Bijlage B Programma van Eisen

Behorende bij de offerteaanvraag voor een Output Management Systeem – Referentie 2024.02

Zie voor een verdere toelichting hoofdstuk 7 in het document “Offerteaanvraag”.
De navolgende eisen zijn van toepassing:

	Algemene eisen
1.	De opdracht wordt uitgevoerd conform de Opdrachtomschrijving zoals omschreven in het document Offerteaanvraag inclusief alle bijlagen A t/m H en Formulieren.
2.	De SAAS oplossing voldoet aan alle eisen gesteld in de relevante wet- en regelgeving.
3.	De aangeboden SAAS oplossing is een bewezen concept. Hiermee wordt bedoeld dat het OMS zichzelf heeft bewezen, in een soortgelijke omgeving als de beoogde omgeving, te functioneren naar tevredenheid van de gebruikers.
4.	Het OMS en bijhorende informatie (handleidingen en release documenten) moet Nederlandstalig zijn en online beschikbaar zijn, met versiebeheer.
5.	Opdrachtnemer garandeert een operationele organisatie die beschikt over ruim voldoende professionele mankracht, zodat de uitvoering van de opdracht conform de SLA is gewaarborgd.

	Functionele eisen
	Algemeen
6.	Het Output Management Systeem gedraagt zich als een centraal component die voorziet in het aanmaken en beheren van templates (teksten en opmaak), het creëren van output (documenten, e-mailberichten en e-mail notificaties) op basis van de templates en aangeleverde variabelen uit de backend systemen en het versturen van de output naar klanten via vooraf gedefinieerde distributiekanalen.
7.	Het vereiste distributiekanaal is e-mail.
8.	Outputformaten die worden ondersteund: PDF, Word, Excel, HTML.
9.	Het aanmaken en of wijzigen van inhoud (teksten / tekstblokken) en templates (inclusief variabelen) kan op een eenvoudige wijze gedaan worden door een gebruiker en kunnen zonder tussenkomst van opdrachtnemer of het Regieteam Informatie Voorziening beheerd worden.
10.	Templates en teksten/tekstblokken kunnen volgens een vooraf gedefinieerde structuur worden opgeslagen zodat deze eenvoudig terug te vinden zijn.
11.	Versie beheer van teksten / tekstblokken en templates is mogelijk.
12.	Er moet een mogelijkheid zijn om documenten geautomatiseerd op te slaan in het DMS
13.	Er moet een mogelijkheid zijn van de uitgaande correspondentie geautomatiseerd een contactmoment vast te leggen in het CRM
14.	Het Output Management Systeem is in staat om informatie uit het backend systeem op te halen en daar de distributie van gegevens op afstemmen.

15.	Teksten kunnen met drag en drop worden samengevoegd
16.	Templates kunnen worden gedupliceerd en vervolgens worden aangepast
17.	Templates moeten eenvoudig terug te vinden zijn
18.	Teksteditor heeft een gebruikersvriendelijke What You See Is What You Get (WYSIWYG) userinterface, vergelijkbaar met Word
19.	Het Output management Systeem heeft een preview functie waarbij de template (inhoud, opmaak en variabelen) in gecreëerde output wordt getoond.

	Non-functionele eisen (IT eisen)
	Informatiehuishouding, Architectuur en koppelingen
20.	Alle niet persoonlijke accounts zijn gekoppeld aan/ herleidbaar naar natuurlijke personen.
21.	Wachtwoorden en authenticatie data, bij interfaces, worden versleuteld tijdens transmissie en opslag middels sterke encryptietechnieken (one-way encryptie en sterke sleutels)
22.	Voor de gebruiker is het visueel duidelijk welke omgeving (productie, acceptatie en/of ontwikkeling) hij/zij in gebruik heeft.
23.	Alle software (maatwerk, pakket, SAAS) dienen te voldoen aan best practice beveiligingsrollen (bij OWASP).
24.	Het systeem is in staat om een SSO koppeling te maken met Entra ID van VfPf (voorheen Azure Active Directory).
25.	Two-factor authentication (2FA) moet worden toegepast.
26.	Gegevens mogen niet vermengd kunnen worden met gegevens van andere Cloud gebruikers.
27.	De applicatie kan met zijn omgeving communiceren door middel van web service technologie.
28.	De applicatie heeft hiervoor een set aan REST API's gedefinieerd.
29.	De clouddienst voldoet (minimaal aan de grenzen) aan de open web standaarden.
30.	Om interoperabiliteit te garanderen dient de Cloudleverancier gebruik te maken van standaard protocollen (bijv. TLS) en algoritmen (bijv. RSA en AES).
31.	Voor geautomatiseerde koppelingen worden specifieke applicatie-accounts gebruikt.
32.	De applicatie onderkent verschillende gebruikersrollen.
33.	In de applicatie gedefinieerde gebruikers kunnen door geautoriseerde gebruikers vrij worden gekoppeld aan een of meer gedefinieerde rollen.
34.	Autorisaties kunnen binnen de applicatie worden toegekend op basis van de rollen en de overzichten van gebruikers inclusief rollen zijn in overzichten in te zien door de gebruikersbeheerder voor IAM (Identity en Access Management) controles.
35.	Er vindt binnen de applicatie logging van transacties plaats, welk te filteren, sorteren en exporteren zijn.
36.	De applicatie bevat gedegen logging en rapportage mogelijkheden over gebruikersactiviteit en permissies.

