Programma van Eisen

E-HRM en Salarisverwerkingsdienst

Alle wijzigingen n.a.v. de Nota van Inlichtingen d.d. 27.02.2025 zijn in het rood verwerkt

Inhoudsopgave

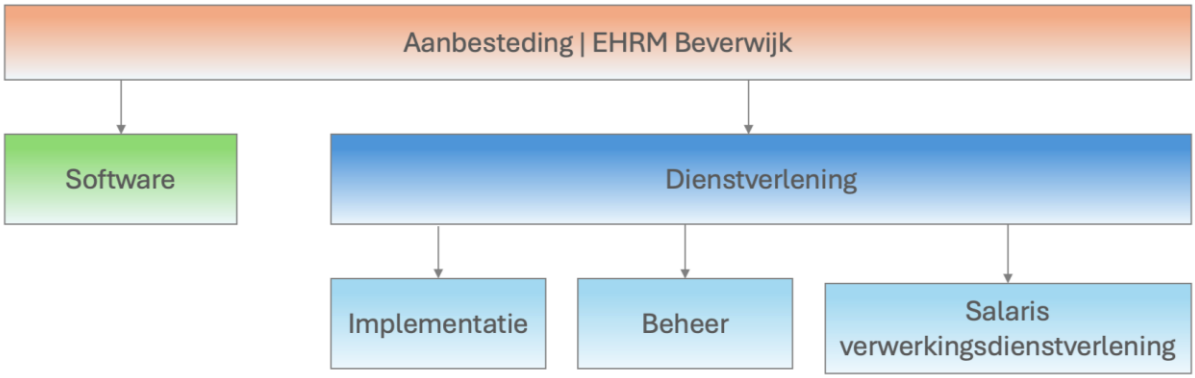
1. Inleiding

In dit document worden onder andere de functionele uitgangspunten beschreven van de technische inrichting en de dienstverlening die hierom heen valt.

Het document wordt als volgt opgedeeld:
Hoofdstuk 2 gaat in op de scope van de opdracht en vereisten
Hoofdstuk 3 gaat in op de algemene uitgangspunten
Hoofdstuk 4 gaat in op de functionele eisen van de software
Hoofdstuk 5 gaat in op de technische eisen van de software
Hoofdstuk 6 gaat in op de exit-strategie
Hoofdstuk 7 gaat in op de SLA afspraken

2. Scope van de opdracht en vereisten

De opdeling is als volgt:



2.1. Implementatie

De implementatie van het E-HRM-systeem bestaat uit een ontwikkel-, test- en acceptatiefase. De leverancier is verantwoordelijk voor de volledige inrichting en ingebruikname van het systeem, inclusief de gefaseerde implementatie van modules.

Per 1 januari 2026 dienen de kern HR-functies, salarisadministratie, en medewerker- en managerportalen operationeel te zijn. De leverancier verzorgt tevens de migratie van data en dossiers vanuit de huidige software naar het nieuwe systeem.

Vereisten voor de Implementatie

1. Migratie van data

- Goedgekeurd migratie plan incl. roll back scenario
- Overzetten van actuele data en saldi uit **Motion (Pro)** naar het nieuwe systeem.
- Archiveren of verwijderen van vervallen data
- Migratie van digitale personeelsdossiers uit **Motion** en **Join**.
- Overzetten van ziekteverzuimgegevens van de afgelopen 3 jaar naar de nieuwe applicatie.
- Opstellen van een verklaring van migratie

2. Test- en acceptatiefase

- Er moet een testomgeving beschikbaar zijn gedurende de volledige implementatie en minimaal 3 maanden na livegang.
- De leverancier faciliteert testrondes, waaronder systeemtesten, integratietesten, en acceptatietesten, waarbij resultaten worden gerapporteerd en verwerkt.

3. Gefaseerde implementatie

- Modules moeten afzonderlijk en in fasen geïmplementeerd kunnen worden om een soepele overgang te waarborgen.
- Kernmodules moeten prioriteit krijgen om live te gaan op 1 januari 2026.

4. Schaduw draaien

- Er moet gedurende minimaal 1 maand een schaduwperiode worden ingepland, waarin het nieuwe systeem parallel draait met de bestaande processen.
- Tijdens deze periode worden data, processen, en uitkomsten nauwkeurig vergeleken en bijgesteld waar nodig.

5. Data-integriteit en validatie

- De leverancier draagt zorg voor de integriteit en volledigheid van gemigreerde data.
- Er dienen controles te worden uitgevoerd op de juistheid en consistentie van de gegevens.

6. Communicatie en begeleiding

- De leverancier dient een communicatie- en opleidingsplan op te stellen en uit te voeren, gericht op de onboarding van gebruikers (HR-professionals, medewerkers, managers).
- Gebruiksvriendelijke trainings- en handleidingsmaterialen moeten beschikbaar zijn vóór livegang en gemakkelijk te delen en raadplegen.

7. Planning en rapportage

- De leverancier stelt een gedetailleerde implementatieplanning op, inclusief mijlpalen, verantwoordelijkheden, en deadlines.
- Regelmatige voortgangsrapportages worden gedeeld met de projectorganisatie

van de gemeente. En wijzigingen worden in samenspraak afgestemd.

8. Ondersteuning tijdens livegang

- De leverancier biedt intensieve ondersteuning tijdens de eerste maand na livegang, inclusief directe beschikbaarheid van een supportteam bij problemen.

9. Training en Begeleiding

De leverancier moet uitgebreide Nederlandstalige trainingen aanbieden voor verschillende doelgroepen, zoals HR-professionals, managers en medewerkers. Trainingsvormen variëren van workshops tot online modules, ondersteund door instructievideo's en handleidingen.

Doelgroepen

- HR-professionals voor functioneel beheer en complexe processen.
- Managers voor teambeheer, selfservice functionaliteiten en rapportages.
- Medewerkers voor selfservice functionaliteiten.

Trainingsvormen

- Workshops en klassikale trainingen en e-learning in gebruiksvriendelijke op B1-taalniveau.
- Online modules en handleidingen in gebruiksvriendelijke op B1-taalniveau.
- Instructievideo's voor veelgebruikte functies in gebruiksvriendelijke op B1-taalniveau.

Nazorg

- Inhoudelijke ondersteuning tijdens de eerste maanden na implementatie inclusief directe beschikbaarheid van een supportteam bij problemen.
- Trainingen voor nieuwe medewerkers als onderdeel van het onboardingproces.

