Programma van Eisen

Dataverduurzaming Fileshares

Opdrachtnummer 25024 | Gemeente Apeldoorn | 3 november 2026

Inhoudsopgave

Inhoudsopgave 2

1 Aanleiding en probleemstelling 3

1.1 Probleemcontext 3

1.2 Kernprobleem 3

1.3 Urgentie 3

2 Leeswijzer en gebruik van dit document 3

3 Governance en organisatie 3

3.1 Inrichting van de besluitvorming 3

3.2 Ondersteuning van de organisatie 4

4 Proceseisen, uitvoering van de werkzaamheden 4

5 Fase 1: Clean 4

6 Fase 2: Structured 5

7 Fase 3: Sustainable 5

8 Duurzame raadpleegomgeving 6

9 Validatie en gebruikersinteractie 6

10 Eisen architectuur en technische randvoorwaarden 6

11 Eisen data 7

12 Eisen gegevensbescherming en AVG 7

13 Eisen informatiebeveiliging 8

14 Eisen contract en leveranciersmanagement 15

15 Eisen beheer en support 15

16 Implementatie, kennisoverdracht en borging 15

17 Bijlage A: Begrippenlijst 16

1 Aanleiding en probleemstelling

1.1 Probleemcontext

Gemeente Apeldoorn staat midden in een digitale transformatie die hoge eisen stelt aan de veiligheid, wendbaarheid en betrouwbaarheid van de informatievoorziening. Binnen de gemeentelijke organisatie (ruim 2.000 medewerkers) bevinden zich omvangrijke, historisch gegroeide Netwerkschijven die jarenlang zijn gebruikt als informele archieflocatie.

De omvang van de te verwerken data is beschreven in het Beschrijvend Document dat bij deze aanbesteding hoort.

1.2 Kernprobleem

De gemeente beschikt onvoldoende over integraal, reproduceerbaar en aantoonbaar inzicht in: de aard en inhoud van informatie op de Netwerkschijven; de archiefstatus en archiveringswaarde van documenten; de toepasselijke Bewaartermijnen en vernietigingsverplichtingen; de mate van duplicatie en versievorming; en de aanwezigheid van privacygevoelige informatie (PII). Hierdoor is de organisatie onvoldoende aantoonbaar in control ten aanzien van de Woo, de Archiefwet en de AVG.

1.3 Urgentie

Het langer bewaren van data dan wettelijk noodzakelijk vergroot het risico op datalekken, onrechtmatige inzage en misbruik van privacygevoelige informatie, met mogelijke boetes van de Autoriteit Persoonsgegevens als gevolg. Bovendien vergroot het bewaren van overbodige informatie de reikwijdte van Woo-verzoeken en de kans op reputatieschade bij onbedoelde openbaarmaking van vertrouwelijke of achterhaalde gegevens.

Tegelijkertijd leidt de huidige situatie tot een afname van de toegankelijkheid en vindbaarheid van informatie, waardoor het moeilijker wordt om informatie tijdig en volledig te ontsluiten voor bedrijfsvoering, besluitvorming en Woo-verzoeken.

Daarnaast bevindt zich op de Netwerkschijven informatie die op grond van de Selectielijst gemeenten en intergemeentelijke organen blijvend te bewaren is. Deze informatie wordt momenteel niet structureel beheerd conform archiefvereisten en dient duurzaam en geordend te worden gearchiveerd en, waar van toepassing, overgebracht te worden naar het e-depot.

2 Leeswijzer en gebruik van dit document

Dit Programma van Eisen (PvE) beschrijft de minimumeisen waaraan de ICT-prestatie en de Opdrachtnemer moeten voldoen.

Eisen zijn knock-outcriteria. Inschrijvers beantwoorden elke eis met Ja of Nee. Een Nee leidt tot uitsluiting.

Begrippen die in dit document met een Hoofdletter worden geschreven, zijn gedefinieerd in Bijlage A, Begrippenlijst. Zie inhoudsopgave.

3 Governance en organisatie

De onderstaande eisen richten zich op de inrichting van de besluitvorming, de rolverdeling en de ondersteuning die Opdrachtnemer daarbij levert.

Uitgangspunt is dat governance niet wordt uitbesteed. Het mandaat, het eigenaarschap en de besluiten blijven bij Opdrachtgever. Opdrachtnemer levert het proces, de sjablonen en de begeleiding; Opdrachtgever stelt vast en beslist.

3.1 Inrichting van de besluitvorming

Nr.	Eis	Ja/Nee
GOV-E01	Opdrachtnemer levert bij aanvang een voorstel voor de projectgovernance waarin is uitgewerkt welke besluiten in het traject genomen moeten worden, wie die neemt, op basis van welk mandaat, in welk ritme en langs welk escalatiepad bij uitblijvende besluitvorming. Opdrachtgever stelt dit vast.	

Nr.	Eis	Ja/Nee
GOV-E02	Opdrachtnemer heeft geen zelfstandig mandaat over inhoudelijke besluiten inzake classificatie, migratie, bewaring en vernietiging. Opdrachtnemer doet voorstellen; Opdrachtgever beslist.	
GOV-E03	Opdrachtnemer ondersteunt bij het inrichten van de mandaatlijn rond bewaring, archivering en vernietiging: wie beslist, wie adviseert, wie tekent, en op welk moment de gemeentearchivaris wordt betrokken.	
GOV-E04	Opdrachtnemer rapporteert periodiek over de voortgang van de besluitvorming: welke besluiten openstaan, bij wie, en sinds wanneer.	

3.2 Ondersteuning van de organisatie

Nr.	Eis	Ja/Nee
GOV-E05	Opdrachtnemer begeleidt de proceseigenaren en informatiebeheerders bij de inhoudelijke beoordeling van hun eigen informatie, in de vorm van sessies of werkbijeenkomsten per organisatieonderdeel.	
GOV-E06	~~Opdrachtnemer biedt de ondersteuning modulair aan en prijst de varianten afzonderlijk, zodat Opdrachtgever per fase kan kiezen tussen volledige uitvoering door Opdrachtnemer, gezamenlijke uitvoering, of uitsluitend advies en projectbegeleiding.~~ **(VERVALT)**	
GOV-E07	Indien Opdrachtnemer gebruikmaakt van AI-functionaliteit, AI-modellen of AI-ondersteunde technieken binnen de ICT-prestatie of de dienstverlening, meldt Opdrachtnemer dit voorafgaand aan de inzet aan Opdrachtgever.	
GOV-E08	Opdrachtnemer organiseert een periodieke evaluatie waarin de werkwijze op basis van praktijkervaring wordt bijgesteld, en legt de uitkomsten vast.	

4 Proceseisen, uitvoering van de werkzaamheden

De onderstaande eisen hebben betrekking op de wijze waarop Opdrachtnemer de werkzaamheden uitvoert: het plan van aanpak, de fasering, de rapportage en de eindoplevering.

