Richtlijn globale aansluitvoorwaarden informatieveiligheid en privacy

	Informatieveiligheid:
Eis	Door indiening van een Inschrijving verklaart Inschrijver zich zonder enig voorbehoud akkoord met het van toepassing zijn van de **GIBIT** 2023 of nieuwer en al haar bijlagen. https://www.vngrealisatie.nl/gibit Specifiek de artikelen opgenomen onder “II Privacy, beveiliging en archivering”.
Eis	De Inschrijver dient in het bezit te zijn van een geldig **ISO 27001** certificaat en een verklaring van toepasselijkheid hiervan met betrekking tot de aangeboden SaaS-ICT-oplossing (bij voorkeur organisatorisch geïmplementeerd conform de best-practices van ISO 27002) of aantoonbaar gelijkwaardig. Graag ontvangen we het certificaat en de bijbehorende scoop (verklaring van toepasselijkheid). In de overeenkomst moet ook het auditrecht worden opgenomen.
Eis	De oplossing moet voldoen aan de internet- en beveiligingsstandaarden van het **Forum Standaardisatie.** Zie hiervoor https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht
Eis	De ICT-oplossing functioneert voor wat betreft aspecten van beveiliging en privacy volledig conform alle betreffende wet- en regelgeving (ten minste **AVG, Cybersecuritywet (Wbni/NIS2) en BIO**) en andere van toepassing zijnde wetgeving, tenzij door de Inschrijver nadrukkelijk anderzijds in de Inschrijving aangegeven en de mitigerende maatregelen hiervoor naar oordeel van Gemeente De Ronde Venen toereikend zijn. De BIO voldoet uiteraard enkel voor de reikwijdte die redelijkerwijs aan een SaaS-leverancier kan en behoort te worden gesteld. Gemeente De Ronde Venen verwijst in dit kader expliciet naar die BIO-eisen waarbij in de kolom ‘Verantwoordelijke’ (onder meer) de ‘Dienstenleverancier’ wordt benoemd.
Eis, Indien van toepassing	Indien er gebruik gemaakt gaat worden van **DigiD**-authenticatie, is het DigiD-normenkader van Logius van toepassing. De jaarlijkse TPM (Third Party Memorandum) is onderdeel van de overeenkomst en inclusief in de prijs.
Eis	Inschrijver garandeert dat de eigen organisatie en partners (onderaannemers) gegevens, welke uit hoofde van de Opdracht verwerkt worden, uitsluitend binnen de **Europese Economische Ruimte** (EER) verwerkt en dat doorgifte naar landen buiten de Europese Economische Ruimte uitgesloten is. Inschrijver toont op het eerste verzoek hiertoe van Gemeente De Ronde Venen aan waar de gegevens staan opgeslagen.
Eis	De gehele ICT-oplossing voldoet aan de vigerende **toegankelijkheidseisen** van de Rijksoverheid (EN 301 549 van Standaardisatie Forum) en ontwikkelt mee met aanpassingen in die eisen. De ICT-oplossing moet (als onderdeel van EN 301 549) ook voldoen aan Web Content Accessibility Guidelines 2.1

