



Hoogheemraadschap van

**Rijnland**



Hoogheemraadschap  
van Schieland en de  
Krimpenerwaard

# **Technisch beheer en hosting websites HHR en HHSK**

## **Programma van eisen**

Archimedesweg 1  
postadres:  
postbus 156  
2300 AD Leiden  
telefoon (071) 3 063 063  
telefax (071) 5 123 916

CORSA nummer: 20.  
versie:  
auteur: Saskia van der Grijp  
datum:  
dossier: DIG-17638

---

## Inhoudsopgave

Inleiding .....	3
1 Implementatie .....	4
1.1 Algemeen .....	4
2 Technisch beheer, hosting & maatwerk .....	5
2.1 Algemeen .....	5
2.2 Beveiligingseisen & AVG .....	6
2.3 Contentbeheer .....	8
2.4 Hosting .....	8
2.5 Technisch beheer en onderhoud .....	8
2.6 Dienstverlening en maatwerk .....	10
2.7 Contract .....	11

---

## **Inleiding**

De contracten voor het hosten en beheren van de websites van de hoogheemraadschappen van Rijnland en Schieland & de Krimpenerwaard (resp. HHR en HHSK) lopen tot medio 2026.

Dit betekent dat er een nieuwe leverancier gevonden moet worden die voor de komende jaren het technisch beheer en hosting op het CMS Wagtail uitvoert. Voor het selecteren van zo'n leverancier is een programma van eisen nodig.

## 1 Implementatie

### 1.1 Algemeen

Nr	Omschrijving
1.	De Opdrachtnemer heeft aantoonbare ervaring met Wagtail, Django en Python. Opdrachtnemer dient een referentie in bij de inschrijving om dit aan te tonen.
2.	De Opdrachtnemer neemt het bestaande Wagtail-CMS-platform over (op het moment van schrijven versie 7.1.1 voor HHR en 7.0.3 voor HHSK) as-is, inclusief al het gemaakte maatwerk, hostingconfiguratie, codebasis, koppelingen, OTAP-omgevingen en documentatie. De Opdrachtnemer verifieert binnen vier weken na start van de opdracht de technische staat van het overgenomen platform en rapporteert eventuele bevindingen aan de Opdrachtgever.
3.	De websites, beheeromgevingen en content van de waterschappen zijn (logisch) van elkaar gescheiden: <ul style="list-style-type: none"><li>a. Webmasters en contentbeheerders van het ene waterschap hebben geen toegang tot die van de ander en vice versa;</li><li>b. Elk waterschap kan de lay-out/structuur, grafische vormgeving en content van zijn websites autonoom bepalen, zonder afhankelijkheden van de andere waterschappen</li></ul>
4.	De opdrachtgever levert, naast de productievoorzieningen, tevens per waterschap minimaal één acceptatieomgeving.  De acceptatieomgevingen zijn: <ul style="list-style-type: none"><li>a. representatief ingericht ten opzichte van de bijbehorende productie-omgeving, maar mogen in overleg tijdelijk één versie (n+1) vooruitlopen ten behoeve van het testen van nieuwe releases;</li><li>b. technisch en functioneel gelijkwaardig aan de productieomgeving</li><li>c. voorzien van test-accounts (bijvoorbeeld DigiD accounts) waarmee alle functionaliteit kan worden getest;</li><li>d. logisch volledig gescheiden van de bijbehorende productieomgevingen;</li><li>e. technisch beheerd en onderhouden door de opdrachtgever, inclusief het garanderen van de representativiteit van de CMS-voorzieningen en functies;</li></ul>
5.	De maximale downtime gedurende de implementatiefase van de websites is maximaal 2 uur per website.
6.	De Opdrachtnemer zorgt voor Single-Sign-On voor de applicatie, zowel productie als acceptatieomgeving.
7.	Bij toegang tot de beheeromgeving vanaf externe devices (devices die geen deel uitmaken van de interne netwerken van de waterschappen) is twee-factor-authenticatie via Azure AD vereist.
8.	Bij toegang tot de beheeromgeving vanaf interne devices wordt geen two-factor authenticatie toegepast.
9.	Tijdens de implementatiefase wordt de exacte set van beheerrechten in overleg met de Opdrachtnemer bepaald. Over toegang tot beheerfuncties die impact kunnen hebben op de verplichtingen en verantwoordelijkheden van de Opdrachtnemer moeten strikte afspraken worden gemaakt. Een voorbeeld hiervan is het installeren van plug-ins die de beschikbaarheid, prestaties en beveiliging van de websites kunnen ondermijnen.
10	De implementatiefase eindigt zodra de productie- en acceptatieomgevingen van beide waterschappen stabiel draaien onder verantwoordelijkheid van de Opdrachtnemer, hetgeen schriftelijk wordt bevestigd door de Opdrachtgever. Uiterlijke opleverdatum is 30 mei 2026.