Nr.	Eis	Ja/Nee
PRO-E01	Opdrachtnemer voert alle werkzaamheden uit op basis van een vooraf goedgekeurd plan van aanpak, waarin aanpak, planning, rollen, risico's en controlemomenten zijn opgenomen. Het plan van aanpak wordt uiterlijk twee weken na gunning ter goedkeuring voorgelegd aan Opdrachtgever.	
PRO-E02	Opdrachtnemer stelt per verwerkingseenheid een deelplan op met planning, freeze-moment en de benodigde inzet van Opdrachtgever, en legt dit ter goedkeuring voor.	
PRO-E03	Opdrachtnemer rapporteert minimaal tweewekelijks aan de projectgroep Woo InfoOpOrde over voortgang, verwerkte volumes, toegepaste classificaties, bevindingen en gesignaleerde risico's. Rapportageformaat en overlegvorm worden bij aanvang schriftelijk vastgelegd.	
PRO-E04	Opdrachtnemer wijst één vast aanspreekpunt aan voor de gehele opdracht.	
PRO-E05	Opdrachtnemer levert uiterlijk binnen één maand na afronding van de opdracht een Opleverpakket op, bestaande uit ten minste: eindrapportages, Auditlogs, Metadataoverzichten, Vernietigingslijsten en een Overdrachtsdocument. Het Overdrachtsdocument beschrijft de uitgevoerde werkzaamheden, gehanteerde uitgangspunten en resterende aandachtspunten zodat Opdrachtgever zelfstandig kan voortgaan.	

5 Fase 1: Clean

De onderstaande eisen gaan verder in op het beschrijvend document, onderdeel 4.3.2 K1 Fase 1, Clean.

Nr.	Eis	Ja/Nee
OPS-E01	Een vernietigingslijst wordt vooraf opgeleverd in een open formaat en bevat per post ten minste: afdeling, periode, omschrijving, aantal bestanden, omvang, categorie en de onderbouwing van de vernietigingsgrond.	
OPS-E02	Van elke vernietigingsactie wordt een verslag opgesteld dat aantoont welke informatie op welke grond en met wiens goedkeuring is vernietigd.	
OPS-E03	De ICT-prestatie voert een initiële Scan uit van alle binnen Scope vallende Netwerkschijven.	

6 Fase 2: Structured

De onderstaande eisen gaan verder in op het beschrijvend document, onderdeel 4.3.2 K2 Fase 2, Structured.

Nr.	Eis	Ja/Nee
CLA-E01	De ICT prestatie classificeert de bestanden op basis van vigerende wetgeving, waaronder archiefwet, AVG en Woo	
CLA-E02	De ICT prestatie classificeert de bestanden met een bewaartermijn op basis van in ieder geval de Selectielijst Gemeenten en het vastgestelde bewaarbeleid van Opdrachtgever.	
CLA-E03	De ICT prestatie maakt voor iedere classificatie inzichtelijk op basis van welke metadata, inhoudelijke kenmerken, regels of modellen deze tot stand is gekomen.	
CLA-E04	Opdrachtnemer voert een statistisch onderbouwde validatie uit op de classificatieresultaten. Omvang en methodiek van de steekproef worden vooraf ter goedkeuring voorgelegd. De steekproef omvat minimaal alle hoog-risicocategorieën, waaronder vernietiging, archiefwaardige informatie en privacygevoelige informatie, en is aantoonbaar representatief. De resultaten worden schriftelijk gerapporteerd en bevatten ten minste de gehanteerde steekproefmethode, de classificatienauwkeurigheid, de geconstateerde foutpercentages, de verbetermaatregelen en de betrouwbaarheid van de uitkomsten.	
CLA-E05	De ICT prestatie maakt vooraf inzichtelijk welke categorieën in aanmerking komen voor bulkverwerking, welke voor steekproefsgewijze controle en welke voor verplichte menselijke beoordeling.	
CLA-E06	De ICT-prestatie kan het bestand verrijken met ten minste de volgende metadata: unieke identificatie, herkomst en oorspronkelijke locatie, eigenaar, afdeling, documenttype, Bewaartermijn, vertrouwelijkheid, juridische grondslag en de onderbouwing van de classificatie.	
CLA-E07	De ICT-prestatie metadateert conform het MDTO metadataschema voor overheidsarchieven.	
CLA-E08	De ICT-prestatie ondersteunt het opnieuw classificeren van Informatieobjecten indien classificatieregels of wettelijke kaders wijzigen.	

7 Fase 3: Sustainable

De onderstaande eisen gaan verder in op het beschrijvend document, onderdeel 4.3.2 K3 Fase 3, Sustainable.

Nr.	Eis	Ja/Nee
MIG-E01	Migratie van informatie vindt plaats conform de door Opdrachtgever vastgestelde Informatiearchitectuur. Opdrachtnemer levert daarbij een migratieplan en een verklaring van migratie.	
MIG-E02	Opdrachtnemer levert een migratiebestemmingenmatrix waarin bestandscategorieën zijn gekoppeld aan de doelomgevingen: samenwerkingsomgeving, ~~vakapplicatie,~~ zaaksysteem, duurzame raadpleegomgeving of vernietiging.	
MIG-E03	Vóór de migratie van een verwerkingseenheid voert Opdrachtnemer een proefmigratie uit. Migratie start pas na goedkeuring van Opdrachtgever.	
MIG-E04	Bij migratie blijven Metadata en herkomstgegevens behouden en is per Informatieobject herleidbaar wat de oorspronkelijke locatie was.	

Nr.	Eis	Ja/Nee
MIG-E05	Na elke migratie levert Opdrachtnemer een controlerapport op waarin documentaantallen, Metadata en bestandsintegriteit tussen bron en doel worden vergeleken, inclusief de geconstateerde afwijkingen.	
MIG-E06	De ICT-prestatie doet op basis van de classificaties per bestand een voorstel voor doelbestemming	
MIG-E07	Er blijft geen restcategorie of grijs gebied achter: elke map, elk bestand en elk dossier krijgt een doelbestemming.	

8 Duurzame raadpleegomgeving

Deze eis(en) vraagt/vragen om advies voor een duurzame raadpleeg omgeving.

Nr.	Eis	Ja/Nee
DRO-E01	Opdrachtnemer adviseert in een duurzame tijdelijke raadpleegomgeving voor informatie die niet vernietigd mag worden maar niet in de overige doelcategorieën past, zodat deze doorzoekbaar en raadpleegbaar zijn.	

9 Validatie en gebruikersinteractie

De onderstaande eisen beschrijven hoe medewerkers van Opdrachtgever de voorstellen van de ICT-prestatie beoordelen en accorderen.

Nr.	Eis	Ja/Nee
VAL-E01	Menselijke validatie door Opdrachtgever vindt plaats vóór elke onomkeerbare handeling: vernietiging, verplaatsing, herstructurering en definitieve metadatatoekenning.	
VAL-E02	Medewerkers kunnen via de ICT-prestatie opschoningsvoorstellen annoteren, beoordelen en accepteren of afkeuren.	

10 Eisen architectuur en technische randvoorwaarden

De onderstaande eisen beschrijven waar en hoe de ICT-prestatie wordt ingezet, hoe toegang tot de Netwerkschijven en de doelomgevingen wordt verkregen, en welke voorzieningen Opdrachtgever daarvoor beschikbaar stelt.

