Informatiebeveiligingseisen aan leveranciers van Enterprise Performance Management (EPM) v1.0

Deze aanbesteding betreft de implementatie, ontwikkeling en het beheer van een Enterprise Performance Management (EPM) oplossing inclusief licenties. De EPM-oplossing ondersteunt ProRail bij de planning, budgettering, rapportage en analyse van bedrijfsresultaten en vormt daarmee een belangrijk onderdeel van de bedrijfsvoering.

Versiebeheer

Versie	Datum	Auteur	Wijziging / Opmerking
0.9	12-10-2025	Catharine de Jong / Houssain Taibi	Conceptversie
1.0	17-10-2025	Catharine de Jong / Houssain Talbi	Definitieve versie

Thema	Eis
A. Persoonsgegevens	Bij de verwerking van persoonsgegevens houdt de leverancier zich aan de eisen uit de Algemene Verordening Gegevensverwerking.
A. Persoonsgegevens	De leverancier verwerkt persoonsgegevens in voorkomende gevallen uitsluitend in opdracht en op basis van schriftelijke instructies van ProRail, tenzij er sprake is van andersluidende wettelijke voorschriften.
B. Awareness	De leverancier zorgt ervoor dat gedurende de uitvoering van het contract zijn medewerkers periodiek en aantoonbaar op het belang van informatiebeveiliging en hun rol daarin worden gewezen (security awareness).
C. Bedrijfscontinuïteit	Voor het betreffende IT- dient ten minste volgens het ingerichte back-up proces een back-up te worden gemaakt na elke (functionele) systeemwijziging of op vooraf bepaalde, periodieke termijnen. Indien het om welke reden dan ook niet mogelijk is om een back-up te maken, dan wordt dit vastgelegd en, op basis van een risicoanalyse, een alternatieve werkwijze gekozen en beschreven.
D. Certificeringen en normenkaders	De leverancier garandeert dat hij voldoet aan alle toepasselijke verplichtingen voortvloeiend uit de komende Cyberbeveiligingswet, inclusief maar niet beperkt tot: 1. Het treffen van passende technische en organisatorische maatregelen ter beheersing van cyberbeveiligingsrisico's; 2. Het melden van betekenisvolle cyberincidenten aan de relevante toezichthoudende autoriteiten en aan de opdrachtgever binnen 24 uur na ontdekking; 3. Het uitvoeren van regelmatige risicoanalyses en het bijwerken van beveiligingsmaatregelen; 4. Het waarborgen van de beveiliging van persoonsgegevens en bedrijfsinformatie van de opdrachtgever; 5. Het faciliteren van audits en inspecties door of namens de opdrachtgever om naleving van deze clausule te verifiëren. Indien de leverancier nalaat te voldoen aan deze verplichtingen, behoudt de opdrachtgever zich het recht voor om het contract per direct te ontbinden en/of schadevergoeding te eisen