## 2 Technisch beheer, hosting & maatwerk

### 2.1 Algemeen

Nr	Omschrijving
11.	Opdrachtnemer houdt kennis bij omtrent wijzigende NL wetgeving en EU-richtlijnen en is op de hoogte van ontwikkelingen in bijv. WOO, NIS2, AVG, AI act, SDG (Single Digital Gateway) en samenwerkende catalogi en borgt deze in nieuwe software releases.
12.	Alles dat nu en in de toekomst ontwikkeld wordt, zoals al het maatwerk, moet voldoen aan de wet digitale toegankelijkheid (op moment van schrijven WCAG 2.2 niveau AA). Opdrachtnemer dient de juiste kennis te hebben over deze wet.
13.	De Opdrachtnemer heeft in een continuïteitsplan aangegeven dat de continuïteit van de dienstverlening in het geval van beëindiging van de organisatie (op grond van faillissement of andere oorzaken) op expliciete en duidelijke wijze gegarandeerd is voor minimaal 6 maanden en die Opdrachtgever voor nog eens 6 maanden kan verlengen indien dat noodzakelijk is.
14.	Er is een vast Nederlands sprekend aanspreekpunt en supportteam beschikbaar bij de Opdrachtnemer.
15.	De Opdrachtnemer werkt volgens een SLA (Service Level Agreement) die na gunning wordt opgesteld door Opdrachtnemer en Opdrachtgever. Het format wordt geleverd door Opdrachtgever.
16.	<p>De vereiste beschikbaarheid van de websites is 99,9% op jaarbasis, uitgaande van een continue openstelling (bedrijfstijd) van 24/7. Onbeschikbaarheid als gevolg van vooraf overeengekomen gepland onderhoud valt hierbuiten.</p> <p>De berekening van de beschikbaarheid is beperkt tot de services en diensten waarvoor de Opdrachtnemer contractueel verantwoordelijk is. Hieronder vallen het CMS-systeem, de websites en alle onderliggende en bijbehorende services zoals webserver, toegangsvoorzieningen en rekencentrumfaciliteiten.</p> <p>Onbeschikbaarheid veroorzaakt in systemen die niet onder de verantwoordelijkheid van de opdrachtnemer vallen, tellen niet mee in de berekening van onbeschikbaarheid. Voorbeelden hiervan zijn onbeschikbaarheid van de CMS-beheerconsole als gevolg van technische problemen op de infrastructuur van de waterschappen zelf of onbeschikbaarheid van DigiD-authenticatie als gevolg van een storing bij Logius.</p>
17.	De vereiste beschikbaarheid van de beheertools van de productieomgeving is 99% tussen 7:00-19:00 uur op werkdagen en 97% buiten deze tijden/werkdagen.
18.	De vereiste beschikbaarheid van de acceptatieomgeving is 99% tussen 7:00-19:00 uur op werkdagen en 97% buiten deze tijden/werkdagen.
19.	De beschikbaarheid van de websites tijdens calamiteiten is essentieel. Van de Opdrachtnemer wordt intensieve(re) monitoring en ondersteuning verwacht om eventuele problemen zo snel mogelijk te verhelpen.
20.	De minimale servicewindow voor support en ondersteuning is van maandag tot en met vrijdag van 09.00 tot 17.00 uur.