37.	Actieve monitoring en alarmering op de workflow. Inzage in de goed en fout gelopen processen waaronder het afleveren aan de koppelingen.

	Governance
38.	VfPf hanteert de Governance als omschreven in hoofdstuk 9 van de offerteaanvraag en stelt daarbij de volgende eisen aan de overlegstructuur: a) Ieder overleg vindt minimaal plaats in de bij de overlegvorm vast te stellen frequentie, waarbij de frequentie aangepast kan worden indien dit door opdrachtgever noodzakelijk wordt geacht. b) Opdrachtgever vervult in de overleggen de rol van voorzitter. c) Opdrachtnemer neemt deel aan de overleggen met medewerkers van gelijkwaardig niveau als de deelnemers vanuit opdrachtgever. d) Opdrachtnemer maakt bij de start van de overeenkomst aan opdrachtgever kenbaar wie deze deelnemers zijn (in de vorm van profielen). Opdrachtnemer garandeert stabiliteit en continuïteit in de inzet van de deelnemers.
39.	Opdrachtnemer is verantwoordelijk voor het opstellen van de SLA, voorafgaand aan de in beheer name van de SAAS-tool. De SLA en DAP dienen hierbij goedgekeurd te zijn door de opdrachtgever.
40.	Opdrachtnemer conformeert zich aan de overeen te komen SLA, rapporteert en stuurt op de afhandeling van incidenten/wijzigingen/problemen.
41.	Opdrachtnemer is verantwoordelijk voor het maken, het beheren en beschikbaar maken van de bedieningsprocedures en gebruikshandleiding voor al hetgeen opdrachtgevert.b.v. effectief gebruik van de tool dient te weten en kan configureren.
42.	Opdrachtnemer levert conform gemaakte afspraken in de SLA, een door opdrachtgever te accorderen rapportage op. De rapportage dient minimaal de volgende informatie te bevatten: a) Minimaal (maar niet uitsluitend) de resultaten o.b.v. de gemaakte afspraken en SLA. b) Technische kwatsbaarheden en (security-)incidenten. c) Door opdrachtnemer te nemen en/of genomen maatregelen bij afwijking o.b.v. de gemaakte afspraken en SLA. Actueel overzicht van de gemaakte afspraken, besluiten en actiepunten.
	Inrichting en configuratie
43.	De opdrachtgever draagt zorg voor het definiëren en specificeren van de gewenste functionaliteit en maakt deze aan de opdrachtnemer in de vorm van business specificaties en procesbeschrijvingen kenbaar. De inrichting en configuratie valt onder de verantwoordelijkheid van de opdrachtnemer.
44.	Alle releases (SAAS-oplossingen) volgen het in de SLA afgesproken wijzigingenproces waarbij elke release formeel door de opdrachtgever wordt vrijgegeven voordat deze naar de productieomgeving wordt doorgezet. Urgente security patches zijn hierop een uitzondering en dienen direct uitgerold te worden.
45.	Na de implementatie organiseert de opdrachtnemer een formeel overdrachtsmoment aan RUN, waarbij projectdocumentatie (incl. acties- en besluitenlijst van het project) en

	bedieningsprocedures beschikbaar worden gesteld conform de in beheer name procedure van opdrachtgever.

