:
- a) De creatiedatum van het document;
- b) De oorsprong (welke scanner, welke mailbox, welke multi-functional, welke sFTP-site, …;
- c) Indien van toepassing: welke gebruiker was ingelogd bij het digitaliseren (bijvoorbeeld op de multi-functional);
- d) Indien van toepassing: wat is het mailadres van de afzender;
- e) De set van geëxtraheerde data, inclusief een eventueel bepaald betrouwbaarheidspercentage.

B4 Geëxtraheerde data wordt buiten het verwerkte document opgeslagen als zelfstandig object.

B5 Het systeem moet documenten met metadata kunnen aanleveren via een API.

B6 Het systeem moet documenten met metadata kunnen aanleveren via een aantal van te voren gedefinieerde netwerklocaties of FTP-verbindingen. Op dit moment is dat in gebruik voor V&O en PGB 2.0.

B7 Het systeem moet in staat zijn gedigitaliseerde documenten te beperken tot een te configureren grootte.
- a) Het moet configureerbaar zijn of deze beperking moet worden gerealiseerd door compressie of door splitsing van het document.

B8 Het systeem moet in staat zijn om een notificatie te geven aan het ontvangende systeem dat een document is aangeleverd.

1.3 Mogelijkheden voor automatische extractie

C1 Het systeem moet in staat zijn tenminste de volgende metadata te kunnen extraheren van een gedigitaliseerd document.
- a) Gedrukte of getypte tekst op een min of meer vaste plek in een document.
  - i) Barcode (de SVB gebruikt voor barcodes nu het font ‘ID Automation C128S’ met puntgrootte 22)
  - ii) QR-code
  - iii) Formuliercode of -naam
  - iv) BSN (Burgerservicenummer)
  - v) gevalsadministratienummer
- b) Handgeschreven tekst op een min of meer vaste plek in een document.
  - i) BSN (Burgerservicenummer)

ii) gevalsadministratienummer

c) Gedrukte of getypte tekst op een willekeurige plek in een document.
   i) BSN (Burgerservicenummer)
   ii) Gevalsadministratienummer
   iii) Naam leverancier
   iv) IBAN
   v) Ordernummer
   vi) Factuur- en factuurregelbedragen
   vii) BTW-bedragen en -percentages
   viii) BTW-nummers
   ix) Datums, zowel met maandnaam als maandnummer
   x) Herkennen onderscheid tussen debet- en creditfacturen. *N.B. creditfacturen zijn herkenbaar aan het woord "credit' in de nabijheid van het totaalbedrag.*

d) Handgeschreven tekst op een willekeurige plek in een document.
   i) BSN (Burgerservicenummer)

C2 De set van te herkennen metadata moet kunnen worden uitgebreid.

1.4 Controles op geëxtraheerde gegevens

D1 Het systeem moet controles kunnen uitvoeren op basis van regels voor een bepaald te extraheren gegeven.
- a) Controle op het juiste type barcode of QR-code en de juiste positie op het document. *N.B. gescande documenten bevatten regelmatig ook voor de SVB niet relevante barcodes.*
- b) Controle of een veld numeriek is.
- c) Controle op 11-proef.

D2 Het systeem moet controles kunnen uitvoeren op een combinatie van geëxtraheerde gegevens.
- a) Is het totaalbedrag op de factuur gelijk aan de som van de factuurregels.

D3 Het systeem moet API's van andere systemen kunnen aanroepen om geëxtraheerde informatie te controleren.
- a) In SVB's financiële systeem moeten via een API de volgende gegevens kunnen worden gecontroleerd:
  - i) Komt deze leverancier voor in onze registratie.
  - ii) Komt deze order voor in onze registratie.
  - iii) Is dit factuurnummer al aanwezig in onze registratie.
  - iv) het factuurbedrag met de aangegane verplichtingen.
- b) In SVB's barcode-registratie moet kunnen worden gecontroleerd of deze SVB-barcode bekend is en zo ja, welk gevalsadministratienummer daarbij hoort.
- c) Dit moet eenvoudig kunnen worden uitgebreid met nieuwe API's naar SVB systemen

1.5 Configuratie

E1 Het systeem moet verschillende configuratieprofielen ondersteunen.
- a) Het configuratieprofiel moet automatisch worden bepaald op basis van de herkomst van de gedigitaliseerde documenten: locatie van scanner of multi-functional, mailbox of bestandslocatie.
- b) Het systeem moet een gebruikers-interface bieden waarmee beheerders deze configuratieprofielen kunnen aanpassen.

E2 Per configuratieprofiel moet kunnen worden gedefinieerd op basis waarvan de scheiding in documenten moet worden gemaakt.