## 2.2 Beveiligingseisen & AVG

Nr	Omschrijving
21.	De Opdrachtnemer levert een up-to-date beveiligingsplan met beschrijving van beheer, hosting, maatwerk en datastromen. Het plan is actueel en geeft een overzicht van maatregelen en verantwoordelijkheden. (zie BIO 5.1; ICO App Dev)
22.	De opdrachtnemer meldt datalekken en beveiligingsincidenten onverwijld en uiterlijk binnen 24 uur. De melding wordt opgevolgd met een rapportage bestaande uit een analyse van de aard en omvang van het beveiligingsincident en/of datalek, aangevuld met de te nemen of genomen maatregelen.
23.	De Opdrachtnemer meldt datalekken met betrekking tot AVG binnen 24 uur aan de verwerkingsverantwoordelijke. (AVG art. 33)
24.	Er wordt een duidelijke verdeling van rollen en verantwoordelijkheden opgesteld tussen I&D, hostingpartij, ontwikkelaar en websitebeheerder (RACI) opgesteld. (zie BIO 6.1)
25.	De Opdrachtnemer past secure development lifecycle toe (SDLC). Ontwikkeling volgens OWASP en secure coding practices; code review en test. (zie BIO12.6; OWASP ASVS)
26.	De Opdrachtnemer gebruikt gescheiden OTAP-omgevingen. Ontwikkeling, test, acceptatie en productie strikt gescheiden. Dit wordt aangetoond door een OTAP-overzicht met rechtenmatrix. (zie BIO 12.6)
27.	Opdrachtnemer documenteert en beheert afhankelijkheden (SBOM). Zijnde een lijst met libraries, frameworks en versies beschikbaar houden en onderhouden. (zie ICO; NCSC Secure SDLC)
28.	De opdrachtnemer dient te beschikken over een geldig NEN-EN-ISO/IEC 27001 certificaat (of aantoonbaar gelijkwaardig bewijs). De scope van de certificering past bij de in te kopen ICT Prestatie. Gedurende de hele looptijd van de overeenkomst moet de opdrachtnemer deze certificering behouden. Op verzoek van de opdrachtgever dient de opdrachtnemer binnen drie werkdagen een kopie van het certificaat aan de opdrachtgever te verstrekken.
29.	Opdrachtnemer zorgt voor versleuteling van data at rest en in transit. Data in CMS is versleuteld opgeslagen en beveiligde verbindingen (HTTPS/TLS). (zie BIO 10.1)
30.	Opdrachtnemer zorgt dat back-ups zijn versleuteld en getest. Er zijn periodieke back-ups van CMS en database en er worden herstelproeven uitgevoerd. (zie BIO 12.3)
31.	Opdrachtnemer implementeert een authenticatie en wachtwoord beleid dat zorgt voor sterke wachtwoorden en MFA voor beheerders; rollen en rechten zijn vastgelegd. (zie BIO 9.2)
32.	Opdrachtnemer zorgt voor dataminimalisatie bij formulierverwerking. Formulierdata wordt alleen opgeslagen indien noodzakelijk en geconfigureerd door functioneel beheerders.(Zie AVG en BIO 10.2)
33.	Opdrachtnemer zorgt voor TLS 1.2+ voor alle communicatie. Alle verbindingen tussen client, beheer en API's zijn beveiligd. (zie BIO 10.1)
34.	Opdrachtnemer zorgt voor beveiligde API's met authenticatie en autorisatie. Alle API's zijn voorzien van toegangscontrole en logging.(Zie OWASP API Security; ICO App Dev)
35.	Beveiligingsupdates worden door Opdrachtnemer tijdig uitgevoerd. Dit betekent voor CMS, plug-ins en frameworks binnen 7 dagen patchen bij kritieke kwetsbaarheden. (zie BIO 12.6)
36.	Kwetsbaarheidsscans worden periodiek uitgevoerd door Opdrachtnemer. Er wordt minimaal kwartaalgewijs gescand op bekende kwetsbaarheden. (zie BIO 12.6)

