Programma van Eisen n.a.v. 1e en 2e nota van inlichtingen

In dit Programma van Eisen wordt aangegeven welke eisen de gemeente Halderberge stelt aan het te selecteren Raadsinformatiesysteem (verder genoemd RIS) voor de Gemeenteraad.

Het Programma van Eisen bestaat uit een pakket van eisen met een knock-out karakter; het niet voldoen of kunnen voldoen aan één van deze eisen leidt automatisch tot uitsluiting van verdere deelname aan deze aanbestedingsprocedure.

Mocht een inschrijver zich niet kunnen vinden in één of meerdere eisen van het Programma van Eisen, dan dient dit (tijdig) te worden aangegeven in de Nota van Inlichtingen.

Dit Programma van Eisen bevat de volgende onderdelen:

- Eisen vanuit de gemeente Raad
- Systeemeisen
- Overige eisen

Eisen van de Raad

	Eisen Raad
1.	Het RIS geeft informatie over de vergaderingen en overige bijeenkomsten en evenementen van en naar de Raad. Bijeenkomsten kunnen openbaar en besloten zijn. Dit kan per groep of per persoon worden ingesteld. De vergaderapp en de web omgeving tonen en ontsluiten dezelfde informatie. De gemeente verwacht een SaaS applicaties waarbij het eventueel mogelijk is om middels een app de front-end te bedienen.
2.	Bijeenkomsten kunnen in ieder geval de volgende informatie bevatten: - Datum, locatie, tijd en tijdsduur - Voorzitter en griffier - Vergaderstukken - Agendadocumenten (los van agendapunten) Er kan bij verschillende vergaderingen gevarieerd worden in de beschikbare velden. Er is een mogelijkheid om velden openbaar en niet-openbaar te publiceren. De kenmerken / velden van een vergadering/bijeenkomst moeten af te schermen zijn in het geval het een niet openbaar of geheim karakter heeft.
3.	Het RIS voorziet in de openbare publicatie van moties, amendementen, toezeggingen, schriftelijke vragen en technische vragen van raads- en burgerleden. Het RIS voorziet ook in de weergave van de voortgang en afdoening van deze documenten. Het is daarbij mogelijk (delen van) informatie af te schermen voor publiek. Bij alle documenten is het mogelijk om betrokken raads- en burgerleden en portefeuillehouder vast te leggen. Op basis van deze gegevens kan ook worden gefilterd. Opdrachtgever ziet het publicatieplatform als onderdeel van de RIS oplossing.
4.	In een lange termijn agenda is zichtbaar welke vergaderingen en bijeenkomsten aankomende maanden plaatsvinden. Deze agenda is voor gebruikers zichtbaar. Tevens bestaat de mogelijkheid deze openbaar te publiceren. Per vergadering wordt aangegeven welke onderwerpen worden behandeld. Per onderwerp is minimaal zichtbaar: - Een korte toelichting op het onderwerp; - Doel van de behandeling (beeldvorming & informatie, consultatie & opinie, advisering, besluitvorming); - Wie portefeuillehouder is; - Wie ambtelijk ondersteuner is; - Of en wanneer het onderwerp gepland staat voor de raadsvergadering; - Welke documenten ter bespreking zijn; - Hoeveel tijd het onderwerp naar verwachting in beslag neemt; - Wanneer het in de agendacommissie is/wordt behandeld. - Wat de historie van een onderwerp is. - Bijlagen
5.	Er is ruimte voor ingekomen stukken van de Raad. Daarbij is een mogelijkheid om deze te koppelen aan een portefeuillehouder en aan een vergadering waarin ze besproken worden. (Delen van) ingekomen stukken kunnen niet-openbaar worden gemaakt. Er kan worden gefilterd op beschikbare velden (datum, ~~poho~~ portefeuillehouder, soort afdoening).
6.	Er kunnen overzichten worden geëxporteerd van de documenten hierboven bij 3, 4 en 5 (Excel en PDF). Het is mogelijk alle beschikbare gegevens in de export op te nemen.
7.	Er is de mogelijkheid om dossiers te vormen met daarin documenten. Beheerders hebben de mogelijkheid om deze dossiers te vormen en aan te passen. Er is een onderscheid mogelijk tussen openbare documenten en documenten die niet-openbaar zijn.
8.	Het RIS voorziet in automatische notificaties voor gebruikers bij toevoegen, wijzigen en verwijderen van bijeenkomsten, stukken, documenten etc. Gebruikers hebben de mogelijkheid om notificaties aan en uit te zetten en te beheren per type document, wijziging of bijeenkomst.

