



Sportbedrijf
Rotterdam

Nr.	Eisen
Algemene eisen	
1.	Alle kosten die nodig zijn om te voldoen aan de eisen uit deze aanbesteding moeten zijn opgenomen in de aangeboden prijzen. Inschrijver kan hiervoor geen aanvullende kosten in rekening brengen, tenzij deze expliciet zijn opgenomen in het prijzenblad.
2.	Opdrachtnemer verplicht zich om aan het eind van de overeenkomst volledige medewerking te verlenen bij de overgang naar een ander systeem en/of bij contractwisseling, al dan niet naar een andere marktpartij. De data wordt kosteloos in een gangbaar formaat beschikbaar gesteld aan SR.
3.	Opdrachtnemer levert gebruikers- en beheerdocumentatie bij oplevering van het online portaal. Deze documentatie bevat ten minste: - Beknopte instructies ("how-to's") voor de belangrijkste gebruikers- en beheerhandelingen. - Praktisch toepasbare documentatie voor dagelijks gebruik.
4.	De dienstverlening en het systeem voldoen aan alle relevante wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG).
Kritische Prestatie Indicatoren	
5.	Opdrachtnemer communiceert proactief over een periode van down time en geeft aan wanneer en hoelang deze periode duurt.
Informatiebeveiliging & Privacybescherming	
6.	Opdrachtnemer voert alle functionele en noodzakelijke beveiligingsupdates uit t.a.v. haar eigen dienstverlening. Kritieke (beveiliging) updates moeten binnen 7 dagen na bekendmaking verholpen zijn.
7.	Gegevens zijn opgeslagen op servers in EER en de opslag van gegevens in het systeem zijn GDPR- / AVG-compliant. Opdrachtnemer verklaart dat dit geldt voor alle betrokken diensten, partners en subverwerkers. Indien een uitzondering noodzakelijk blijkt, wordt deze ter beoordeling en goedkeuring voorgelegd aan de Servicemanager ICT en de Informatiearchitect van Sportbedrijf Rotterdam.
8.	Opdrachtnemer kan aantonen dat passende maatregelen zijn genomen voor het maken van back-ups en het herstellen van gegevens. Inschrijver beschrijft in het gunningscriterium welke risico's er zijn voor back-up en herstel en welke maatregelen worden genomen om deze risico's te beperken.
9.	Opdrachtnemer stelt een contactpersoon aan die aangesproken kan worden over de voortgang c.q. afhandeling van een incident of melding.
10.	Opdrachtnemer is gedurende de gehele looptijd van de overeenkomst verantwoordelijk voor het uitvoeren van updates en upgrades. Hiermee worden fouten hersteld, de beveiliging op peil gehouden en functionaliteiten verbeterd. SR wordt altijd vooraf geïnformeerd.
Technische eisen	
11.	Het systeem is een SaaS-oplossing voor SR. Inschrijver mag gebruik maken van een PaaS-dienst voor een systeem.
12.	Indien API's worden gebruikt, worden deze beveiligd alsof zij toegankelijk zijn vanaf internet (extern). De API's controleren welke gebruikers en systemen toegang hebben en welke acties zij mogen uitvoeren. Daarnaast controleert het systeem of aangeleverde gegevens voldoen aan de afgesproken gegevensstructuur en invoerregels. De API's voldoen hierbij aan de geldende standaarden voor OpenAPI en JSON Schema. Opdrachtnemer is verantwoordelijk voor het leveren, onderhouden en documenteren van de API-endpoints en stelt een testomgeving beschikbaar voor het testen van koppelingen. Hiermee wordt de veiligheid, betrouwbaarheid en beheerbaarheid van koppelingen gewaarborgd.
13.	Het systeem ondersteunt Multi-Factor Authenticatie (MFA) en Single Sign-On (SSO) via Microsoft Entra ID. Hiermee kunnen gebruikers veilig inloggen met hun bestaande organisatieaccount.
14.	Alle communicatie van en naar het systeem verloopt via beveiligde en versleutelde verbindingen volgens gangbare marktstandaarden. Minimaal TLS 1.2 of TLS 1.3 moeten ondersteund worden.
15.	Opdrachtnemer is verantwoordelijk voor het aanvragen, beheren, monitoren en tijdig vernieuwen van certificaten die nodig zijn voor de beveiliging van de verbinding.

16.	Toegang tot de beheeromgeving is afgeschermd en alleen beschikbaar voor geautoriseerde gebruikers.
-----	--