



**Belastingsamenwerking**  
gemeenten & hoogheemraadschap Utrecht

## **Annex XV Eisen privacy, informatiebeveiliging en ICT**

De Gemeenschappelijke Regeling Belastingsamenwerking gemeenten en hoogheemraadschap Utrecht (BghU)



**Belastingsamenwerking**  
gemeenten & hoogheemraadschap Utrecht

Versie : Definitief  
Datum : 25 november 2022

# Eisen

## Algemeen

#	Omschrijving
1	Het klantportaal voor zowel gebruik is volledig Nederlandstalig.
2	Inschrijver en de eventuele hostingpartij zijn gevestigd onder Nederlands of Europees recht. Hosting van het klantportaal en de gegevens vindt fysiek plaats in de Europese Economische Ruimte (EER) en in overeenstemming met de eisen van de Europese Unie.
3	Inschrijver biedt binnen de binnen het klantportaal een seamless login ervaring, waarbij een gebruiker niet meerdere malen hoeft in te loggen.
4	In geval van het gebruik van een webserver: de webserver is ingericht volgens een configuratie-baseline.
5	Het klantportaal voorziet de Aanbestedende dienst in een systeembeschrijving waarin de cloud diensten inzichtelijk en transparant worden gespecificeerd en waarin de jurisdictie, onderzoeksmogelijkheden en certificaten worden geadresseerd.
6	Het klantportaal heeft voor de cloud diensten een Service Management beleid geformuleerd met daarin richtlijnen voor de beheersingsprocessen, controleactiviteiten en rapportages.

## Interoperabiliteit

#	Omschrijving																																	
7	De uitwisseling van gegevens dient plaats te vinden op basis van open standaarden zoals vastgesteld en geadviseerd door het Forum Standaardisatie.																																	
8	De volgende aanbevolen standaarden vanuit het Forum Standaardisatie dient Inschrijver -waar van toepassing- toe te passen:																																	
	<table border="1"> <thead> <tr> <th>Standaard</th> <th>Typering</th> <th>Versie</th> </tr> </thead> <tbody> <tr> <td>AES</td> <td>Versleutelingstechniek</td> <td>FIPS 197</td> </tr> <tr> <td>CMIS</td> <td>Content-uitwisseling tussen CMS-/DMS-systemen</td> <td>1.0</td> </tr> <tr> <td>SFTP</td> <td>Bestandsuitwisseling</td> <td>RDC 959</td> </tr> <tr> <td>IP Sec</td> <td>Beveiligde IP verbindingen</td> <td>RFC 4301 met RFC4309 + RFC 6040 en 7619</td> </tr> <tr> <td>JSON</td> <td>Uitwisseling van datastructuren</td> <td>RFC8259 december 2017</td> </tr> <tr> <td>SHA-2</td> <td>authenticatie en integriteitscontrole</td> <td>ISO/IEC 10118- 3:2016</td> </tr> <tr> <td>SSH-2</td> <td>Versleuteld inloggen</td> <td>RFC 4251:2006</td> </tr> <tr> <td>WSDL</td> <td>Interface van webservices</td> <td>2.0</td> </tr> <tr> <td>X509</td> <td>Authenticatie (PKI certificaten)</td> <td>RFC5280 en update RFC6818</td> </tr> <tr> <td>XML</td> <td>Opmaaktaal voor gestructureerde gegevens</td> <td>1.0</td> </tr> </tbody> </table>	Standaard	Typering	Versie	AES	Versleutelingstechniek	FIPS 197	CMIS	Content-uitwisseling tussen CMS-/DMS-systemen	1.0	SFTP	Bestandsuitwisseling	RDC 959	IP Sec	Beveiligde IP verbindingen	RFC 4301 met RFC4309 + RFC 6040 en 7619	JSON	Uitwisseling van datastructuren	RFC8259 december 2017	SHA-2	authenticatie en integriteitscontrole	ISO/IEC 10118- 3:2016	SSH-2	Versleuteld inloggen	RFC 4251:2006	WSDL	Interface van webservices	2.0	X509	Authenticatie (PKI certificaten)	RFC5280 en update RFC6818	XML	Opmaaktaal voor gestructureerde gegevens	1.0
Standaard	Typering	Versie																																
AES	Versleutelingstechniek	FIPS 197																																
CMIS	Content-uitwisseling tussen CMS-/DMS-systemen	1.0																																
SFTP	Bestandsuitwisseling	RDC 959																																
IP Sec	Beveiligde IP verbindingen	RFC 4301 met RFC4309 + RFC 6040 en 7619																																
JSON	Uitwisseling van datastructuren	RFC8259 december 2017																																
SHA-2	authenticatie en integriteitscontrole	ISO/IEC 10118- 3:2016																																
SSH-2	Versleuteld inloggen	RFC 4251:2006																																
WSDL	Interface van webservices	2.0																																
X509	Authenticatie (PKI certificaten)	RFC5280 en update RFC6818																																
XML	Opmaaktaal voor gestructureerde gegevens	1.0																																

