Bijlage 7.2 Programma van Eisen privacy, informatiebeveiliging en ICT

Belastingsamenwerking
gemeenten & hoogheemraadschap Utrecht

Versie : 1.0 herzien

Datum: 13 juli 2021

1 Algemeen

#	Omschrijving
1	De applicatie, voor zowel gebruik als beheer, is volledig Nederlandstalig.
2	Leverancier en de hostingpartij zijn gevestigd onder Nederlands of Europees recht. Hosting van de applicatie en de gegevens vindt fysiek plaats in de Europese Economische Ruimte (EER) en in overeenstemming met de eisen van de Europese Unie.
3	Leverancier biedt binnen de binnen de applicatie 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	De applicatie voorziet de opdrachtgever in een systeembeschrijving waarin de cloud diensten inzichtelijk en transparant worden gespecificeerd en waarin de jurisdictie, onderzoeksmogelijkheden en certificaten worden geadresseerd.
6	De applicatie heeft voor de cloud diensten een Service Management beleid geformuleerd met daarin richtlijnen voor de beheersingsprocessen, controleactiviteiten en rapportages.

2 Architectuur

#	Omschrijving
7	De architectuur van applicatie voldoet aan de principes van de Nederlandse Overheid Referentie Architectuur (NORA/GEMMA).

3 Interoperabiliteit

#	Omschrijving
8	De uitwisseling van gegevens dient vanaf 1 januari 2017 plaats te vinden op basis van open standaarden zoals vastgesteld en geadviseerd door het Forum Standaardisatie.
9	De volgende aanbevolen standaarden vanuit het Forum Standaardisatie dient Leverancier toe te passen:

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
10	De applicatie werkt met geautomatiseerd (binnengemeentelijk) berichtenverkeer op basis van actuele standaarden die door VNG-Realisatie of Forum Standaardisatie zijn vastgesteld en/of voorgeschreven.		

4 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
11	De Leverancier heeft ISO 27001 certificering om aan te tonen dat interne procedures op orde zijn.
12	Alle gegevens zijn en blijven te allen tijde eigendom van de Opdrachtgever, zijn ten alle tijden toegankelijk en mogen door de Leverancier niet voor andere doeleinden worden gebruikt.
13	De integriteit van data blijft gewaarborgd door bedrijfskritische data van Opdrachtgever aantoonbaar te scheiden van andere klanten.
14	In de applicatieomgeving 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.
15	Alle onderdelen van servers met opslagmedia behoren te worden geverifieerd, om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.
16	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
17	Ter bescherming tegen malware behoren beheersmaatregelen te worden geïmplementeerd voor detectie, preventie en herstel in combinatie met een passend bewustzijn van de gebruikers.
18	De applicatie, de inrichting daarvan en de autorisatie voor gebruik voldoen minimaal aan de richtlijnen van:

	• het Nationaal Cyber Security Centrum; • de Baseline Informatiebeveiliging Overheden (BIO); • de meest recente ISO normering voor informatiebeveiliging: ISO 27001 (of een vergelijkbare certificering).; • alle wettelijke eisen van de AVG en aanpalende wetgeving (zoals o.a. de uitvoeringswet, archiefwet 1995).; • al het Informatiebeveiligingsbeleid van de opdrachtgever (gebaseerd op de Baseline Informatiebeveiliging Overheid). met inbegrip van de geldende policies t.a.v. autorisatie, logging, wachtwoordbeleid en verwerking van persoonsgegevens.
19	De Leverancier 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, kosteloos een TPM als bewijs van de audit.
20	Functionaliteiten van de applicatie worden jaarlijks en kosteloos door de Leverancier voorzien van een TPM.
21	De applicatie dient zelf standaardcontroles uit te voeren. Dit omvat bestands- en berekencontroles, integriteitcontroles, verbandscontroles, validiteitcontroles, domeincontroles en controles op onlogische data en dergelijke.
22	De Leverancier behoort regelmatig de naleving van debeveiligingsovereenkomsten op compliancy te beoordelen, jaarlijks een assurance verklaring aan de Opdrachtgever uit te brengen en ervoor te zorgen voor onderlinge aansluiting van de resultaten uit deze twee exercities.
23	Informatie over technische kwetsbaarheden van gebruikte informatiesystemen 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. STIX en TAXII (Uitwisseling van cyberdreigingsinformatie)
24	De performance van de informatiebeveiliging van de cloud omgeving behoort regelmatig te worden gemonitord en hierover behoort tijdig te worden gerapporteerd aan de verschillende stakeholders.