	Beheer, ondersteuning en wijzigingen
46.	Opdrachtgever en opdrachtnemer leggen de vereisten voor het functioneel & technisch beheer vast in een Service Level Overeenkomst (SLA) die voldoet aan de ISO 27001 Standaard.
47.	In ieder geval worden de volgende punten beschreven in de SLA: • Dienstenniveau (bijv. openingstijden, bereikbaarheid en reactietijd van incidentmeldingen en afhandeling, escalatieprocedures, recht op audit) • Beveiligingseisen & verplichtingen (bijv. rapportage over Security incidenten)
	<u>Beschikbaarheid</u> *Beschikbaarheid is de mate waarin 'het systeem' operationeel en toegankelijk is voor klanten.*
48.	Het systeem dient een beschikbaarheid te hebben van minimaal 99,5% op kantoordagen. De beschikbaarheid wordt per maand gemeten door het aantal minuten dat het systeem niet beschikbaar was en te delen door de totale tijd in het betreffende 'service window'.
49.	Alle meldingen (incidenten, wijzigingen, problemen etc.) worden vastgelegd in een servicemanagementsysteem van de opdrachtnemer.
50.	Zowel opdrachtnemer als opdrachtgever kunnen in dit servicemanagementsysteem meldingen aanmaken en aanpassen. Opdrachtnemer en opdrachtgever hebben toegang tot dit systeem waarbij alle meldingen centraal geregistreerd zijn en hierover in de SLR gerapporteerd wordt.
	<u>Schaalbaarheid</u> *Indien bij groeiende volumes de prestaties afnemen, dan moet het systeem (combinatie applicatie en infrastructuur) kunnen worden opgeschaald.*
51.	Opdrachtnemer is in staat de prestaties van De SAAS tool te analyseren en hier adequaat op te acteren, wanneer de situatie hierom vraagt.
	<u>Incidentbeheer</u> *Incidentbeheer is de wijze waarop gehandeld wordt en omvat het tijdsbestek waarin het incident verholpen wordt. VfPf gebruikt drie prioriteiten bij incidenten met daarbij een behorende maximale oplostijd.* *Meldingen komen binnen bij VfPf of haar werkplekleverancier en worden vervolgens uitgezet bij de relevante betrokken partijen. Deze afspraken worden in een Operationeel Leveranciers Overeenkomst (OLA) vastgelegd.*

<table>
<tr><td>52.</td><td>Opdrachtnemer draagt zorg voor een incidentbeheerproces met minimaal de onderstaande prioriteiten en reactietijden.
<table>
<tr><td>Priori-teit</td><td>Impact</td><td>Responstijd</td></tr>
<tr><td>1</td><td>Hoge impact: de dienst is niet beschikbaar. Veel klanten of medewerkers worden geraakt door het incident.</td><td>≤ 4 werkuren</td></tr>
<tr><td>2</td><td>Gemiddelde impact: de dienst is beperkt beschikbaar. Een klein aantal klanten of medewerkers wordt geraakt.</td><td>≤ 1 werkdag = 8 werkuren</td></tr>
<tr><td>3</td><td>Kleine impact: de dienst is beschikbaar, maar niet alle functionaliteit is beschikbaar of er is sprake van een acceptabele work around. Een klein aantal klanten of medewerkers wordt geraakt.</td><td>≤ 2 werkdagen = 16 werkuren</td></tr>
</table></td></tr>
<tr><td></td><td><u>Wijzigingsbeheer en Onderhoud</u>
Opdrachtnemer richt een effectief en efficiënt proces in voor wijzigingsbeheer en onderhoud t.b.v. mogelijke maatwerk oplossingen die moeten worden gebouwd voor VfPf. Opdrachtnemer houdt zich daarbij minimaal aan de volgende eisen:</td></tr>
<tr><td>52a.</td><td>Wijzigingen worden tijdig gecommuniceerd en vinden op het afgesproken moment plaats.</td></tr>
<tr><td>52b.</td><td>Voor wijzigingen en nieuwe initiatieven sluit opdrachtnemer aan op het VfPf-wijzigingsproces en de overeengekomen SLA en DAP.</td></tr>
<tr><td>52c.</td><td>Opdrachtnemer stelt na een aanpassing in de inrichting -zodra deze beschikbaar wordt gesteld- de opdrachtgever in staat om een GebruikersAcceptatieTest (GAT) uit te voeren.</td></tr>
<tr><td>52d.</td><td>Opdrachtnemer zorgt ervoor dat een roll back uitgevoerd kan worden als een nieuwe release teruggedraaid moet worden, zodat altijd een goed functionerende tool beschikbaar is.</td></tr>
<tr><td>52e.</td><td>Opdrachtnemer voert een actief life-cycle management uit over de applicatie, wat resulteert in periodieke (minimaal 1x per maand) security patches. Critical security patches worden onmiddellijk uitgevoerd.</td></tr>
<tr><td>52f.</td><td>Opdrachtnemer voert een actief life-cycle management uit over de functionaliteit van de applicatie, wat resulteert in periodieke (minimaal 1x per jaar) functionele updates. Of frequenter indien afgesproken in de SLA.</td></tr>
<tr><td></td><td><u>Onderhoud</u>
Bij onderhoud onderscheidt VfPf drie (3) categorieën, welke hieronder worden toegelicht:

