ProRail

**TN572179 Landelijk – Detectie en beoordeling spoorstaafdefecten**

# Vraagspecificatie Annex 16.0: Informatiebeveiligingseisen voor Leveranciers

**Versie 1.0**

# Inhoudsopgave

**Gehanteerde definities**
De in dit document gebruikte definities zijn opgesomd in Annex 0.0 – Leeswijzer. Definities die zijn opgenomen in de leeswijzer staan met een hoofdletter in dit document.

**Referentielijst**
De referentielijst bevindt zich in Annex 0.0 – Leeswijzer.

## Inleiding

ProRail is voornemens middels deze aanbesteding een overeenkomst te sluiten voor de levering van ‘Meten als een Service’, gericht op het verkrijgen van een actueel en betrouwbaar inzicht in de conditie van de Nederlandse spoorinfrastructuur.

De gecontracteerde leverancier is verantwoordelijk voor het plannen en uitvoeren van de benodigde meetritten, het verwerken van de ingewonnen gegevens en het opleveren van gevalideerde dataproducten aan ProRail. In voorkomende gevallen kan ook het analyseren en duiden van de ingewonnen data tot de scope behoren.

De metingen ondersteunen het primaire proces van Asset Management binnen ProRail en vormen een belangrijk instrument voor het gericht uitvoeren van onderhoud, het prioriteren van investeringen en het waarborgen van de veiligheid en beschikbaarheid van het spoor.

## Informatiebeveiligingseisen

De volgende informatiebeveiligingseisen zijn van toepassing:

A. n.v.t.

B. Awareness

a) 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. n.v.t.

D. n.v.t.

E. Contactpersoon

a) Zowel ProRail als de leverancier hebben een contactpersoon voor informatiebeveiligings-aspecten, 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.

F. n.v.t.

G. n.v.t.

H. Gegevensuitwisseling

a) Digitale gegevensuitwisselingen vinden plaats conform een gestandaardiseerde en beveiligde manier. Alle gegevens die digitaal worden verstuurd of opgeslagen, dienen te worden versleuteld conform de cryptografiestandaarden van ProRail. Dit geldt zowel voor gegevens in transit als at rest.
b) Alle door de leverancier ingewonnen of gegenereerde meetgegevens vallen volledig onder het eigendom van ProRail of worden aan ProRail in exclusieve gebruiksrechten verstrekt. De leverancier mag de gegevens niet hergebruiken of delen met derden zonder voorafgaande schriftelijke toestemming.

I. Gegevensverwerking en -opslag

a) De leverancier maakt alleen gebruik van de verstrekte en gegenereerde gegevens voor het uitvoeren van de gecontracteerde werkzaamheden.
b) De leverancier verwerkt uitsluitend de data die nodig is voor het uitvoeren van de gecontracteerde diensten en uitsluitend voor dat doel. Verzameling van additionele gegevens is niet toegestaan zonder schriftelijke toestemming van ProRail.
c) 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)
d) 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.
e) De leverancier dient passende maatregelen te treffen voor het waarborgen van de integriteit van de ingewonnen en verwerkte meetdata. Validering van gegevens dient plaats te vinden voorafgaand aan levering aan ProRail. Op verzoek wordt inzicht gegeven in validatie-mechanismen en kwaliteitseisen.

J. n.v.t.

K. Incidenten

a) Bij constatering van een kwetsbaarheid of beveiligingsincident dient de leverancier onverwijld contact op te nemen met de Centrale Servicedesk van ProRail, bereikbaar op nummer 0882312600, en de betreffende contractmanager.
b) De leverancier meldt (beveiligings-)incidenten en kwetsbaarheden direct aan ProRail, en als dat wettelijk noodzakelijk is, ook aan de Autoriteit Persoonsgegevens. Bij niet-gemelde incidenten waar persoonsgegevens bij betrokken zijn, kan ProRail de leverancier in gebreke stellen.
c) De leverancier geeft (beveiligings-)incidenten volgens gemaakte afspraken opvolging en rapporteert daarover aan ProRail.

L. Monitoren en loganalyse

a) De leverancier registreert en bewaart logs van alle geleverde datasets aan ProRail, inclusief timestamp, verwerkingsstatus en verantwoordelijke medewerker. Deze logs worden op verzoek beschikbaar gesteld aan ProRail. De bewaartermijn van deze loggegevens wordt afgestemd met ProRail.

M. Onderaanneming en toeleveranciers

a) 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.
b) Alle voorwaarden en eisen 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.

N. n.v.t.

O. Personeel

a) 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.
b) Extern personeel dient zich te houden aan de gedragsregels van ProRail.

P. Retour/vernietiging bedrijfsmiddelen en informatie

a) 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

a) 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. Het nut / de noodzaak van een audit wordt kleiner 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.

R. n.v.t.

S. n.v.t.

T. n.v.t.

U. Toegang tot digitale infrastructuur en gegevens

a) De toegang van medewerkers van de leverancier is beperkt tot systemen bij ProRail, de leverancier en afgenomen diensten bij derden, die benodigd zijn voor het leveren van de dienst (need to know principe).
b) Toegang tot de systemen is beperkt met wachtwoorden volgens de wachtwoordeisen zoals opgenomen in het informatiebeveiligingsbeleid van ProRail.

V. Toegang tot fysieke infrastructuur

a) Alle toegangsmiddelen (waaronder sleutels, pasjes, tokens) mogen uitsluitend worden gebruikt voor het doel waarvoor deze beschikbaar zijn gesteld en niet worden gedeeld met anderen, wat geborgd is in een (mechanisch) sluitplan.

W. Wijzigingsbeheer

a) 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.