2.2. Beheer & onderhoud

Het beheer en onderhoud van de E-HRM-applicatie wordt uitgevoerd door de leverancier op basis van vooraf vastgestelde SLA's. Deze afspraken waarborgen responstijden, beschikbaarheid en transparantie in de dienstverlening.

Rollen en Verantwoordelijkheden
Leverancier
Verantwoordelijk voor zowel functioneel als technisch beheer van de applicatie.

Gemeente
Levert een key user die verantwoordelijk is voor regie en coördinatie van het beheer.
Stelt ongeveer 6 kerngebruikers beschikbaar die door de leverancier worden opgeleid voor operationele ondersteuning.

Key user
Zorgt voor het verzamelen van gebruikersfeedback en werkt samen met de leverancier aan verbeteringen.

Beheervereisten
Updates en patches
Kritieke patches moeten binnen 24 uur worden geïmplementeerd.
Regelmatige updates worden minimaal per kwartaal uitgevoerd en vooraf afgestemd met de gemeente.

Proactieve monitoring
De leverancier voert continue proactieve monitoring uit op BIV (Beschikbaarheid, Betrouwbaarheid en Vertrouwelijkheid) om incidenten of problemen vroegtijdig te signaleren en escalaties te voorkomen.

Continuïteit
Bij langdurige storingen stelt de leverancier een noodoplossing beschikbaar om essentiële processen operationeel te houden.

2.3. Salaris verwerkingsdienstverlening

De leverancier verzorgt de gehele salarisadministratie waarbij duidelijke SLA's gelden om responstijden en foutmarges te garanderen. De leverancier is bekwaam in het verwerken van salarissen in het softwareprogramma en de wettelijke eisen in het bijzonder de cao-gemeente.

Vereisten t.b.v. de salaris verwerkingsdienstverlening

- Het verwerken van wijzigingen in wet- en regelgeving (o.a. CAO Gemeenten CAO Rijk) en verzorgt de aanpassingen op grond van wijzigingen in wet- en regelgeving. Het tijdig informeren over de invloed van deze wijzigingen voor de salarisverwerking.
- Het verwerken van alle voorkomende - van eenvoudige tot complexe - salarismutaties en declaraties en het controleren daarvan.
- De uitvoering van de salarisberekeningen en controles middels 4 ogen principe.
- Het controleren van de salarisverwerking op afwijkingen zoals bij de afdrachten, de nettoloonbetalingen en de loonjournaalpost.
- Het aanleveren van gegevens aan derden en het verzorgen van afdrachten aan derden zoals de Belastingdienst en het Pensioenfonds,
- Het aanleveren van een digitaal gegevensbestand (journaalpostenbestand) voor het inlezen in de financiële administratie.
- Het zorgdragen voor een tijdig en juist betaalbestand ten behoeve van het uitvoeren van de betalingen.
- Het tijdig beschikbaar stellen van de proefsalarisverwerking, er voldoende tijd is om de proefoutput te controleren en de salarisverwerker voldoende tijd heeft om de laatste wijzigingen en controles te doen.
- Het beschikbaar stellen van de salarisstroken en jaaropgave aan de werknemers.
- Het op verzoek van opdrachtgever aanleveren van gegevens voor de accountantscontrole.
- Het fungeren als vraagbaak bij salarisvraagstukken voor de gemeente (tweedelijns helpdesk). Voorwaarde is één vast contactpersoon die rechtstreeks te benaderen is.
- Het volledig inrichten van het salarispakket op werkkostenregeling.

Rapportages en evaluaties:

- Maandelijkse rapportages over incidenten, prestaties en verbeterpunten.
- Periodieke evaluaties om SLA-naleving en samenwerking te beoordelen.

3. Algemene uitgangspunten

De uitgangspunten zoals in dit hoofdstuk beschreven zijn geldend voor zowel de inrichting van de technische implementatie als voor de dienstverlening.

3.1. Juridische en Beleidseisen

Deze paragraaf behandelt de wettelijke en beleidsmatige vereisten die gelden voor de HR-applicatie, met nadruk op beveiliging, transparantie, en compliance.

Uitgebreide beschrijving:
De HR-applicatie moet voldoen aan eisen die voortkomen uit de AVG, Archiefwet, BIO en overige relevante wetgeving. De leverancier moet beschikken over actuele ISO 27001~~:2023 (NEN-EN-ISO/IEC 27001:2023 nl) en ISO 27002~~ en ISAE 3402 ~~3401 type II~~ is vereist voor informatiebeveiliging.
Leveranciers moeten hun compliance aantonen via een DPIA (Data Protection Impact Assessment).

AVG-compliance:

- Verwerking van uitsluitend noodzakelijke persoonsgegevens.
- Logging van toegang en het raadplegen van gegevens.
- Automatische dataretentie en verwijdering na de wettelijke bewaartermijn.

Beveiligingsstandaarden:

- Geldig ~~ISEA 3401 type II~~ ISAE 3402.
- De leverancier werkt volgens de vereisten zoals gesteld in de cyberbeveiligingswet en de BIO 1.4 en later de BIO 2.0.
- De applicatie moet voldoen aan de voorwaarden zoals gesteld in de GIBIT 2023 voorwaarden.
- Leveranciers moeten transparantie bieden over hun beveiligingsmaatregelen en dataprocessen.

Archiefvereisten:

- Instellen van bewaartermijnen per informatieobject.
- Mapping mogelijk op basis van de MDTO (Metagegevens voor duurzaam toegankelijke overheidsinformatie)

Toegangsbeheer:

- Rollen- en rechtenmodellen met gedetailleerde logging van wijzigingen en toegang.
- Toegang via Single Sign On (SSO)

Audits en logging

- Alle wijzigingen en mutaties worden in een log opgeslagen
- De applicatie volstaat in het uitvoeren van inhoudelijke audits

3.2. Toekomstbestendigheid

Deze paragraaf beschrijft hoe de applicatie flexibel en schaalbaar moet zijn om in te spelen op toekomstige veranderingen en groei.

Uitgebreide beschrijving:
De applicatie moet zich aanpassen aan wijzigingen in HR-processen, wetgeving en cao-wijzigingen. Schaalbaarheid is vereist om groei in gebruikers en functionaliteiten te ondersteunen. Leveranciers moeten proactief nieuwe technologieën aanbieden, zoals AI-gebaseerde analyses, automatiseringen of functionaliteiten.

Flexibiliteit:

- Ondersteuning voor toevoegen/wijzigingen in workflows en velden in informatieobjecten zonder technische aanpassingen.
- Toepassing van modulaire architectuur voor toekomstige uitbreidingen.
- Technische updates en upgrades zonder aanpassingen op bestaande inrichting/workflows

Schaalbaarheid:

- Capaciteit om een groeiend of dalend aantal gebruikers te ondersteunen.
- Mogelijkheden om nieuwe functies toe te voegen, zoals automatische loopbaananalyses.