E3 Per configuratieprofiel moet configureerbaar zijn welke metadata moeten worden herkend.
- a) En of dit ook handgeschreven kan zijn.
- b) En welke controles hierop moeten worden uitgevoerd.
- c) En onder welk percentage zekerheid uitval plaats moet vinden.

E4 Per configuratieprofiel moet configureerbaar zijn in welke kwaliteit en of in kleuren, grijstinten of zwart-wit moet worden gescand.

E5 Per configuratieprofiel moet configureerbaar zijn hoe de output naar het gewenste SVB-systeem moet worden gestuurd; welke API of welke sFTP-verbinding.

1.6 Scankwaliteit en herstel

F1 Het systeem moet de scanstroom van de standaard scanners automatisch in documenten onderverdelen.
- a) Dit moet kunnen worden geregeld met specifieke scheidingsvellen.
- b) Dit moet kunnen worden geregeld door herkenning van een nieuwe formulier-, bar- of QR-code.
- c) Bij input vanaf de multi-functionals wordt elke door de gebruiker gestarte scan als één document gezien.

F2 Het systeem moet automatisch blanco bladzijden kunnen verwijderen.

F3 Het systeem moet oriëntatie van gescande pagina's automatisch kunnen corrigeren.

F4 Het systeem moet bij formulieren met paginanummers automatisch de volgorde kunnen corrigeren.

F5 Het systeem moet bij formulieren met een door SVB uitgegeven barcode of QR-code ook achteraf kunnen herkennen dat er meerdere formulieren in hetzelfde document zijn opgenomen.
- a) En moet in dit soort gevallen het document automatisch splitsen.

F6 Het systeem moet de gebruiker de mogelijkheid bieden tot visuele inspectie na verwerking van de scanbatch.

1.7 Verwerking uitval

G1 Het systeem moet op basis van een betrouwbaarheidspercentage van de herkenning bepalen of het document al dan niet moet uitvallen.
- a) Dit percentage moet per te herkennen gegeven kunnen worden geconfigureerd.

G2 Het systeem moet een gebruikers-interface bieden om uitval te verwerken.
- a) Het systeem moet eventuele foutmeldingen aangeven.
- b) Het systeem moet per herkend veld het betrouwbaarheidspercentage aangeven.
- c) Het moet mogelijk zijn om daarin metadata aan te vullen en te corrigeren.
- d) Het moet mogelijk zijn het document te selecteren voor een hernieuwde scan, eventueel met een ander configuratieprofiel.
  - i) Het opnieuw scannen is een handmatige actie.
  - ii) De afgekeurde scan wordt niet doorgestuurd naar een documentmanagementsysteem.
  - iii) In het systeem blijft wel zichtbaar dat bij dit document een herscan is gepland.

1.8 Rapportage

H1 Het systeem rapporteert periodiek over aantallen verwerkte documenten en pagina's.
- a) Uitgesplitst naar locatie en configuratieprofiel.
- b) Indien van toepassing wordt ook gerapporteerd over aantallen per gebruikte modules van de scanstraat.
- c) Deze rapportage moet aansluiten op de facturering van de variabele kosten.

H2 Het systeem rapporteert periodiek over herkende metadata, het gemiddelde betrouwbaarheidspercentage van die herkenning en het percentage onder en boven de gedefinieerde grens voor uitval.

H3 Rapportage kunnen eenvoudig worden geëxporteerd naar een formaat dat in SVB's BI-systeem kan worden ingelezen.

2 Non-functional requirements

2.1 Business

NA1 De Leverancier hanteert een regulier update schema voor functionele updates en fixes

NA2 Trainings,- en instructiemateriaal wordt door de Opdrachtnemer in het Nederlands aangeleverd.

NA3 De gebruiker kan de Oplossing benaderen via een webbased applicatie (browser).

a) De geleverde Oplossing dient qua standaarden en technische specificaties te voldoen aan de standaarden zoals opgesteld door het World Wide Web Consortium (W3C), dan wel de logische opvolgers daarvan

b) De Oplossing werkt naar behoren voor geautoriseerde gebruikers voor zover zij gebruik maken van de standaardinrichting van een werkstation binnen de SVB. Dit houdt onder meer in dat er geen aanvullende software of scripts vereist zijn voor het gebruik van de Oplossing.

c) De presentatielaag van de Oplossing (browser) functioneert met minimaal de laatste twee versies van Google Chrome en Microsoft Edge en moet marktconforme browsers ondersteunen (Marktconform als het een aandeel heeft van 5% van de markt, volgens W3.org, of de natuurlijke opvolger is van een bestaande marktconforme browser).