Nr.	Eis	Ja/Nee
ARC-E01	Opdrachtnemer houdt zich bij de technische uitvoering van de ICT Prestatie aan de technische kaders en randvoorwaarden die zijn opgenomen in hoofdstuk 1.4 van het Beschrijvend Document bij deze aanbesteding.	
ARC-E02	Opdrachtnemer beschrijft welke rekencapaciteit de verwerking vraagt en waar deze wordt geleverd. Indien de verwerking rekencapaciteit binnen de omgeving van Opdrachtgever gebruikt, geeft Opdrachtnemer aan welke servercapaciteit daarvoor nodig is; indien de verwerking schaalbare rekencapaciteit in een tenant van Opdrachtgever gebruikt~~, geeft Opdrachtnemer de verwachte kosten daarvan op.~~	
ARC-E03	Indien de verwerking op infrastructuur van Opdrachtgever draait, specificeert Opdrachtnemer de minimale serverconfiguratie en de verwachte doorlooptijd per hoeveelheid data, zodat Opdrachtgever de benodigde capaciteit tijdig kan inrichten.	
ARC-E04	De ICT-prestatie biedt mogelijkheden voor throttling, planning, prioritering en gefaseerde verwerking van bestanden zodat netwerk-, opslag- en servercapaciteit beheerst kunnen worden gebruikt.	

11 Eisen data

De onderstaande eisen beschrijven hoe de ICT-prestatie omgaat met data-eigenaarschap, opslag en uitwisselbaarheid.

Nr.	Eis	Ja/Nee
DAT-E01	Alle data die in het kader van deze opdracht wordt verwerkt, valt uitsluitend onder de zeggenschap van Gemeente Apeldoorn. Opdrachtnemer verwerkt deze data uitsluitend in opdracht van Opdrachtgever en heeft geen zelfstandig gebruiksrecht. Opdrachtnemer verleent op eerste verzoek volledige medewerking aan overdracht, export of verwijdering van alle data.	
DAT-E02	De ICT-prestatie ondersteunt export in open standaarden, ten minste CSV, XML en JSON.	
DAT-E03	Opdrachtnemer werkt mee aan opname en actualisatie van AI-toepassingen in het AI-register van Gemeente Apeldoorn en verstrekt gedurende de looptijd van de overeenkomst tijdig alle relevante informatie en wijzigingen die nodig zijn voor registratie, toezicht en naleving van toepasselijke wet- en regelgeving.	

12 Eisen gegevensbescherming en AVG

De onderstaande eisen hebben betrekking op de verwerking van Persoonsgegevens en de naleving van de AVG gedurende de gehele opdracht.

Nr.	Eis	Ja/Nee
AVG-E01	Indien Opdrachtnemer persoonsgegevens verwerkt als Verwerker van Opdrachtgever, de Verwerkingsverantwoordelijke, gaat Opdrachtnemer akkoord met het sluiten van de standaard Verwerkersovereenkomst van de Vereniging Nederlandse Gemeenten (VNG), de standaard Verwerkersovereenkomst van de Vereniging Nederlandse Gemeenten (VNG) inzake Avg-Wpg of de standaardovereenkomst Modelovereenkomst voor gezamenlijke verantwoordelijken (VNG), indien de Opdrachtgever dit verzoekt op basis van de feitelijke situatie. Van deze standaardovereenkomst wordt niet afgeweken dan na schriftelijke instemming van Opdrachtgever.	
AVG-E02	Opdrachtnemer draagt zorg voor de naleving van beroepscodes en een geheimhoudingsplicht van al het voor de gemeente Apeldoorn ingezette personeel en organisaties.	
AVG-E03	Opdrachtnemer verleent volledige medewerking aan de uitvoering van een DPIA en verstrekt daartoe alle noodzakelijke informatie aan Opdrachtgever.	
AVG-E04	Persoonsgegevens onder de verantwoordelijkheid van Opdrachtgever worden gescheiden opgeslagen van gegevens van andere klanten van Opdrachtnemer.	
AVG-E05	Opdrachtnemer verwerkt Persoonsgegevens uitsluitend voor de doeleinden die zijn overeengekomen met Opdrachtgever (Doelbinding).	
AVG-E06	Zodra Persoonsgegevens niet langer nodig zijn voor de overeengekomen verwerkingsdoeleinden wist Opdrachtnemer deze Persoonsgegevens binnen een maand (31 dagen) na het einde van de dienstverlening.	
AVG-E07	Gegevens van Opdrachtgever worden niet gebruikt voor het trainen of hertrainen van AI-modellen.	
AVG-E08	Opdrachtnemer overhandigt privacydocumentatie aan Opdrachtgever, zoals een actueel privacybeleid, een actuele privacyverklaring, en genomen maatregelen ter beveiliging van persoonsgegevens	
AVG-E09	De ICT-prestatie voldoet aantoonbaar aan de principes van Privacy by Design en Privacy by Default.	
AVG-E10	De ICT-prestatie is in staat (bijzondere) Persoonsgegevens, financiële gegevens, BSN-nummers en strafrechtelijke gegevens te herkennen en te signaleren en deze vervolgens te rapporteren aan Opdrachtgever in een overzicht, bijvoorbeeld via een Excel-bestand of ander gangbaar bestandsformaat, zodat Opdrachtgever deze kan beoordelen.	
AVG-E11	Het is mogelijk om in de ICT-prestatie meerdere/verschillende bewaartermijnen in te richten	
AVG-E12	Het is mogelijk om persoonsgegevens te vernietigen uit de ICT-prestatie, automatisch dan wel handmatig, conform de Archiefwet	

13 Eisen informatiebeveiliging

De onderstaande eisen beschrijven de minimale beveiligingsvereisten voor de ICT-prestatie en de Opdrachtnemer.