37.	Opdrachtnemer meldt beveiligingsincidenten direct aan de systeembeheerder van de Opdrachtgever met analyse. Melding gebeurt binnen 24 uur middels een incidentenrapport. (zie BIO 16.1)
38.	Opdrachtnemer zorgt voor logging en monitoring van beheeracties. Inlogpogingen, formulierverwerking en beheeracties worden gelogd. (Zie BIO 12.4)
39.	Opdrachtnemer werkt actief mee aan pentesten en security-audits van Opdrachtgever. Indien hier verbeterpunten uitkomen werkt Opdrachtnemer actief mee aan verbetering en dient een verbeterplan in. (zie BIO 18; ICO App Dev)
40.	De Opdrachtnemer heeft het geheel van het CMS inclusief hosting en beheeromgeving privacy by design en privacy by default ingericht. De applicatie vraagt bij elke verzameling van persoonsgegevens vrijelijk en ondubbelzinnig toestemming aan betrokkene, waarvan de persoonsgegevens worden verwerkt, om de gegevens te mogen verwerken. Daarbij worden standaard zo min mogelijk persoonsgegevens verwerkt. (zie CIP De Privacy Baseline 2020: U.05, AVG art. 25)
41.	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. Het geheel van het CMS inclusief hosting en beheeromgeving behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast. (zie AVG art. 5 lid 2 en art. 33 lid 5)
42.	De Opdrachtgever dient te zorgen voor een toegangsstructuur waarbij gebruikers uitsluitend toegang hebben tot functionaliteiten en gegevens binnen het CMS die noodzakelijk zijn voor het uitvoeren van hun specifieke taken en verantwoordelijkheden.
43.	Het geheel van het CMS inclusief hosting en beheeromgeving voldoet aan dataminimalisatie. De Opdrachtnemer behoort een proces te hebben ingericht, waarbinnen een analyse wordt gemaakt en aantoonbaar is dat het verzamelen van de persoonsgegevens rechtmatig en noodzakelijk is en het ontwerp getoetst wordt aan het uitgangspunt dataminimalisatie, de juiste wijze van opslag en het hanteren van de bewaartermijn. (zie AVG art. 6 lid 1) De loginformatie wordt niet langer dan 6 maanden bewaard, tenzij het logbestand als bewijsmiddel in een analyse wordt gebruikt. Als uit analyse blijkt dat verder onderzoek niet nodig is geldt de standaard bewaartermijn van 6 maanden en wordt het bij overschrijden van de termijn onmiddellijk verwijderd. Als uit analyse blijkt dat er sprake is van schending van de gedragsregels of een strafbaar feit worden de logfiles handmatig veiliggesteld voor forensisch onderzoek en maximaal 3 jaar bewaard.
44.	Het geheel van het CMS inclusief hosting en beheeromgeving dient zodanig ingericht te zijn dat persoonsgegevens uitsluitend worden verwerkt op een wijze die correct, rechtmatig en doelgericht is. De verwerking voldoet aan de beginselen van gegevensbescherming. ( zie AVG art. 7, 11, 12, 16, 17, 18, 19, 20, 21, 22 en 23)
45.	Om de gegevens te mogen verwerken wordt de betrokkene, waarvan de persoonsgegevens worden verwerkt, geïnformeerd betreffende welke verwerking (van de persoonsgegevens) plaatsvindt en krijgt deze betrokkene een waarschuwing bij het verkrijgen van toegang tot bijzondere persoonsgegevens. (zie CIP De Privacy Baseline 2020: U.05, AVG art. 14, AVG overweging 60)

46.	Het CMS moet zodanig zijn ingericht dat gegevens, functies en gebruikersgroepen logisch en technisch van elkaar gescheiden zijn. (zie AVG art. 6 lid 1, NISA strategie (January 12, 2015 ) 'scheiden')
47.	De Opdrachtnemer neemt technische en organisatorische maatregelen om persoonsgegevens te beveiligen. (zie AVG art. 32)
48.	De Opdrachtnemer garandeert dat de data (inclusief de backups) nu en in de toekomst binnen de Europese Economische Ruimte wordt opgeslagen. (AVG art 3)

### 2.3 Contentbeheer

Nr	Omschrijving
49.	De gegevens die in het systeem vermeld staan zijn te allen tijde eigendom van de Opdrachtgever en mogen door de Opdrachtnemer enkel gebruikt worden voor de uitvoering van de werkzaamheden, zulks ter bepaling van de Opdrachtgever.