NA4 De presentatielaag van de Oplossing functioneert zonder aanvullende propriety plugins of extensies.

NA5 De Oplossing is gebruikersvriendelijk. Dit houdt ten minste in dat het aantal handelingen dat nodig is om een taak uit te voeren zo beperkt mogelijk is, dat de user interface overzichtelijk is, dat de user interface en de user experience intuïtief zijn en beperkte training vereisen, dat er een eenvoudig en snelle zoekfunctie beschikbaar is voor gebruikers waarmee informatie en functies eenvoudig vindbaar zijn. Ondersteuning conform WCAG 2.1/2.2 is gewenst.

2.2 Servicemanagement

2.2.1 Servicelevels

NB1 Opdrachtnemer draagt zorgt voor de volledige infrastructuur van de Oplossing, waaronder de housing, hosting en het technisch beheer.

NB2 De leverancier levert binnen de virtueel private cloud voor SVB twee omgevingen. Een productieomgeving en een test/acceptatieomgeving, waarbij de applicaties en data logisch en functioneel van elkaar gescheiden zijn. Dit vereist onder andere bijvoorbeeld aantoonbare instance-isolatie, gescheiden dataopslag, gescheiden logging/audittrail en gescheiden test-beheer- en supporttoegang. Voor het testen wordt geen productiedata toegepast.

NB3 De Opdrachtnemer stelt in overleg met de SVB een Exit plan op waarin de continuïteit van de Oplossing en de werkzaamheden en verplichtingen bij het aflopen of beëindigen van de Overeenkomst vastgelegd worden.

NB4 De scanstraat moet beschikbaar zijn op maandag t/m vrijdag van 7:00 tot 19:00 uur.

a) Gedurende deze periode is een Nederlandstalige servicedesk telefonisch en per e-mail bereikbaar voor ondersteuning.

b) Binnen deze uren garandeert leverancier een beschikbaarheid van 98% op maandbasis. Dat betekent een maximale onbeschikbaarheid van ca. 5 uur per maand.

NB5 Downtime in het kader van installatie van nieuwe content- en functionele componenten is alleen in overleg toegestaan.

NB6 Opdrachtnemer hanteert de volgende respons- en oplostijden voor incidenten en problemen t.a.v. de productie-omgeving van de Oplossing:

a) Prio 1: responsetijd < 10 min, en 95% in minder dan 4 uur opgelost

b) Prio 2: responsetijd < 1 uur, en 95% in minder dan 8 uur opgelost

c) Prio 3: responsetijd < 2 uur, en 95% in minder dan 16 uur (2 dagen) opgelost

d) Prio 4: responsetijd < 4 uur, en 95% in minder dan 120 uur (3 weken)opgelost

Met responsetijd bedoeld de SVB een respons op basis van (1) het incident / probleem bekend is bij Leverancier; (2) het probleem binnen Leverancier belegd is; (3) leverancier aangegeven heeft dat informatie of medewerking vanuit SVB benodigd is.

e) Ingeval van een P1 zal de leverancier per uur een update op de voortgang verstrekken aan SVB.

NB7 De productieomgeving van de Oplossing moet voldoende schaalbaar en performant zijn zodat deze initieel piekmomenten tot 10 gelijktijdige gebruikers kan opvangen, tegen gelijkblijvende performance in overeenstemming met SLA. Vanaf fase 3 moet dit kunnen worden opgeschaald naar 30 gelijktijdige gebruikers.

NB8 De oplossing is in staat om ten minste 700 documenten / 4000 pagina's per uur te verwerken.

a) Dit geldt voor de gehele SVB gezamenlijk.

b) De centrale postkamer in Utrecht moet tenminste 70% van deze performance bieden.

NB9 Schermwisselingen bij gegevensinvoer mogen 90% van de gevallen maximaal 2 seconden duren

a) Schermwisselingen bij het weergeven van zoeklijsten mogen in 90% van de gevallen maximaal 5 seconden duren

b) Samengestelde rapportages en dashboards moeten in 90% van de gevallen binnen 10 seconden na elke gebruikersinteractie worden opgebouwd en getoond worden aan de Eindgebruiker

NB10 Opdrachtnemer zorgt voor back-ups (en restoremogelijkheden) zodat er maximaal 24 uur dataverlies kan optreden. Opdrachtnemer is verantwoordelijk voor controle van de integriteit van die back-ups, alsmede het waarborgen van de vertrouwelijkheid en beschikbaarheid daarvan.

a) Een geheel of gedeeltelijke restore kan door zowel Opdrachtgever als Opdrachtnemer ingeroepen worden.