Nr.	Eis	Ja/Nee
IB-E01	Zeggenschap en verwerkingslocatie van informatie Opdrachtnemer dient de aangeboden dienstverlening en bijbehorende tooling zodanig in te richten dat Opdrachtgever te allen tijde de volledige zeggenschap behoudt over de door de Opdrachtgever beschikbaar gestelde informatie en de daarvan afgeleide gegevens, waaronder begrepen metadata, classificaties, analyseresultaten, logs en rapportages. De inhoudelijke gegevens van Opdrachtgever mogen uitsluitend worden verwerkt binnen een door Opdrachtgever aangewezen en door Opdrachtgever beheerste verwerkingsomgeving. Verwerking buiten deze omgeving, waaronder opslag, analyse, indexering, verwerking door AI-/ML-diensten of doorgifte aan externe cloud- of SaaS-diensten, is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van Opdrachtgever. De ICT-prestatie dient daarom bij voorkeur te kunnen functioneren zonder dat de brongegevens naar een externe cloudomgeving hoeven te worden gekopieerd of verplaatst. Het moet mogelijk zijn de tooling binnen de infrastructuur van de opdrachtgever te plaatsen of deze rechtstreeks op de bestaande opslagomgeving te laten werken, bijvoorbeeld door middel van een lokaal geïnstalleerde component, appliance of agent. Eventuele technische gegevens die noodzakelijkerwijs buiten de omgeving van de opdrachtgever worden verwerkt, dienen vooraf expliciet te worden gespecificeerd, waarbij Opdrachtnemer de aard, locatie, doeleinden, bewaartermijn en betrokken derden beschrijft. Opdrachtgever behoudt gedurende en na afloop van de opdracht het recht en de technische mogelijkheid om de verzamelde en gegenereerde gegevens zelfstandig te beheren, te exporteren, te verwijderen en – voor zover de licentievoorwaarden dit toestaan – de tooling zelfstandig voort te zetten.	
IB-E02	Continuïteit en zelfstandig gebruik De ICT-prestatie dient na beëindiging van de dienstverlening door Opdrachtgever zelfstandig te kunnen worden gebruikt voor het raadplegen, analyseren, classificeren en beheren van de tijdens de opdracht opgebouwde informatie en resultaten, zonder dat hiervoor structurele afhankelijkheid bestaat van Opdrachtnemer of diens dienstverlening, tenzij dit door Opdrachtgever uitdrukkelijk is geaccepteerd. Alle voor zelfstandig gebruik noodzakelijke configuraties, classificaties, metadata, rapportages, beslisregels, koppelingen en overige gegevens dienen in een gedocumenteerd en gangbaar formaat aan de opdrachtgever beschikbaar te worden gesteld.	
IB-E03	IB-ALG-001 - Algemeen (governance) - Actieve samenwerking Opdrachtnemer werkt gedurende de volledige levenscyclus van de ICT-prestatie actief samen met Opdrachtgever aan het beheersen en continu verbeteren van de informatiebeveiliging. Opdrachtnemer informeert Opdrachtgever tijdig en proactief over relevante risico's, kwetsbaarheden, dreigingen, afhankelijkheden, wijzigingen en verbetermogelijkheden die van invloed kunnen zijn op de beveiliging of continuïteit van de dienstverlening. Opdrachtnemer denkt actief mee over passende beheersmaatregelen, ondersteunt Opdrachtgever bij het maken van afgewogen beveiligingskeuzes en spant zich aantoonbaar in om beveiligingsvraagstukken in onderling overleg op te lossen, met behoud van de overeengekomen verantwoordelijkheidsverdeling tussen partijen.	
IB-E04	IB-ALG-002 - Algemeen (governance) - Blijvende compliance Opdrachtnemer zorgt ervoor dat de ICT-prestatie gedurende de gehele contractperiode blijft voldoen aan alle overeengekomen beveiligingseisen en dat afwijkingen aantoonbaar worden hersteld.	

Nr.	Eis	Ja/Nee
IB-E05	IB-ALG-003 - Algemeen (governance) - ISMS verplichting Opdrachtnemer heeft een aantoonbaar ingericht Information Security Management System (ISMS), gebaseerd op een erkend normenkader (bijv. ISO/IEC 27001 of gelijkwaardig), waarmee technische en organisatorische maatregelen structureel worden beheerd en verbeterd. De werking van het ISMS wordt periodiek beoordeeld door een onafhankelijke auditor, waarvan de resultaten op verzoek van Opdrachtgever beschikbaar worden gesteld.	
IB-E06	IB-ALG-004 - Algemeen (governance) - Overlap, samenhang en verantwoordelijkheden Alle relevante eisen binnen dit kader gelden in onderlinge samenhang voor de onderdelen van de ICT-prestatie, dienstverlening en infrastructuur waarvoor Opdrachtnemer op grond van de overeenkomst verantwoordelijk is. Domeinspecifieke en aanvullende eisen vervangen generieke eisen niet, maar concretiseren of versterken deze waar zij hetzelfde beveiligingsdoel betreffen. Opdrachtnemer blijft gedurende de gehele contractperiode verantwoordelijk voor het voldoen aan de beveiligingseisen voor alle onderdelen waarvoor hij verantwoordelijk is. Indien de uitvoering van een beveiligingsmaatregel afhankelijk is van een onderdeel dat onder verantwoordelijkheid van Opdrachtgever of een derde valt, maakt Opdrachtnemer deze afhankelijkheid en de bijbehorende verantwoordelijkheidsverdeling voorafgaand aan de implementatie aantoonbaar inzichtelijk. Bij overlap gelden de volgende uitgangspunten: - generieke eisen blijven van toepassing; - aanvullende of domeinspecifieke eisen concretiseren of versterken de generieke eisen; - productspecifieke eisen vullen generieke eisen aan voor zover deze relevant zijn voor de betreffende ICT-prestatie; - een specifiekere eis prevaleert boven een generieke eis indien beide betrekking hebben op hetzelfde beveiligingsdoel en dezelfde situatie; - tegenstrijdigheden of afwijkingen worden voorafgaand aan implementatie schriftelijk met Opdrachtgever afgestemd.	
IB-E07	IB-ALG-005 - Algemeen (governance) - Gegevenseigendom Opdrachtgever behoudt gedurende de volledige levenscyclus van de ICT-prestatie de zeggenschap over alle gegevens die in het kader van de dienstverlening worden verstrekt, verwerkt, gegenereerd of opgeslagen. Opdrachtnemer verkrijgt uitsluitend die rechten die noodzakelijk zijn voor de uitvoering van de overeengekomen dienstverlening en verwerkt gegevens uitsluitend overeenkomstig de schriftelijke instructies van Opdrachtgever en de overeengekomen doeleinden. Opdrachtnemer erkent dat verwerking van gegevens in opdracht niet leidt tot overdracht van eigendom, zeggenschap, intellectuele eigendomsrechten of zelfstandige gebruiksrechten aan Opdrachtnemer, tenzij dit uitdrukkelijk en schriftelijk is overeengekomen.	
IB-E08	IB-ALG-006 - Algemeen (governance) - Baseline Informatiebeveiliging Overheid Opdrachtnemer levert een ICT-prestatie die zodanig is ontworpen, ingericht en onderhouden dat Opdrachtgever kan voldoen aan de Baseline Informatiebeveiliging Overheid (BIO2), voor zover van toepassing op de aard en de risicoklasse van de dienstverlening. Opdrachtnemer is verantwoordelijk voor het identificeren en implementeren van passende beveiligingsmaatregelen binnen zijn eigen domein, die in lijn zijn met de BIO2 en gangbare informatiebeveiligingsstandaarden (zoals ISO/IEC 27001/27002).	
IB-E09	IB-ALG-010 - Algemeen (governance) - Beveiligingsniveau Opdrachtnemer informeert Opdrachtgever tijdig over ontwikkelingen, wijzigingen, kwetsbaarheden of afhankelijkheden die invloed kunnen hebben op het vastgestelde beveiligingsniveau.	
IB-E10	IB-AUD-002 - Auditing - Auditeerbaarheid Opdrachtnemer stelt Opdrachtgever in staat om zelfstandig autorisaties, uitzonderingen en effectieve toegangsrechten zelfstandig te raadplegen, beoordelen en auditen.	