	Ook voor beheerders is het mogelijk wijzigingen te includeren of excluderen voor notificaties.
9.	Gebruikers kunnen notities maken bij documenten en deze delen met andere gebruikers, ook groepsgewijs. Notities blijven behouden als een document wordt vervangen door een nieuwe versie of nadien wordt bewerkt.
10.	Gebruikers kunnen tekenen en arceren in documenten.
11.	Beheerders kunnen documenten uploaden in Word, Excel, JPEG, PNG. Applicatie zet deze om naar PDF-formaat met behoud van lay-out en hyperlinks die blijven werken.
12.	Het aantal handmatige handelingen bij het opbouwen van een vergaderagenda is minimaal. Verzenden van uitnodigingen, vergaderoproepen etc. kan geautomatiseerd.
13.	Het RIS heeft een zoekfunctie, die: - Kan zoeken in het hele media-archief en in het archief van vergaderingen (en metadata); - filtering en sortering kent op alle mogelijke zoekvelden; - voor alle gebruikers en openbaar beschikbaar is; - specifiek kan zoeken naar vergaderingen, agendapunten, documenten, sprekers
14.	Het RIS voorziet in een webversie en een vergaderapp voor Windows, IOS en Android. Het gebruik van iOS apparatuur is breder in de gebruikersgroep en er wordt ook gewerkt in de web omgeving middels laptops met Windows.
15.	Het toevoegen, wijzigen, verwijderen van stukken aan/bij vergaderingen is vanuit de griffie te allen tijde mogelijk.
16.	Gedurende het proces (van moment van starten tot ondertekening raadsbesluit) kunnen de documenten leven in het RIS. Aan het einde van de rit is het mogelijk om de gewijzigde documenten terug te schrijven naar het Zaaksysteem (xxllnc Zaken)
17.	Gebruikers kunnen zich 'aanmelden' voor vergaderingen en de data van deze vergaderingen exporteren naar de agenda op hun device (iCal-bestand). Dit moet ook en groupe kunnen voor een reeks vergaderingen.
18.	Stukken of agendapunten die tijdens een vergadering worden toegevoegd of worden gemuteerd zijn onmiddellijk zichtbaar voor de deelnemers.
19.	Adequate ondersteuning tijdens uitzending van vergaderingen / bereikbare helpdesk/hulplijnen voor ondersteuning bij technische issues tijdens de (avond)vergaderingen. Bereikbaarheid minimaal tot 23:00 uur.
20.	Op verzoek verzorgt de Opdrachtnemer trainingen en instructie aan gebruikers. De training en instructie aan gebruikers voor in gebruik name zit bij het offertebedrag inbegrepen. Overige trainingen en instructies worden op basis van nacalculatie gefactureerd.
21.	In de video- en audiofragmenten is terug te zoeken wat per spreker, fractie, vergadering, agendapunt de inbreng en stemming was. In de fragmenten moet een kijker/luisteraar kunnen zoeken en selecteren op waar door wie wat gezegd wordt en wat de stemmingsuitslag was bij een stemming. Een inwoner wil bijvoorbeeld in de vergadering van een bepaalde datum het stukje bekijken van een specifiek fractielid van een bepaalde partij.
22.	Het RIS dient volledig Nederlandstalig te zijn.
23.	Bij installatie/implementatie van het RIS is een duidelijke begeleiding/uitleg (door middel van een fysieke training op locatie) voor het in gebruik nemen van het RIS noodzakelijk.
24.	Het RIS moet grote (> 250 pagina's) documenten, zoals bij bestemmingsplantekeningen, kunnen laden.
25.	Er kunnen direct stukken vanuit het RIS naar de griffie worden doorgezet. Vanuit de vergaderomgeving kunnen stukken doorgezet worden naar de griffie of griffiemedewerkers. Dit mag een mailkoppeling zijn of een koppeling naar een opslaglocatie zijn. Er is geen afzonderlijk griffiesysteem.
26.	Er is een mogelijkheid om op verschillende niveaus rechten te kunnen toebedelen (openbare stukken, vertrouwelijke en p-dossiers).
27.	Er is een mogelijkheid om onderscheid te kunnen maken tussen een openbare en een vertrouwelijke agenda en daarbij twee verschillende besluitenlijsten te kunnen genereren.
28.	Er is een mogelijkheid voor het bestuurssecretariaat/gemachtigden om zelf aan de 'achterkant' van een agenda nog stukken te uploaden.

	Onder toezicht van de griffie kunnen gemachtigden nog stukken toevoegen aan agenda's van vergaderingen. Bijvoorbeeld om op het laatste moment alsnog een stuk komende vanuit het college toe te voegen. Is dus wel heel specifiek voor en door griffie gemachtigde gebruiker.
29.	Er is een mogelijkheid om besluiten te kunnen vastleggen in het RIS en op basis hiervan een besluitenlijst te kunnen genereren.
30.	Vergaderstukken dienen direct vanuit het RIS beschikbaar te zijn bij vergaderingen. Dit geldt ook voor de vergaderapp.
31.	Er is een mogelijkheid om geheime stukken toe te voegen aan een openbare vergadering. De geheime stukken blijven alleen voor geautoriseerde personen zichtbaar en worden niet openbaar gemaakt.
32.	Het RIS voorziet volledig in papierloos vergaderen. Wel dient de mogelijkheid te worden geboden aan gebruikers om documenten (indien gewenst) te kunnen printen. Bij het printen van een agenda kan per bijlage worden aangegeven of deze wel of niet geprint wordt.
33.	Bij het openen van een agendapunt zijn alle documenten met eventuele annotaties die bij dit agendapunt horen te zien.

