Bijlage 16- SaaS voorwaarden checklist (ter invulling)
Vervangen afvalkalender-app, website en CMS Afvalstoffendienst
Gemeente ’s-Hertogenbosch
Europees openbare aanbesteding

A	Algemene voorwaarden SAAS applicaties en websites	Toelichting leverancier
	I.g.v. uit-huis-oplossing d.w.z. buiten het gemeentelijk ICT netwerk, dient de oplossing / systeemleverancier te voldoen aan de volgende SaaS-voorwaarden.	
a	De applicatie is een webapplicatie of webservice die werkt onder de in deze TA ondersteunde browsers en hoger met standaard beveiligingsinstellingen. De interface is zonder beperking van functionaliteit, benaderbaar zonder gebruik te maken van browser plug-ins of andere methodieken/software.	
b	Interfaces voor inwoners en bedrijven van de ICT-oplossing voldoen aan de eisen vermeld op www.digitoegankelijk.nl.	
c	De applicatie voldoet aan de beveiligingsrichtlijnen voor webapplicaties van het NCSC1, is versleuteld met protocollen en algoritmen volgens de laatste stand van de techniek2 en moet voldoen aan de pas-toe-of-leg-uit lijst (PTOLU) van het Forum Standaardisatie3 (o.a. https://, DNSSEC, IPv6 etc.)	
d	Het gebruik van TLS en HTTP headers voldoet aan de laatste stand van de techniek. De vereiste maatregelen op dit punt zijn uitgewerkt in het document: “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/ **Wat is de URL van de Saas applicatie?**	
e	Webapplicaties maken bij voorkeur gebruik van een koppeling met Single Sign On (SSO) met Azure AD als de Identity Provider. De SAAS-leverancier mag hierbij gebruik maken van SAML 2.0 of Open-id connect (OAuth 2.0). We gaan uit van minimale set aan gegevens en attributen: voor- en achternaam, email en afdeling. De SSO koppeling is bedoeld voor authenticatie, autorisatie dient plaats te vinden binnen de gekoppelde applicatie. Voor de toegang tot applicaties wordt gebruik gemaakt van Conditional Access. Indien SSO via Azure AD niet mogelijk is, is het mogelijk om de toegang tot de applicatie te beperken tot het IP-adres van het vaste netwerk van de gemeente (dit is niet mogelijk voor mobiele apps), of gebruik te maken van 2-factor authenticatie.	

A	Algemene voorwaarden SAAS applicaties en websites	Toelichting leverancier	
f	Indien er sprake is van de verwerking van persoonsgegevens dient applicatie een verwerkersovereenkomst te worden afgesloten.		
g	Bij verwerking van bijzondere en/of gevoelige persoonsgegevens levert de SAAS-Leverancier jaarlijks een SOC II Type II verklaring en/of een TPM op basis van een andere erkende norm op het gebied van informatieveiligheid.		
h	Wanneer de SAAS applicatie een financieel proces verwerkt dat bijv. voor de jaarrekening van materieel belang kan zijn levert de SAAS leverancier jaarlijks een ISAE 3402 Type II verklaring.		
i	De SaaS-Leverancier en de hostende partij beschikken over een ISO27001-certificering. Waarbij de verklaring van toepasbaarheid dient te worden aangeleverd.		
j	De data moet zijn opgeslagen binnen de Europese Economische Ruimte. Tevens is de vestigingsplaats van de inschrijver binnen de Europese Economische Ruimte.		
k	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;		
l	Uitzonderingen en andere gebeurtenissen die van belang zijn voor de beveiliging worden vastgelegd in zogenaamde “audit logs”, die tenminste het volgende bevatten:		

A	Algemene voorwaarden SAAS applicaties en websites	Toelichting leverancier	
	• 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 's-Hertogenbosch.		
Extra	Het eigenaarschap van de data in het systeem ligt bij de gemeente 's-Hertogenbosch en wordt (kosteloos) bij beëindiging SaaS looptijd in een door de Gemeente 's-Hertogenbosch voorgeschreven formaat beschikbaar gesteld.		