(Door)Ontwikkeling:

- Leveranciers moeten n-1 updates garanderen voor compatibiliteit.
- Leverancier staat open voor feedback, wensen en doorontwikkelingen vanuit de klant.
- Leverancier volgt landelijke ontwikkelen en sluit aan bij innovaties waar mogelijk.

3.3. Documentatie & architectuur

Documentatievereisten
De leverancier is verantwoordelijk voor het opleveren van uitgebreide en gedetailleerde documentatie die bijdraagt aan een duurzaam en goed beheersbaar E-HRM-systeem. De volgende documentatie wordt geëist:

1. **Inhoudelijke documentatie van de applicatie-inrichting**:
    - Beschrijving van de configuratie en inrichting van de applicatie, inclusief workflows, rollen, autorisatiematrix, rechtenstructuur, en specifieke instellingen.
    - Beschrijving (separaat) van de gebruikte algoritmes ten behoeve van de registratie in het landelijke algoritme register
    - Gedetailleerde uitleg van de integraties met gekoppelde systemen, inclusief API-specificaties, mapping-tabellen op basis van MDTO, en gegevensstromen.

2. **Documentatie voor het medewerkersportaal**:
    - Gebruikershandleidingen gericht op medewerkers, inclusief stapsgewijze uitleg van de belangrijkste functionaliteiten, gebruiksvriendelijke op B1-taalniveau.
    - FAQ-documenten en visuele ondersteuning (zoals screenshots en video's) om de toegankelijkheid van de informatie te verbeteren.

3. **Documentatie voor het managers portaal**:
    - Specifieke handleidingen voor managers gericht op functionaliteiten zoals rapportages, teambeheer, en goedkeuringen, gebruiksvriendelijke op B1-taalniveau.
    - Uitleg over het gebruik van dashboards en filters binnen het portaal, gebruiksvriendelijk op B1-taalniveau.

4. **Beheer- en onderhoudsdocumentatie**:
    - Handleidingen voor technisch en functioneel beheer, inclusief procedures voor probleemoplossing, updates, en configuratiewijzigingen, gebruiksvriendelijke op B1-taalniveau.
    - Richtlijnen voor de implementatie van nieuwe modules of functionaliteiten.
    - Tijdige documentatie over updates (releasenotes) incl. impact en risicoanalyse.

Architectuurvereisten
De applicatiearchitectuur dient helder en toekomstgericht te worden beschreven. De volgende elementen zijn hierbij verplicht:

1. **Applicatiearchitectuur**:
   - Een gedetailleerde beschrijving van de opbouw van de applicatie, inclusief de structuur van modules, databronnen, en gebruikersinterfaces.
   - Specificaties van de schaalbaarheid en flexibiliteit van de architectuur om toekomstige uitbreidingen te faciliteren.

2. **Integraties en koppelingen**:
   - Uitwerking van alle koppelingen tussen de E-HRM-applicatie en andere systemen, zoals financiële systemen, rapportagetools, elektronische handtekeningtools en het gezondheidsportalen (bijv. bedrijfsarts en/of UWV).
   - Technische specificaties van de gebruikte integratieprotocollen (bijvoorbeeld API's, SFTP) en beveiligingsmaatregelen voor gegevensuitwisseling.

3. **Informatie-uitwisseling**:
   - Gedetailleerde beschrijving van de datastromen, inclusief gegevensformaten, frequenties, en datavelden.
   - Waarborging van datakwaliteit, consistentie, en compliance met wettelijke vereisten zoals de AVG en Archiefwet.

4. **Visuele representatie**:
   - De architectuurdocumentatie moet visueel worden ondersteund door diagrammen (bijvoorbeeld BPMN of ArchiMate) die inzicht geven in de werking van de applicatie, modules, en koppelingen.

5. **Regelmatige updates**:
   - De architectuurdocumentatie wordt periodiek bijgewerkt bij significante wijzigingen in de applicatie of omgeving.

Levering en Goedkeuring
- Alle documentatie en architectuurbeschrijvingen dienen bij oplevering door de gemeente te worden goedgekeurd.
- De documentatie moet in het Nederlands worden opgeleverd en toegankelijk zijn voor verschillende doelgroepen, waaronder HR-professionals, technisch beheerders, en eindgebruikers.

4. Functionele Eisen software

Dit hoofdstuk beschrijft de kernfunctionaliteiten die de HR-applicatie minimaal moet ondersteunen, gericht op het verbeteren van HR-processen en gebruiksvriendelijkheid.

Uitgebreide beschrijving:
De SaaS-applicatie wordt in de Nederlandse taal aangeboden en moet voorzien in de essentiële applicatie functies zodat een medewerker, de HR-professional en de beheerder de vragen en werkzaamheden in één geïntrigeerde omgeving kunnen uitvoeren. Zowel manager als medewerker moet de mogelijkheid hebben om via een portaal de wensen/verantwoordelijkheden uit te kunnen voeren. De selfservice processen/modules met een directe relatie met de salarisverwerking dienen in één omgeving met vergelijkbare vormgeving en werkwijze te worden geleverd.

Categorie	Doel	Functie
Kern HR-functies	Basisgegevens	**Personeelsadministratie**: beheer van (NAW-)gegevens, arbeidsvoorwaarden, dienstverbanden. Het toevoegen, aanpassen, importeren, exporteren en verwijderen van gegevens.
	Personeelsdossier	Beheer digitaal personeelsdossier per medewerker conform Archiefwet en wettelijk bewaartermijnen. Incl. briefsjablonen, salarisstroken en jaaropgaves. De documenten moeten kunnen worden geëxporteerd. Notificatie zodra er een stuk is toegevoegd.
	In dienst, doorstroom en uitstroom	In dienstmelding (invoering), wijziging arbeidsvoorwaarden, uitdienstmelding (uitschrijving) Mogelijkheid om externen op te nemen in de personeelsadministratie waarin workflows voor intern/extern verschillend kunnen zijn.
	Organisatie inrichting	Organisatiebeheer: structuurbeheer, organogrammen.