Systeemeisen

	Systeemeisen
34.	Live-uitzending van de vergadering in beeld en geluid via internet. Achteraf terugkijken van vergaderingen in beeld en geluid via internet blijft altijd mogelijk (de vergaderingen worden gearchiveerd). De oude agenda's inclusief de daarbij behorende opnames blijven vindbaar en te bekijken. Opdrachtnemer houdt deze oude agenda's beschikbaar gedurende de looptijd van de overeenkomst.
35.	Live-uitzending en archivering van de (soms gelijktijdige) vergaderingen in beeld en/of geluid via internet. Achteraf terugkijken van deze vergaderingen in beeld en/of geluid via internet blijft altijd mogelijk (de vergaderingen worden gearchiveerd).
36.	Live-uitzending van andere incidentele bijeenkomsten (bijv. bijeenkomsten of verkiezingsdebat). Achteraf terugkijken van deze bijeenkomsten in beeld en/of geluid via internet blijft altijd mogelijk (de bijeenkomsten worden gearchiveerd).
37.	Opdrachtnemer dient vergaderingen uit te zenden die zowel fysiek (in raadzaal), digitaal (MS Teams) en hybride worden gehouden. De raadsvergaderingen dienen via een livestream via het internet toegankelijk te zijn.
38.	Overschakelen van fysieke naar digitale vergaderingen en vice versa is kosteloos en onbeperkt mogelijk gedurende de looptijd van de overeenkomst.
39.	Na afloop van de vergadering dient de vergadering binnen 1 werkdag online te staan, geïndexeerd doorzoekbaar op agendapunt.
40.	Na uitzending dient de vergadering binnen 3 werkdagen ook geïndexeerd doorzoekbaar op spreker te zijn (bij een vergadering op dinsdagavond betekent dit uiterlijk maandagochtend 8.00 uur).
41.	Na de uitzending dient binnen 5 werkdagen ondertiteling te zijn toegevoegd (achteraf toegevoegd binnen 5 werkdagen, live ondertiteling is geen eis). De ondertiteling is doorzoekbaar via de zoekfunctie.
42.	Het RIS moet geschikt zijn voor het verwerken en uitzenden van videobeelden van derden. Het moet mogelijk zijn om videobeelden die tijdens een vergadering in de raadszaal getoond worden, onderdeel te maken van de videotulen.
43.	Het RIS moet geschikt zijn om videobeelden (en geluid) in een aparte internetstream (zonder aanvullende informatie) aan te bieden aan derden, bijvoorbeeld de lokale of de regionale omroep.
44.	De opdrachtnemer zorgt voor het opstarten van de encoder. De griffie hoeft hier geen handelingen voor te verrichten. Dit wordt gedaan door een signaal vanaf de encoder naar de Opdrachtnemer te sturen en niet andersom.
45.	Op de dag van de vergadering kan een testuitzending voor beeld en/of geluid worden uitgevoerd door opdrachtgever, zonder tussenkomst van de opdrachtnemer.
46.	Tijdens de **live uitzending van de raadsvergadering** dient het RIS zorg te dragen voor: • het markeren van het actieve agendapunt; • het correct en snel markeren van de actieve spreker; • het aanpassen, indien nodig, van de volgorde van de agendapunten; • het toevoegen van commentaar over de uitzending van de vergadering (bijvoorbeeld schorsing en de duur hiervan).Over de aard van het tijdens de uitzending door de regisseur toe te voegen commentaar, worden vooraf afspraken gemaakt. • het beschikbaar stellen van een mogelijkheid om digitaal te stemmen.

47.	Tijdens de **live uitzending van de commissie en informatieve vergaderingen** dient het RIS zorg te dragen voor: • het markeren van het actieve agendapunt; • het aanpassen, indien nodig, van de volgorde van de agendapunten; • het toevoegen van commentaar over de uitzending van de vergadering (bijvoorbeeld schorsing en de duur hiervan).Over de aard van het tijdens de uitzending door de opdrachtnemer toe te voegen commentaar, worden vooraf afspraken gemaakt. • Verslaglegging.
48.	Het digitaal verslag van de raadsvergadering en overige vergaderingen bestaat uit: • de agenda en bijbehorende vergaderstukken. • de opname in beeld en/of geluid. Het digitale verslag is voorzien van ondertiteling. • indexering op agendapunt en spreker. Indexering op spreker gebeurt binnen 3 werkdagen na de vergadering (bij een vergadering op donderdag betekent ditvóór woensdagochtend 8.30 uur). • Communicatie en dus ook verslaglegging vindt plaats in de Nederlandse taal. • De uitslag van de stemmingen, waarbij de stemming per raadslid en per fractie zichtbaar is.
49.	Opdrachtnemer verstrekt de gemeente iedere maand kijkcijfers over alle vergaderingen die in de betreffende maand zijn uitgezonden, zowel live als on demand.
	Archivering
50.	Het RIS voldoet aan de Gemeentelijke ICT kwaliteitsnormen met betrekking tot archiveren van de conform de geldende GIBIT Toolbox van VNG Realisatie en aan de Archiefwet.
51.	Het RIS voldoet aan de relevante, van toepassing zijnde wet- en regelgeving.
52.	Bij overstap van de huidige Opdrachtnemer naar de nieuwe Opdrachtnemer dient de nieuwe Opdrachtnemer de archiefbestanden van de huidige Opdrachtnemer kunnen migreren. Na migratie moeten de archiefbestanden vindbaar, beschikbaar, leesbaar en betrouwbaar (de kwaliteit van de gemigreerde bestanden niet merkbaar slechter is geworden dan de originelen) zijn.
53.	Vanuit de RIS omgeving is het mogelijk om archiefbestanden over te dragen aan een andere Oplossing dan wel e-Depot. Volgens het metadatamodel MDTO geëiste metadata moet geëxporteerd kunnen worden. Op termijn moeten de archieven van de vergaderingen overgeplaatst worden naar een e-Depot van het West-Brabants archief. Dit middels een gedefinieerde standaard.
54.	Het digitaal verslag moet na een vergadering beschikbaar en toegankelijk zijn om (openbaar) te raadplegen. Na vaststelling moet het digitaal verslag duurzaam toegankelijk zijn: vindbaar, beschikbaar, leesbaar, interpreteerbaar, betrouwbaar en bestand tegen veranderingen. Opdrachtgever verwacht van de leverancier dat hij de zorgdraagt voor een adequate opslag en beheer van de digitale stukken van de vergaderingen.
55.	Het digitaal verslag wordt opgeslagen in een open format dat recht doet aan het gebruiksdoel en duurzame opslag mogelijk maakt, zo nodig zonder conversies. Voorkeur gaat uit naar MXF, MPEG-4 of MKV.
56.	Het RIS biedt de mogelijkheid vernietigingstermijnen bij archiefbestanden in te stellen op basis van de op dat moment geldende Gemeentelijke Selectielijst.
57.	Het moet mogelijk zijn om een Vernietigingslijst samen te stellen in het RIS. Daarop staan de archiefbestanden die in aanmerking komen voor vernietiging. De vernietigingstermijn op archiefbestanden moet gewijzigd kunnen worden op verzoek van de Opdrachtgever.

