TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Inkoopvoorwaarden en informatieveiligheidseisen

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Inkoopvoorwaarden en beveiligingseisen’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Doel

Dit document beschrijft de beleidsuitgangspunten ten aanzien van informatiebeveiligingseisen voor een invulling van de inkoopvoorwaarden voor organisaties binnen de Rijksoverheid. Deze uitgangspunten over informatiebeveiliging zijn afkomstig uit de BIR en het beleid voldoet daarmee aan de BIR.

Doelgroep

Dit document is van belang voor de verantwoordelijke inkopers en beveiligers van organisaties binnen de Rijksoverheid.

Reikwijdte

Dit document heeft voornamelijk betrekking op maatregel 6.2 en maatregelen 12.1.1. van de Baseline Informatiebeveiliging Rijksdienst (BIR). Het document gaat in op personele, organisatorische en technische informatiebeveiligingsaspecten die organisaties binnen de Rijksoverheid dienen te overwegen in relatie tot inkoopvoorwaarden.

Relatie met overige producten

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Informatiebeveiligingsbeleid
- De bewerkersovereenkomst
- De Service Level Agreement (SLA)

Inhoudsopgave

1 Inleiding

Organisaties binnen de Rijksoverheid passen in veel gevallen eigen inkoopvoorwaarden toe in combinatie met algemene inkoopvoorwaarden, zoals de Algemene Rijksinkoopvoorwaarden Diensten (ARVODI). Naast de beveiligingsvoorschriften van de ARVODI zijn aanvullende afspraken nodig. Inkoopvoorwaarden voorzien veelal (nog) niet in deze aanvullende informatiebeveiligingseisen. Dit document beschrijft deze informatiebeveiligingseisen met als doel de inkoopvoorwaarden van overheidsorganisaties te versterken.

In de BIR worden eisen benoemd met betrekking tot de inkoopvoorwaarden. Deze staan benoemd in hoofdstuk 6.2 en hoofdstuk 12.1.1.

1.1 Het belang van beveiligingseisen in inkoopvoorwaarden

Bij het verwerven van producten of diensten is het van belang om in een vroegtijdig stadium aan mogelijke leveranciers kenbaar te maken welke beveiligingseisen de organisatie wenst te stellen aan het product of de dienst. Door vroegtijdig aan te geven welke beveiligingseisen worden gesteld aan het product of de dienst, wordt ervoor gezorgd dat leveranciers hier tijdig op kunnen inspelen. De inkopende organisatie heeft te allen tijde de verantwoordelijkheid voor informatiebeveiliging, ook bij het outsourcen en uitbesteden van ICT-diensten.

1.2 Raakvlakken

Overige verbintenissen en beleidsafspraken met beveiligingseisen die raakvlakken kennen met de inkoopvoorwaarden zijn:

- Informatiebeveiligingsbeleid
- ICT-beheer
- Service Level Agreements (SLA)
- Bewerkersovereenkomsten
- (ICT-)contracten.
- Informatiebeveiligingsgerelateerde requirements bij RFP/RFI’s