	Verlof	Toekennen, registeren en aanvragen van alle verlofsoorten volgens FTE% en werkrooster. Verlofsparen zonder verjaring. Bewaken en prioriteren in vervaldata. Ouderschapsverlof conform CAO gemeente.
	Verzuim	Verzuim registratie; met datum, percentage, oorzaak, herstel, samengesteld verzuim. Verzuimdossieropbouw, Wet verbetering poortwachter, verzuimprotocol, vangnet registratie, berekenen kortingspercentage.
	IKB	Budgetbeheer, doelen, verwerken aanvragen en verwerken mutaties, verwerking t.b.v. uitbetalen IKB, IKB uitruil verwerking
	Declaraties	Declaratiebeheer: onkosten en kilometervergoeding via (een) routeplanner indienen, bewijsstuk toevoegen. Beoordelen, registreren en uitbetalen. Controleren van declaraties die niet op 1 dag dubbel gedeclareerd mogen worden. Declaraties verwerking via workflow management.
	Signaleringen en meldingen mail	Vanuit kern HR-functies; bijv. Arbeidsovereenkomst, ziekte, (tijdelijke)toelages.
	Contractbeheer/arbeidsvoorwaarden	Contractbeheer: opstellen, bijwerken en archiveren van templates van contracten
Salarisadministratie	Mutaties	Verwerking toekomstige- en terugwerkende salarismutaties per medewerker en bulk invoer, tot 2 dagen voor de salarisbetaling. Automatisch en handmatig toekennen periodiek.
	Elektronische gegevens levering	Loonaangifte, gegevensuitwisseling, loonstaat

	Proefverwerking en herberekening	Onbeperkt maken van proefberekeningen, simulatieberekeningen
	Levering overzichten	Leveren output cumulatieve op werkgevers- en werknemersniveau en bestanden. Loonjournaalpost moet uitgesplitst kunnen worden tot looncodes. Mutatielogging.
	Werkkostenregeling	Inrichten, beheren en uitvoeren van de werkkostenregeling
	Salarisberekening/ betaling	Berekenen toelagen volgens een vast bedrag of een percentage van het salaris. De gemeente bepaald de betaaldata.
Talentmanagement	Gesprekken cyclus	Doelen stellen, evaluaties, 360-graden feedback.
	Academy	Opleiding en ontwikkeling (Academy): aanbieden leeractiviteiten zowel op individueel als op teamniveau. Tweezijdig koppelbaar aan het personeelsdossier. Ontwerpen van leeractiviteiten. Aanmaken en toewijzen van een leerlijn. Koppelen met SCROM pakket en een LTI provider. kwalificatiemanagement en rapportage.
	Loopbaanontwikkeling	Carrièreplanning. Aanvragen, registreren, fiatteren en toekennen van een studie aanvraag. Vastleggen & contracteren studieovereenkomst.
	Werving en selectie (*optioneel*)	Vacaturebeheer, sollicitatietracking, kandidaat registratie, verwerking en overdracht bijlages.
Formatiebeheer	Bezetting beheer	Beheren van bezetting op organisatie en teamniveau.

		Bepaling op basis vastgestelde functies. Bijvoorbeeld HR21.
	Formatiebeheer	Beheren van beschikbare formatie op organisatie en teamniveau
	Loonsombeheer	Actuele en prognose loonsommen, loonsomscenario bepaling
	Kostenplaats	Kostenplaatsen & kostendragers koppelen aan organisatorische eenheden, rollen en medewerkers.
(Medewerker)portalen	Manager portaal	Teamstatistieken, basisgegevens, personeelsdossier, goedkeuren van verlof, beoordelingsprocessen (declaraties, tijdcompensatie), IKB, gesprekcyclus en mutaties doorvoeren. Instellen vervanger tijdens afwezigheid, Instroom inhuur/indienst.
	Medewerkersportaal	Basisgegevens muteren personeelsdossier, loonstroken, verlof, declaratie, tijdcompensatie, IKB aanvraag/verwerking, gesprekcyclus.
	Centrale communicatie en updates.	Communicatieplatform: interne mededelingen, nieuws.
	Procesoptimalisatie	Workflow management: automatisering van o.a.: goedkeuringsprocessen, notificaties, taken, verwerkingen, berekeningen en herinneringen.
Beheer-Functionaliteiten	Beheer van functies en verantwoordelijkheden.	Functiebeheer: beheren van functiebeschrijvingen en -profielen.
	Inzicht verkrijgen in HR-prestaties en trends.	KPI-dashboards: metrics zoals verloop, ziekteverzuim, trainingseffectiviteit.
	Beschermen van gevoelige gegevens en toegang reguleren.	Rollen en rechten: gelaagd toegangssysteem voor gebruikers.

Data-analyse en rapportage	Rapportage	Rapportages zoals; Formatie- en bezetting, verzuim en Vitaliteit, opleiding en ontwikkeling, (loon-)kosten en arbeidsvoorwaarden, status ingediende aanvragen, medewerkerstevredenheid en retentie. Zie verdieping in 5.1
	Analyse en insights	Analyses en inzichten die vanuit het systeem beschikbaar gesteld worden en geëxporteerd leesbare formats zoals CSV of PDF.
	Data toegankelijkheid	Data is toegankelijk en beschikbaar om ontsloten te worden. Data kan zowel via export als via een API ontsloten worden

4.1. Integraties

In dit hoofdstuk worden de eisen besproken voor integraties met bestaande systemen. Het doel is een naadloze uitwisseling van gegevens en procesondersteuning.

De applicatie moet koppelingen bieden met essentiële HR- en bedrijfsapplicaties, zoals salarisadministratie en documentondertekening. Integraties moeten gebruikmaken van REST- of SOAP-API's voor flexibele en veilige gegevensuitwisseling.

Categorie	**Integratie**	**Omschrijving**
Salaris- en Payrollsystemen	Belastingdienst	Automatische gegevensuitwisseling voor loonheffingen en belastingen.
	Pensioenfondsen	Rapportage en overdracht van pensioengegevens. Gekoppeld met Loyalis
	HR21	Functiewaarderingssysteem gekoppeld aan salarisadministratie.
	Financieel pakket	Integratie met financiële pakketten t.b.v. uitwisseling van betaal batches en journaalposten b.v. Key2Financiën
Financiële Systemen	Betaalbestanden via EQUENS	Betalingen en financiële transacties
Recruitment en ATS	Vacaturebanken	Integratie met platforms zoals LinkedIn, Indeed, of Monsterboard.
	ATS-tools	Bijvoorbeeld Recruitee, Bullhorn, of Greenhouse voor werving en selectie.
	CAO-gegevensbanken	Automatische updates van arbeidsvoorwaarden.
Arbeidsvoorwaarden en Compliance	Arbodiensten	Integraties mogelijkheden met arbodiensten zoals ArboNed of HumanCapitalCare (tweezijdig).
	Roosterplanningssystemen	Integratiemogelijkheid met systemen zoals TimeChimp, Planning.nl, of Shiftbase.
Tijdregistratie en Planning	Urenregistratie	Koppeling met systemen voor urenregistratie, zoals Clockwise of Exact Time.