5 Dataportabiliteit

Geen aanvullende eisen anders dan de reeds gestelde eisen in de GIBIT 2020 (art. 18.2 sub i).

6 Toegankelijkheid

#	Omschrijving
25	Leverancier dient met haar applicatie te voldoen aan alle eisen uit de Europese toegankelijkheidsnorm EN 301 549. De eisen voor websites, apps en downloadbare documenten in deze norm zijn identiek aan de niveau A en AA succescriteria van de wereldwijd toegepaste toegankelijkheidsstandaard WCAG 2.1.

7 Archivering

Aanvullende eisen anders dan de reeds gestelde eisen in de GIBIT 2020 (art. 26):

#	Omschrijving
26	De applicatie dient te voorzien in functionaliteiten tot het archiveren en opschonen van historie in de administratie.

8 Infrastructuur

#	Omschrijving
27	Leverancier volgt GDI en GGI ontwikkelingen en werkt mee aan de ondersteuning van deze standaarden.

9 Documentatie

#	Omschrijving
28	Alle documentatie, voor zowel gebruik als beheer, zijn volledig Nederlandstalig.
29	De documentatie bevat minimaal volledige handleidingen en helpfunctie(s) voor eindgebruikers en beheerders. Hierbij moet ook inzichtelijk gemaakt worden welke parameters binnen de configuratie ingesteld kunnen worden en wat de werking en impact per parameter is.
30	De opdrachtgever heeft het recht de documentatie vrij en kosteloos te verspreiden ten behoeve van de gebruikers.
31	Bij ontbreken van bepaalde documentatie is Leverancier verplicht om op eerste verzoek van Opdrachtgever binnen 5 werkdagen de aanvullende documentatie kosteloos op te stellen en aan te leveren als aanvulling op de reeds beschikbare, officiële documentatie.

32	Bij elke release (update en upgrade) wordt een geactualiseerde versie handleidingen en release notes verstrekt, waarin duidelijk wordt beschreven wat de wijziging zijn en eventuele consequenties voor de werking van de applicatie ten opzichte van de vorige versie.
33	Volledige, actuele en relevante beschrijvingen van de applicatie waarin tenminste de volgende onderwerpen duidelijk worden toegelicht: architectuur, functies en functionele werking en technische specificaties waaronder die voor de koppelvlakken voor technische integratie met de andere applicaties.
34	Volledige en actuele technische infrastructuur van de applicatie waarin tenminste de volgende onderwerpen duidelijk worden toegelicht: ip-adressen, certificaten, locatie, dns naam etc.

10 E-facturering

#	Omschrijving
35	Leverancier moet bij elektronische facturen (e-factureren) de Europese richtlijn 2014/55/EU volgen, conform art. 9.7 GIBIT 2020.