NB11 De gevraagde dienstverlening dient audit / logbestanden minimaal 18 maanden te bewaren voor toekomstig onderzoek en toegangscontrole. Alle transacties moeten gelogd worden.

a) Audit-logs mogen (binnen 18 maanden) niet verloren gaan, ook niet bij verstoringen

b) De audittrail van acties kan niet worden aangepast

NB12 Opdrachtnemer moet voorzien in passende technische en organisatorische maatregelen, waaronder monitoring, om incidenten in de productieomgeving van de Oplossing snel te kunnen detecteren, onderzoeken en op te lossen.

NB13 De Oplossing stelt een bemenste tweedelijns telefonische Nederlandstalige ondersteuning beschikbaar tijdens werkdagen van 7:00-17:30 uur Nederlandse tijd.

NB14 Opdrachtnemer verplicht zich om tijdig correctief, perfectief, preventief, adaptief en vernieuwend Onderhoud aan de Oplossing te plegen. De Opdrachtnemer verricht alle Onderhoud op de Oplossing zonder daarvoor extra kosten in rekening te brengen.

a) De Opdrachtnemer verplicht zich tot verbeteren/ vernieuwen / bijhouden van de Oplossing naar aanleiding van nieuwe of gewijzigde wet- en regelgeving en landelijke standaarden voor overheden zonder hiervoor extra kosten in rekening te brengen.

b) Daarnaast geeft de Opdrachtnemer vooraf inzage in de wijzigingen die per toekomstige Release worden uitgerold en de invloed ervan op het gebruik van de Oplossing door de SVB."

2.2.2 Overleg en rapportage

NB15 Opdrachtnemer zal een SLA beschikbaar stellen die onderdeel zal worden van de Overeenkomst die ten minste voldoet aan de eisen van dit programma van eisen en waarin opgenomen zullen worden;

a) de overeen te komen komen Service levels

b) de overeen te komen KPI's

c) een lijst van contactpersonen.

d) De definitieve SLA is uiterlijk beschikbaar bij Go Live van de Oplossing.

NB16 De Opdrachtnemer heeft een Single Point Of Contact voor escalaties rondom communicatie met hun Service Desk en/of Incidenten, problemen en andere verzoeken

NB17 Opdrachtnemer moet voorzien in technische en organisatorische maatregelen, waaronder een incidentmanagementool (en daar waar mogelijk een koppeling met de ITSM tooling (API)), voor het prompt registeren, administreren en rapporteren van incidenten, problemen, wijzigingen, en vergelijkbare correspondentie. Opdrachtnemer zorgt ervoor dat de SVB te allen tijde toegang heeft tot die incidentmanagementtool, en dat de SVB te allen tijde de status van incidenten, problemen, wijzigingen, en vergelijkbare correspondentie kan inzien.

NB18 Opdrachtnemer dient in de SLA - in overleg met de SVB - de parameters te bepalen op basis waarvan de prioriteit van incidenten en problemen wordt vastgesteld (i.e. P1 tot en met P4). De prioritering dient te worden bepaald aan de hand van "scope impact x scope urgentie (kritiek/normaal/laag) tevens uitgedrukt in een prioriteiten matrix. Voor incidenten en problemen m.b.t. informatiebeveiliging dient een aparte prioritering in de SLA te staan op basis van enkel "scope impact" x "scope urgentie".

NB19 Een Root Cause Analysis (RCA) bevat ten minste de volgende onderstaande elementen (niet limitatief):

a) Beschrijving van het Incident of afwijking en het aantal (bij benadering) Eindgebruikers dat hierdoor getroffen kan zijn.
b) Beschrijving van de oorzaak van het Incident of afwijking
c) Beschrijving van de tijdelijke en of permanente oplossing.
d) Beschrijving van de maatregelen die genomen zijn en zullen worden om zeker te stellen dat dit Incident of afwijking niet nogmaals plaatsvindt.
e) planning
f) Feiten en cijfers.

NB20 De Opdrachtnemer kan aantonen dat het beschikt over een Disaster Recovery plan (incl. het Backup and restore plan) m.b.t. de afgesproken dienstverlening op en zorgt tenminste 1 keer per 2 jaar voor een continuiteïtstest

NB21 Gepland Onderhoud wordt uiterlijk 14 kalenderdagen ervoor gecommuniceerd (incl. waarop het Onderhoud betrekking heeft)
a) Gepland onderhoud (waardoor de Dienstverlening wordt onderbroken) gaat niet ten koste van de beschikbaarheid van de Oplossing, mits op Werkdagen uitgevoerd tussen 19:00 uur en 7:00 uur.