Overheid en Wetgeving	UWV-interface	Automatische meldingen voor WAZO, langdurig ziek etc.
	Learning Management Systems (LMS)	Integratie met tools zoals Moodle, Cornerstone, of Studytube voor trainingen en certificeringen.
Trainings- en E-learning Platforms	Academy-functionaliteit	Directe synchronisatie van leerplannen en trainingen.
Rapportage- en Analysetools	BI-tools	Bijvoorbeeld Power BI, Cognos, Tableau, of Qlik voor HR-analyse.
Documentmanagement	E-signature tools	Integratie via API-koppeling. Bijvoorbeeld met ValidSign, Octobox, Adobe Sign.
	Documentbeheer	Bijvoorbeeld SharePoint, Teams, Decos Join, Atabix, Djuma etc.
	Occupational Health Portals	Voor samenwerking met bedrijfsartsen en verzuimbeheer.
Gezondheids- en Verzuimbeheer	Bedrijfsartsportaal	Voor ziekmeldingen en verzuimbeheer (Tweezijdig).
Identity en Access Management	Single Sign-On (SSO)	Koppelingen met systemen zoals Azure AD, Okta, GOVconnect of OneLogin.
	Multi-Factor Authentication (MFA)	Veiligheid via tools als Microsoft Authenticator, Google Authenticator of Auth0.
	Pardon	Workflowbeheer voor gemeentelijke processen.
Service Management Systeem		Topdesk, Authenticatie via Microsoft Azure Active Directory

4.2. Toekomstbestendigheid

Dit hoofdstuk beschrijft hoe de applicatie flexibel en schaalbaar moet zijn om in te spelen op toekomstige veranderingen en groei.

Uitgebreide beschrijving:
De applicatie wordt door aanbieder bijgehouden voor afnemer geldende wet- en regelgeving en is aangepast alvorens ingang van de betreffende wijziging. Voorgaande is van toepassing op wijzigingen binnen HR-processen en geldende wet- en regelgeving. Dit betreft onder andere (maar niet uitsluitend) de richtlijnen in het kader van de AVG, NIS2, AI-act, de CAO Gemeenten, De applicatie en in het systeem gebruikte wettelijke formulieren van instanties zoals het UWV en de sociale en fiscale wet- en regelgevingen. Schaalbaarheid is vereist om groei of afname in gebruikers en functionaliteiten te ondersteunen. Leveranciers moeten proactief nieuwe technologieën aanbieden, zoals kunstmatige intelligentie, machine learning etc.

Belangrijkste punten:
Technische flexibiliteit:

- Ondersteuning voor wijzigingen in workflows zonder technische aanpassingen.
- Het product moet niet alleen schaalbaar zijn bij groei in organisatie (kwantitatief), maar ook op de breedte (functionaliteit) waardoor voordeel behaald kan worden in prijs voor afnemer (niet teveel functionaliteit afnemen). Tevens dient er een modulaire opzet te zijn zodat toekomstige ontwikkelingen eenvoudig beschikbaar gesteld kunnen worden

Schaalbaarheid:

- Capaciteit om een groeiend of afnemend aantal gebruikers te ondersteunen.
- Mogelijkheden om nieuwe functies toe te voegen, zoals kunstmatige intelligentie en/of machine learning.

Innovatie:
Leveranciers moeten n-1 updates garanderen voor compatibiliteit.

5. Technische Eisen

Dit hoofdstuk behandelt de technische vereisten van de HR-applicatie, met nadruk op beveiliging, prestaties, en compatibiliteit met bestaande systemen.

Uitgebreide beschrijving:
De applicatie moet voldoen aan strikte technische eisen om beschikbaarheid, vertrouwelijkheid en integriteit te waarborgen. Standaarden zoals ISO 27001 ~~en ISO 27002~~ en beveiligingsmaatregelen zoals multi-factor authenticatie (MFA) zijn verplicht. Onder andere hosting binnen de EER, inregelen van functiescheiding en automatische logging is essentieel.

Hosting en infrastructuur:

- De applicatie moet als SaaS-oplossing worden aangeboden en rechtstreeks benaderbaar via een URL. Beschikbaar via gangbare browsers zoals Chrome, Edge etc.
- Optioneel; beschikbaarheid van app voor personele afhandelingen en verzoeken
- Hosting binnen de Europese Economische Ruimte (EER) is verplicht.
- Het systeem biedt de mogelijkheid om zonder dienstverband (en zonder zakelijk email adres) relevante stukken (loonstroken of jaaropgave) op te halen.

Prestaties:

- Een minimale uptime van 99,8% 24/7.
- Reactieve en proactieve monitoring van systeemprestaties.

Compatibiliteit:

- Ondersteuning voor API's volgens REST- en SOAP-standaarden.

5.1. Rapportage en Dashboards

De applicatie moet standaard KPI-rapportages bieden en gebruikers in staat stellen zelf aangepaste rapportages te maken zonder technische kennis. Dashboards moeten eenvoudig te gebruiken zijn en gepersonaliseerd kunnen worden voor verschillende gebruikersgroepen.

Rapportages:

- Standaardrapportages moeten KPI's omvatten zoals ziekteverzuim, personeelsverloop, verlof, signaleringen, actuele status van ingediende aanvragen, en formatie- en bezetting beheer, realisatieoverzichten en prognoses.
- Mogelijkheden voor gebruikers om zelf rapportages samen te stellen via drag-and-drop interfaces.
- Rapportages zijn gemakkelijk te downloaden in leesbare formats zoals bijvoorbeeld csv of pdf.

Dashboards:

- Visueel aantrekkelijke dashboards voor HR-professionals, managers, en medewerkers.
- Standaarden voor filters voor afdelingen, tijdsperioden, en andere relevante criteria maar ook handmatig instelbaar.

Integraties:

- Integratie met Power BI is een sterke pre voor diepgaande analyses.