11 Authenticatie en autorisatie

#	Omschrijving
36	De applicatie ondersteunt SSO (Single Sign On) in combinatie met Windows Active Directory 2012 of hoger (ADFS) en Azure Active Directory.
37	De autorisaties van de applicatie kunnen door de opdrachtgever worden ingesteld.
38	De applicatie wordt ingericht met accounts, die individueel herleidbaar zijn naar medewerkers/personen, voor alle gebruikers en beheerders, zodat in logging duidelijk is wie, wat, wanneer heeft aangepast. Persoonlijke accounts voor applicatiebeheerders en systeembeheerders dienen hiervoor voldoende rechten te hebben, waarbij het niet mogelijk is voor beheerders om via een generiek superuser account te werken.
39	De applicatie ondersteunt autorisaties per rol. Per gebruiker en groepen van gebruikers is te autoriseren of gegevens mogen worden aangemaakt, geraadpleegd, gemuteerd en/of worden verwijderd.
40	Autorisaties van een specifieke gebruiker van de applicatie kunnen worden overgenomen cq gekopieerd om (nieuwe) gebruikers aan te maken of aan te passen.
41	Voor autorisaties binnen de applicatie geldt dat voor controle en audits een gedetailleerd overzicht van alle gebruikers en bijhorende autorisaties kan worden gegenereerd. De applicaties toont eveneens wijzigingen in autorisaties en een overzichtsscherm van de actuele ingelogde gebruikers.
42	Indien Leverancier toegang tot de applicatie (en/of de database) nodig heeft wordt hiervan te allen tijde melding gemaakt bij de desbetreffende afdeling van Opdrachtgever.
43	De applicatie dient voor alle gebruikers tenminste gebruik te worden gemaakt van 2FA/MFA voor authenticatie.

#	Omschrijving
44	De applicatie ondersteunt ook het bieden van via de IAM-omgeving (op dit moment Azure/ADFS) van Opdrachtgever.
45	De applicatie dient ook via openbare netwerken benaderbaar te zijn en enkel via een door de Opdrachtgever beheerd device, door medewerkers van Opdrachtgever 'in het veld' en vanaf de locatie van organisaties. Hierbij dient tenminste gebruik te worden gemaakt van 2FA/MFA en een VPN verbinding.

12 Logging

#	Omschrijving
46	Er is een automatische mutatielogging in werking binnen de applicatie op handeling, gebruiker en tijdstip. De mutatielogging is ingericht volgens normkaders (vaste logregels). Van alle processen wordt een volautomatische mutatielogging aangemaakt. Een nieuwe mutatie mag een oude mutatielogging niet overschrijven. Deze logbestanden zijn beperkt toegankelijk en extra beveiligd.
47	De applicatie voorziet in functionaliteiten voor het borgen en het inzichtelijk maken in de logging van gegevensmutaties, inclusief de oorsprong van de mutatie (gebruiker, tijdstip en/of proces) en behoud van de gegevens voor de mutatie. De invloed hiervan mag geen dusdanig negatieve invloed op de performance tot gevolg hebben dat het werken met de applicatie praktisch onwerkbaar wordt.
48	Er moet een automatisch (technisch) foutmeldingen register worden bijgehouden in de applicatie. Dit geldt voor fouten bij invoer als ook foutmeldingen m.b.t. koppelingen met andere applicaties. Het register is raadpleegbaar, ook voor niet-technisch gebruikers.
49	De applicatie voorziet om geautomatiseerd IT-gerelateerde beveiligingsinformatie te verzamelen, te combineren en te analyseren of kan geautomatiseerd IT-gerelateerde beveiligingsinformatie door zetten naar een Security Information & Event Management oplossing (SIEM).

13 Koppelingen en digitaal uitwisselen

#	Omschrijving
50	De applicatie is bruikbaar (interoperabiliteit) op verschillende IT-platforms en kunnen op basis van standaarden verschillende IT-platforms met elkaar verbinden en data overdragen (portabiliteit) naar andere cloud service providers.
51	De Leverancier levert documentatie aan, waarin alle (incl. tweezijdige) koppelingen/koppelvlakken van de applicatie zijn beschreven.
52	De applicatie wordt ontsloten op basis van een beveiligde verbinding volgens de geldende (en toekomstige) veiligheidsstandaarden.
53	De koppeling tussen de applicatie en de externe applicaties vindt plaats via een ipsec VPN verbinding of gelijkwaardige verbinding (datalijn) die aan de volgende eisen voldoet:

	• AES encryptie 128 bit of hoger • SHA2-256 authenticatie of beter
54	Sessie versleuteling. De applicatie past encryptie toe op de communicatie van vertrouwelijke gegevens over niet veilige netwerken, middels: • TLS 1.2 of hoger, HTTPS en HSTS (beveiligde verbinding) • DNSSEC (ondertekende domeinnaam)
55	Alle gegevens uit de database van de applicatie kunnen tenminste o.b.v. API, ESB of ETL worden geëxtraheerd via een beschikbaar koppelvlak en in het kader van datagedreven sturing worden gebruikt in een datawarehousing of andere omgeving.
56	De Leverancier van de applicatie geeft inzage in het datamodel van de database indien gewenst onder non-disclosure agreement. In de applicatie moet van ieder schermveld eenvoudig te achterhalen zijn wat de naam van het veld in de database is en in welke tabellen dit veld voorkomt.