NB22 De Opdrachtnemer stelt naast standaard documentatie van de Oplossing specifieke documentatie op met betrekking tot de specifieke implementatie van de Oplossing voor de SVB, conform de Niet-Functionele eisen

NB23 Opdrachtnemer geeft periodiek inzicht (ten minste éénmaal per maand) in de geleverde prestaties, dmv een SLA rapportage op de afgesproken KPI's

NB24 Direct na inwerkingtreding van de Overeenkomst zal de Opdrachtnemer met de SVB afspraken maken over de invulling van een Dossier Afspraken en Procedures (DAP), waarin operationele afspraken worden geborgd op basis van de beschreven dienstverlening in de SLA.

NB25 Bij het in 3 aansluitende maanden niet halen van de afgesproken service levels van de Omgeving en/of Dienstverlening, start Opdrachtnemer onverwijld een onderzoek naar de oorzaak daarvan door opleveren van een RCA en rapporteert zij schriftelijk hierover aan de SVB. Aansluitend stelt de opdrachtnemer een voorlopig Service Improvement Plan (SIP) op en communiceert deze aan de opdrachtgever. Opdrachtnemer moet steeds het initiatief nemen om een bespreking van dat rapport te plannen met de SVB en voor te zitten. Wanneer in gebreke wordt gebleven kan een bonus/malus regeling van toepassing zijn.

NB26 Opdrachtnemer moet periodiek (ten minste éénmaal per maand) rapporteren over de voortgang van de realisatie van alle eventuele Service Improvement Plannen. Indien nodig kunnen er aanvullende overleggen naast het maandelijks rapportage worden ingeregeld zoals: security overleg, tactisch overleg, strategisch overleg en architectuur overleg.

2.3 Informatiebeveiliging en privacy

NC1 Medewerkers van de Opdrachtnemer die in aanraking komen met vertrouwelijke informatie van de Opdrachtgever dienen een geheimhoudingsovereenkomst (NDA) te hebben ondertekend en op basis hiervan te handelen.

NC2 Generieke eisen aan de informatiebeveiliging
a) Opdrachtnemer dient voor het onderhoud en/of doorvoeren van aanpassingen met betrekking tot de geleverde oplossing een wijzigingsproces te hebben en te hanteren, waarbij de nadruk ligt op het voorkomen van beveiligings- en privacy incidenten, storingen en/of onderbrekingen tijdens het doorvoeren van veranderingen.
b) Opdrachtnemer dient informatiebeveiliging en bedrijfscontinuïteit gestandaardiseerd, gestructureerd en gebaseerd op een cyclus van continue verbeteren in alle lagen van de organisatie en de geleverde dienstverlening te hebben ingericht.
c) Opdrachtnemer dient de continuïteit van de geleverde dienstverlening te waarborgen in geval van calamiteiten en/of rampen middels een getest crisisplan, Business Continuity Plan (BCP) en Disaster Recovery Plan (DRP).
d) De Opdrachtnemer dient de Opdrachtgever schriftelijk te informeren op het moment dat deze wordt overgenomen door of fuseert met een andere entiteit.
e) De Opdrachtnemer dient elke voorgenomen wijziging in eventuele subverwerkers vooraf schriftelijk te melden aan de Opdrachtgever.
f) Opdrachtnemer dient de aan Opdrachtnemer gestelde informatiebeveiligings- en privacy-eisen door te vertalen naar de gehele keten van betrokken toeleveranciers.

g) De Opdrachtgever heeft het recht om, bij een aantoonbare aanleiding zoals een beveiligingsincident, auditverplichting of periodieke controle, een security assessment (bijvoorbeeld een penetratietest of infrastructuurtest) te laten uitvoeren op de door opdrachtnemer geleverde dienstverlening. Dit assessment wordt uitgevoerd door een door de Opdrachtgever geselecteerde onafhankelijke derde partij.

h) Het assessment vindt plaats in overleg met de Opdrachtnemer, waarbij planning, scope en impact vooraf worden afgestemd, zodat verstoring van de dienstverlening tot een minimum wordt beperkt. De Opdrachtnemer verleent redelijke medewerking aan het assessment, waaronder het beschikbaar stellen van relevante documentatie en toegang, voor zover noodzakelijk en proportioneel. Eventuele kosten en verantwoordelijkheden worden vooraf tussen Opdrachtgever en Opdrachtnemer afgestemd."

NC3 Encryptie

a) De geleverde oplossing dient gevoelige en/of vertrouwelijke gegevens 'in transit' en 'at rest' te versleutelen op basis van algemeen geaccepteerde internationale best practices en in lijn met de adviezen van het Nationaal Cyber Security Centrum (NCSC).

b) Bij gunning dient Opdrachtnemer een gedocumenteerd sleutelbeheer te hebben ingericht met vastlegging van sleutelhouderschap, sleutellocatie binnen de EER, en aantoonbare vernietiging van sleutelmateriaal bij exit.