	XSL	Transformeren XML berichten	XSL family
--	-----	-----------------------------	------------

### Informatiebeveiliging en privacy

Aanvullende eisen anders dan de reeds gestelde eisen in de GIBIT 2020 (art. 24 en 25) en de Standaard Verwerkersovereenkomst Gemeenten:

#	Omschrijving
9	Alle gegevens zijn en blijven te allen tijde eigendom van de Aanbestedende dienst, zijn ten alle tijden toegankelijk en mogen door de Inschrijver niet voor andere doeleinden worden gebruikt.
10	De integriteit van data blijft gewaarborgd door bedrijfskritische data van Aanbestedende dienst aantoonbaar te scheiden van andere klanten.
11	In het klantportaalomgeving zijn signaleringsfuncties (registratie en detectie) actief, effectief en beveiligd ingericht. De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.
12	Alle onderdelen van servers met opslagmedia behoren te worden geverifieerd, om te waarborgen dat gevoelige gegevens voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.
13	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
14	Ter bescherming tegen malware behoren beheersmaatregelen te worden geïmplementeerd voor detectie, preventie en herstel in combinatie met een passend bewustzijn van de gebruikers.
15	<p>Het klantportaal, de inrichting daarvan en de autorisatie voor gebruik voldoen minimaal aan de richtlijnen van:</p> <ul style="list-style-type: none"> <li>• het Nationaal Cyber Security Centrum;</li> <li>• de Baseline Informatiebeveiliging Overheden (BIO);</li> <li>• alle wettelijke eisen van de AVG en aanpalende wetgeving (zoals o.a. de uitvoeringswet, archiefwet 1995).;</li> <li>• al het Informatiebeveiligingsbeleid van de Aanbestedende dienst (gebaseerd op de Baseline Informatiebeveiliging Overheid).</li> </ul> <p>met inbegrip van de geldende policies t.a.v. autorisatie, logging, wachtwoordbeleid en verwerking van persoonsgegevens.</p>
16	De Inschrijver stemt in met een jaarlijkse en kosteloze audit op informatiebeveiliging conform eerder genoemde richtlijnen door een onafhankelijke auditor en levert, als onderdeel van de tot stand te komen overeenkomst, <u>kosteloos</u> een TPM als bewijs van de audit.
17	Functionaliteiten van het klantportaal worden jaarlijks en kosteloos door de Inschrijver voorzien van een TPM.



18	De Inschrijver behoort regelmatig de naleving van de beveiligingsovereenkomsten op compliancy te beoordelen, jaarlijks een assurance verklaring aan de Aanbestedende dienst uit te brengen en ervoor te zorgen voor onderlinge aansluiting van de resultaten uit deze twee exercities.
19	Informatie over technische kwetsbaarheden van het gebruikte klantportaal behoort tijdig te worden verkregen; de blootstelling aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.
20	De performance van het klantportaal behoort regelmatig te worden gemonitord en hierover behoort tijdig te worden gerapporteerd aan de verschillende stakeholders.