Nr.	Eis	Ja/Nee
IB-E11	IB-CRY-003 - Cryptografie - Certificaten algemeen Certificaten passen binnen een vooraf vastgesteld en beheerd vertrouwensmodel, waarin minimaal is vastgelegd welke certificaatautoriteiten worden vertrouwd, welke certificaatketens worden geaccepteerd, welke identiteiten toegang mogen verkrijgen en hoe certificaatbeheer gedurende de levenscyclus wordt uitgevoerd. Voor authenticatie van servers, diensten en systemen worden certificaten toegepast die: - een valide en controleerbare identiteit van de server, dienst, applicatie, domein of organisatie waarvoor zij worden gebruikt bevatten; - een eenduidige en controleerbare identiteit bevatten (niet anoniem); - binnen een vooraf vastgesteld en beheerd vertrouwensmodel passen. Opdrachtnemer ondersteunt certificaten die zijn uitgegeven door: - het PKI-systeem van Opdrachtgever; en/of - door Opdrachtgever goedgekeurde en vertrouwde certificaatautoriteiten; en/of - een gelijkwaardig, aantoonbaar veilig PKI-model. Voor communicatie met inwoners, burgers of andere externe partijen wordt gebruikgemaakt van certificaten uitgegeven door een publiek vertrouwde certificaatautoriteit. Waar de toepassing en de risicoklasse dit vereisen, wordt gebruikgemaakt van PKIoverheid of een gelijkwaardig gekwalificeerd vertrouwensmodel.	
IB-E12	IB-CRY-004 - Cryptografie - Certificaatinfrastructuur en trustmodel Indien integratie met het PKI-systeem van Opdrachtgever niet mogelijk is, wordt een alternatieve certificaatinfrastructuur toegepast die: - geen self-signed (dus zonder tussenkomst van een CA) certificaten gebruikt voor externe communicatie of productiecomponenten binnen het primaire vertrouwensmodel, tenzij expliciet overeengekomen met Opdrachtgever; - gebruikmaakt van expliciet beheerde trust anchors; - certificaatuitgifte, vervanging, rotatie en intrekking ondersteunt; - gebruikmaakt van beheerde certificaatketens; - aantoonbaar voldoet aan gangbare beveiligingsstandaarden en best practices. Opdrachtnemer legt het gebruikte trustmodel, de toegepaste certificaatautoriteiten en relevante certificaatketens op verzoek ter beoordeling voor aan Opdrachtgever. Beveiligde communicatie door middel van versleuteling en sterke authenticatie is verplicht voor alle relevante gegevensuitwisseling. Het is niet toegestaan om parallelle of alternatieve onbeveiligde communicatiekanalen te gebruiken voor dezelfde functionaliteit, tenzij vooraf schriftelijk overeengekomen met Opdrachtgever.	

Nr.	Eis	Ja/Nee
IB-E13	IB-CRY-005 - Cryptografie - Clientcertificaten en mutual TLS (mTLS) Voor machine-to-machine en service-to-service communicatie waarbij clientauthenticatie vereist is, wordt mutual TLS (mTLS) toegepast met clientcertificaten die: - niet self-signed (zonder tussenkomst van een CA) zijn; - zijn uitgegeven door het PKI-systeem van Opdrachtgever (voorkeur); - zijn uitgegeven door een door Opdrachtgever expliciet goedgekeurde certificaatautoriteit; - passen binnen het overeengekomen trustmodel; - voorzien in unieke identificatie van de betreffende applicatie, service of entiteit waar nodig voor traceerbaarheid en toegangscontrole. Clientcertificaten bevatten de juiste gebruiksdoeleinden, waaronder Client Authentication (Extended Key Usage), indien van toepassing. Clientcertificaten voldoen aan actuele cryptografische standaarden, waaronder passende: - sleutelgroottes; - hashing-algoritmen; - cryptografische parameters. Opdrachtnemer deelt private keys nooit tussen applicaties, organisaties of omgevingen. Private keys blijven te allen tijde uniek per certificaat en worden uitsluitend gebruikt binnen de context waarvoor zij zijn gegenereerd. Het delen of exporteren van private keys is niet toegestaan.	
IB-E14	IB-DAT-001 - Gegevensbescherming - Relevante richtlijnen Beveiligingsmaatregelen worden gedurende de volledige levenscyclus toegepast, periodiek geëvalueerd en voortdurend aangepast aan actuele risico's, dreigingen en relevante standaarden en richtlijnen. Richtlijnen van het NCSC, Forum Standaardisatie en Open Web Application Security Project (OWASP) zijn hierbij normstellend.	
IB-E15	IB-DAT-003 - Gegevensbescherming - Gegevensbescherming algemeen Opdrachtnemer beschermt alle gegevens die onderdeel uitmaken van de ICT-prestatie, waaronder (persoons)gegevens, configuratiegegevens, loggegevens, metadata, back-ups en (persoons)gegevens in niet-productieomgevingen, met passende technische en organisatorische maatregelen tegen verlies, ongeautoriseerde toegang, wijziging, openbaarmaking en vernietiging tijdens gebruik ("data in use"), tijdens transport ("data in motion") en tijdens opslag ("data at rest"), rekening houdend met aard, gevoeligheid, kritikaliteit en de risicoklasse van de dienstverlening.	
IB-E16	IB-DEV-001 - Development - Security by design Opdrachtnemer ontwikkelt, beheert en onderhoudt alle softwarecomponenten (front-end, back-end, API's en ondersteunende componenten) volgens algemeen geaccepteerde kwaliteits- en beveiligingsprincipes (stand van de techniek). Alle betrokken systeemcomponenten zijn zodanig ontworpen en ingericht dat zij de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens ondersteunen.	
IB-E17	IB-DEV-003 - Development - Dependency en third-party risico's Opdrachtnemer beheert en controleert afhankelijkheden van externe softwarecomponenten en softwarelibraries op kwetsbaarheden gedurende de gehele levenscyclus.	
IB-E18	IB-DEV-004 - Development - SBOM Opdrachtnemer stelt op verzoek een Software Bill of Materials (SBOM) beschikbaar voor de ICT-prestatie.	
IB-E19	IB-DEV-005 - Development - Beheer van kwetsbaarheden Opdrachtnemer zorgt ervoor dat geïdentificeerde kwetsbaarheden worden geclassificeerd en binnen redelijke termijnen worden verholpen op basis van ernst.	
IB-E20	IB-DEV-008 - Development - Geen hardgecodeerde toegangsgegevens Opdrachtnemer zorgt ervoor dat geheimen zoals wachtwoorden, security-keys en certificaten niet hardgecodeerd worden opgeslagen, in broncode of elders.	