NC4 Risicoanalyses

a) Opdrachtnemer dient minimaal eens per 3 maanden te rapporteren, tenzij contractueel anders overeengekomen, over de status van de onderkende risico's en de bijbehorende voortgang van de geplande te implementeren mitigerende maatregelen.

b) Opdrachtnemer dient Opdrachtgever binnen 24 uur op de hoogte te stellen, via het overeengekomen communicatiekanaal en tijdslijnen, van risico's die een directe impact op de opdrachtgever (kunnen) hebben.

NC5 De geleverde oplossing dient aan te sluiten op de Multifactor Authenticatie (MFA) en 'single sign-on (SSO)' implementatie van de Opdrachtgever welke is gebaseerd op standaard protocollen (bv. OpenID, OAUTH2, SAML, etc.).

NC6 Opdrachtnemer dient minimaal eens per 3 maanden te rapporteren, tenzij contractueel anders overeengekomen, over afgesproken relevante Key Performance Indicatoren (KPIs) met betrekking tot het Security hardening proces inclusief de status van de opvolging / afhandeling van geconstateerde bevindingen.

NC7 Opdrachtnemer dient minimaal eens per 3 maanden te rapporteren, tenzij contractueel anders overeengekomen, over afgesproken relevante KPIs met betrekking tot Vulnerability Management inclusief de status van de opvolging / afhandeling van geconstateerde bevindingen.

NC8 Opdrachtnemer dient minimaal eens per 3 maanden te rapporteren, tenzij contractueel anders overeengekomen, over afgesproken relevante KPIs met betrekking tot de Lifecycle en Patch Management processen inclusief de status van de opvolging / afhandeling van geconstateerde bevindingen.

NC9 Penetratietesten

a) Opdrachtnemer dient volgens een beschreven Penetratietesting beleid en proces penetratietesten uit te voeren op alle ICT-componenten van de geleverde oplossing.

b) Opdrachtnemer dient minimaal eens per jaar te rapporteren, tenzij contractueel anders overeengekomen, over de uitgevoerde penetratietesten inclusief bevindingen, de risico's en de status van de opvolging / afhandeling van de geconstateerde bevindingen.

NC10 De geleverde oplossing dient audit / logbestanden minimaal 18 maanden te bewaren voor toekomstig onderzoek en toegangscontrole.

NC11 Opdrachtnemer dient loggings- en detectie-informatie (registraties en alarmeringen) en de beveiligingsstatus van ICT-componenten actief te monitoren (bewaking en analyse) en eventuele bevindingen te rapporteren en op te volgen volgens een proces.

NC12 Cloud

a) Voor een SaaS-oplossing is een Virtual Private Cloud (VPC) voor de SVB een eis. Een Virtual Private Cloud (VPC) is een veilig, logisch geïsoleerd deel van een publieke cloud. Hiermee kan code uitgevoerd worden, gegevens opgeslagen worden en applicaties gehost worden in een private, aanpasbare omgeving. Deze VPC moet logische isolatie kennen ten aanzien van de applicatie en gegevens. Dit vereist onder andere bijvoorbeeld aantoonbare tenant-/instance-isolatie, een gescheiden IAM-omgeving, gescheiden dataopslag, gescheiden logging/audittrail, beheer- en supporttoegang voor de VPC, gescheiden back-ups (en terugzetten in geïsoleerde omgevingen), gescheiden test-/trainingsdata en aantoonbare scheiding van SVB-data ten opzichte van andere klanten.

b) Als de leverancier gebruik maakt van AI-modellen gehost of beschikbaar gesteld door derden dan moeten deze aan dezelfde beveiligings- en compliance-eisen voldoen zoals gesteld aan de hoofdaannemer van de scansoftware. Deze moeten als onderaannemer/subverwerker formeel gecontracteerd zijn door de hoofdaannemer en inzet van deze partijen moet aan SVB kenbaar worden gemaakt vanaf het moment van inschrijven op de aanbesteding. De dienst(en) van deze derde partijen moeten tevens als onderdeel van de inschrijving beschreven worden. Na inschrijven dienen nieuwe onderaannemers voorgelegd te worden aan SVB, en pas geïmplementeerd na schriftelijke goedkeuring.

NC13 In geval van beëindiging van de overeenkomst dient data van de Opdrachtgever welke nog in het bezit is van de Opdrachtnemer na overdracht aan de Opdrachtgever vervolgens op verzoek van de Opdrachtgever conform daarvoor geldende internationale standaarden vernietigd te worden.