B	Eis t.a.v. koppelingen	Toelichting leverancier	
	Indien het noodzakelijk is dat de SAAS oplossing wordt gekoppeld aan ander systeem, gelden hierbij de volgende uitgangspunten:		
a	Koppelingen met een externe applicatie met een intern systeem van Gemeente 's-Hertogenbosch kunnen zowel synchroon als asynchroon plaatsvinden. Gezien de complexiteit geldt dat nieuwe ontwerpen van koppelingen altijd van een intakeprocedure lopen. Voor transportbeveiliging en vaststelling van identiteit over onvertrouwde netwerken wordt altijd, ongeacht het vertrouwelijkheidsniveau van de informatie, gebruik gemaakt van PKI. Bij informatieverwerkingen van persoonsgegevens en of gegevens met een vertrouwelijkheidsniveau van 'vertrouwelijk' of hoger, moeten mogelijk aanvullende maatregelen worden genomen. Deze afweging wordt gemaakt op de basis van de resultaten van dataclassificatie en risicoanalyse.		

B	Eis t.a.v. koppelingen	Toelichting leverancier	
b	Asynchrone koppelingen tussen een intern systeem en een externe applicatie worden ondersteund op onderstaande wijzen: - Vanuit de applicatie kunnen gegevens worden gepusht naar onze omgeving. Hierbij wordt gebruik gemaakt van ebMS XML of webservice berichtenverkeer wat in een interne queue wordt gezet voor onze broker. - Vanuit een applicatie in het interne netwerk van Gemeente 's-Hertogenbosch wordt periodiek gecontroleerd op de gegevens in de applicatie. Dit gaat altijd via een veilige verbinding. Voor https koppelingen gebruiken we de Service Gateway. Voor sftp, ftps etc. gebruiken we GoAnywhere. - Gegevens worden aangeboden aan een interne applicatie door middel van een webformulier en de broker. Systeemtechnische koppelingen, zoals bijvoorbeeld automatische updates, kunnen via de webproxy of de loadbalancer lopen.		
c	Bij synchrone koppelingen wordt gebruik gemaakt van webservices om informatie tussen systemen uit te wisselen. Via een webservice aanroep wordt de benodigde informatie opgevraagd en direct teruggeleverd. De koppelingen met applicaties via webservices lopen via een Service Gateway.		
d	Voor applicaties kan indien nodig een DigiD koppeling worden aangevraagd. De applicatie dient hiervoor te voldoen aan de eisen uit de DigiD checklist testen van Logius en het Beveiligingsassessment DigiD. Voor het Beveiligingsassessment DigiD dient jaarlijks een TPM worden afgegeven door de SAAS-leverancier.		

C	Eis t.a.v. mailen vanuit externe applicaties	Toelichting leverancier	
a	Het beleid van de gemeente staat niet toe dat e-mail voor domeinen die gebruikt worden door de organisatie zelf wordt verstuurd via e-mail-servers van derden. Mail kan worden verzonden via de volgende mogelijkheden:		

C	Eis t.a.v. mailen vanuit externe applicaties	Toelichting leverancier	
b	E-mail versturen via externe, niet in beheer van de gemeente zijnde mailservers, met zelf aan te vragen domeinen (al bij de gemeente horende domeinen zoals @s-hertogenbosch.nl kunnen dus niet worden gebruikt). 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).		
c	E-mail versturen via de gemeentelijke mailservers met al door de gemeente in gebruik zijnde domeinen. De gemeente biedt de mogelijkheid om via mutual TLS (MTLS) verbindingen met IP-restricties door derden te versturen e-mail via de Microsoft Graph API te ontvangen en via de eigen e-mail infrastructuur te versturen. Alle te versturen mail wordt verzonden namens een no-reply-adres. De voorwaarden voor het opzetten en gebruiken van een MTLS-verbindingworden door de gemeente in overleg met de externe partij bepaald.		

Toetsing van een volledige en correcte implementatie van deze voorwaarden vindt vóór in gebruik name in overleg met de gemeentelijke security-officer plaats. Deze toets zal jaarlijks worden herhaald. In geval van SAAS applicaties blijft de leverancier te allen tijden verantwoordelijk voor de goede en veilige werking inclusief compliancy van de complete oplossing.