	Level AA (WCAG2AA). Dit geldt zonder uitzondering voor alle interne en externe componenten van de aangeboden ICT-oplossing, ook die componenten die achter een login schuil gaan. Inschrijver toont haar compliancy op ieder eerste verzoek hiertoe van Gemeente De Ronde Venen aan.
Wens	De ICT-oplossing heeft de mogelijkheid op functionaliteit-, module-, registratie-, tabel-, veld- proces- en documentniveau te **autoriseren** op basis van **functiegroepen en rollen**. Eveneens ontstaat hiermee de mogelijkheid om functionaliteiten, registraties, processen en documenten ontoegankelijk te kunnen maken voor functiegroepen en rollen.
Eis	De ICT-oplossing heeft een mogelijkheid om vastgelegde autorisaties op alle niveaus inzichtelijk te maken per persoon, per gebruikersgroep en rol. Hiervoor is het toegepaste **autorisatieschema** te exporteren naar een bestand dat leesbaar is voor, en correct geïnterpreteerd kan worden door, derden (zoals toezichthouders zoals bijvoorbeeld de accountant, auditors, etc.).
Eis	De Inschrijver treft zelfstandig aantoonbaar maatregelen, zodat de borging van **continuïteit en integriteit** van (de gegevens in c.q. te benaderen via) de ICT-oplossing uitvoerig wordt geborgd.
	Techniek
Eis	Alle web-based onderdelen van de ICT-oplossing dienen zich in een webomgeving te presenteren, die volledig functioneel en remote wordt ondersteund op de in gebruik zijnde **standaardbrowsers** Microsoft Edge Chromium, Google Chrome, Apple Safari en Mozilla Firefox. De ICT-oplossing maakt hierbij geen gebruik van extra configuratie, plug-ins (zoals Flash, Silverlight, ActiveX, etc., enkel een plug-in voor integratie met kantoorautomatisering hierop uitgezonderd) en software, anders dan de standaardconfiguratie van de voorgenoemde webbrowsers.
Eis	Vanuit de techniek ondersteunt de ICT-oplossing een Azure AD-koppeling, waarmee eveneens kan worden voorzien in **Single-Sign-On**. De ICT-oplossing ondersteunt hiertoe authenticatie op basis van Azure AD via Enterprise Application. Gebruikers van (de verschillende onderdelen van) de aangeboden ICT-oplossing hoeven hiermee slechts eenmalig (Single-Sign-On) te authentiseren om geautoriseerd toegang te krijgen.
Eis	Alle componenten van de ICT-oplossing dienen off-premise (**SAAS**) geleverd te worden.
Wens	Netwerkverbindingen tussen de gemeente De Ronde Venen en de leverancier lopen bij voorkeur via het Diginetwerk.
Eis	Met betrekking tot alle web-omgevingen de verbinding daar naartoe en de adressering hierbij, voldoet de ICT-oplossing aan de volgende **web-standaarden**: DNSSEC en HTTPS en HSTS en IPv4 en IPv6 en TLS 1.3 of hoger, bij voorkeur inclusief het gebruik van security-headers.
Eis	Bij formulieren zijn de validaties niet te omzeilen

Eis	Foutmeldingen van het systeem worden niet rechtstreeks aan een bezoeker getoond. (Geen debug/Error reporting)
Eis	Er zijn geen oude, tijdelijke of backup bestanden aanwezig (config.php.old, config.php~ e.d.)
Eis	Er worden geen gevoelige gegevens in cookies geplaatst. Robots.txt bevat geen gevoelige informatie.
Eis	Formulieren zijn "beschermd" tegen "ververs'-acties (Door de pagina te verversen kan een gebruiker het formulier niet direct opnieuw versturen, op die manier kan geen spam worden verstuurd bijvoorbeeld)
Eis	Pagina's die gevoelige informatie versturen, zijn geëncrypteerd via een **SSL**-verbinding
Eis	De gebruikte web-applicatie is up-to-date
Eis	De gebruikte web-applicatie heeft geen bekende exploits
Eis	Eventuele **koppelingen**/uitwisselingen tussen applicaties gaan op basis van geaccepteerde standaarden (ODBC, XML. SOAP, Stuf3, 10etc)
Eis	Bij integratie met **MS Office** wordt versie M365 ondersteund, inclusief het op XML-gebaseerde bestandsformaat van deze versie
Eis	Er is voorzien in een **Coordinated Vulnerability Disclosure** (CVD)-pagina (en beleid) en een security.txt
	Overeenkomst
Eis	De voor de geboden oplossing benodigde kennis voor koppelingen moet worden aangegeven evenals de te verwachten **tijdsbesteding** voor het systeembeheer en technisch applicatiebeheer
Eis	De Gemeente De Rond Venen stelt zich niet beschikbaar als '**proefpersoon**' en de applicatie mag zich niet in een bèta stadium bevinden
Eis	Er wordt verwacht dat ook met hogere uitgebrachte en binnenkort uit te brengen versies van de diverse pakketten gewerkt kan worden
Eis	Er moet in de hoofdovereenkomst beschreven staan hoe er wordt omgegaan met **data-sanering, backup/herstel, archivering**. Er moet in de overeenkomst een **exit-strategie** beschreven staan. Alle data is en blijft eigendom van gemeente De Ronde Venen en moet na afloop van de overeenkomst in een gangbaar formaat aan de gemeente overhandigd worden. Ook moet de procedure van datavernietiging beschreven zijn.
	Privacy
Eis	Parallel aan de implementatie kan een **Data Protection Impact Assessment (**hierna genoemd: DPIA) worden uitgevoerd. Deze heeft betrekking op de beoogde verwerking(en) van (persoons-)gegevens die voortvloeien uit het gebruik van de nieuwe ICT-oplossing. Uit deze DPIA kan blijken dat additionele technische of organisatorische beveiligingsmaatregelen moeten worden uitgevoerd teneinde de