NC14 Relevante logdata moet aan de hand van use cases geleverd worden aan het Security Information en Event Management (SIEM) systeem van de SVB via het SVB SOC koppelvlak voor logging.

NC15 De geleverde oplossing dient qua (cryptografische) beveiligingsmaatregelen te voldoen aan de NCSC-beveiligingsrichtlijnen, dan wel de logische opvolger daarvan.

NC16 Privacy

a) De geleverde oplossing dient gedurende de gehele looptijd van de overeenkomst te voldoen aan voor de opdrachtgever van toepassing zijnde wet- en regelgeving, waaronder de AVG (Algemene Verordening Gegevensbescherming).

b) De geleverde oplossing dient op het gebied van Informatiebeveiliging en Privacy technische, organisatorische en fysieke maatregelen te hebben geïmplementeerd, op basis van een aantoonbaar uitgevoerde (Data) Privacy Impact Assessment ((D)PIA), passend bij de soort persoonsgegevens die worden verwerkt en in lijn met algemeen geaccepteerde standaarden.

c) De geleverde oplossing dient uitsluitend persoonsgegevens te verwerken, te transporteren en op te slaan (inclusief de back-ups) binnen de Europese Economische Ruimte (EER). Tevens dienen de eventuele (privacy) restrisico's tot binnen de Risk Tolerance van de Opdrachtgever gereduceerd te zijn.

d) Voorafgaand aan in productie name / gebruik van de geleverde oplossing dient een verwerkersovereenkomst (bij voorkeur de modelverwerkersovereenkomst van de SVB) afgesloten te zijn tussen de Opdrachtgever als verwerkingsverantwoordelijke en de Opdrachtnemer als verwerker indien er persoonsgegevens worden verwerkt door de Opdrachtnemer.

e) Opdrachtnemer dient bij beëindiging van de dienstverlening de voor de Opdrachtgever verwerkte persoonsgegevens te retourneren dan wel op verzoek van de Opdrachtgever te vernietigen, tenzij er sprake is van een wettelijke bewaarplicht.

f) Opdrachtnemer dient een proces te hebben en te hebben geïmplementeerd om datalekken onverwijld, maar uiterlijk binnen 24 uur, aan de opdrachtgever te melden.

g) Opdrachtnemer dient opdrachtgever op verzoek te allen tijde te ondersteunen bij het afhandelen van verzoeken van betrokkenen ter uitoefening van hun rechten en/of de opvolging of afhandeling van datalekken.

h) Opdrachtnemer dient de opdrachtgever onverwijld, maar uiterlijk binnen 24 uur, over verzoeken tot aanlevering van (persoons)gegevens door buitenlandse inlichtingen- en opsporingsdiensten in het kader van de geleverde dienstverlening te informeren.

NC17 IB Incidenten

a) Opdrachtnemer dient bij een informatiebeveiligings- en/of privacy incident zo snel als mogelijk passende maatregelen te treffen om de gevolgen en de schade voor alle betrokkenen te beperken en/of te voorkomen.

b) Opdrachtnemer dient te allen tijde volledige medewerking te verlenen bij het onderzoeken en oplossen van informatiebeveiligings- en/of privacy incidenten en stelt, indien gevraagd, alle informatie met betrekking tot het incident ter beschikking aan de Opdrachtgever en/of een door de Opdrachtgever aangewezen derde partij.

NC18 Compliance

a) Opdrachtnemer dient de opdrachtgever het recht te verlenen om een onderzoek (of audit) in te stellen met betrekking tot de naleving van het 'Beschrijvend document', 'De Raamovereenkomst', 'De Wachtkamerovereenkomst', 'De Verwerkersovereenkomst (indien van toepassing)' en de 'Bijlagen opgenomen verplichtingen aangaande de geleverde dienstverlening'.

b) De audit wordt altijd door een onafhankelijke geaccrediteerde derde partij (auditor) uitgevoerd in samenspraak met de Opdrachtnemer."

NC19 Opdrachtnemer levert met betrekking tot de ISO 27001 of aantoonbaar gelijkwaardige certificering jaarlijks een nieuwe formele auditverklaring aan die uiterlijk dertig kalenderdagen na afgifte door de Opdrachtgever is ontvangen.