58.	In het RIS moet het mogelijk zijn om na goedkeuring van de Vernietigingslijst door de Opdrachtgever, de archiefbestanden die op de Vernietigingslijst staan te kunnen vernietigen. Vernietiging van archiefbestanden moet op zodanige wijze gebeuren dat deze niet meer kunnen worden gereproduceerd. Na vernietiging moet er een Verklaring vanVernietiging opgesteld kunnen worden. In deze Verklaring staat welke informatie is vernietigd, wie de vernietiging heeft uitgevoerd, de wijze van vernietiging en de vernietigingsdatum. Er dient conform de archiefwetgeving met de opgeslagen stukken omgegaan worden. Indien iets volgens de regelgeving in aanmerking komt voor vernietiging, en dus voorkomt op de vernietigingslijst, dient het vernietigd te worden. Terughalen is dan niet meer mogelijk.
59.	De archiefbestanden die voor blijvende bewaring in aanmerking komen moeten duurzaam toegankelijk zijn: vindbaar, beschikbaar, leesbaar, interpreteerbaar, betrouwbaar en bestand tegen veranderingen.
60.	Het metadatamodel van het RIS voldoet aan het metadatamodel MDTO. Daarnaast is het mogelijk om extra metadatavelden toe te voegen die van toepassing zijn.
61.	Oprachtnemer dient te beschikken over een aantoonbare ISO 16175:2020 certificering om te voldoen aan de gestelde archiveringseisen.
	Digitale toegankelijkheid
62.	Van de opdrachtnemer wordt verwacht dat alle digitaal opgeleverde en gepubliceerde uitingen voldoen aan de wensen die gesteld worden in het Besluit digitale toegankelijkheid.
	Eisen aan oplossing
63.	RIS is compatibel met aanwezige voorzieningen in Raadzaal Halderberge en zal na oplevering en in gebruik name naadloos daarmee samenwerken. Dit betreft: • **Discussie systeem televic:** Draadloos discussiesysteem (op basis van o.a. centrale unit en acces point), 30 x draadloze discussieposten incl. NFC/RFID kaartlezer, stemfunctionaliteit, 33 accu's, 30 microfoons (circa 50 cm), 30 licenties voor ID identificatie, 24 licenties voor digitaal stemmen; • **Vergadermanagement systeem:** MVI EasyConf inclusief connect • **Camera's:** 5 Avonic HD IP PTZ camera's met 30 x zoom, inclusief overzichtscamera; • **Overig:** Audio DSP met 12 analoge in en 24 uitgangen en of Dante kanalen. Nieuwe digitale infrastructuur op basis van virtuele AV matrix t.b.v. AV over IP systeem met uitbreiding encoders en decoders bij apparatuur kast. Totaal 8 x decoder/encoder t.b.v. Aansluitingen in 19 inch apparatuur kast.
64.	Gebruikers hebben met 1 inlogcode toegang tot alle onderdelen, waarop bij dit Programma van Eisen wordt ingegaan.
65.	Opdrachtnemer beschikt over de benodigde bandbreedte om uitzendingen Full HD uit te kunnen zenden.
66.	Het RIS dient zowel binnen de huidige als de toekomstige ICT-architectuur van de gemeente Halderberge probleemloos te kunnen functioneren.
67.	Het RIS wordt als een (Cloud native) SaaS-Oplossing aangeboden.
68.	Het benaderen van de frontend van de SaaS oplossing dient op basis van HTTPS te verlopen.