14 Onderhoud en Technisch Beheer

#	Omschrijving
57	De applicatie wordt aangeboden als SaaS-oplossing. Dit betekent dat: • Opdrachtgever heeft toegang tot de applicatie via internet of een privénetwerk. • de applicatie en alle benodigde overige software en de daarvoor benodigde hardware zijn in eigendom van Leverancier. Opdrachtgever hoeft niets aan te schaffen, maar betaalt slechts voor het gebruik ervan. • De applicatie en overige software en hardware wordt niet bij de Opdrachtgever geïnstalleerd, maar bij Leverancier. • Leverancier verzorgt de hosting, het technisch beheer en het applicatiebeheer, zoals het maken van back-ups, het onderhoud en de installatie van nieuwe versies en updates, beveiliging tegen ongeautoriseerde toegang, en dergelijke.
58	Het beheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.
59	Het functioneel beheer wordt door Opdrachtgever uitgevoerd, waarbij Opdrachtgever de volledige vrijheid heeft de applicatie functioneel naar eigen wens in te richten binnen de mogelijkheden die de applicatie biedt en door de Leverancier wordt ondersteund.
60	Het is mogelijk voor Opdrachtgever om de applicatie af te sluiten dan wel toegang tijdelijk te blokkeren voor (groepen van) geautoriseerde gebruikers ten behoeve van beheerwerkzaamheden.
61	Wijzigingenbeheer is procesmatig en wordt procedureel zodanig uitgevoerd dat wijzigingen door Leverancier in de ICT-voorzieningen van de applicaties tijdig (tenminste 5 werkdagen vooraf), geautoriseerd door Opdrachtgever en getest door Leverancier worden doorgevoerd.
62	Leverancier biedt een Service Level Agreement en een Dossier Afspraken en Procedures (DAP) binnen 3 maanden na ondertekening van de Overeenkomst ter acceptatie aan Opdrachtgever. De opgenomen

	normen in de SLA zijn minimaal gelijk of hoger dan gesteld in de servicenormen in dit Programma van Eisen.

15 Productie en testomgevingen

#	Omschrijving
63	De productieomgeving (gegevens en inrichting) is direct en zelfstandig door Opdrachtgever, of op eerste verzoek van Opdrachtgever door Leverancier binnen 5 werkdagen te kopiëren naar de testomgeving en (t.b.v. testen). Deze testomgeving is tevens te gebruiken voor proef(conversies) en opleidingen.
64	Leverancier heeft eigenstandig de beschikking over zowel een separate test- als productieomgeving. De testomgeving betreft een volwaardige omgeving met alle data, inrichting en koppelingen gelijk aan de productieomgeving. Bij updates en upgrades wordt de testomgeving tenminste 10 werkdagen voor het bijwerken van de productieomgeving bijgewerkt naar de nieuwe, beoogde versie van de applicatie voor de productie-omgeving.

16 Upgrades en Updates

#	Omschrijving
65	Bij het ontwikkelen van software wordt https://cve.mitre.org/ gebruikt om kwetsbaarheden in software te identificeren.
66	Alle gebruikte software wordt, na het ontdekken, binnen onderstaande termijnen voorzien van beschikbare beveiligingsupdates dan wel een workaround voor een adequate mitigering van de kwetsbaarheid: • voor kwetsbaarheden met een CVSS base score lager dan 4: de eerstvolgende major of minor release van de software; • voor kwetsbaarheden met een CVSS base score tussen 4.0 en 6.9: binnen 3 maanden na het uitkomen van een patch; • voor kwetsbaarheden met een CVSS base score tussen 7.0 en 8.9: binnen 1 maand na het uitkomen van een patch; voor kwetsbaarheden met een CVSS base score tussen 9.0 en 10: binnen 72 uur na het uitkomen van een patch.
67	De Leverancier ondersteunt de werking van de applicatie op Windows 10 Pro en Enterprise en nieuwere Windows besturingssystemen, zolang dit besturingssysteem ondersteund wordt door Microsoft conform de kenbaar gemaakte ondersteuningscyclus door Microsoft.
68	In geval van een webapplicatie, ondersteunt de Leverancier de werking van de applicatie op zowel de nieuwste versies browsers van Microsoft Edge o.b.v. Chromium (voor bedrijven), Google Chrome (voor bedrijven) en Mozilla Firefox alsmede de voorliggende versies van maximaal 2 jaar oud.