### 2.4 Hosting

Nr	Omschrijving
50.	De hostingomgeving is geoptimaliseerd voor Django/Wagtail.
51.	Er is een minimale uptime van 99,9% per jaar.
52.	Hosting vindt, in verband met AVG, plaats binnen de EU.
53.	Back-ups van de productie- en acceptatieomgeving worden dagelijks gemaakt en minimaal 30 dagen bewaard.
54.	Er is mogelijkheid tot schaalbare hosting (bij piekbelasting).
55.	Inrichten van een sFTP server voor HHSK (met als basis de URL <a href="http://www.schielandendekrimpenewaard.nl/kaart">www.schielandendekrimpenewaard.nl/kaart</a> ), optioneel ook voor HHR.
56.	De Opdrachtnemer monitort maandelijks de status op basisbeveiliging.nl en rapporteert afwijkingen. De Opdrachtgever draagt zorg voor correct DNS-beheer (SPF, DKIM, DMARC, DNSSEC) om gezamenlijk een 'groene' score te realiseren.
57.	De Opdrachtnemer garandeert dat de website zonder dataverlies of onredelijke kosten kan verhuizen naar een andere hostingsaanbieder.

### 2.5 Technisch beheer en onderhoud

Nr	Omschrijving
58	<p>Het technisch beheer bevat minimaal voor de vaste prijs:</p> <ul style="list-style-type: none"> <li>• CMS-updates en upgrades (minor en major releases), service releases, patches en plug-ins</li> <li>• Doorvoeren van beveiligingsupdates, het proactief monitoren op beveiligingsincidenten en aanvallen binnen de door hem beheerde omgevingen.</li> <li>• Bij detectie van een incident of aanval meldt hij dit onverwijld aan de Opdrachtgever en onderneemt in overleg met de Opdrachtgever passende mitigerende acties.</li> <li>• Continu controleren van de prestaties van de website, het oplossen van technische storingen en het analyseren van logs om problemen te voorkomen</li> </ul>



	<ul style="list-style-type: none"> <li>• Beheer van integraties met andere applicaties zoals Archieven.nl, Bekendmakingen, Regelgeving, PDC (Productencatalogus).</li> <li>• Technische testen uitvoeren vóór functionele testen, bijvoorbeeld bij wijzigingen of nieuwe releases</li> <li>• Servicedesk</li> <li>• Bugs oplossen;</li> </ul> <p>De Opdrachtnemer is verantwoordelijk voor het oplossen van storingen en fouten die optreden in componenten of configuraties die onder zijn beheer vallen en die niet voortkomen uit ontwerp- of ontwikkelfouten uit eerdere fasen. Fouten in bestaande functionaliteit die terug te voeren zijn op eerdere ontwikkeling worden, na overleg met de Opdrachtgever, als wijzigingsverzoek behandeld.</p>
59	De Opdrachtnemer zorgt dat de websites snel en stabiel functioneren. Dit betekent dat pagina's vlot laden, de server adequaat reageert bij piekbelasting en dat prestatieproblemen actief worden opgespoord en opgelost. De Opdrachtnemer monitort periodiek de performance en adviseert de Opdrachtgever over mogelijke verbeteringen binnen een week na signalering.
60	De Opdrachtnemer bewaakt de levenscyclus van het CMS Wagtail en het onderliggende framework Django en adviseert de Opdrachtgever tijdig over noodzakelijke updates en de impact daarvan. Minor-updates en beveiligingspatches worden binnen het reguliere onderhoud uitgevoerd en uiterlijk binnen twee maanden na release doorgevoerd, tenzij er een aantoonbare blokkade is. Bij major-updates van Wagtail of Django treden Opdrachtgever en Opdrachtnemer tijdig met elkaar in overleg. Major-updates worden uiterlijk binnen zes maanden na release ingepland en uitgevoerd. Indien de update wezenlijke aanpassingen aan maatwerk of infrastructuur vereist, meldt de Opdrachtnemer dit uiterlijk binnen één maand na de release en doet een voorstel voor aanpak, planning en eventuele kosten buiten de SLA.
61	De Opdrachtnemer bewaakt de levenscyclus van de Python-runtime die benodigd is voor het functioneren van het CMS en adviseert de Opdrachtgever tijdig over relevante wijzigingen of het einde van ondersteuning (EoL) van de gebruikte versie. De Opdrachtnemer signaleert wanneer wijziging van de Python-versie impact heeft op het CMS, maatwerk of koppelingen. Wijzigingen die uitsluitend de runtime betreffen en binnen reguliere beheerwerkzaamheden passen worden uitgevoerd binnen het onderhoud; wijzigingen met functionele of infrastructurele impact worden uiterlijk binnen één maand na release/EoL-aankondiging gemeld met een voorstel voor aanpak, planning en eventuele kosten buiten de SLA.
62	Versiebeheer gebeurt door Opdrachtnemer via Git (bij voorkeur GitHub of GitLab)
63	Opdrachtnemer zorgt voor documentatie van technische wijzigingen en releases.
64	De Opdrachtnemer is in staat tot het technisch beheer van de bestaande koppelingen tussen het CMS en de midoffice- en backoffice-systemen van de waterschappen. De concrete in beheername van koppelingen gebeurt op basis van door de Opdrachtgever te verstrekken technische specificaties en/of documentatie. Na in beheername bewaakt de Opdrachtnemer de werking binnen het CMS-domein en meldt storingen of afwijkingen aan de Opdrachtgever. De Opdrachtnemer is niet verantwoordelijk voor de werking van de gekoppelde externe systemen zelf of voor wijzigingen in hun API's of interfaces, tenzij uitdrukkelijk anders overeengekomen.
65	Koppelingen tussen het CMS en de lokale koppelvlakken van de waterschappen zijn beveiligd op basis van https en/of VPN.
66	Verbindingen met de beheerconsoles van het CMS zijn https beveiligd.