69.	De securitylagen van de verbindingen mogen maximaal 6 maanden één (1) versie achterlopen (N-1) van wat als de security standaard wordt beschouwd.
70.	De oplossing dient geschikt te zijn voor het gebruik in de volgende webbrowsers: 1. Microsoft Edge Chromium; 2. Mozilla Firefox; 3. Apple Safari; 4. Google Chrome (desktop). 5. In onderhavige gevallen: ook browsers van mobiele devices. De oplossing moet werken onder actief door Microsoft, Apple, Google en Mozilla ondersteunde versies van deze browsers.
71.	De oplossing dient benaderbaar te zijn via een 'fully qualified domain name'.
72.	De oplossing ondersteunt authenticatie op basis van Azure Active Directory en SAML 2.0.
73.	Het gebruik van plug-ins is toegestaan indien het een generieke plug-in betreft die in alle bij eis 23 genoemde webbrowsersen versies functioneert en waarbij de installatie- en configuratieprocedure voor alle webbrowsers gelijk is. Specifieke instellingen en/of installaties per browser of browserversie zijn niet toegestaan. Opdrachtnemer stelt een beschrijving van de doelstelling en werkwijze van de plug-ins beschikbaar aan de gemeente Halderberge
74.	Buiten eventueel benodigde plug-ins zijn er voor het functioneren van de oplossing op het cliënt device geen verdere instellingen/installaties benodigd.
75.	Het RIS heeft een app beschikbaar voor de raadsleden en andere gebruikers.
76.	Opdrachtnemer biedt de gemeente Halderberge de mogelijkheid om gegevens opgeslagen in de SaaS-database en het datamodel te exporteren. Hierbij is het noodzakelijk dat de gemeente Halderberge de hiervoor benodigde documentatie ontvangt, zodat zij in staat is om op basis van deze documentatie te allen tijde de gegevens te exporteren.
77.	Opdrachtnemer stemt er mee in dat End-user performance monitoring (EUP) de basis vormt om beschikbaarheid en performance afspraken te verifiëren.
	Overige eisen en voorwaarden
78.	Alle opnames, metadata en informatie zijn en blijven eigendom van de gemeente Halderberge.
79.	Alle beschikbare opnames en documenten kunnen aan het einde van het contract worden overgezet naar een andere Opdrachtnemer dan wel digitaal worden gearchiveerd.
80.	De opdrachtnemer stelt de informatie beschikbaar volgens het principe van Open (Overheids) Data.
81.	Opdrachtnemer dient aan te geven hoe (structureel) met zijn oplossing wordt voldaan aan de wettelijke vereisten en de gestelde (juridische) kaders.
82.	Opdrachtnemer verstrekt per kwartaal informatie over de performance van het RIS. Hierbij wordt ingegaan op storingen, gevoeligheid en verbindingsproblemen met andere systemen, zowel kwantitatief als voorzorgsmaatregelen en maatregelen om de kans op herhalingen te verkleinen. Periodiciteit is minimaal eens per half jaar.
83.	Het RIS is adaptive voor laptop, IPad, telefoons en tablets. De hoge mate van gebruikersvriendelijkheid is voor alle genoemde devices gelijk.

84.	Om de gebruikersvriendelijkheid te verhogen is de lay-out alsmede het gebruik gelijk voor alle onderdelen van het systeem. Bijvoorbeeld manieren van openen, opslaan, zoeken etc. is zoveel mogelijk gelijk.
85.	Privacy by design / Privacy by default: De software/het systeem moet zodanig voldoen aan de eisen van Privacy by Design en Privacy by default dat de gemeente Halderberge invulling kan geven aan de eisen die de AVG aan de verwerking van persoonsgegevens stelt.
~~86.~~	~~Indien van toepassing voor de ICT-prestatie zijn de volgende open standaarden van het Forum Standaardisatie onder meer en expliciet verplicht:~~ ~~• DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv6, SAML, SPF, STARTTLS, DANE, STIX en TAXII, TLS en WPA2.~~ ~~• NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002 (Informatiebeveiliging).~~
87.	De ICT-Prestatie stelt de opdrachtgever in staat te voldoen aan: • De (U)AVG; • De Baseline Informatiebeveiliging Overheid; • ISO 27001:2017; • ~~ISO 27002:2017;~~ • De beveiligingsrichtlijnen voor webapplicaties van het NCSC; • Archiefwet 1995, Archiefbesluit 1995; • Het Algemeen en Technisch Informatiebeveiligingsbeleid van Opdrachtgever • ~~Opdrachtnemer licht toe hoe de ICT-Prestatie de Opdrachtgever ondersteund om hieraan te voldoen.~~
88.	Opdrachtnemer (in haar rol als verwerker) zal aan de Opdrachtgever (in haar rol als verwerkingsverantwoordelijke) zo snel mogelijk, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) inbreuk in verband met persoonsgegevens (datalek). Opdrachtnemer vermeldt hierbij voor zover bekend de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie persoonsgegevens, de categorie betrokkenen en het aantal betrokkenen. Daarbij wordt ook vermeld welke verbetermaatregel zijn/worden getroffen door de opdrachtnemer. Met de opdrachtnemer zal een verwerkersovereenkomst afgesloten worden die gekoppeld is aan de hoofdovereenkomst.
89.	Indien de opdrachtnemer gebruik maakt van een onderaannemer gelden alle eisen onverminderd voor de onderaannemer. De opdrachtnemer is verantwoordelijk voor een juiste invulling en werking van de eisen bij de onderaannemer.
90.	De opdrachtnemer zal voor de prestaties voldoende personen inzetten met voldoende opleiding, vaardigheden en kennis van de bedrijfsvoering en organisatie van de Opdrachtgever, om de prestaties te verrichten. Wanneer de hierboven genoemde personen zich bij de Opdrachtgever bevinden, of in direct contact met de Opdrachtgever staan, zal het personeel van de opdrachtnemer de gedragsvoorschriften van de Opdrachtgever naleven. Hiermee zal gevolg gegeven worden aan redelijke verzoeken van de Opdrachtgever.
91.	De opdrachtnemer maakt gebruik van best practices zoals ITIL en ASL voor beheer en onderhoud van applicaties en systemen.
92.	De opdrachtnemer geeft transparant en kosteloos inzicht in certificeringsdocumenten en rapportages opgesteld door EDP-auditors.
93.	Opdrachtnemer stelt opdrachtgever in de gelegenheid om o.a. de volgende rapportages op te stellen: • Rapportages rondom het authenticatieproces: inlogtijd, uitlogtijd, mislukte inlogpogingen (gebruikersnaam en IP-adres); • Rapportages rondom het gebruikersbeheer: aangemaakte accounts, verwijderde accounts, geblokkeerde accounts, wijzigingen op accounts (door wie), groepen; • Rapportages rondom rollen, en autoRISaties; • Raadplegingen van persoonsgegevens: aantal raadplegingen per gebruiker, raadplegingen per zoeksleutel.

