| nr | Omschrijving eis |
|---|---|
| | **Algemeen** |
| NWG02 | NIS2/Cbw(Cyberbeveiligingswet) > Zorgplicht, meldplicht, risicobeheer - Bevoerziers moeten voldoen aan de NIS2/Cbw |
| NWG05 | Data Act (Europese Dataverordening) - Leveranciers moeten voldoen aan de Data Act indien hun -omgeving- IoT-data verwerkt, en dat ze dit kunnen scheiden van persoonsgegevens conform AVG |
| NWG06 | AI Act (Algoritmische Transparantie) - Leveranciers moeten bij inzet van AI voldoen aan de AI Act, inclusief risicobeoordeling, documentatie en uitlegbaarheid van algoritmen. |
| | **Certificaten** |
| C01 | Opdrachtnemer beschikt over passende informatiebeveiligingsmaatregelen en kan de opzet, implementatie en werking daarvan aantonen.<br>De opdrachtgever bepaalt op basis van een risicoanalyse welke mate van assurance noodzakelijk is. Afhankelijk van het risicoprofiel van de dienstverlening kan opdrachtgever verlangen dat opdrachtnemer beschikt over een informatiebeveiligingsmanagementsysteem gebaseerd op een algemeen erkende norm, zoals ISO/IEC 27001, NEN 7510 of een gelijkwaardige standaard.<br>De toereikendheid van de informatiebeveiliging wordt desgevraagd aangetoond door middel van één of meer van de volgende bewijsmiddelen:<br>een actueel en geldig certificaat inclusief verklaring van toepasselijkheid (SoA);<br>onafhankelijke assurance-rapportages, zoals ISAE3402 Type II, SOC 2 Type II of gelijkwaardig;<br>rapportages van audits, penetratietesten of security assessments;<br>een Statement of Compliance of vergelijkbare verklaring van getroffen beveiligingsmaatregelen;<br>andere door opdrachtgever geaccepteerde vormen van aantoonbare assurance.<br>Opdrachtgever kan, gelet op het risicoprofiel van de dienstverlening, aanvullende eisen stellen aan de aard, omvang en frequentie van de vereiste assurance. |
| | **Architectuur** |
| NA01 | De omgeving dient voor de in gebruiksname van de oplossing beschikbaar en functioneel te zijn voor opdrachtgever |
| NA02 | De omgeving gebruikt uitsluitend de standaard applicatiecode van de leverancier. Klantspecifieke wijzigingen in de applicatiecode zijn niet toegestaan. De voor opdrachtgever gebruikte applicatiecode en releaseversie zijn gelijk aan de reguliere, door de leverancier ondersteunde productversie. |
| NA03 | De omgeving is webbased. |
| NA04 | De omgeving wordt als SaaS aangeboden waarbij geen componenten van het softwareplatform lokale installatie vereisen. |
| NA06 | De omgeving levert standaard operationele rapportages om te kunnen sturen op de processen die het systeem ondersteunt en op de gegevenskwaliteit. |
| NA14 | De user interface van de omgeving is responsive. |
| NA16 | De omgeving functioneert goed in combinatie met de laatste versies (n of n-1) van alle gangbare webbrowsers, inclusief de standaard beschikbare plug-ins. |
| NA18 | Na definitieve gunning verstrekt Opdrachtnemer een globale beschrijving van de technische opbouw van de oplossing, met daarin ten minste:<br>de gebruikte componenten en het onderliggende platform;<br>de gebruikte datacentra en het land waarin deze zich bevinden;<br>per component en platform de leverende en/of beheerende partij. |
| NA09 | De omgeving koppelt met Microsoft Entra ID voor authenticatie conform de gangbare SAML of OAuth-omgeving. |
| | **Informatieveiligheid** |
| NIV01 | De omgeving en in het geval van SaaS ook de technische omgeving waar deze op draait, voldoet aan relevante wetgeving |
| NIV02 | De Oplossing voldoet aan de technische beveiligingsspecificaties zoals opgenomen in het overzicht met Standaarden van het Forum van Standaardisatie (zie ook NIA07; 'Pas toe tog uit' standaarden (verplicht) \| Forum Standaardisatie, daar waar relevant. |
| NIV03 | Periodiek legt de Opdrachtnemer verantwoording af via een Statement of Compliance (zif deel-ICV; met toepasselijke rekwijtte) aan de Opdrichtgever. De prestatie van Opdrachtnemer op het gebied van informatiebeveiliging wordt beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is. Een technische audit (penetratietest) in relatie tot de -omgeving- maakt hier deel van uit. |