## 2.6 Dienstverlening en maatwerk

Nr	Omschrijving
67.	Gepland onderhoud met downtime is beperkt tot maximaal 18 uur op jaarbasis met een maximale downtime van 3 uur per onderhoudswindow.
68.	Gepland onderhoud met downtime wordt alleen uitgevoerd in overleg met de waterschappen. De waterschappen hebben het recht om gepland onderhoud op specifieke momenten te weigeren als ze daar zwaarwegende redenen voor hebben, bijvoorbeeld tijdens een calamiteitsituatie.
69.	Incidenten kunnen zowel telefonisch, via e-mail en via een online ticketsysteem worden ingediend. Het online-ticketsysteem is 24/7 beschikbaar voor het aanmelden en raadplegen van de status van incidenten. Tickets met prioriteit kritiek worden binnen 4 uur opgepakt. Tickets met hoge prioriteit worden binnen 1 werkdag opgepakt. Binnen 3 werkdagen krijgen we een persoonlijke, niet geautomatiseerde reactie op de overige tickets met een planning of voortgang. Zie hiervoor ook de incidentenmatrix op pagina 7 van de SLA (bijlage 5).
70.	De helpdesk ondersteunt bij het beantwoorden van (eenvoudige) gebruikersvragen. Er zal een lijst worden samengesteld van contactpersonen die vragen kunnen/mogen indienen. Deze lijst zal worden beperkt tot enkele medewerkers per waterschap.
71.	Er is geen limiet op het aantal incidenten/vragen dat kan worden ingediend.
72.	Incidenten dienen conform het gestelde in de Service Level Agreement (SLA) te worden afgehandeld: De reactietijd is gedefinieerd als de tijd waarbinnen een ter zake deskundige medewerker van de Opdrachtnemer contact opneemt om het incident te analyseren. Bij alleen een terugmelding dat het incident in goede orde is ontvangen en zal worden opgepakt, wordt niet voldaan aan deze eis. Zie pagina 7 in de SLA (Bijlage 5) voor incidentenmatrix.
73.	Classificatie (inschatting ernst) van incidenten geschiedt door de waterschappen tijdens het indienen daarvan. Wijziging van classificatie vindt alleen plaats in onderling overleg tussen supportmedewerkers van de Opdrachtnemer (incidentcoördinator) en de waterschappen
74.	De Opdrachtnemer levert per waterschap ieder kwartaal een rapportage met aangemelde en afgehandelde incidenten, gebruikte uren per functie en beschikbaarheidspercentages. De vormgeving en verdere inhoud van de rapportages is beschreven in de SLA.
75.	Wijzigingsverzoeken (het maatwerk) worden door de Opdrachtnemer afgehandeld op basis van een changemanagementproces. De Opdrachtnemer dient aangevraagde wijzigingen te toetsen op potentiële impact op beveiliging, prestaties en beschikbaarheid en conformiteit aan de wet- en regelgeving.
76.	Per wijzigingsverzoek wordt een leverdatum overeengekomen tussen Opdrachtnemer en Opdrachtgever.
77.	Voor wijzigingen die op initiatief van de Opdrachtnemer worden uitgevoerd geldt een meldplicht richting de waterschappen, ongeacht of daarbij sprake is van downtime of functionele impact.
78.	De servicedesk is verantwoordelijk voor het registreren, melden, routeren, (laten) oplossen, bewaken, (tussentijds) informeren over en afmelden van incidenten m.b.t. het systeem volgens de procedure zoals vastgelegd in de SLA. De Opdrachtgever bepaalt de prioriteit van incidenten. De servicedesk draagt tevens zorg voor relateren van incidenten aan reeds bekende problemen.