94.	Persoonsgegevens zijn niet binnen of buiten de applicatie zichtbaar of te benaderen, behalve als de benadering gekoppeld is aan een specifieke rol- en of functiegebaseerde authenticatie en autoRISatie.
95.	De opdrachtnemer maakt het mogelijk dat vastgelegde persoonsgegevens en de verwerking ervan centraal (alle persoonsgegevens van een individu) binnen de applicatie getoond kunnen worden in een overzicht.
96.	Opdrachtnemer treft beheersmaatregelen om onbevoegde toegang tot, schade aan en interferentie (storing/uitval) met informatie en informatieverwerkende faciliteiten van Opdrachtgever te voorkomen, zodat de bedrijfsvoering niet wordt onderbroken of aangetast.
97.	Opdrachtnemer heeft beheersmaatregelen tegen malware getroffen.
98.	De applicatie wordt periodiek en minimaal eens per jaar op kwetsbaarheden onderzocht (kwetsbaarheidsscans en penetratietesten). Kwetsbaarheden worden geclassificeerd en krijgen opvolging.
~~99.~~	~~De opdrachtnemer draagt zorg voor een Escrow. Zo heeft de Opdrachtgever in voorkomend geval de mogelijkheid om bij het in vervulling gaan van één of meer in de Escrow genoemde voorwaarden, software die onderdeel is van het contract, eigenmachtig te (laten) gebruiken voor het herstellen van fouten en anderszins het onderhouden en beheren van de standaardprogrammatuur.~~
100.	In het geval van af te nemen diensten of ondersteuning op applicaties wordt tussen de opdrachtnemer en de Opdrachtgever een Service Level Agreement (SLA) afgesloten.
101.	Er vindt minimaal eens per jaar rapportage plaats op de SLA.
102.	Voor de software is sprake van een gescheiden test en productie omgeving (OTAP). Opdrachtgever wil een nieuwe versie kunnen testen en beoordelen alvorens akkoord te geven voor uitrol aan de gebruikers. Zodat deze goed begeleid kunnen worden bij de nieuwe versie.
103.	De opdrachtnemer heeft een wijzigings- en acceptatieproces. De acceptatie wordt hierbij uitgevoerd door de opdrachtgever.
104.	Er is een exitplan en -strategie (en export van data) • De Opdrachtnemer maakt een Exitplan en strategie en stemt deze af met de Opdrachtgever. • Gegevens worden op basis van standaarden opgeslagen met als doel portering naar andere dienstverleners mogelijk te maken in geval van een exit. • ~~Alle gegevens (grafische bronbestanden, grafische producten en bijbehorende metadata) worden door de Opdrachtnemer bij exit kosteloos geëxporteerd.~~ Opdrachtnemer en opdrachtgever maken in de hoofdovereenkomst afspraken over de teruggave of vernietiging van persoonsgegevens na beëindiging van de opdracht.
105.	• Beschikbaarheid tijdens werktijd 99% (min.) (7-21) • Beschikbaarheid buiten werktijd 96,1% (min.) • MTBF: 100 dagen (min.) • MTTR: Voor storingen langer dan 3 minuten: 4 uur (max.) • Maximaal dataverlies 24 uur • Maximale hersteltijd in geval van incidenten is binnen 16 werkuren (2 dagen van 8 uur).
106.	Onderliggende software componenten, zoals operating systemen, database software, browser versie, programmeer framework enz., waarop de software is gebouwd en draait dienen altijd een door de oorspronkelijke opdrachtnemer van de betreffende software of framework ondersteund te zijn. Bijvoorbeeld: als Microsoft Windows gebruikt wordt, is dit op basis van een nog door Microsoft ondersteunde versie. Windows10 zou acceptabel zijn, maar Windows7 niet meer omdat het end-of-life is.
107.	Onderliggende software (inclusief frameworks en libraries) wordt structureel voorzien van beveiligingspatches. In het contract of SLA worden hiervoor reguliere afspraken gemaakt aangaande frequentie en betaling.