• Standaard onderhoud
Standaard onderhoud bestaat uit vaste periodieke onderhoudsvensters voor regulier (kort) onderhoud aan de applicaties (fixes en small changes). Onderhoudsvensters worden vooraf aangekondigd en alleen uitgevoerd tijdens kantooruren als er geen impact is op de dienstverlening. Uitzonderingen hierop (indien van toepassing) moeten nader worden afgestemd.

• Preventief groot onderhoud
Wordt ingezet voor het aanbrengen van wijzigen en/of installeren van nieuwe versies van applicaties. Deze vorm van onderhoud wordt minimaal 10 werkdagen van tevoren aangekondigd en na toestemming van de opdrachtgever ingepland.</td></tr>
</table>

	• *Correctief spoed onderhoud* *Correctief spoed onderhoud betreft het oplossen van geconstateerde incidenten en problemen. Hiervan wordt zo snel mogelijk vooraf melding van gedaan. De communicatielijnen volgen hierbij de gegeven richtlijn in het Governance model.*
53.	Opdrachtnemer zorgt dat noodzakelijke technisch onderhoud en wijzigingen tijdig zijn afgestemd met de opdrachtgever voorafgaand aan de uitvoering, conform vast te stellen SLA.
	Gebruikers
54.	Vrijelijk overdraagbaar De licenties voor de gebruikers (alle soorten gebruikers) zijn binnen de organisatie vrijelijk overdraagbaar tussen medewerkers van de organisatie zonder dat daar kosten aan verbonden zijn.

	Implementatie
55.	Opdrachtnemer dient binnen zes weken na de definitieve gunning van de dienstverlening een definitief implementatieplan op te stellen en deze ter beoordeling aan opdrachtgever voor te leggen. Opdrachtgever dient akkoord te gaan met dit implementatieplan vóór de start van de werkzaamheden voor de implementatie.
56.	Om de overdracht in goede banen te leiden, stelt opdrachtnemer één ervaren en vaste contactpersoon aan, die de totale opdracht overziet en verantwoordelijk is voor alle activiteiten die tijdens de implementatie- en transitie periode plaatsvinden.
57.	Tijdens implementatie dient een testomgeving beschikbaar te zijn waarop opdrachtgever een uitgebreide controle kan uitvoeren voor livegang.
58.	Tijdens implementatie zal door opdrachtgever worden getest op de eisen gesteld in dit PvE en overige bijlagen. Waar niet wordt voldaan aan het gestelde zal opdrachtnemer kosteloos zorgen voor het aanleveren van oplossingen en/of ondersteunende informatie binnen een daartoe afgesproken tijd.
59.	De implementatie dient binnen uiterlijk 7 maanden (1 september 2025) na akkoord implementatieplan (Fase 1) te zijn afgerond. Fase 2 zal onderling overleg worden afgestemd.