| NIV04 | De leverancier implementeert passende maatregelen waarmee zowel aan de voor hem relevante eisen uit de BIO2 wordt voldaan als waarmee de opdrachtgever aantoonbaar in staat wordt gesteld te voldoen aan de voor de opdrachtgever geldende BIO2-eisen. |
| NIV05 | De -omgeving- dient geen softwarematig maatwerk te bevatten. Wanneer er nieuwe functionaliteiten moet worden ontwikkeld binnen de kaders van de aanbesteding of specifiek ontwikkeld zou moeten worden, bijv. als gevolg van een wijziging in de wet- en regelgeving, dient deze in de eerstvolgende release opgenomen te zijn als standaardfunctionaliteit. |
| NIG03 | De -omgeving- houdt een logging bij van alle transacties. De logbestanden zijn voor opdrachtgever beschikbaar en bruikbaar. |
| | **Privacy** |
| NPR01 | De Opdrachtnemer mag de door de gemeente verzamelde persoonsgegevens slechts in uitoefenelijke opdracht van de Opdrachtgever verwerken. Persoonsgegevens mogen bovendien alleen worden verwerkt voor zover dat noodzakelijk is voor de oplossing. De Opdrachtnemer mag persoonsgegevens dus niet voor eigen doeleinden gebruiken |
| NPR02 | De opdrachtnemer verleent tijdig alle benodigde medewerking aan de door opdrachtgever uit te voeren DPIA en voert, voor zover hij zelf verwerkingsverantwoordelijke is, zijn eigen DPIA-verplichtingen uit. |
| NPR03 | De (persoons)gegevens die in opdracht van gemeente Almere (verantwoordelijke) worden verwerkt zullen te allen tijde worden opgeslagen op servers die zich fysiek binnen de **EER (Europese Economische Ruimte)** bevinden. |
| NPR04 | De Opdrachtnemer mag de persoonsgegevens niet langer bewaren dan noodzakelijk om de clouddiensten (-omgeving-) aan de gemeente te leveren. De opdrachtnemer moet garanderen en aantonen dat de gegevens na beëindiging van de overeenkomst worden vernietigd. Dit wordt vastgelegd in het Eailplan. |
| NPR05 | Met de Privacy Officer van Almere wordt een procedure afgesproken inzake rechtmatige inzageverzoeken van bevoegde autoriteiten. |
| NPR06 | De Opdrachtnemer heeft een datalekkenprotocol, datalekkenregister en is in staat om de opdrachtgever binnen 24 uur na ontdekking of kennisname van een datalek op de hoogte te stellen van de benodigde informatie over het datalek en maatregelen te nemen in de afhandeling (artikel 28 lid 3 onder artikel 33 AVG). |
| NPR07 | De Opdrachtnemer is verplicht de persoonsgegevens adequaat te beveiligen. De Opdrachtnemer maakt expliciet welke beveiligingsmaatregelen met betrekking tot de door de gemeente verzamelde persoonsgegevens worden genomen. Bij de beveiligingsmaatregelen moet worden gedacht aan de eisen die hierboven onder informatieveiligheid zijn omschreven. Tevens moet een actuele en volledige beschrijving van het gehanteerde beveiligingsbeleid beschikbaar zijn voor de gemeente. |
| NPR08 | Indien opdrachtnemer bij de uitvoering van de opdracht gebruikmaakt van AI, algoritmen of andere geautomatiseerde systemen, verstrekt(t) de gemeente Almere (designvraag) voldoende informatie over de werking, het gebruik en de risico's hiervan. Opdrachtnemer verleent alle medewerking die nodig is om de gemeente Almere in staat te stellen te voldoen aan haar wettelijke verplichtingen op het gebied van transparantie, verantwoordingen gegevensbescherming. |
| | **Implementatie** |
| NIM02 | Opdrachtnemer beschrijft op welke wijze de implementatie en eventuele migratie van de aangeboden omgeving wordt uitgevoerd. Opdrachtnemer gaat daarbij minimaal in op de inrichting van de omgeving, waaronder accounts, rollen, autorisaties, rechten, codetabellen en overige organisatiespecifieke instellingen, de inrichting en validatie van eventuele koppelingen, interfaces en verbindingen, de migratiestrategie, de test- en acceptatiestrategie, de planning en fasering, de rollen en verantwoordelijkheden van Opdrachtnemer en Opdrachtgever, en de belangrijkste risico's inclusief beheersmaatregelen. Opdrachtnemer maakt inzichtelijk hoe wordt gebogd dat de omgeving na acceptatie gebruiksklaar is voor de eindgebruikers van Opdrachtgever.<br>Richtlijn cza C AA. |