D. Certificeringen en normenkaders	Een certificering tegen de ISO27001 norm voor Informatiebeveiliging en de bijbehorende beheersmaatregelen is vereist, waarbij de dienstverlening aan ProRail volledig in de scope van de certificering valt. Indien deze daarover niet beschikt, dient de leverancier de verzekering te geven dat de informatiebeveiliging op een vergelijkbaar niveau als de ISO-norm is ingericht door het overleggen van bewijsstukken.
D. Certificeringen en normenkaders	De leverancier beschikt over een ISAE 3402 Type II-verklaring of een gelijkwaardige assurance-verklaring, waarin de dienstverlening aan ProRail volledig binnen de scope van de assurance-verklaring valt.
D. Certificeringen en normenkaders	Relevante certificaten (bv. ISO 27001) en assurance verklaringen (bv. SOC2, ISAE 3402) worden ter beschikking gesteld aan ProRail. De scope en inrichting van het ISMS wordt door ProRail getoetst op relevantie en effectiviteit.
E. Contactpersoon	Zowel ProRail als de leverancier hebben een contactpersoon voor informatiebeveiligingsaspecten, vastgelegd in bijvoorbeeld de SLA. Deze contactpersonen zijn adviserend en ondersteunend aan het contract- en leveranciersmanagementproces. Afstemming vindt altijd plaats onder regie van de contractmanager.
G. Exit-strategie	De leverancier beschikt over een uitwerking van een exit-strategie, die goedgekeurd is door ProRail. Deze strategie omvat minimaal afspraken over hoe de data overgedragen en daarna verwijderd/vernietigd wordt bij wisseling van leverancier of overname van de dienst door ProRail.
H. Gegevensuitwisseling	Digitale gegevensuitwisselingen vinden plaats conform een gestandaardiseerde en beveiligde manier, nader af te spreken.
I. Gegevensverwerking en -opslag	De leverancier maakt alleen gebruik van de verstrekte en gegenereerde gegevens voor het uitvoeren van de gecontracteerde werkzaamheden.
I. Gegevensverwerking en -opslag	Indien informatie opgeslagen wordt binnen de infrastructuur van de leverancier, dient deze beveiligd te worden conform het beveiligingsniveau dat bij deze informatie is overeengekomen. Dit betekent dat persoonsgegevens per definitie minimaal Vertrouwelijk geclassificeerd zijn. (Bij bijzondere persoonsgegevens : Geheim)
I. Gegevensverwerking en -opslag	De websites, servers en databasesystemen met alle daarop opgeslagen informatie bevinden zich fysiek binnen de Europese Economische Ruimte (EER) en mogen alleen vanuit een locatie buiten de EER toegankelijk zijn en/of bewerkt worden vanaf een beveiligd werkstation waarbij lokale opslag niet mogelijk is en een beveiligde verbinding en multi-factor authenticatie gebruikt wordt. De data mogen de EER niet verlaten.
J. Geheimhouding	Ter waarborging van de vertrouwelijkheid van Vertrouwelijke en/of Geheime informatie wordt een Non Disclosure Agreement (NDA) of vergelijkbare vertrouwelijkheidsverklaring ondertekend door de leverancier (en indien relevant door ProRail). De leverancier verplicht zijn personeel aantoonbaar om de geheimhoudingsverplichting na te komen.
K. Incidenten	Bij constatering van een kwetsbaarheid, beveiligingsincident of datalek dient de leverancier onverwijld contact op te nemen met de Centrale Servicedesk van ProRail, bereikbaar op nummer 0882312600, en de betreffende contractmanager.
K. Incidenten	De leverancier meldt (beveiligings-)incidenten en kwetsbaarheden direct aan ProRail, en als dat wettelijk noodzakelijk is, ook aan een toezichthouder zoals de Autoriteit Persoonsgegevens of IL&T. Bij niet-gemelde incidenten waar persoonsgegevens bij betrokken zijn, kan ProRail de leverancier in gebreke stellen.
K. Incidenten	De leverancier geeft (beveiligings-)incidenten volgens gemaakte afspraken opvolging en rapporteert daarover aan ProRail.

L. Monitoren en loganalyse	Monitoring is ingericht voor alle IT- en OT-systemen in scope van het contract. Wanneer monitoring niet mogelijk is of niet rendabel is, dan dient hiervoor een risico gebaseerde redeneerlijn te worden opgesteld. Monitoring van de remote toegang en beheer op afstand dient altijd te worden ingericht.
L. Monitoren en loganalyse	Activiteiten van gebruikers en beheerders dienen ten behoeve van audittrailing vastgelegd te worden in beveiligde registraties. Deze registratie wordt op verzoek van ProRail door de leverancier op een door ProRail te definiëren wijze beschikbaar gesteld.
M. Onderaanneming en toeleveranciers	De leverancier dient inzicht te geven in welke derden mogelijk toegang kunnen hebben tot ProRail data. Denk aan hosting providers, softwareleveranciers, support partijen, subverwerkers, etc.
M. Onderaanneming en toeleveranciers	Alle voorwaarden en eisen van ProRail op het gebied van informatiebeveiliging die gelden voor de leverancier zijn ook van toepassing op derden, die in opdracht van de leverancier diensten verrichten voor ProRail.
M. Onderaanneming en toeleveranciers	De leverancier moet desgevraagd inzage geven in de maatregelen die hij genomen heeft om de aan hem opgelegde eisen ook door te vertalen naar derden.
M. Onderaanneming en toeleveranciers	Het is de leverancier niet toegestaan, zonder voorafgaande uitdrukkelijke schriftelijke toestemming van ProRail, de uitvoering van een contract geheel of gedeeltelijk aan derden over te dragen of uit te besteden, dan wel gebruik te maken van ter beschikking gestelde of ingeleende arbeidskrachten. Deze toestemming zal niet op onredelijke gronden geweigerd worden.
N. Periodiek overleg en rapportages	In de contracten worden, indien relevant, expliciete prestatie-indicatoren en bijbehorende verantwoordingsrapportages gespecificeerd met betrekking tot informatiebeveiliging.
N. Periodiek overleg en rapportages	ProRail ontvangt periodiek rapportages van de leveranciers over de geleverde prestatie met betrekking tot informatiebeveiliging en bespreekt die conform een vooraf afgesproken frequentie.
N. Periodiek overleg en rapportages	In het geval van af te nemen diensten met afgesproken serviceniveaus op gebied van informatiebeveiliging wordt tussen de leverancier en ProRail een SLA afgesloten.
O. Personeel	De leverancier toont aan dat het personeel voldoende kennis en kunde heeft om de werkzaamheden binnen ProRail te verrichten. Dit hangt samen met beveiligingseisen, die bijvoorbeeld door scholing en/of voldoende kennis en kunde gebruikersfouten beperken.
O. Personeel	Extern personeel dient zich te houden aan de gedragsregels van ProRail. <wordt meegestuurd>
O. Personeel	Indien een medewerker van de leverancier, die door zijn werkzaamheden op locatie van ProRail komt en/of toegang heeft tot infrastructuren en gegevens, uit dienst gaat, wordt dit minimaal twee weken van tevoren gemeld aan de contractmanager van ProRail.
P. Retour/vernietiging bedrijfsmiddelen en informatie	Op verzoek retourneert of vernietigt de leverancier, dit naar keuze van ProRail, onverwijld alle door ProRail ter hand gestelde documenten, boeken, bescheiden en andere zaken (waaronder begrepen gegevensdragers en back-ups). Dit geldt ook voor alle gegevens, inclusief persoonsgegevens, ook in cloudomgevingen.
Q. Auditrecht	ProRail kan op enig moment een audit, waaronder een penetratietest, (laten) uitvoeren om te controleren dat aan beveiligingseisen die van toepassing zijn wordt voldaan. Dit gebeurt in overleg met de leverancier. Een audit hoeft niet nodig te zijn als de leverancier door middel van certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd, dan wel aantoont dat een onafhankelijke audit heeft plaatsgevonden en de relevante resultaten deelt met ProRail. ProRail behoudt zich echter te allen tijde het recht voor om alsnog zelf een audit uit te voeren, indien daartoe aanleiding is.