NC20 Overleg & Rapportage

a) Opdrachtnemer dient in samenspraak met de opdrachtgever een overlegstructuur inclusief minimaal jaarlijkse, tenzij contractueel anders overeengekomen, overleggen in te richten om de overeengekomen opgeleverde rapportages, eventuele issues en ontwikkelingen rond de geleverde dienstverlening te bespreken. De kosten van deze overleggen zijn onderdeel van de vermelde kosten in het Prijzenblad.

b) Opdrachtnemer dient minimaal eens per jaar te rapporteren, tenzij contractueel anders overeengekomen, over relevante overeengekomen Key Performance en Risk Indicators (KPIs / KRIs) met betrekking tot de geleverde dienstverlening.

NC21 Bij een toekomstige overstap moet de SVB alle informatie over de SVB-configuratie ontvangen van de dienstverlener. Tenminste als documentatie en waar mogelijk als data om de portabiliteit naar de opvolgende dienstverlener te vergroten. De configuratie omvat tenminste maar niet uitsluitend documenttypeconfiguraties, labels, workflows, validatieregels, confidence thresholds, trainings-/testdatasets, metadatainrichting, dataextractie-inrichting, prompts en/of modelinstellingen.

2.4 Architectuur

ND1 Alleen gebruikers, uit hoofde van hun functie en rol in het bedrijfsproces, hebben toegang en bepaalde rechten tot de voorziening.

a) De Oplossing ondersteunt Role Based Access Control (RBAC). De oplossing kan een role claim van een aangemelde gebruiker ontvangen. Toelichting: De gebruiker en zijn rollen worden buiten de oplossing bijgehouden in een IAM-tool. Zo wordt identificatie en toegang tot een applicatie centraal bijgehouden en gecontroleerd.

ND2 Eisen aan het gebruik van AI.

a) Geïntegreerde AI functionaliteit in een IDP oplossing moet voldoen aan de vigerende wet- en regelgeving, met name de EU AI Act.

b) De IDP leverancier geeft inzicht in de gebruikte AI functionaliteit, met name op toegepaste AI modellen, trainingsgegevens en finetuning.

c) Indien een IDP oplossing gebruik maakt van AI functionaliteit dient de leverancier de garantie te kunnen geven dat gegevens en verwerking niet buiten de EER zullen plaatsvinden; dit geldt ook in het geval van AI functionaliteit vanuit een derde partij.

d) De IDP oplossing gebaseerd op SaaS dient een enterprise private workspace voor het gebruik van AI modellen te bieden om gegevensprivacy te waarborgen. Met een enterprise private workspace wordt een afgeschermde AI werkomgeving geboden voor de opdrachtgever waarin de gegevens van de opdrachtgever beschermd blijven, toegang wordt gecontroleerd en data niet standaard wordt gebruikt voor het trainen van publieke AI-modellen.

e) Gegevens van de SVB worden niet gebruikt voor het trainen van generatieve AI modellen gebruikt door de leverancier; dit geldt ook voor levering van generatieve AI functionaliteit door een derde partij.

f) Aanvullende AI functionaliteit moet uitgeschakeld zijn of uitgeschakeld kunnen worden.

g) Het is toegestaan om expliciete gebruikers feedback te gebruiken om AI modellen te verbeteren, mits geen data anders dan de feedback zelf gedeeld wordt.

ND3 De Oplossing gebruikt de voorkeursstandaard REST/JSON web services of opvolgers hiervan voor de koppeling van gebruikende applicaties.

a) Voor REST API koppelingen moet de open standaard OpenAPI Specification (OAS) voor het specificeren en documenteren van de API gebruikt worden. Zie: https://www.forumstandaardisatie.nl/open-standaarden/openapi-specification.

b) Koppelingen die in beheer zijn bij Opdrachtnemer hebben duidelijke specificaties (descriptor documents). Voor elke koppeling met een interne of externe applicatie wordt minimaal het volgende beschreven:

i) Functie(s)
ii) Wijze toegang
iii) Aanroep (call)
iv) Berichtsoorten en -inhoud
v) Technische limieten

ND4 Open standaarden verplicht gesteld op Forum Standaardisatie en/of door het Nationaal Archief (lijst met voorkeurs- en acceptabele formaten) worden toegepast.

a) Voor het vastleggen van datum en tijd dient de door Forum standaardisatie aanbevolen open standaard 'Datum en tijd' (https://www.forumstandaardisatie.nl/open-standaarden/datum-en-tijd) gevolgd te worden.

ND5 Ingeval van gegevensuitwisseling op basis van bestandsuitwisseling voor grote bestanden dient de aanbevolen open standaard SFTP gebruikt te worden.

ND6 De scansoftware slaat gegevens en documenten niet langer permanent op dan nodig om eventuele uitval te verwerken. Na overdracht aan en bevestiging door het ontvangende systeem worden deze verwijderd.

www.svb.nl

voor het leven
Sociale Verzekeringsbank