| NIM50 | De oplossing ondersteunt Single Sign-On voor medewerkers van Opdrachtgever via Microsoft Entra ID, op basis van OpenID Connect en OAuth 2.0. De oplossing kan worden gekoppeld aan Oribi SmartID, zodat de door Opdrachtgever via Oribi SmartID toegekende gebruikersrollen en autorisaties binnen de oplossing correct worden verwerkt en toegepast. |
| NIM04 | De -omgeving- is in Nederlands. De opdrachtnemer gebruikt Nederlands als voertaal in woord en geschrift tijdens de implementatie en biedt de trainingen (voor gebruikers en functioneel Beheerders) aan in het Nederlands. |
| NIM07 | Acceptatie kan plaatsvinden wanneer aangetoond is dat:<br>De (set van) (opleveringen) voldoet aan gestelde eisen, compleet is - waarbij verificatierapportage onderdeel uitmaak van de (set van) (op)leveringen) - en consistent is, en voldoet aan de gestelde acceptatiecriteria. |
| | **Functioneel beheer - generiek** |
| NFB04 | Onderhoud aan de -omgeving- wordt tijdig aangekondigd<br>Opdrachtgever verstaat onder het onderhoud: Correctief, preventief, innovatief onderhoud en gebruikersondersteuning. |
| NFB08 | De functioneel beheerder kan in de -omgeving- zelf het autorisatiebeheer op basis van verschillende rechten (roadpleeg en mutenrechten) en op een eenvoudige wijze autoriseren. Er is een functiescheiding tussen functioneel applicatiebeheer, supervisor en gewone gebruikers. De autorisaties kunnen door een functioneel beheerder per administratie op een centrale plek worden bijgehouden. |
| NFB09 | De -omgeving- biedt de beheerder van de Opdrachtgever de mogelijkheid om een overzicht te genereren met alle autorisaties van de gebruikers met bijbehorende functies. |
| NIG04 | De -omgeving- waarborgt bij storing en calamiteiten de volledigheid en integriteit van de opgeslagen gegevens. |
| | **Contract- en Leveranciersmanagement** |
| NCC06 | De Opdrachtnemer mag bij het verwerken van de persoonsgegevens alleen groepsorganisatiehuppigen en onderaannemers inschakelen met wie hij een schriftelijke overeenkomst heeft gesloten waarin geheimhoudings- en beveiligingsverplichtingen op basis van dezelfde voorwaarden zijn opgenomen als in de tnerwerkersovereenkomst. |
| NCB02 | De Opdrachtnemer garandeert dat de -omgeving- en het deel van de functionaliteit die Opdrachtgever nodig heeft am haar deel van de werkzaamheden uit te gedurende de hele looptijd van de overeenkomst inclusief verlengingen als SaaS voor gebruik beschikbaar is en ondersteund wordt. |
| NCB03 | De -omgeving- blijft gedurende de gehele looptijd voldoen aan de uitvoering van de bestaande en nieuwe landelijke relevante wet- en regelgeving en het relevant lokale beleid in het kader van alle genoemd regelingen in de projectscope. Het onderhoud dat hiervoor benodigd is wordt geacht onderdeel uit te maken van de door u aangeboden prijs. |
| NCB04 | Opdrachtnemer hanteert onderstaande normen ten aanzien van Recovery Point Objective, Recovery Time Objective en Beschikbaarheid die noodzakelijk zijn om de informatievoorziening richting aanbestedende dienst en ketenpartijen tijdig uit te voeren:<br>• maximaal 1 uur dataverlies;<br>• maximaal 4 uur herstelbijt tot dienstverlening weer op niveau; |
| NCW01 | Updates en upgrades die leiden tot nieuwe functionaliteiten binnen de scope van de dienstverlening worden zonder aanvullende licentie-, implementatie- of gebruikskosten aan opdrachtgever beschikbaar gesteld. |
| NCI01 | Opdrachtnemer levert bij beëindiging van de overeenkomst alle gegevens, metadata en benodigde documentatie overdraagbaar aan de gemeente op en verleent redelijke medewerking aan de migratie. Na schriftelijke bevestiging van de overdracht verwijdert Opdrachtnemer alle gemeentelijke gegevens aantoonbaar uit de beheeromgeving. |
| NCI02 | Alle gegevens die Opdrachtnemer voor de gemeente verwerkt, blijven van de gemeente. Binnen drie maanden na definitieve gunning beschrijft Opdrachtnemer hoe de gemeente toegang houdt tot haar gegevens en hoe deze gegevens worden overgedragen wanneer Opdrachtnemer onverwacht stopt met de dienstverlening. |