Bijlage 12 Architectuurrichtlijnen

Dit betreft de standaarden die voor SaaS-applicaties conform de VNG ICT Kwaliteitsnormen verplicht en aanbevolen zijn.

Applicatiefunctie	Verplichte standaard (pas toe of leg afwijking uit)	Aanbevolen standaard	Implementatie
Gegevensintegratie	OpenAPI Specification 3.0 REST-API Design Rules 1.0 NL GOV Assurance Profile for OAuth 2.0	REST OData 4.0 SOAP 1.2	Koppelingen tussen SaaS en SaaS-applicaties dienen Native koppelingen te zijn zonder dat hiervoor ontwikkeld hoeft te worden. Koppeling met on premise systemen van gemeente uitsluitend via gemeentelijke (API) gateway. Transformatie en Queuing d.m.v on premise ESB mogelijk. SFTP mogelijk voor bestandsuitwisseling. Geen rechtstreekse koppeling (ODBC, JDBC, SQL Net) met databases toegestaan. Geen rechtstreekse koppelingen tussen externe en interne systemen zonder ontkoppeling (proxy). Rechtstreekse koppelingen tussen leveranciers onderling zijn (onder voorwaarden) toegestaan. Gegevens worden uitsluitend binnen EER opgeslagen en verwerkt, maar bij voorkeur binnen Nederland.
Authenticatie & SSO	SAML 2.0	OIDC, OAUth 2.0 RBAC Least privilige	Vereist is een koppeling met de gemeentelijke Azure AD op basis van een van de genoemde standaarden. Door deze koppeling wordt tevens voorzien in twee factor authenticatie en single sign-on. Deze eis impliceert dat een eventuele eigen 2 factor authenticatie implementatie van de leverancier uitgeschakeld moet kunnen worden, zodat de 2fa van gemeente gebruikt kan worden.
Identity provisioning	SCIM 2.0	Actuele versie MS Graph API	SCIM d.m.v. Azure AD heeft de voorkeur.
E-mail	DKIM DMARC SPF DNSSEC Exchange webservices		Mailhosting alleen on premise, Microsoft Exchange. Wanneer als onderdeel van de applicatie e-mail verzonden moet worden uit naam van de gemeente, dan is dit alleen toegestaan wanneer de leverancier vanuit een eigen e-mailvoorziening de mail verstuurt en verwerkt. Gemeente stelt daarvoor een subdomein ter beschikking. De mailserver van leverancier die dit subdomein host, wordt opgenomen in de gemeentelijke SPF-records. Overige vormen van e-mail integratie zijn niet toegestaan.
Data migratie	Inzicht Informatiemodel.		
Front-end	Voor het gebruik van de applicatie(s) volstaat een HTML5 compliant Web Browser (browser onafhankelijk) Digitoegankelijk (EN 301 549 met WCAG 2.1) Ontwikkeld en ingericht op basis richtlijnen OWASP Top 10, of aantoonbaar gelijkwaardige richtlijnen.		Gemeente Groningen heeft een HTML5 compliant Web Browser.
Verbinding	HTTPS HSTS TLS 1.2 DNSSEC	TLS 1.3 IPv6	Voor burgers en bedrijven toegankelijke voorzieningen moeten zowel via IPv4 als IPv6 bereikbaar zijn. Verbinding over Internet d.m.v. TLS heeft voorkeur, alternatief kan een IPsec verbinding over Internet worden gerealiseerd. Leverancier dient applicatie uitsluitend naar het IP-adres van gemeente te ontsluiten, bijvoorbeeld door middel van whitelisting. (TLS) encryptie ingericht conform actuele richtlijnen Nationaal Cyber Security Centrum (NCSC).
Cryptografie/ versleuteling		Gegevens die de SaaS-applicatie opslaat dienen versleuteld te zijn.	Er dient een gedegen versleuteling van toepassing te zijn op data die door de SaaS-applicatie wordt opgeslagen. Richtlijn: Elk wachtwoord heeft een eigen salt waarde (minimaal 64 bits) en wordt gehashed met een SHA-2 algoritme met minimaal 1000 iteraties).
Inloggegevens		Inloggegevens worden alleen over versleutelde verbindingen verstuurd.	Zie verbindingsstandaarden
Toegang tot applicatie via netwerk		SaaS-applicaties dienen voor de gebruikers uitsluitend benaderbaar te zijn via het netwerk van de gemeente Groningen.	Let hierbij op het gebruik van mobiele applicaties zonder aansluiting op het bestaande Gemeente Groningen netwerk.