

Bijlage 12 - 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 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 Hierbij opgemerkt dat nieuwe normen binnen een termijn van 3 maanden dienen te zijn gerealiseerd.
Eis	De ICT-oplossing functioneert voor wat betreft aspecten van beveiliging en privacy volledig conform alle betreffende wet- en regelgeving (ten minste AVG, Wbni en BIO) en andere van toepassing zijnde wetgeving, tenzij door de Inschrijver nadrukkelijk anderszijds in de Inschrijving aangegeven en de mitigerende maatregelen hiervoor naar oordeel een van de deelnemende gemeenten toereikend zijn. De BIO voldoet uiteraard enkel voor de reikwijdte die redelijkerwijs aan een SaaS-leverancier kan en behoort te worden gesteld. De deelnemende gemeenten verwijzen in dit kader expliciet naar die BIO-eisen waarbij in de kolom ‘Verantwoordelijke’ (onder meer) de ‘Dienstenleverancier’ wordt benoemd.
Eis	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 een van de deelnemende gemeenten 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 compliance op ieder eerste verzoek hiertoe van een van de deelnemende gemeenten. Zie ook www.digitoegankelijk.nl
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 toegankelijk 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.).

Bijlage 12 - Richtlijn globale aansluitvoorwaarden informatieveiligheid en privacy

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.
Eis	De ICT-oplossing heeft de mogelijkheid op gebruikersgroep niveau vast te leggen dat een gebruiker én een pashouder gekoppeld zijn aan 1 gemeente, waarmee elke gebruiker van betreffende gemeente uitsluitend toegang heeft tot informatie van zijn/haar eigen inwoners.
	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 voornoemde 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. Medewerkers van (de verschillende onderdelen van) de aangeboden ICT-oplossing hoeven hiermee slechts eenmalig (Single-SignOn) te authentifieren om geautoriseerd toegang te krijgen.
Eis	Alle componenten van de ICT-oplossing dienen off-premise (SAAS) geleverd te worden.
Wens	Netwerkverbindingen tussen de gemeenten 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 webstandaarden : DNSSEC en HTTPS en HSTS en IPv4 en IPv6 en TLS 1.3 of hoger, bij voorkeur inclusief het gebruik van security-headers.
Eis	Het gebruik van TLS en HTTP headers voldoet aan de laatste stand van de techniek. De vereiste maatregelen op dit punt zijn uitgewerkt in Bijlage 1, Gebruik van TLS en HTTP response headers. Daarin o.a. de eis om bij onderstaande test-tools moet de SaaS applicatie minimaal een A te scoren: https://www.ssllabs.com/ssltest/index.html https://securityheaders.io/ De URL van de SaaS applicatie = https://groenehartpas.nl
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	Alle pagina's zijn geëncrypteerd via een SSL verbinding
Eis	De gebruikte web-applicatie is up-to-date als ook alle gebruikte componenten.
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

Bijlage 12 - Richtlijn globale aansluitvoorwaarden informatieveiligheid en privacy

	XML-gebaseerde bestandsformaat van deze versie
Eis	Er is voorzien in een Coordinated Vulnerability Disclosure (CVD)-pagina (en beleid) en een security.txt
Eis	Alle kwetsbaarheden worden gescored met behulp van het The Common Vulnerability Scoring System (CVSS). Bij een kritieke kwetsbaarheid wordt de benodigde oplossing (c.q. workaround) door middel van een speedupdate verholpen. Een hoog gescoorde kwetsbaarheid binnen 1 week en een score op middel of laag niveau bij de eerste volgende geplande update van het systeem.
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	Geen van de deelnemende gemeenten 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 onderdelen van het gehele systeem 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 de deelnemende gemeenten en moet na afloop van de overeenkomst in een gangbaar formaat aan de gemeente overhandigd worden. Ook moet de procedure van datavernietiging beschreven zijn. De gerelateerde kosten zijn voor rekening opdrachtnemer
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 en daaraan gerelateerde processen. 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 relevante informatie, te leveren aan de deelnemende gemeenten 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 overeengekomen 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 voor elke deelnemende gemeente welke uitsluitend in het VNG-formaat zal worden vastgelegd.
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 privacy beleid 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).

Bijlage 12 - Richtlijn globale aansluitvoorwaarden informatieveiligheid en privacy

	• 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	Aantoonbaar Privacy by Design/Privacy by Default toepassen bij de ontwikkeling van de ICT-oplossing. Expliciet bij de deelnemende gemeente De Ronde Venen is op aanvraag een Privacy Handboek verkrijgbaar.

Aanvullende voorwaarden	
Eis	De volgende aandachtspunten moeten in ieder geval worden opgenomen in de SLA: • een autorisatieproces voor toegang en rechten van gebruikers en beheerders van de applicatie; • de verplichting tot het bijhouden van een lijst van geautoriseerde personen tot het gebruik van een dienst en hun rechten en privileges ten aanzien van een dergelijk gebruik; • beperkingen ten aanzien van het kopiëren en openbaar maken van informatie; • verantwoordelijkheden ten aanzien van installatie en onderhoud van hardware en software; • het beoogde niveau van de service (responsetijden, beschikbaarheid), evenals onaanvaardbare serviceniveaus; • het recht om contractueel vastgelegde verantwoordelijkheden te controleren of deze controle door een derde te laten uitvoeren; • het vaststellen van een escalatieproces voor het oplossen van problemen;
	• het vastleggen van kwetsbaarheden conform gestelde eis CVSS;
Eis	Uitzonderingen en andere gebeurtenissen die van belang zijn voor de beveiliging worden vastgelegd in zogenaamde “audit logs”, die tenminste het volgende bevatten: • gebruikers-ID's; • data en tijdstippen van aanloggen en afmelden; • overzichten van geslaagde en geweigerde pogingen om toegang te krijgen tot het systeem; • overzichten van geslaagde en geweigerde en andere pogingen om toegang te krijgen tot individuele onderdelen van het systeem en bestanden; • overzichten van raadplegingen en mutaties inclusief gebruikers-ID's, data en tijdstippen in geval van verwerking van persoonsgegevens en of vertrouwelijke gegevens; • De audit logs zijn beschermd zodat ze niet aangepast of gemanipuleerd kunnen worden; • De audit logs zijn 24/7 raadpleegbaar en exporteerbaar (en een gangbaar bestandsformat) voor geautoriseerde medewerkers van de gemeente. • De logs dienen te kunnen worden aangeboden aan SIEM/SOC's.

Bijlage 12 - Richtlijn globale aansluitvoorwaarden informatieveiligheid en privacy

Mailen vanuit externe applicaties	
Eis	E-mail versturen via externe, niet in beheer van de gemeente zijnde mailservers, met zelf aan te vragen domeinen. De oplossing moet voldoen aan het gemeentelijke beveiligingsbeleid en moet gebruik maken van de relevante technieken zoals op de pas-toe-of-leg-uit lijst (PTOLU) 4 staan vermeld (SPF, DKIM, DMARC, STARTTLS+DANE). Te baseren op https://(www.)groenehartpas.nl en @groenehartpas.nl Of E-mail versturen via (een van de deelnemende) gemeentelijke mailservers met al door betreffende gemeente in gebruik zijnde domeinen. De voorwaarden voor het opzetten en gebruiken van de mailserver en bijhorende instellingen worden door de gemeente in overleg met de externe partij bepaald.

Ondertekening			
Onderneming			
Plaats		Datum	
Naam		Functie	
Handtekening			

(NOTE: bij ondertekening garandeert inschrijver alle gestelde eisen en zullen de aangegeven wensen in nadere afstemming met aanbestedende dienst worden bepaald)