	geconstateerde hoge risico's te mitigeren. Inschrijver dient alle medewerking, waaronder het verstrekken van alle relevantie informatie, te leveren aan Gemeente De Ronde Venen om ervoor te zorgen dat de DPIA kan worden uitgevoerd en tijdig kan worden afgerond. Eventuele kosten die hieraan verbonden (kunnen) zijn - voor medewerking aan de DPIA en oplossen van tekortkomingen naar aanleiding van de DPIA, in afwijking op het overeengekomene in de aanbestedingsdocumenten en de Overeenkomst die op basis hiervan tot stand is gekomen, dienen onderdeel te zijn van de Inschrijving. De DPIA zal binnen een termijn van drie maanden na definitieve gunning worden afgerond, voor zover Inschrijver alle relevante informatie tijdig heeft verstrekt.
Eis	Indien er persoonsgegevens van inwoners en/of medewerkers worden verwerkt, moet er een **Verwerkersovereenkomst** worden afgesloten. Gemeente De Ronde Venen hanteert uitsluitend het VNG-formaat.
Eis	Er moet aantoonbaar voldaan worden aan de **Algemene Verordening Gegevensbescherming** (AVG). In aanvulling/aansluiting op GIBIT en met verwijzing naar het door VNG gehanteerde normenkader (https://www.informatiebeveiligingsdienst.nl/product/avg-borgingsproduct-2-0) benoemen we specifiek: • Er wordt voldaan aan geformuleerd, geaccordeerd en gepubliceerd privacybeleid en reglement. • Ten grondslag liggende werkprocessen zijn vastgesteld waarbij verwerkingsactiviteiten worden opgenomen in het register van verwerkingsactiviteiten. • De verwerkingsactiviteiten zijn getoetst aan de beginselen van de AVG (artikel 5 en 6). • Er wordt voorzien in de facilitering van de rechten van betrokkenen alsmede functionaliteit voor de vastlegging en intrekking van toestemming als grondslag voor de verwerkingsactiviteit. • Daar waar noodzakelijk wordt volgens standaard procedure en formaat zo snel als mogelijk een DPIA uitgevoerd waarmee invulling gegeven kan worden aan het principe van Privacy by Design/ Default. • Een functionaris gegevensbescherming en/of privacy officer zijn aanspreekpunt voor de privacy organisatie en dragen zorg voor de borging van de privacy beginselen binnen het werkveld. • Er wordt voldaan aan het staande beleid op het gebied van autorisatie en logging.
Wens	Aansluiting op VNG ontwikkelingen m.b.t. bijvoorbeeld een referentie verwerkingsregister is gewenst met duiding van onderhavige Gemmacomponent(en).
Eis	**Privacy by Design**/ Default van gemeente De Ronde Venen, zie Privacy Handboek, bijlage 4 (hieronder).

Privacy by Design

Kernvraag	Toelichting			
Is er sprake van persoonsgegevens?	Dit zijn gegevens die (in)direct herleidbaar zijn tot een natuurlijk persoon.	☐ Ja	☐ Nee	
Privacynorm	**Toelichting**	**Maatregelen**		
Beperken persoonsgegevens	Uitsluitend gegevens die noodzakelijk zijn mogen verwerkt worden.	☐ Anonimiseren	☐ Pseudonimiseren	☐ Dataminimalisatie
Beveiliging	De toegang tot gegevens moet zoveel mogelijk beperkt zijn.	☐ Versleuteling	☐ Toegangs-controle/ autorisatie	☐ Beveiligde verzending
Standaardinstellingen	De betrokkene moet controle hebben over wat er gebeurt met diens gegevens.	☐ Privacy-vriendelijkste instellingen	☐ Informeren over het doel van gegevensverzameling	☐ Standaard niet-aangevinkte toestemming
Bewaartermijnen	Gegevens mogen zolang bewaard worden als noodzakelijk of wettelijk bepaald.	☐ Archivering	☐ Automatische of handmatige vernietiging	☐ Beleid op oude documenten en apparaten
Faciliteren privacy rechten	De betrokkene heeft het recht om hun gegeven in te zien, te wijzigen en te verwijderen.	☐ Controle over gegevens door de betrokkene	☐ Support aan betrokkene	☐ Beleid op verzoeken