Analyses, innovaties

- Inhoudelijke punten t.a.v. innovaties zijn opgenomen in de leidraad

5.2. Eisen Informatiebeveiliging en privacy

Generiek

1. De Leverancier accepteert de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT 2023) als leidende inkoopvoorwaarden.
2. Indien van toepassing voor de ICT-prestatie zijn de volgende open standaarden van het Forum Standaardisatie onder meer en expliciet verplicht:
    a. DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv6, SAML, SPF, STARTTLS, DANE, STIX en TAXII, TLS en WPA2.
    b. NEN-ISO/IEC 27001 ~~en NEN-ISO/IEC 27002~~ (Informatiebeveiliging).
3. De ICT-Prestatie stelt de opdrachtgever in staat te voldoen aan:
    a. De (U)AVG;
    b. De Baseline Informatiebeveiliging Overheid;
    c. ISO 27001~~:2023 (NEN-EN-ISO/IEC 27001:2023 nl)~~
    ~~d. ISO 27002~~
    ~~e. ISEA 3401 type II~~ ISAE 3402
    f. De beveiligingsrichtlijnen voor webapplicaties van het NCSC;
    g. Archiefwet 1995, Archiefbesluit 1995;
    h. Het Algemeen en Technisch Informatiebeveiligingsbeleid van Opdrachtgever
4. Leverancier licht toe hoe de ICT-Prestatie de Opdrachtgever ondersteund om hieraan te voldoen.
5. Indien de Leverancier gebruik maakt van een onderaannemer gelden alle eisen onverminderd voor de onderaannemer. De Leverancier is verantwoordelijk voor een juiste invulling en werking van de eisen bij de onderaannemer.
6. De Leverancier geeft transparant en kosteloos inzicht in certificeringsdocumenten en rapportages opgesteld door EDP-auditors. TPM verklaringen moeten in bezit van de opdrachtgever zijn vóór 30 oktober van het verantwoordingsjaar.
7. De Leverancier licht toe hoe de principes van ‘privacy bij design’ en ‘privacy by default’ zoals beschreven in de AVG zijn toegepast.
8. Leverancier 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.
9. Leverancier heeft beheersmaatregelen tegen malware getroffen

10. Risico's voor informatiebeveiliging en privacy zijn expliciet benoemd en passende beheersmaatregelen zijn expliciet belegd
11. De applicatie wordt periodiek en minimaal eens per jaar op kwetsbaarheden onderzocht (kwetsbaarheidsscans en penetratietesten). Kwetsbaarheden worden geclassificeerd en krijgen opvolging.
12. Multi-factor authenticatie (MFA) en Single Sign-On (SSO) zijn toegepast
13. Versleuteling van data tijdens transport (TLS) en opslag is verplicht
14. Mogelijkheid om toegang te beperken via een vast ip adres

Integriteit

1. 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 Leverancier 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 of Windows 11 zou acceptabel zijn met de nog ondersteunde build versie,
2. 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.
3. De Leverancier heeft maatregelen genomen om de toegang tot de broncode van informatiesystemen te beperken tot de medewerkers, die deze code onderhouden of installeren.
4. De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door checksums).
5. Versies van de software worden voor de in productiename door de Leverancier onder meer getest op invoer van gegevens (grenswaarden, format, inconsistentie, SQL injectie, cross site scripting, etc.).
6. Applicaties worden ontwikkeld en getest op basis van Internationale 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
7. De opdrachtgever heeft het recht om in overleg met de Leverancier webapplicaties of servicekoppelingen te onderwerpen aan penetratietesten op kosten van de opdrachtgever. De Leverancier 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.
8. De applicatie voorziet in validatiecontroles op ten minste de volgende aspecten:
    a. Gegevens en verwerkingen kunnen worden gecorrigeerd vanuit de applicatie na invoer
9. Consistentiecontroles zijn in de applicatie voorzien om de correcte verwerking van gegevens te waarborgen

a. De logging biedt voldoende inzicht in de bijhouding, uitwisseling, en selecties van gegevens om het gebruik van een gegeven door een applicatie te kunnen achterhalen en hierop te signaleren of acteren.
b. Onderdelen die minimaal in de logging opgenomen dienen te zijn:
    - Gebruikerslogging
    - Datum/tijd van actie
    - Gebruikersnaam of gebruiker ID
    - Uitgevoerde handeling
    - Object waarop de handeling werd uitgevoerd
    - Handelingen van gebruikers met speciale bevoegdheden
    - Systeemlogging
    - Opgetreden fouten (error log)
    - (Poging tot) ongeautoriseerde toegang
    - (Poging tot) wijziging van beveiligingsinstellingen
c. In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, etc.). In de logregel mogen ook geen persoonsgegevens worden opgenomen uit systemen van de Opdrachtgever zelf (dus wel gebruikersnamen of inlog accounts)."

10. Er is sprake van logging in de applicatie. Relevante zaken om te loggen zijn:
    a. Type gebeurtenis (zoals back-up/restore, reset wachtwoord, betreden ruimte);
    b. (poging tot) Ongeautoriseerde toegang;
    c. Handelingen met speciale bevoegdheden, waarbij alle handelingen van "superusers" worden gelogd;
    d. Systeemwaarschuwingen;
    e. (poging tot) Wijziging van de beveiligingsinstellingen.
11. De logging is alleen beschikbaar voor daartoe geautoriseerde medewerkers.
12. Een logregel bevat in ieder geval geen gegevens die tot het het doorbreken van de beveiliging kunnen leiden
13. De logging is read-only. Het muteren en verwijderen van log-records is niet toegestaan.
14. Gelogde informatie wordt minimaal 6 maanden bewaard, zodat onderzoek kan plaatsvinden in geval van een opgetreden informatiebeveiligingsincident.
15. Logging kan naar een extern logging systeem (SIEM) gestuurd worden. De uitwisseling van deze informatie is mogelijk op basis van STIX en TAXII.
16. 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).
17. 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.
18. Voor het configureren van platformen is een worden hardeningsrichtlijnen van de vendor toegepast of bijvoorbeeld van het CIS framework