Nr.	Eis	Ja/Nee
IB-E21	IB-IAM-002 - Identity & Access - Multi-factor authenticatie Indien de ICT-prestatie kan worden gekoppeld aan het federatief identity platform van Opdrachtgever, waaronder SAML 2.0 en/of OpenID Connect via Microsoft Entra ID of een gelijkwaardig platform, wordt authenticatie volledig via dit federatieve mechanisme uitgevoerd, inclusief afdwinging van MFA via Conditional Access policies van Opdrachtgever. Indien koppeling met het federatieve identity platform van Opdrachtgever niet mogelijk is, ondersteunt Opdrachtnemer een zelfstandige authenticatievoorziening die voldoet aan ten minste: - MFA op basis van “iets dat de gebruiker heeft”; - gebruik van een in de markt gangbare authenticator-app (TOTP of gelijkwaardig), of een sterker mechanisme; - verplichte toepassing van MFA voor alle externe en beheertoegang; - geen mogelijkheid tot single-factor authenticatie voor externe toegang; - gebruikers- en beheerdershandelingen zijn op persoon herleidbaar. Ongeacht het gekozen authenticatiemechanisme wordt MFA toegepast op: - alle beheerfuncties; - alle externe toegang; - alle administratieve accounts; - alle toegang via onvertrouwde netwerken. De ICT-prestatie bevat geen alternatieve toegangswegen, backdoors of interne authenticatiemechanismen die de in deze eis gestelde MFA-vereisten kunnen omzeilen, ongeacht rol, interface of integratievorm.	
IB-E22	IB-IAM-004 - Identity & Access - Role-Based Access Control Opdrachtnemer zorgt ervoor dat Opdrachtgever alle autorisaties in kan richten op basis van "role-based access control" (RBAC) en de principes "least privilege" en "need-to-know" toe kan passen.	
IB-E23	IB-IAM-005 - Identity & Access - Account lifecycle management Opdrachtnemer zorgt ervoor dat Opdrachtgever alle accounts uniek, herleidbaar en levenscyclus-gestuurd kan beheren (aanmaak, wijziging, intrekking), inclusief logging van alle wijzigingen.	
IB-E24	IB-IAM-006 - Identity & Access - Service-accounts Opdrachtnemer zorgt ervoor dat service- en systeemaccounts niet interactief zijn en voorzien zijn van sterke, beheerde authenticatie zonder hardgecodeerde toegangsgegevens of vastlegging in elke vorm van leesbare tekst.	
IB-E25	IB-IAM-007 - Identity & Access - Wachtwoordbeleid Indien wachtwoorden worden gebruikt, zorgt Opdrachtnemer ervoor dat: - minimale lengte en complexiteit worden toegepast (12 tekens en uit ten minste 3 van 4 categorieën: kleine letters, 1 hoofdletter, 1 leesteken, 1 cijfer.); - een minimale geldigheid van 1 dag wordt toegepast; - geen verplichte periodieke wijziging zonder aanleiding plaatsvindt; - veilige hashing wordt toegepast; - hergebruik wordt voorkomen; - reverse engineering niet mogelijk is; - zwakke, veelvoorkomende, eerder gecompromitteerde, herhalende, opeenvolgende of voorspelbare - wachtwoorden worden geweigerd; - geen standaard-, gedeelde of hardgecodeerde wachtwoorden toegepast; - accounts zonder passende authenticatiebeveiliging niet worden toegestaan; - wachtwoorden niet op het scherm worden getoond bij invoer; - wachtwoorden niet in leesbare tekst worden opgeslagen; - wachtwoorden via zelfservice op een veilige wijze kunnen worden gewijzigd.	
IB-E26	IB-IAM-008 - Identity & Access - Geautoriseerde toegang Opdrachtnemer waarborgt dat de ICT-prestatie identificatie, authenticatie en autorisatie ondersteunt, zodat uitsluitend geautoriseerde gebruikers, systemen en processen toegang kunnen verkrijgen tot de ICT-prestatie en de bijbehorende beheervoorzieningen.	

Nr.	Eis	Ja/Nee
IB-E27	IB-IAM-009 - Identity & Access - Speciale bevoegdheden Accounts met speciale bevoegdheden, beheeraccounts en accounts voor noodtoegang (waaronder break-glass accounts) worden aanvullend beschermd, afzonderlijk beheerd en aantoonbaar gelogd en gemonitord.	
IB-E28	IB-IAM-010 - Identity & Access - Opdrachtnemerstoegang Opdrachtnemer verleent zichzelf geen structurele beheer- of ondersteuningstoegang tot gegevens of functionaliteit van Opdrachtgever zonder expliciete autorisatie en aantoonbare noodzaak. Eventuele toegang is altijd beperkt, gecontroleerd en gelogd.	
IB-E29	IB-IAM-012 - Identity & Access - Need-to-know Toegangsrechten worden zodanig ingericht dat uitsluitend toegang wordt verleend die noodzakelijk is voor de uitvoering van overeengekomen taken en verantwoordelijkheden. (need-to-know principe)	
IB-E30	IB-KI-001 - Artificial Intelligence - AI-functionaliteit Opdrachtnemer maakt transparant waar en op welke wijze AI-functionaliteit wordt toegepast binnen de ICT-prestatie en welke impact dit heeft op gegevensverwerking, besluitvorming en functionaliteit. AI-functionaliteit wordt zodanig ingericht dat Opdrachtgever gedurende de volledige levenscyclus aantoonbaar regie behoudt over gebruik, configuratie, dataverwerking en uitkomsten. Indien AI wordt toegepast op gegevens van Opdrachtgever, wordt dit uitsluitend gedaan voor overeengekomen doeleinden en onder gecontroleerde voorwaarden. Hergebruik van gegevens voor training of verbetering van modellen vindt uitsluitend plaats met expliciete toestemming van Opdrachtgever. AI-uitkomsten zijn in voldoende mate uitlegbaar en herleidbaar om evaluatie, controle en verantwoording mogelijk te maken, waarbij ten minste inzicht kan worden gegeven in relevante inputgegevens, configuratie en modelgedrag. Opdrachtnemer waarborgt dat AI-functionaliteit wordt beschermd tegen misbruik, manipulatie en ongeautoriseerde beïnvloeding, waaronder ongewenste input of verstoring van modelgedrag. Wijzigingen in AI-modellen, parameters of werking worden gecontroleerd, getest en vooraf afgestemd met Opdrachtgever indien deze impact hebben op functionaliteit, veiligheid of uitkomsten. Opdrachtnemer blijft volledig verantwoordelijk voor AI-functionaliteit, ook indien deze wordt geleverd via of gebaseerd is op diensten van derden, inclusief naleving van overeengekomen eisen op het gebied van beveiliging, privacy en continuïteit. Opdrachtgever kan AI-functionaliteit uitschakelen, vervangen of beëindigen indien dit noodzakelijk is vanuit beveiligings-, privacy- of kwaliteitsrisico’s, zonder verlies van controle over gegevens.	
IB-E31	IB-KOP-001 - Koppelingen - Algemene eisen aan koppelingen en API's Indien de ICT-prestatie gegevens uitwisselt met interne of externe systemen, richt Opdrachtnemer koppelingen, API's, interfaces en overige vormen van gegevensuitwisseling zodanig in dat deze gedurende de volledige levenscyclus veilig, betrouwbaar, beheersbaar, controleerbaar, interoperabel en overdraagbaar functioneren. API's worden consistent ontworpen conform breed geaccepteerde API-ontwerprichtlijnen, zodat interoperabiliteit, voorspelbaar gedrag en beheersbaarheid worden bevorderd. Opdrachtgever behoudt gedurende de volledige levenscyclus regie over toegang, gebruik, wijziging en beëindiging van koppelingen.	
IB-E32	IB-KOP-003 - Koppelingen - Inrichting en specificaties De exacte inrichting en specificatie van koppelingen wordt per koppeling afgestemd met Opdrachtgever. Hierbij worden o.a. doel en services van de koppeling, de inzet van de integratievoorziening van gemeente Apeldoorn, het type koppelvlak, de uitwisselspecificatie, de uitgangspunten voor certificaten, endpoints en API keys, de hoeveelheid dataverkeer en de wijze waarop foutmeldingen gegenereerd worden getoetst.	
IB-E33	IB-KOP-004 - Koppelingen - Instemming en toestemming Koppelingen en integraties worden niet zonder uitdrukkelijke schriftelijke toestemming van Opdrachtgever gelegd. Opdrachtnemer levert daarbij op verzoek van Opdrachtgever kosteloos technische documentatie en/of een visualisatie van de te realiseren koppeling(en)/integratie(s) aan.	