	Einde opdracht
60.	Om het einde van de opdracht (afloop contract of bij vroegtijdige beëindiging) in goede banen te leiden, wordt opdrachtnemer geacht alle medewerking te verlenen die nodig is voor een geruisloze overgang. Op deze manier worden risico's (onder andere verlies van informatie en communicatie) vermeden en worden de activiteiten gerelateerd aan het overgangsproces effectief gemanaged.
61.	Tijdens het overgangsproces is opdrachtnemer verplicht om te blijven voldoen aan de gestelde eisen conform de offerteaanvraag inclusief alle bijlagen waaronder dit Programma van Eisen. De reeds geplande periodieke werkzaamheden dienen tot einddatum uitgevoerd te worden. De reeds geplande opdrachten alsmede de resterende facturen worden afgehandeld. Hier dienen opdrachtnemer en opdrachtgever overeenstemming over te bereiken.

62.	Er is een exit-strategie beschreven in een exitplan die een migratie naar een andere opdrachtnemer en naar de interne ICT-omgeving beschrijft.
63.	Opdrachtnemer is verantwoordelijk voor het opleveren van een exitplan wat ter toetsing wordt voorgelegd aan opdrachtgever, 3 maanden na in productie name van de tool.
64.	De einddatum van de overeenkomst blijft te allen tijde ongewijzigd, ook bij mutaties c.q. wijzigingen blijft`, tenzij dit gebeurt met wederzijdse goedkeuring.

	Privacy en Security
	VfPf heeft een Technisch Security Beleid (zie Bijlage F) opgesteld om een adequaat beveiligingsniveau en zorgvuldige omgang met (persoons)gegevens ten aanzien van de dienstverlening te verzekeren. Deze maatregelen waarborgen tevens dat betrokkenen hun wettelijke rechten kunnen uitoefenen en VfPf aan de daaruit voortvloeiende verplichtingen tegemoet kan komen.
65.	Opdrachtnemer beschikt over het ISO27001 certificaat en de door opdrachtnemer te leveren dienst(verlening) en/of product (zoals omschreven in deze opdracht) is in scope van dit certificaat. Daarnaast heeft opdrachtnemer passende beheersmaatregelen getroffen afkomstig uit de ISO27002, hetgeen blijkt uit de aan het certificaat gekoppelde verklaring van toepasselijkheid. Opdrachtnemer draagt er aantoonbaar zorg voor steeds de nieuwste versies van de ISO-certificeringen te behalen.
66.	Opdrachtnemer voldoet aan de voor het VfPf geldende wet- en regelgeving omtrent privacy en treft daartoe passende technische en organisatorische maatregelen, waarmee in ieder geval voldaan wordt aan de gangbare vormen van data-encryptie en beveiligingsprotocollen. Het OMS is aantoonbaar ingericht dat zij opdrachtgever ondersteunt en in staat stelt om te voldoen aan haar Privacy- & Securitybeleid (zie Bijlage G) en alle relevante wet- en regelgeving. Opdrachtnemer dient dit te kunnen aantonen.
67.	VfPf gebruikt BIV-classificatie, te weten: beschikbaarheid (Continuïteit), integriteit en vertrouwelijkheid. Opdrachtnemer garandeert voldoende maatregelen te treffen om risico's t.a.v. de beschikbaarheid, integriteit en vertrouwelijkheid van de dienstverlening te mitigeren. De BIV-classificatie is opgenomen en kunt u terugvinden in de Verwerkersovereenkomst (zie Bijlage E).
68.	Opdrachtnemer / Verwerker verwerkt alleen persoonsgegevens binnen de Europese Economische Ruimte (EER), Europese Vrijhandelsassociatie(EVA) en Groot-Brittannië.
69.	Het Participatiefonds is verwerkingsverantwoordelijke en de opdrachtnemer is verwerker in de zin van de AVG. Gelet daarop wordt een Verwerkersovereenkomst afgesloten (zie bijlage E). Verwerker is verantwoordelijk en aansprakelijk voor alle subverwerkers die namens Verwerker ingezet worden om deze opdracht te vervullen; aantoonbaar en opvraagbaar worden minimaal dezelfde eisen door Verwerker aan subverwerkers gesteld.

