

Informatiebeveiligingseisen aan leveranciers

Buitencommunicatie v 1.0

Eisenset t.b.v. de aanbesteding Buitencommunicatie

Versiebeheer

Versie	Datum	Auteur	Wijziging / Opmerking
1.0	17-04-2026	Catharine de Jong	Definitief

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.
A. Persoonsgegevens	Met alle derde partijen die als verwerker voor of namens ProRail persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld. 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).
D. Certificeringen en normenkaders	De leverancier garandeert dat hij voldoet aan alle toepasselijke verplichtingen voortvloeiend uit de komende Cyberbeveiligingswet, inclusief maar niet beperkt tot: <ol style="list-style-type: none"> 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

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.
H. Gegevensuitwisseling	Digitale gegevensuitwisselingen vinden plaats conform een gestandaardiseerde en beveiligde manier. Verbindingen zijn ingericht en worden onderhouden conform de standaarden van ProRail.
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 volgens 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 en de betreffende contractmanager.
K. Incidenten	De leverancier meldt (beveiligings-)incidenten en kwetsbaarheden die veiligheid van het systeem raken 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.
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.
M. Onderaanneming en toeleveranciers	ProRail wordt zo snel mogelijk op de hoogte gebracht indien de leverancier wijzigingen aanbrengt bij het uitbesteden van zijn eigen (deel)processen. Hierdoor kan ProRail bepalen of er zwaarwegende risico's bestaan (bv. uitbesteding aan onveilige landen) en tevens inzicht verkrijgen in de wijze van beheersing van de door de leverancier uitbestede (deel) processen. Deze inzet, beheersing en wijziging van sub verwerking wordt opgenomen in de overeenkomst met de leverancier.

O. Personeel	Personeel van de leverancier dat werkzaamheden verricht voor ProRail houdt zich aan de geldende gedragsregels van ProRail, zoals opgenomen in de Gedragscode van ProRail (beschikbaar via de website van ProRail), en handelt in lijn met de daarin opgenomen principes, waaronder integriteit, onafhankelijkheid en zorgvuldige omgang met informatie. De leverancier borgt dat het personeel voorafgaand aan de werkzaamheden over deze regels is geïnformeerd.
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.
P. Retour/vernietiging bedrijfsmiddelen en informatie	Voorafgaand aan hergebruik of verwijdering van apparatuur dienen alle gegevens op de daarin aanwezige opslagmedia op betrouwbare wijze te worden verwijderd. Dit gebeurt door een hiertoe gecertificeerde organisatie. Als bewijs van verwijdering dient een certificaat door het vernietigingsbedrijf te worden aangeleverd.
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.