Nr.	Eis	Ja/Nee
IB-E34	IB-LOG-001 - Logging & Monitoring - Bruikbare logging Logging en monitoring zijn zodanig ingericht dat beschikbaarheid, prestaties, wijzigingen, beveiligingsincidenten en ongeautoriseerde of afwijkende activiteiten tijdig kunnen worden gedetecteerd, onderzocht en gereconstrueerd.	
IB-E35	IB-NET-002 - Netwerk - Beheerde en gecontroleerde netwerktoegang Opdrachtnemer zorgt ervoor dat netwerktoegang tot de ICT-prestatie uitsluitend plaatsvindt via gecontroleerde en beveiligde netwerkpaden.	
IB-E36	IB-NET-004 - Netwerk - Beveiligde externe toegang Opdrachtnemer zorgt ervoor dat externe toegang tot de ICT-prestatie uitsluitend plaatsvindt via versleutelde en geauthenticeerde verbindingen.	
IB-E37	IB-OPS-003 - Operations - Compatibiliteit Applicatieprogrammatuur is zodanig ontworpen en onderhouden dat deze compatibel blijft met ondersteunde versies van onderliggende systeemprogrammatuur, middleware en infrastructuurcomponenten. Afhankelijkheden tussen softwarecomponenten mogen het tijdig kunnen toepassen van beveiligingsupdates niet verhinderen.	
IB-E38	IB-OPS-005 - Operations - Hardening van systemen Opdrachtnemer zorgt ervoor dat systemen worden geleverd en beheerd met een geharde configuratie waarbij onnodige functionaliteit is uitgeschakeld.	
IB-E39	IB-OPS-006 - Operations - Scheiding van beheerrollen Opdrachtnemer zorgt ervoor dat beheertaken logisch worden gescheiden op basis van rollen en verantwoordelijkheden.	
IB-E40	IB-OPS-009 - Operations - On premises inrichtingseisen Indien (een deel van) de ICT-prestatie zich bij Opdrachtgever on-premises of in een door Opdrachtgever beheerde infrastructuur bevindt, dient Opdrachtnemer te waarborgen dat de ICT-prestatie kan functioneren binnen een gangbare enterprise security-architectuur. Hieronder wordt verstaan dat de ICT-prestatie in staat is om te integreren met door Opdrachtgever toegepaste beveiligingsmaatregelen, waaronder netwerksegmentatie, firewalling, web application firewalls, reverse proxies en netwerk- en traffic monitoring oplossingen. De ICT-prestatie ondersteunt veilige communicatie en verkeerafhandeling conform actuele beveiligingsstandaarden, waarbij encryptie in transport (TLS) behouden blijft en, waar noodzakelijk en proportioneel, inspectie van netwerkverkeer mogelijk kan worden ingericht binnen de kaders van geldende wet- en regelgeving (waaronder AVG). Opdrachtnemer werkt mee aan technische integratie en security testing teneinde interoperabiliteit met de beveiligingsarchitectuur van Opdrachtgever te borgen.	
IB-E41	IB-OPS-010 - Operations - Koppeling met interne systemen Indien koppelingen met internet-facing systemen van Opdrachtgever noodzakelijk zijn, dient de gegevensuitwisseling plaats te vinden via logisch gescheiden en beveiligde koppelvlakken die zijn ingericht volgens gangbare beveiligingsprincipes zoals segmentatie, zero trust en least privilege. Gegevensuitwisseling met ketenpartners en/of derden vindt uitsluitend plaats via beveiligde en geauthenticeerde interfaces, waarbij passende maatregelen worden getroffen om vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te waarborgen.	
IB-E42	IB-SUP-001 - Supply chain - Subverwerker governance Opdrachtnemer blijft integraal verantwoordelijk voor de naleving van de overeengekomen verplichtingen door onderaannemers, subverwerkers, hostingpartijen en overige ingeschakelde derden en borgt dat ten minste gelijkwaardige eisen contractueel en operationeel worden toegepast.	

Nr.	Eis	Ja/Nee
IB-E43	IB-SUP-002 - Supply chain - Transparantie in ketenafhankelijkheden Opdrachtnemer geeft inzicht in alle relevante ketenafhankelijkheden die invloed hebben op de ICT-prestatie.	
IB-E44	IB-SUP-003 - Supply chain - Leverancierswijzigingen Opdrachtnemer informeert Opdrachtgever voorafgaand aan relevante wijzigingen in subverwerkers of kritieke ketencomponenten.	

14 Eisen contract en leveranciersmanagement

De onderstaande eisen hebben betrekking op de contractuele en operationele afspraken tussen Opdrachtgever en Opdrachtnemer.

Nr.	Eis	Ja/Nee
CON-E01	~~Inschrijver levert bij inschrijving een concept-SLA aan, die minimaal gelijkwaardig is aan de eisen uit dit Programma van Eisen. De definitieve SLA wordt in de implementatiefase in overleg vastgesteld.~~	
CON-E02	De SLA beschrijft ten minste: de producten waarop de SLA van toepassing is, frequentie en inhoud van periodieke rapportages, de overlegstructuur, en een escalatiematrix op operationeel, tactisch en strategisch niveau.	
CON-E03	Facturen van Opdrachtnemer bevatten ten minste: facturatiekenmerk en referentiegegevens van Opdrachtgever, factuurdatum, omschrijving van het geleverde product of de dienst, totaalprijs exclusief btw, btw-bedrag en totaalprijs inclusief btw. Facturen waarop een of meer van deze gegevens ontbreken kunnen door Opdrachtgever worden geweigerd.	
CON-E04	Bij een prioriteit P1-incident levert Inschrijver binnen vijf werkdagen een Root Cause Analysis-rapportage aan Opdrachtgever.	
CON-E05	Minimaal 95% van de eerstelijnsincidenten wordt binnen de afgesproken oplostijden afgehandeld, gemeten per kalendermaand.	
CON-E06	Opdrachtgever ontvangt vóór facturatie een facturatievoorstel; facturatie vindt uitsluitend plaats na schriftelijk akkoord van Opdrachtgever.	

15 Eisen beheer en support

De onderstaande eisen hebben betrekking op de servicedesk en de ondersteuning van medewerkers van Gemeente Apeldoorn.

Nr.	Eis	Ja/Nee
SUP-E01	Incidenten worden opgepakt en afgehandeld conform de P1 tot en met P4 prioriteitsindeling zoals vastgelegd in de SLA. Zie hiervoor de bijlage Incindentenmatrix.	
SUP-E02	Leverancier verzorgt trainingen voor medewerkers van Gemeente Apeldoorn die met de ICT prestatie gaan werken.	