69	Upgrades en Updates worden vanuit de Leverancier na overleg met Opdrachtgever via SaaS op de testomgeving beschikbaar gesteld. De releases en updates kunnen dan functioneel worden getest door Opdrachtgever. Technische tests worden door de Leverancier uitgevoerd.
70	Bij Upgrades en Updates geeft de Leverancier tijdig aan wanneer deze plaatsvinden
71	Bij Upgrades en Updates van de applicatie zorgt de Leverancier ervoor dat bestaande koppelingen blijven functioneren.
72	Bij Upgrades en Updates garandeert de Leverancier dat de bestaande inrichting en werkstromen en instellingen intact blijven en hun werking behouden. Het moet duidelijk zijn welke invloed de wijzigingen hebben op de inrichting en/of werkstromen, zodat deze wijzigingen op zelf ontwikkelde inrichting en werkstromen kunnen worden doorgevoerd.

17 Service Levels

De volgende minimale Service Levels voor Onderhoud, Technisch Beheer en ondersteuning zijn van toepassing en dienen door Leverancier na contractering verwerkt te worden in haar standaard SLA en een DAP:

#	Omschrijving

73	<u>Incidenten/problemen, prioriteit en hersteltijd</u>
	• De servicedesk van Leverancier is bereikbaar op Werkdagen van 8:00 tot 17:00.
	• Elk incident/probleem dat bij de servicedesk wordt gemeld, krijgt een bepaalde prioriteitsstelling. Prioriteitstelling vindt plaats op grond van impact en urgentie. De prioriteit van een incident wordt vastgesteld in samenspraak met de contactpersoon van de leverancier. Indien er geen overeenstemming is, stelt Opdrachtgever de prioriteit, en in geval van meerdere incidenten, de volgorde van afwikkeling van de incidenten vast.
	• Een incident/probleem met de hoogste prioriteit, prioriteitsgroep 1, wordt als volgt bepaald: de urgentie van het incident is hoog, want het betreft een kritisch bedrijfsvoeringsproces of de doorgang/voortgang van de bedrijfsvoering is/wordt ernstig verhinderd, en de impact op de organisatie van Opdrachtgever en/of de gebruikers is groot, omdat de gehele organisatie, een of meerdere locaties getroffen zijn dan wel de doorgang/voortgang van de bedrijfsvoering is/wordt ernstig verhinderd.
	• Er geldt geen beperking voor wat betreft het aantal (telefonische) meldingen/calls.
	• Leverancier incidenten/problemen met prioriteit 1 moeten binnen vier (4) uur na het melden van het incident/probleem verholpen zijn.
	  ○ Herstelwerkzaamheden ten behoeve van een prioriteit 1 incident/probleem zullen ononderbroken en ook buiten werkdagen worden uitgevoerd en op kortst mogelijke termijn worden voltooid, mits het incident/probleem tijdens Werkdagen tussen 8:00 en 17:00 is gemeld..
	  ○ Leverancier zal redelijkerwijs voorzien in een werkbare tijdelijke oplossing, indien het systeem - om welke reden ook - langer dan acht (8) uur buiten werking is c.q. niet beschikbaar is c.q. voorzienbaar is of wordt dat het systeem langer dan acht (8) uur buiten werking zal zijn en/of niet beschikbaar zal zijn. Leverancier zal binnen vier (4) uur