Vertrouwelijkheid

1. De Opdrachtgever blijft eigenaar van de gegevens binnen applicatie en deze gegevens mogen niet voor andere doeleinden gebruikt worden door de Leverancier van de applicatie. Dit geldt zowel voor gegevens in de Test-, Acceptatie- als Productieomgevingen.
2. Het is de Leverancier 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.
3. De Leverancier heeft een geheimhoudingsplicht aangaande alle vertrouwelijke gegevens dan wel anderszins gevoelige informatie van de opdrachtgever die de Leverancier in het kader van de opdracht ter kennis is gekomen.
4. De Leverancier heeft een geheimhoudingsplicht aangaande de informatie opgenomen in de systemen.
5. De Leverancier is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. Leverancier waarborgt hierbij tevens ook met scheiding van taken onbedoelde of ongeautoriseerde toegang. De opdrachtgever heeft het recht hierop te controleren.
6. De Leverancier 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.
7. Alle voorwaarden en eisen die gelden voor personeel van de Leverancier zijn ook van toepassing op derden, die in opdracht van de Leverancier diensten verrichten voor de Opdrachtgever
8. Autorisaties kunnen worden ingericht op basis van functies (rol-gebaseerd) waarbij functie-scheiding is toegepast.(RBAC model)
9. Leverancier geeft aan welke accounts nodig zijn voor beheer en ondersteuning
10. Binnen de test omgeving wordt geen gebruik gemaakt van productie data
11. Bij gebruik van PKI(o) certificaten beschikt de Leverancier over vastgestelde procedures voor sleutelbeheer. De Leverancier geeft bij de aanbesteding inzicht in de manier waarop sleutelbeheer is geregeld.
12. De hosting en opslag van data vindt plaats binnen de Europese Economische Ruimte (EER)

Privacy

1. De Leverancier stelt opdrachtgever in staat om zelf access management uit te voeren. Opdrachtgever dient direct invloed uit te kunnen oefenen over de accounts (en bijbehorende autorisaties) van de eigen medewerkers.
2. De Leverancier houdt een actuele registratie bij van geautoriseerde accounts/gebruikers.
3. De Leverancier verschaft relevante informatie over de wijze waarop – en onder welke voorwaarden – cryptografie wordt gebruikt om persoonsgegevens van betrokkenen te beschermen.
4. De Leverancier 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.
5. Uitwisseling van persoonsgegevens dienen altijd te voorzien van encryptie, zowel voor fysieke media als transport
6. Bij informatiebeveiligingsincidenten aan de kant van de Leverancier wordt door de Leverancier expliciet onderzocht of bij dat incident persoonsgegevens zijn gemoeid, tenzij dat redelijkerwijs niet aannemelijk is.
7. Indien het uitvoeren van audits door opdrachtgever onwenselijk of redelijkerwijs niet mogelijk is, overlegt de Leverancier – voorafgaand aan het afsluiten van het servicecontract – onafhankelijk bewijs waaruit blijkt dat de getroffen beveiligingsmaatregelen conformeren aan de door opdrachtgever gestelde eisen en beleid.
8. De Leverancier zorgt dat tijdelijke bestanden (cache) die persoonsgegevens bevatten periodiek worden verwijderd.
9. De Leverancier legt alle verstrekkingen van persoonsgegevens (waar opdrachtgever verwerkingsverantwoordelijke voor is) aan andere partijen schriftelijk vast.
10. De Leverancier en opdrachtgever maken schriftelijke afspraken over de manier waarop persoonsgegevens worden verwijderd of geanonimiseerd. De Leverancier heeft over dit onderwerp beleid opgesteld. In dat beleid wordt ook ingegaan op de bewaartermijn van persoonsgegevens na eindigen van het contract.
11. De Leverancier 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 Leverancier eveneens inzichtelijk te maken.
12. Indien er algoritmes en/of Artificial Intelligence (AI) wordt toegepast, dient de Leverancier dit aan te geven inclusief toelichting op de werking van dit algoritme en/of AI.

6. Exit-strategie

1. Inhoud van de Exit-strategie

De exit-strategie moet minimaal de volgende onderdelen bevatten:

Migratie van gegevens

De leverancier draagt zorg voor een volledige en veilige overdracht van alle gegevens, inclusief historische gegevens, digitale personeelsdossiers, en alle relevante metadata en logs. Gegevens moeten in een gespecificeerd formaat worden opgeleverd, zoals XML, CSV, of een andere overeengekomen standaard.

Documentatieoverdracht

De leverancier levert volledige documentatie op, waaronder technische specificaties, architectuurdocumenten, handleidingen voor beheerders en eindgebruikers, en instructies voor het opnieuw configureren van koppelingen en integraties.

Overdracht van rechten en licenties

De leverancier specificeert welke rechten en licenties moeten worden overgedragen of beëindigd. Eventuele aanpassingen aan licenties moeten zonder extra kosten voor de gemeente plaatsvinden.

Begeleiding en ondersteuning tijdens de transitie

De leverancier biedt ondersteuning gedurende een overgangsperiode van minimaal 3 maanden. Dit omvat technische ondersteuning, functionele begeleiding en beantwoording van vragen, en de aanwezigheid van een contactpersoon voor escalaties.

2. Procesafspraken

De leverancier dient samen met de gemeente een proces te hanteren dat de exit-strategie soepel uitvoert.

Tijdsplanning en fasering

De exit-strategie bevat een gedetailleerd stappenplan met mijlpalen en deadlines. De totale uitvoering mag niet langer duren dan een vooraf overeengekomen periode, bijvoorbeeld 6 maanden.

Testen van overdracht

Voordat de overdracht definitief wordt afgerond, moet de gemeente de mogelijkheid hebben om de kwaliteit en volledigheid van de data, documentatie, en koppelingen te testen.

Continuïteit van dienstverlening

De leverancier waarborgt dat essentiële processen; salarisverwerking, declaraties, verlof en verzuim blijven functioneren tijdens de overdracht.

3. Standaardvoorwaarden van Gemeenten

Databeveiliging en AVG

De gegevensoverdracht moet volledig AVG-compliant zijn. De leverancier garandeert dat alle gegevens na de overdracht veilig worden verwijderd uit hun systemen.

Kostenstructuur

De leverancier mag geen additionele kosten rekenen voor de uitvoering van de exit-strategie, behalve waar dit vooraf is overeengekomen.

Samenwerking met opvolgende leverancier

Indien een opvolgende leverancier betrokken is, werkt de huidige leverancier actief mee aan een soepele kennisoverdracht.

4. Evaluatie en Afsluiting

Evaluatierapport

Na afronding van de exit-strategie stelt de leverancier een evaluatierapport op, waarin de uitvoering wordt beschreven en eventuele verbeterpunten worden benoemd.

Afsluitende goedkeuring

De exit-strategie wordt formeel afgesloten met goedkeuring van de gemeente, inclusief een verklaring dat alle overeengekomen onderdelen zijn uitgevoerd.

7. SLA afspraken

De inschrijver die het voornemen tot gunning van deze aanbesteding heeft ontvangen, wordt gevraagd een concept SLA in te dienen voorafgaand aan de ondertekening van de overeenkomst. Leverancier dient om te gaan met de voorwaarden zoals deze zijn vermeld in de aanbestedingsstukken. De gemeente accepteert (daarbij) geen andere voorwaarden.