108.	De opdrachtnemer heeft maatregelen genomen om de toegang tot de broncode van informatiesystemen te beperken tot de medewerkers, die deze code onderhouden of installeren.
109.	De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door checksums).
110.	Versies van de software worden voor de in productiename door de opdrachtnemer onder meer getest op invoer van gegevens (grenswaarden, format, inconsistentie, SQL injectie, cross site scripting, etc.).
111.	Applicaties worden ontwikkeld en getest op basis van landelijke normen en richtlijnen voor beveiliging, zoals de richtlijnen voor beveiliging van webapplicaties. Er wordt tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de Open Web Application Security Project (OWASP) top 10
112.	De opdrachtgever heeft het recht om in overleg met de opdrachtnemer webapplicaties of servicekoppelingen te onderwerpen aan penetratietesten op kosten van de opdrachtgever. De opdrachtnemer heeft hierbij de verplichting om geconstateerde kwetsbaarheden in de applicatie op te lossen zonder meerkosten. Termijnen van de oplossing worden in overleg met een gebruikersvereniging of bij gebrek hieraan in overleg met de opdrachtgever bepaald.
113.	De applicatie voorziet in validatiecontroles op ten minste de volgende aspecten: • Gegevens en verwerkingen kunnen worden gecorrigeerd vanuit de applicatie na invoer • Consistentiecontroles zijn in de applicatie voorzien om de correcte verwerking van gegevens te waarborgen
114.	Een logregel bevat minimaal: • De gebeurtenis; • De benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleden tot een natuurlijk persoon; • Het gebruikte apparaat; • Het resultaat van de handeling; • De datum en het tijdstip van de gebeurtenis.
115.	Er is sprake van logging in de applicatie. Relevante zaken om te loggen zijn: • Type gebeurtenis (zoals back-up/restore, reset wachtwoord, betreden ruimte); • (poging tot) Ongeautoriseerde toegang; • Handelingen met speciale bevoegdheden, waarbij alle handelingen van "superusers" worden gelogd; • Systeemwaarschuwingen; • (poging tot) Wijziging van de beveiligingsinstellingen.
116.	Bij de verwerking van persoonsgegevens worden in de log aanvullend de volgende zaken opgenomen: • Ontvangen gegevens; • Gestelde vraag; • Datum/tijdstip van aanroep; • Naam van leverende of afnemende bron of systeem; • Een gebruikersnaam of ID; • Eventuele transformaties of verrijkingen; • Eventueel opgetreden fouten.
117.	De logging is alleen beschikbaar voor daartoe geautoriseerde medewerkers.
118.	Een logregel bevat in ieder geval geen gegevens die tot het het doorbreken van de beveiliging kunnen leiden
119.	De logging is read-only. Het muteren en verwijderen van log-records is niet toegestaan.
120.	Gelogde informatie wordt minimaal 6 maanden bewaard, zodat onderzoek kan plaatsvinden in geval van een opgetreden informatiebeveiligingsincident.

121.	Logging kan naar een extern logging systeem (SIEM) gestuurd worden. De uitwisseling van deze informatie is mogelijk op basis van STIX en TAXII.
122.	Bij interne of externe applicatiekoppelingen biedt de applicatie voldoende waarborgen tussen componenten zodat er geen verlies van berichten optreedt (bijvoorbeeld buffering van berichten) en dat de validiteit van berichten beschermd is (uitsluiting van oa spoofing, MITM).
123.	Bij webservice koppelingen wordt uitgegaan van "dubbel SSL," dat wil zeggen een PKI-certificaat voor TLS en een PKI-certificaat om de serveridentiteit vast te stellen.
124.	De Opdrachtgever blijft eigenaar van de gegevens binnen applicatie en deze gegevens mogen niet voor andere doeleinden gebruikt worden door de Opdrachtnemer van de applicatie. Dit geldt zowel voor gegevens in de Test-, Acceptatie- als Productieomgevingen.
125.	Het is de opdrachtnemer verboden, zonder voorafgaande uitdrukkelijke schriftelijke toestemming van de opdrachtgever, de uitvoering van een overeenkomst geheel of gedeeltelijk aan derden over te dragen of uit te besteden.
126.	De opdrachtnemer heeft een geheimhoudingsplicht aangaande alle vertrouwelijke gegevens dan wel anderszins gevoelige informatie van de opdrachtgever die de opdrachtnemer in het kader van de opdracht ter kennis is gekomen.
127.	De opdrachtnemer heeft een geheimhoudingsplicht aangaande de informatie opgenomen in de systemen.
128.	De opdrachtnemer is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. Opdrachtnemer waarborgt hierbij tevens ook met scheiding van taken onbedoelde of ongeautoriseerde toegang. De opdrachtgever heeft het recht hierop te controleren.
129.	De opdrachtnemer is verantwoordelijk voor de kwalificaties en screening van het eigen personeel. Op verzoek van opdrachtgever dient een VOG te worden overlegd, van personen die worden ingezet op de opdracht.
130.	Alle voorwaarden en eisen die gelden voor personeel van de opdrachtnemer zijn ook van toepassing op derden, die in opdracht van de opdrachtnemer diensten verrichten voor de Opdrachtgever
131.	Autorisaties kunnen worden ingericht op basis van functies (rol-gebaseerd) waarbij functie-scheiding is toegepast.
132.	Er zijn geen "algemene" accounts / gebruikers binnen de software. Als deze noodzakelijk zijn, betreft het een beperkt aantal en met specifieke doelen. De opdrachtnemer dient hierin inzicht te geven.
133.	Wachtwoord eisen en geldigheidsduur kunnen gesteld worden vanuit de software. Het kan daarmee voldoen aan het wachtwoordbeleid van de Opdrachtgever.
134.	Wachtwoorden zijn beschermd tegen inzage en wijziging door onbevoegden tijdens transport en opslag door middel van hashing en encryptie.
135.	Er is sprake van toepassing van een vorm van multi-factor authenticatie.
136.	Beleid inzake het gebruik van cryptografische beheersmaatregelen zoals vastgelegd door het Forum van Standaardisatie. Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
137.	De opdrachtnemer stelt de opdrachtgever in staat om zelf access management uit te voeren. De opdrachtgever dient direct invloed uit te kunnen oefenen over de accounts (en bijbehorende autorisaties) van de eigen medewerkers.
138.	De opdrachtnemer houdt een actuele registratie bij van geautoriseerde accounts/gebruikers.