Q. Auditrecht	Indien ProRail in het kader van acceptatie of validatie een security test (laat) verricht(en), stelt ProRail zo spoedig mogelijk een testverslag op en zendt dat ondertekend aan Opdrachtnemer. In het testverslag worden geconstateerde bevindingen en gebreken vastgelegd alsook of ProRail de geteste asset goed- of afkeurt. Afspraken worden tussen ProRail en de leverancier gemaakt over de opvolging van de bevindingen.
R. Risicomanagement	De leverancier vult na contractering een self-assessment in waaruit de mate van beveiliging blijkt, met als kader het beveiligingsbeleid van ProRail.
R. Risicomanagement	De leverancier dient ProRail (op verzoek) te informeren over de getroffen beheersmaatregelen die relevant zijn binnen het kader van de dienstverlening.
S. Security by Design	De gangbare principes rondom Security by Design/Default zijn uitgangspunt voor de ontwikkeling van software en systemen. Over wat dit concreet binnen de opdracht inhoudt worden afspraken gemaakt tussen ProRail en de leverancier.
U. Toegang tot digitale infrastructuur en gegevens	Er wordt een gedocumenteerde formele en actuele procedure afgesproken voor het registreren, verlenen, wijzigen en intrekken van logische toegang tot IT-systemen van ProRail. Deze procedure wordt periodiek (minimaal eens per jaar) beoordeeld en geactualiseerd.
U. Toegang tot digitale infrastructuur en gegevens	De toegang van medewerkers van de leverancier tot ProRail informatie en systemen is beperkt tot datgene dat nodig is voor het leveren van de dienst (need to know principe).
U. Toegang tot digitale infrastructuur en gegevens	Alleen bij een aantoonbare noodzaak krijgen leveranciers remote toegang tot de ProRail omgeving.
U. Toegang tot digitale infrastructuur en gegevens	Remote toegang tot en beheer op afstand van IT- en OT-omgevingen, uitgevoerd door de leverancier, dienen te worden gemonitord.
U. Toegang tot digitale infrastructuur en gegevens	Om toegang te krijgen tot de systemen en netwerken van ProRail wordt gebruik gemaakt van beveiligde verbindingen met Single Sign-On (SSO) met multi-factor authenticatie (MFA).
V. Toegang tot fysieke infrastructuur	Alle toegangsmiddelen (waaronder sleutels, pasjes, tokens) mogen uitsluitend worden gebruikt voor het doel waarvoor deze beschikbaar zijn gesteld en niet worden gedeeld met anderen.
W. Wijzigingsbeheer	Substantiële wijzigingen van de leveranciersorganisatie en -processen met impact voor ProRail dienen door de leverancier tijdig kenbaar gemaakt te worden aan ProRail. Dit wordt opgenomen als onderdeel van de overeenkomst met de leverancier.