Tijdens de implementatieperiode leggen de partijen concrete afspraken vast over Service Levels ter zake van het in artikel 10.3 van GIBIT 2023 bedoelde Onderhoud waarin maatregelen zijn opgenomen ter zake van het al dan niet halen van de afgesproken Service Levels.

Service Level Agreements (SLA's) beheer

De leverancier is verplicht een SLA op te stellen waarin de volgende vereisten in opgenomen zijn:

Incidenten

Kritieke incidenten:
Reactietijd: Binnen 1 uur.

Oplostijd: Binnen 8 werkuren.

Niet-kritieke incidenten:
Reactietijd: Binnen 4 werkuren.
Oplostijd: Binnen 2 werkdagen.

Change requests:
Reactietijd: Binnen 2 werkdagen.
Oplostijd: Binnen 10 werkdagen of zoals overeengekomen.

<u>Meldingen, Rapportages en Evaluaties</u>

Meldingen:
Gebruikers dienen meldingen digitaal in via een klantenportaal van de leverancier
Meldingen worden voorzien van een uniek nummer voor tracking en terugkoppeling.

Toegang tot informatie:
De gemeente krijgt toegang tot een online kennisbank waarin releasenotes, gebruikershandleidingen en informatie over storingen beschikbaar zijn.
Nieuwe releases en updates worden minimaal 2 weken van tevoren aangekondigd.

Maandelijkse rapportages:
Inzicht in het aantal incidenten, de reactietijden en oplostijden.
Prestaties van de applicatie, zoals uptime en systeemgebruik.
Adviezen over mogelijke verbeterpunten en trends in incidenten.

Periodieke evaluaties:
Elk kwartaal vindt een evaluatie plaats om de naleving van de SLA's en de samenwerking te beoordelen.
Feedback van gebruikers wordt verzameld en besproken om de dienstverlening te optimaliseren.

Service Level Agreements (SLA's) salarisverwerkingsdienstverlening
De leverancier is verplicht een SLA op te stellen waarin de volgende vereisten in opgenomen zijn wat betreft de salarisverwerkingsdienst.

Responsetijden: Reactietijd binnen 8 uur op werkdagen, opgelost binnen 24 werkuren.
Foutmarge: in de verwerking mag maximaal 2% aan fouten worden geconstateerd.

Escalatieprocedure

De leverancier dient een duidelijke en uitvoerbare escalatie- en calamiteitenprocedure te beschrijven als onderdeel van het aanbod. Deze procedure moet zorgen voor een snelle en effectieve oplossing van problemen die niet binnen de reguliere serviceafspraken kunnen worden afgehandeld. Transparantie en communicatie staan hierin centraal. De leverancier dient daarnaast een RASCI-matrix op te nemen in de beschrijving van de escalatie- en calamiteitenprocedure, waarin de verantwoordelijkheden en betrokkenheden helder worden vastgelegd.

1. Inhoud van de Escalatie- en calamiteitenprocedure

De escalatie- en calamiteitenprocedure moet minimaal de volgende elementen bevatten:

Definities en classificatie van incidenten
De leverancier definieert welke situaties aanleiding geven tot escalatie, zoals herhaalde verstoringen, niet-opgeloste kritieke incidenten, of afwijkingen van de overeengekomen SLA's. Classificatie van incidenten moet duidelijk worden aangegeven (bijvoorbeeld laag, medium, hoog, of kritisch).

Escalatieniveaus en verantwoordelijken
De procedure beschrijft de escalatieniveaus, inclusief verantwoordelijke rollen binnen de organisatie van de leverancier. Bijvoorbeeld:

- Niveau 1: Operationele ondersteuning.
- Niveau 2: Teamleider of functioneel beheerder.
- Niveau 3: Management van de leverancier.

Escalatiecriteria en -triggers
De leverancier specificeert de criteria die een escalatie activeren, zoals het overschrijden van oplostijden, herhaald falen, of kritieke impact op bedrijfsprocessen.

RASCI-matrix
De leverancier dient een RASCI-matrix op te nemen waarin de verantwoordelijkheden en betrokkenheden van alle partijen tijdens een escalatie zijn vastgelegd:

- Responsible: Wie voert de acties uit?
- Accountable: Wie is eindverantwoordelijk voor de escalatie?
- Support: Wie ondersteunt bij de uitvoering?
- Consulted: Wie wordt geconsulteerd?
- Informed: Wie moet geïnformeerd worden?

2. Procesafspraken

De leverancier dient een helder proces te hanteren voor escalaties, met duidelijke afspraken over communicatie en opvolging.

Reactie- en oplostijden tijdens escalaties
De leverancier moet in escalatiegevallen binnen de volgende tijdframes reageren en oplossen:

Kritieke escalaties: Reactie binnen 30 minuten, oplossing binnen 4 werkuren.
Niet-kritieke escalaties: Reactie binnen 2 werkuren, oplossing binnen 2 werkdagen.

Communicatie tijdens escalaties
De leverancier communiceert proactief met de gemeente gedurende het gehele escalatieproces, inclusief:
Het benoemen van een contactpersoon voor de escalatie.
Het geven van updates op vaste intervallen (bijvoorbeeld elke 2 uur bij kritieke incidenten).
Het rapporteren van voortgang en verwachte oplostijden.

Overlegmomenten en beslissingen
Indien een escalatie niet binnen de overeengekomen termijn kan worden opgelost, organiseert de leverancier een overleg met de gemeente om aanvullende maatregelen te bepalen.

3. Standaardvoorwaarden van Gemeenten

Rapportage na escalatie
Na afronding van een escalatie levert de leverancier een gedetailleerd rapport op met:
De oorzaak van het incident.
De genomen acties en opgeloste problemen.
Voorgestelde preventieve maatregelen om herhaling te voorkomen.

Transparantie in escalaties
De leverancier dient escalaties direct en zonder vertraging te melden, inclusief een volledige beschrijving van de impact op de dienstverlening.

Kostenstructuur
De kosten voor het oplossen van escalaties worden geacht binnen de reguliere serviceovereenkomst te vallen, tenzij anders vooraf overeengekomen.

4. Evaluatie en Afsluiting

Evaluatierapport
De leverancier stelt na een escalatie een evaluatierapport op waarin de effectiviteit van de escalatieprocedure wordt beoordeeld. Eventuele verbeterpunten worden besproken en geïmplementeerd.

Afsluitende goedkeuring
De escalatie wordt afgesloten met goedkeuring van de gemeente, waarin wordt bevestigd dat alle afgesproken acties zijn uitgevoerd en eventuele preventieve maatregelen zijn geïmplementeerd.