79.	De opdrachtnemer biedt de mogelijkheid om binnen de SLA te werken met een strippenkaart waarop uren voor het realiseren van kleine werkzaamheden/maatwerk afgeboekt kunnen worden.
-----	--

## 2.7 Contract

Nr	Omschrijving
80.	De Opdrachtgever organiseert periodiek (minimaal 2 keer per jaar) een voortgangsbespreking (operational review) met een gezamenlijke vertegenwoordiging van de waterschappen om de kwaliteit van de dienstverlening te bespreken. Daarnaast wordt er minimaal eenmaal per jaar een beoordelingsgesprek gehouden.
81.	De Opdrachtnemer dient akkoord te gaan met het ondertekenen van de verwerkersovereenkomst AVG van de waterschappen.
82.	De Opdrachtnemer erkent dat het eigendom van de gegevens (content) en het gebouwde maatwerk (broncodes) die verwerkt worden in de CMS-oplossing bij de waterschappen ligt en garandeert het eigendomsbehoud en de beschikbaarheid van deze gegevens bij beëindiging van het contract, ongeacht de reden van beëindiging.
83.	De Opdrachtnemer werkt bij contractbeëindiging actief mee aan de overdracht van de dienstverlening naar een andere partij gedurende een periode van 3 maanden voorafgaand aan de datum van contractbeëindiging. Actief meewerken houdt in: <ul style="list-style-type: none"> <li>a. Het opleveren van alle content (teksten, CSS stylesheets, HTML-code, scripts, etc.) in een systeemafhankelijk digitaal formaat (XML/JSON) via een beveiligd digitaal kanaal dat voldoet aan de BIO-eisen voor vertrouwelijkheid en integriteit, binnen een versleutelde file-transferomgeving of managed cloud-opslag binnen de EU.;</li> <li>b. Het opleveren van gebruikersdata (accountnamen, overzicht rollen en autorisaties, etc.);</li> <li>c. Het realiseren van een actieve datasynchronisatie-koppeling naar de nieuwe CMS- SaaS oplossing indien dit technisch mogelijk is.</li> </ul> <p>Dit gebeurt dusdanig dat de gegevens volledig bruikbaar zijn voor toekomstige inzage en gebruik. De Opdrachtnemer werkt voorafgaand aan beëindiging voor een redelijke en vooraf overeengekomen vergoeding mee aan de overdracht.</p>
84.	Op 1 juni 2026 wordt door Opdrachtnemer een exit- en dataverwijderingsplan overlegd waarin beschreven wordt hoe zij gaan zorgen voor een soepele, veilige overgang naar een (mogelijk) nieuwe partij bij beëindiging van de overeenkomst. Dit plan is onderdeel van de overeenkomst en dient bij contract beëindiging uitgevoerd te worden. Tevens wordt beschreven hoe CMS-data verwijderd wordt. Dit in lijn met AVG en BIO 18. De kosten voor deze plannen vallen onder de implementatiefase en dienen in het totaalbedrag voor implementatie verwerkt te zijn (zie tarievenblad bijlage 3).
85.	Na de contractbeëindiging en succesvolle overdracht van de klantgegevens aan de opdrachtgever, vernietigt de opdrachtnemer in opdracht van de opdrachtgever alle gegevens (inclusief back-ups) en levert bewijs dat dit is uitgevoerd.
86.	De verwerkingsverantwoordelijke legt in de (verwerkers) overeenkomst afspraken vast, met de persoon of partij die persoonsgegevens verwerkt, over

---

	het verwijderen of overdragen van persoonsgegevens bij beëindiging van de relatie; eventuele derden worden over de beëindiging geïnformeerd.
87.	Opdrachtnemer levert een Conformiteitsverklaring BIO/AVG aan om aan te tonen dat ze voldoen aan naleving relevante normen en eisen.