139.	De opdrachtnemer verschaft relevante informatie over de wijze waarop – en onder welke voorwaarden – cryptografie wordt gebruikt om persoonsgegevens van betrokkenen te beschermen.
140.	Indien het gebruik van persoonsgegevens voor test doeleinden noodzakelijk blijkt, bijvoorbeeld omdat er geen testomgeving voorhanden is, voert de provider een risico analyse uit en neemt zij de vereiste maatregelen om het risico tot een minimum te beperken.
141.	De opdrachtnemer maakt gebruik van een proces waarbij logbestanden periodiek gecontroleerd worden teneinde onrechtmatig gebruik of andere onregelmatigheden vast te stellen. De logbestanden dienen informatie te verschaffen over de vertrouwelijkheid, beschikbaarheid en integriteit van persoonsgegevens, en of daarop een inbreuk is geweest.
142.	De opdrachtnemer bepaalt onder welke voorwaarden dergelijke logbestanden aan de opdrachtgever worden verstrekt. Deze voorwaarden worden aan de opdrachtgever medegedeeld.
143.	De opdrachtnemer zorgt dat er passende maatregelen worden getroffen waarmee persoonsgegevens die in dergelijke logbestanden verschijnen, voldoende worden beschermd en niet voor andere doeleinden worden gebruikt.
144.	Bij informatiebeveiligingsincidenten aan de kant van de opdrachtnemer wordt door de opdrachtnemer expliciet onderzocht of bij dat incident persoonsgegevens zijn gemoeid, tenzij dat redelijkerwijs niet aannemelijk is.
145.	Indien het uitvoeren van audits door de opdrachtgever onwenselijk of redelijkerwijs niet mogelijk is, overlegt de opdrachtnemer – voorafgaand aan het afsluiten van het servicecontract – onafhankelijk bewijs waaruit blijkt dat de getroffen beveiligingsmaatregelen conformeren aan de door de opdrachtgever gestelde eisen en beleid.
146.	De opdrachtnemer zorgt dat tijdelijke bestanden (cache) die persoonsgegevens bevatten periodiek worden verwijderd.
147.	De opdrachtnemer legt alle verstrekkingen van persoonsgegevens (waar de opdrachtgever verwerkingsverantwoordelijke voor is) aan andere partijen schriftelijk vast.
148.	De opdrachtnemer en de opdrachtgever maken schriftelijke afspraken over de manier waarop persoonsgegevens worden verwijderd of geanonimiseerd. De opdrachtnemer heeft over dit onderwerp beleid opgesteld. In dat beleid wordt ook ingegaan op de bewaartermijn van persoonsgegevens na eindigen van het contract.
149.	De opdrachtnemer dient (doorlopend) inzichtelijk te maken in welke landen persoonsgegevens (kunnen) worden opgeslagen. Eventuele contractuele waarborgen in het kader van hoofdstuk V van de AVG dient de opdrachtnemer eveneens inzichtelijk te maken.Opdrachtgever wil opslag van persoonsgegevens binnen landen van de Europese Unie houden.
150.	De opdrachtnemer is NEN/ISO 27001 gecertificeerd. De opdrachtnemer overlegt het certificaat.

Overige eisen

	Overige eisen
151.	Het RIS dient een geïntegreerd systeem te zijn, waarbij de diverse functies in samenhang werken. De aanbieding dient dan ook het gehele RIS te betreffen, zodat we later niet verrast worden met extra kosten voor aan te schaffen modules voor de geboden en gewenste functionaliteiten.
152.	Een geïntegreerd systeem wil ook zeggen dat autorisaties, rollen, rechten eenmalig en centraal worden toegekend en in het hele RIS worden gehanteerd. Dit alles uiteraard middels role based acces en bij voorkeur met Single Sign on via ons Azure AD. Ook two factor authentication (microsoft authenticator) dient beschikbaar te zijn.
153.	Wij hebben een koppeling met openraadsinformatie en deze verwachten wij uiteraard ook in de nieuwe oplossing als standaardonderdeel.
154.	Indien er gedurende de contractperiode wijzigingen plaatsvinden in wettelijke wensen ten aanzien van digitale toegankelijkheid, zal opdrachtnemer, in samenspraak met opdrachtgever, de nodige acties ondernemen om ervoor te zorgen dat de digitale toegankelijkheid voldoet aan de wettelijke wensen, zonder dat daar extra kosten voor de opdrachtgever aan verbonden zijn.