70.	Binnen de scope van de dienstverlening wordt toegang tot persoonsgegevens en overige gevoelige informatie afgeschermd, zodat alleen personen toegang hebben tot informatie die noodzakelijk is voor hun eigen werkzaamheden. De gebruikersaccounts zijn persoonsgebonden. Daarnaast wordt binnen het technisch beheer het volgende afgedwongen: • Functiescheiding: fraudegevoelige processen liggen niet in de hand van één medewerker; • Verificatie: belangrijke administratieve handelingen moeten door een andere medewerker worden beoordeeld en geëffectueerd via het zogenaamde '4-ogen principe'; • Toegang op basis van need-to-know; • Wanneer gebruikers inloggen in de applicatie worden ze geauthentiseerd middels multi-factor authentication. Middels een conditional access policy wordt gecontroleerd of de gebruiker via een geregistreerd apparaat probeert in te loggen. Het beschikbaar stellen van rapportages wordt beveiligd door het onmogelijk te maken de rapportages te downloaden, het onmogelijk te maken de rapportages door te zenden/te versturen en door middel van een tijdslot voor toegang tot die rapportage.
71.	Opdrachtnemer zorgt (blijvend) voor een adequate beveiliging op alle niveaus (fysiek, netwerk, applicaties, firewall, IDS/IPS, ACL, IP-accesslist, etc.) en monitort dagelijkse kwetsbaarheden om zero-day-exploits te voorkomen. Dit betreft in ieder geval: • Opdrachtnemer dient alle niveaus van NCSC-beveiligingsadviezen op te volgen, voor zover deze betrekking hebben op systemen die relevant zijn voor het leveren van de dienstverlening. Specifiek geldt hierbij dat een H /H melding binnen 1 week opgelost te worden. Ook dient over de NCSC-adviezen gerapporteerd te worden, waarbij ook de opvolgingsacties naar aanleiding van deze adviezen worden vermeld; • Het blokkeren van bepaalde e-mails, zoals spam, phishing, e-mailvirussen en malware. Eventuele onterecht tegengehouden e-mails moeten door de Service Desk van Opdrachtnemer weer teruggezet kunnen worden; • Het beveiligen van de internetverbinding tegen alle mogelijke soorten aanvallen gebeurt via IDS, IPS en continue monitoring, bewaking en proactief en reactief beheer bij aanvallen; • Het voorkomen, detecteren, blokkeren en verwijderen van virussen; • Het offline bewaren van back-ups ouder dan een week (i.v.m. mogelijke ransomware); • Handelingen van systeemadministrators en systeemoperators worden vastgelegd en deze zijn niet aanpasbaar; • Alle koppelingen met de SAAS worden beveiligd tegen de laatste stand der techniek, met als uitgangspunt de meest recente versie van ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS); • Alle hiervoor benodigde apparatuur, licenties en dergelijke zijn de verantwoordelijkheid van opdrachtnemer.
72.	Er een up-to-date lijst beschikbaar van de personen die bevoegd zijn om toegang te krijgen tot de systemen die worden ingezet voor het leveren van de gevraagde dienst. Deze lijst dient door opdrachtnemer up-to-date gehouden te worden

73.	Opdrachtgever heeft het recht audits/assessments (waaronder in ieder geval jaarlijks een pentest) te laten uitvoeren op het gebied van informatiebeveiliging en privacy. Hieronder valt tevens minimaal éénmaal per jaar de eigen organisatie auditen op de volgende onderwerpen: A) Beveiliging B) Kwaliteitssysteem. De schriftelijke resultaten van de jaarlijkse audits/assessments worden overlegd en besproken met opdrachtgever. Opdrachtnemer werkt volledig mee aan privacy en securityaudits/-assessments, in welke vorm en op welk moment dan ook. De kosten die hiermee gemoeid zijn komen voor rekening van opdrachtgever.
74.	Opdrachtnemer meldt security gebeurtenissen én security incidenten conform het Incident response plan van VfPf onverwijld maar uiterlijk binnen 24 uur na constatering van een gebeurtenis/incident, aan opdrachtgever en verleent volledige medewerking en deelt alle beschikbare informatie over de gebeurtenis. In het geval van een security incident moet de Opdrachtnemer redelijkerwijs maatregelen treffen om de mogelijk nadelige gevolgen te beperken voortkomend uit het incident (zie Bijlage H).
75.	Daar waar opdrachtnemer cookies inzet gebeurt dit in lijn met de Telecommunicatiewet; eventuele plaatsing van cookies vindt uitsluitend plaats in afstemming met VfPf.
76.	Opdrachtnemer hanteert de volgende principes. ‘Privacy by design’ en ‘default’ staan centraal bij de dienstverlening, en opdrachtnemer hanteert deze waar mogelijk bij de verwerking en bescherming van persoonsgegevensencryptie c.q. versleuteling en pseudonimisering. Voor encryptie geldt als standaard de ‘Handreiking Encryptiebeleid (PKI) voor privacy by design’ versie 2.0 van maart 2019 van de Informatiebeveiligingsdienst. Voor privacy by design geldt als standaard ‘20170507 Handleiding Privacy by Design v3_0 van het CIP (Centrum informatiebeveiliging en privacybescherming).’
77.	Opdrachtnemer dient de gebruikte applicaties en tooling (applicatiestack) up-to-date te houden door tijdige patches en updates toe te passen. Daarnaast moet de aanbieder volledige verantwoordelijk accepteren voor het identificeren en wegnemen van alle securityrisico's binnen een redelijke termijn na ontdekking, om de integriteit en beveiliging van het systeem te waarborgen. Deze termijn moet in overeenstemming zijn met industrienormen en best practices.
78.	Opdrachtnemer moet een privacy- en een securityaanspreekpunt en -verantwoordelijke hebben die in overleg met opdrachtgever testen, beoordelingen en evaluaties van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging reviewt
79.	Binnen de scope van de dienstverlening vindt logging plaats, met als verplichte standaard de set met beheersmaatregelen uit hoofdstuk 12.4 van de ISO27002-norm; voor de verdere invulling en uitwerking van logging is de ‘Handreiking Aanwijzing Logging versie 2.0’ (maart 2019) van de Informatiebeveiligingsdienst verplicht. Bijzondere aandacht verdient logging van bestanden die een audit trail vastleggen.