	na aanvang van het onderzoek naar de geëigende herstelmaatregelen een urenschatting afgeven. o Een werkbare tijdelijke oplossing voldoet als oplossing, mits de werkbare tijdelijke oplossing ook binnen de gestelde maximale oplostijd beschikbaar is en niet langer dan 48 uur na melding van het incident benodigd is; binnen 48 uur is de oorzaak en het incident volledig opgelost met een structurele oplossing. • Alle incidenten/problemen/vragen worden geregistreerd in een servicemanagement tool. Opdrachtgever heeft te allen tijde inzage in (de status van) deze registraties. • De servicemanagement tool van de Leverancier moet (automatisch) kunnen koppelen met de meest gangbare servicemanagement tools in de markt. Leverancier koppelt kosteloos met de huidige servicemanagement tool van Opdrachtgever (TOPdesk).
74	<u>Onderhoud</u> Regulier onderhoud zal alleen uitgevoerd mogen worden met de voorafgaande toestemming of op verzoek van BghU op werkdagen tussen 18:00 uur en 7:00 uur of buiten werkdagen. Het uitvoeren van onderhoud zal minimaal vijf (5) werkdagen van tevoren worden aangekondigd.
75	<u>Beschikbaarheidsvenster en beschikbaarheid</u> • Het systeem is in ieder geval gegarandeerd beschikbaar tussen 7:00 en 22:00 uur op werkdagen voor gebruikers (beschikbaarheidsvenster). Het systeem is beschikbaar indien er, gedurende het tijdsvenster, geen incidenten uit met prioriteit 1 en minimaal 95% van de gebruikers het systeem op normale wijze kan gebruiken. • Buiten het beschikbaarheidsvenster is het systeem ook te allen tijde beschikbaar voor gebruikers, maar op basis van best-effort en behoudens gepland onderhoud. • De norm voor de gemiddelde beschikbaarheid van het systeem is 98,75% gedurende het gegarandeerde beschikbaarheidsvenster over een periode van een maand. • De maximaal aaneengesloten onbeschikbaarheid gedurende het beschikbaarheidsvenster mag niet meer dan 4 uren overschrijden. o Minimaal 98,75% beschikbaarheid betekent maximaal 1,25% onbeschikbaarheid per maand. Gemiddeld 261 werkdagen in een jaar, derhalve 21,75 werkdagen per maand. Het gegarandeerde beschikbaarheidsvenster omvat de tijdsperiode 7:00 tot 22:00 = 15 uur. De totale maximale onbeschikbaarheid per maand in het van een 98,0% beschikbaarheid bedraagt daarom: 1,25% x 15 x 21,75 = 4 uur en 5 minuten per maand binnen het beschikbaarheidsvenster.
76	<u>Capaciteit/performance</u> De leverancier garandeert voldoende systeemcapaciteit voor het gebruik van het systeem in relatie tot het aantal gelijktijdige gebruikers voor tenminste 60 gelijktijdige gebruikers en biedt voldoende mogelijkheden voor uitbreiding van de capaciteit in het geval, toename van het gebruik of anderszins, van het systeem in relatie tot dit toegenomen gebruik zonder dat dit leidt tot problemen dan wel degradatie in de beschikbaarheid en/of de prestaties van het systeem.
77	<u>Backup en herstel</u> • Leverancier voert dagelijks back-ups uit voor hersteldoeleinden op twee niveaus: o database back-ups o server back-ups

	• De Recovery Point Objective (maximale dataverlies) bedraagt maximaal 4 uur. • De Recovery Time Objective (maximale hersteltijd) bedraagt maximaal 4 uur.
78	<u>Monitoring</u> Leverancier zal het systeem zodanig inrichten dat het voor de leverancier, die de bewaking uitvoert, mogelijk is om de beschikbaarheid, capaciteit en performance van alle vitale hardware- en softwarecomponenten die noodzakelijk zijn voor (het normale gebruik van) het systeem 24 uur/7 dagen per week te kunnen bewaken. De bewaking van het systeem is zodanig ingericht dat de realisatie van de overeengekomen servicenormen gewaarborgd zijn.

---oOo---