# Informatiebeveiligingseisen aan leveranciers van SAP v1.0

*Een dienst wordt aanbesteed waarbij de toekomstig opdrachtnemer ProRail gaat helpen bij het op orde brengen van de SAP Configuratiedata. Deze dienst voert opdrachtnemer uit op een ProRail laptop in de systemen van ProRail zelf. Het doel van de dienst is het op orde brengen van data en adviseren hoe ProRail deze data in de toekomst op orde houdt.*

Van de volgende gegevens is verder uitgegaan:

- Tier 2 bij **toegang tot gegevens** en **wet- en regelgeving**. Tier 3 bij **business impact** en **werken aan systemen** (risicoprofiel leverancier uit het intakeformulier).

**Versiebeheer**

| Versie | Datum | Auteur | Wijziging / Opmerking |
|---|---|---|---|
| 0.9 | 06-05-2026 | Maarten Bunschoten | Conceptversie |
| 1.0 | 13-05-2026 | Maarten Bunschoten | Definitieve versie |

| Thema | Eis |
|---|---|
| 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 | De leverancier heeft aantoonbaar en actueel inzicht in de risico's binnen zijn bedrijfsprocessen die een bedreiging zouden kunnen vormen voor de continuïteit en/of veiligheid van de bedrijfsprocessen van ProRail. |
| D. Wet- en regelgeving, certificeringen en normenkaders | De leverancier garandeert dat hij voldoet aan alle toepasselijke verplichtingen voortvloeiend uit de komende Cyberbeveiligingswet, inclusief maar niet beperkt tot:<br>1. Het treffen van passende technische en organisatorische maatregelen ter beheersing van cyberbeveiligingsrisico's;<br>2. Het melden van betekenisvolle cyberincidenten aan de relevante toezichthoudende autoriteiten en aan de opdrachtgever binnen 24 uur na ontdekking;<br>3. Het uitvoeren van regelmatige risicoanalyses en het bijwerken van beveiligingsmaatregelen;<br>4. Het waarborgen van de beveiliging van persoonsgegevens en bedrijfsinformatie van de opdrachtgever;<br>5. Het faciliteren van audits en inspecties door of namens de opdrachtgever om naleving van deze clausule te verifiëren.<br><br>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 | 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 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. |
| K. Incidenten | De leverancier geeft (beveiligings-)incidenten volgens gemaakte afspraken opvolging en rapporteert daarover aan ProRail. |

| | |
|---|---|
| O. Personeel | Een recente Verklaring Omtrent het Gedrag (VOG) is vereist voor medewerkers van de leverancier die werkzaamheden uitvoeren op locaties van ProRail of die toegang krijgen tot apparatuur, infrastructuur of gegevens van ProRail. De noodzaak en wijze van aanlevering wordt vooraf afgestemd met ProRail. |
| 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. |
| 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. |
| 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. |
| 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). |
| 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. |