	Facturatie
80.	Facturatie geschiedt conform (concept)overeenkomst (Bijlage C) en ARBIT (Bijlage D).
81.	Structurele wijzigingen in de omvang dienen direct doorgevoerd te worden in de Overeenkomst. De facturatie dient hier direct op aangepast te worden zodat er geen verrekening hoeft te worden uitgevoerd.
82.	Uitbreiding van de opdracht zal tegen dezelfde tarieven en voorwaarden geschieden als overeengekomen in de overeenkomst.

	Meerwerk Onder meerwerk wordt verstaan een aantoonbare verzwaring of uitbreiding van de door opdrachtnemer te leveren prestatie. Tot meerwerk wordt niet gerekend werkzaamheden die opdrachtnemer redelijkerwijs bij het sluiten van de overeenkomst had kunnen of moeten voorzien en die voor de uitvoering van de overeenkomst redelijkerwijs vereist zijn. Evenmin worden tot meerwerk gerekend werkzaamheden die het gevolg zijn van onjuiste en/of onvolledige specificaties, indien deze door of in opdracht van opdrachtnemer zijn opgesteld of door opdrachtnemer zijn geaccepteerd. Opdrachtnemer toont aan dat er sprake is van meerwerk.
83 .	Indien opdrachtnemer meent dat van meerwerk sprake is, stelt hij de opdrachtgever daarvan zo spoedig mogelijk in kennis. Die kennisgeving kan opdrachtgever aanleiding geven om opdrachtnemer te verzoeken ter zake van dat meerwerk een offerte aan opdrachtgever uit te brengen met de daaraan verbonden tijdsduur en kosten. Opdrachtnemer voert het meerwerk niet eerder uit dan nadat opdrachtgever die offerte schriftelijk heeft aanvaard.
84.	Ter zake van het door opdrachtnemer te verrichten meerwerk gelden de bepalingen van de overeenkomst, waaronder de tarieven, voor zover deze door de aanvullende schriftelijke opdracht, bedoeld in deze eis, niet worden gewijzigd. Opdrachtnemer is niet gerechtigd bij het uitbrengen van een offerte nadere dan wel zwaardere voorwaarden te stellen, tenzij opdrachtgever hiermee instemt.
	Minderwerk Indien door gewijzigde inzichten van opdrachtgever of door wijziging van de voor de te verrichten diensten van belang zijnde wettelijke voorschriften, de werkzaamheden die opdrachtnemer op grond van de overeenkomst moet verrichten, aantoonbaar worden verlicht dan wel verminderd, is er sprake van minderwerk.
85.	Indien er van minderwerk sprake is, zal opdrachtgever opdrachtnemer daarvan zo spoedig mogelijk schriftelijk op de hoogte stellen. Opdrachtnemer is tevens verplicht minderwerk maandelijks te melden bij opdrachtgever.