16 Implementatie, kennisoverdracht en borging

De onderstaande eisen beschrijven de implementatie en de wijze waarop Opdrachtgever na afronding zelfstandig verder kan.

Nr.	Eis	Ja/Nee
IMP-E01	Opdrachtnemer draagt kennis over via trainingen voor informatiebeheerders en Key-users van Gemeente Apeldoorn, en levert documentatie over installatie, gebruik, beheer en werkwijze.	
IMP-E02	Opdrachtgever kan na afronding zelfstandig opschoningscycli uitvoeren, het Classificatiemodel toepassen op nieuwe informatie en steekproefsgewijze controles uitvoeren.	
IMP-E03	Opdrachtnemer draagt de configuratie, beslisregels, Classificatiemodellen, sjablonen en procesbeschrijvingen over aan Opdrachtgever in een open en herbruikbaar formaat. Deze zijn eigendom van Opdrachtgever.	
IMP-E04	Alle data en resultaten zijn exporteerbaar in open formaten, zonder afhankelijkheid van Opdrachtnemer.	

17 Bijlage A: Begrippenlijst

Deze bijlage bevat de begrippen die in dit Programma van Eisen met een hoofdletter zijn geschreven. Waar een begrip is ontleend aan de GIBIT, de Archiefwet of andere regelgeving, is de betekenis daarop gebaseerd.

Begrip	Uitleg
Begrippen in het Beschrijvend Document	In het Besschrijvend Document worden begrippen toegelicht die in dat document gebruikt worden. Een aantal daarvan komen ook terug in de eisen.
Archiefwet	De wet die de zorg voor en het beheer van overheidsinformatie regelt, inclusief bewaring, vernietiging en overbrenging naar een archiefbewaarplaats.
Auditlog	Een vastlegging van handelingen in het systeem waarmee achteraf herleidbaar is welke gebruiker welke actie heeft uitgevoerd, en wanneer.
AVG	De Algemene verordening gegevensbescherming, de Europese verordening voor de bescherming van persoonsgegevens.
Bewaarregime	Het geheel van afspraken over hoe lang en op welke wijze een categorie informatie wordt bewaard.
Bewaarschema	Het overzicht van bewaartermijnen per informatiecategorie, gebaseerd op de Selectielijst Gemeenten.
Bewaartermijn	De periode gedurende welke informatie op grond van wet- en regelgeving bewaard moet blijven voordat zij mag of moet worden vernietigd.
BIO	De Baseline Informatiebeveiliging Overheid, het normenkader voor informatiebeveiliging binnen de overheid.
Citrix	De virtuele werkomgeving waarmee medewerkers toegang hebben tot het interne netwerk en de Netwerkschijven.
Classificatiemodel	Het geheel van regels waarmee informatie wordt ingedeeld naar bestemming, bewaartermijn en vertrouwelijkheid.
Djuma	Het zaaksysteem van Gemeente Apeldoorn, een van de doelomgevingen voor de migratie.
DPIA	Data Protection Impact Assessment, een beoordeling van de privacyrisico's van een verwerking van persoonsgegevens.
Duplicaat	Een bestand waarvan de inhoud identiek is aan die van een ander bestand, vast te stellen op basis van een hash van de inhoud.
Duurzame raadpleegomgeving	Een voorziening waarin informatie die niet vernietigd mag worden maar niet in de overige doelomgevingen past, doorzoekbaar en raadpleegbaar wordt bewaard.
Entra ID	De identity- en accessvoorziening van Microsoft, voorheen Azure Active Directory.
GIBIT	De Gemeentelijke Inkoopvoorwaarden bij IT, de standaardvoorwaarden die gemeenten hanteren bij de inkoop van IT.

Begrip	Uitleg
ICT-prestatie	Het geheel van producten en diensten dat Opdrachtnemer op grond van de overeenkomst levert, zoals gedefinieerd in de GIBIT. Hieronder vallen naast de programmatuur ook de bijbehorende dienstverlening, ondersteuning, documentatie en onderhoud.
Informatiearchitectuur	De vastgestelde ordening van informatie, systemen en doelomgevingen waarbinnen de migratie plaatsvindt.
Informatieobject	Een op zichzelf staand geheel van informatie, zoals een document of een dossier, dat als eenheid wordt beheerd.
Managementsamenvatting	Een beknopte samenvatting van de analyseresultaten, gericht op besluitvorming.
MDTO	Metagegevens voor Duurzaam Toegankelijke Overheidsinformatie, het metadatastandaard voor overheidsarchieven, opvolger van het TMLO.
Metadata	Gegevens die een informatieobject beschrijven, zoals herkomst, documenttype, bewaartermijn en vertrouwelijkheid.
Netwerkschijven	De on-premise fileservers van Gemeente Apeldoorn, in dit document de J- en K-schijf, die binnen de scope van de opdracht vallen.
Opleverpakket	Het geheel van documenten en bestanden dat Opdrachtnemer bij afronding oplevert, waaronder rapportages, auditlogs, metadata-overzichten, vernietigingslijsten en het overdrachtsdocument.
OTAP	Ontwikkel-, Test-, Acceptatie- en Productieomgeving, de gescheiden omgevingen in een beheerd softwareproces.
Pilotfase	De fase waarin de aanpak wordt beproefd op een afgebakend deel van de organisatie, ook aangeduid als leerfase.
PIM	Privileged Identity Management, het beheer van verhoogde toegangsrechten.
Risicoclassificatie	De indeling van informatie naar risico, zoals de aanwezigheid van persoonsgegevens of vertrouwelijke informatie.
ROT-data	Redundant, Obsolete en Trivial data: overbodige, verouderde en triviale informatie zonder bewaarwaarde.
Scan	De geautomatiseerde inventarisatie van de Netwerkschijven waarbij technische en inhoudelijke kenmerken worden vastgelegd.
Scope	De afbakening van de opdracht: circa ~~30 TB~~ 20,2 TB afdelingsdata op de J- en K-schijf.
Selectielijst Gemeenten	De wettelijk vastgestelde lijst met bewaartermijnen voor gemeentelijke informatie, hier de Selectielijst Gemeenten en Intergemeentelijke Organen 2020.
SLA	Service Level Agreement, de overeenkomst waarin de afgesproken serviceniveaus zijn vastgelegd.
Vernietigingslijst	Een overzicht van te vernietigen informatie met per post de onderbouwing, dat vooraf ter accordering wordt voorgelegd.
Verwerkersovereenkomst	De overeenkomst als bedoeld in artikel 28 AVG tussen verwerkingsverantwoordelijke en verwerker.
Woo	De Wet open overheid, die de actieve en passieve openbaarmaking van overheidsinformatie regelt.
Zaaksysteem	Het systeem waarin zaakgericht gewerkte informatie wordt vastgelegd; bij Gemeente Apeldoorn is dit Djuma.
Doelbestemming	Een doelbestemming is een passende omgeving waar het bewaar- en vernietigingsbeleid uitgevoerd kan worden dat voor een bestand van toepassing is. Daarnaast is een passende doelomgeving een omgeving die technisch en economisch aansluit bij de aard van het bestand.