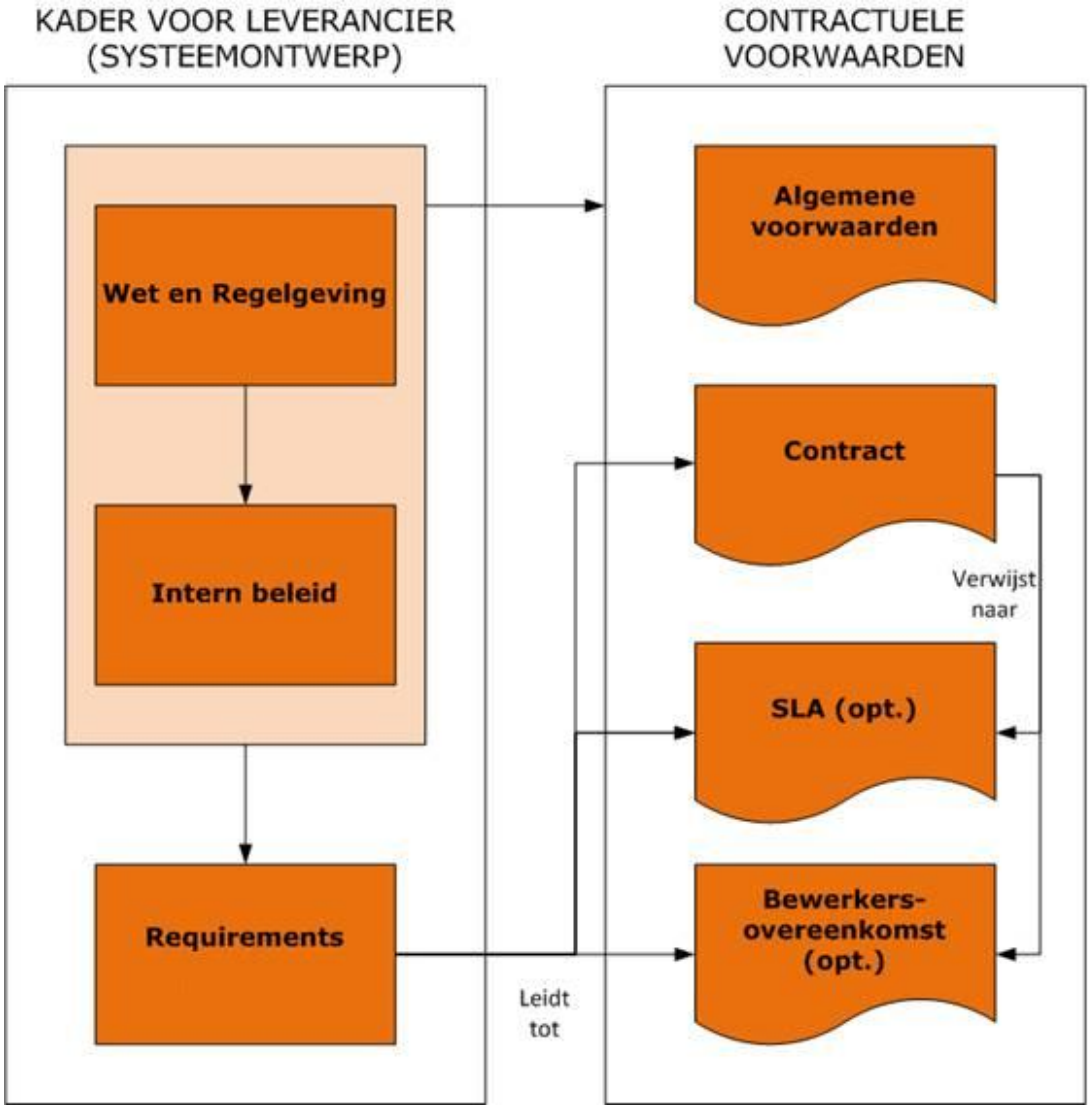
2 Beveiligingseisen in inkoopvoorwaarden

2.1 Algemeen

Rijksoverheidsorganisaties hanteren veelal eigen Algemene Inkoopvoorwaarden (AIV) voor het afnemen van producten en diensten. In deze inkoopvoorwaarden moet rekening gehouden worden met de BIR-beveiligingseisen en het daarvan afgeleide informatiebeveiligingsbeleid van organisaties binnen de Rijksoverheid.

2.2 Verhoudingen tussen voorwaarden

De verhouding tussen informatiebeveiligingsbeleid van een organisatie en de inkoopvoorwaarden is als volgt:



De inkoopcontracten kunnen bestaan uit een aantal documenten, zoals algemene voorwaarden en het contract dat specifiek is voor dat product of dienst. Het is van belang de onderlinge verhoudingen tussen de verschillende voor de inkoop relevante documenten in het kader van informatiebeveiliging te onderzoeken. De beveiligingseisen moeten in de

documenten goed worden verankerd, omdat wet- en regelgeving samen met beveiligingsbeleid de contractuele voorwaarden bepaalt.

De algemene inkoopvoorwaarden zijn standaardcontracten die een organisatie voor meerdere partijen hanteert. Daarin staan de algemene afspraken die richting verschillende partijen kunnen gelden. Daarnaast worden in een specifiek contract de afspraken tussen twee specifieke partijen geregeld. In dit contract zijn de wensen en eisen nader gespecificeerd, en de concrete beveiligingseisen uitgewerkt. In veel gevallen is per leverancier maatwerk vereist. Tevens kan een Service Level Agreement (SLA) nodig zijn voor het borgen en meetbaar maken van serviceafspraken. In de ICT heeft een SLA doorgaans betrekking op het onderhoud van een ICT-systeem, nadat een systeem is opgeleverd.

Indien tijdens de uitvoering van een contract persoonsgegevens zullen worden verwerkt, of mogelijkerwijs persoonsgegevens kunnen worden ingezien, is aanvullend een bewerkersovereenkomst nodig. Dit wordt beschreven in artikel 12 Wet bescherming persoonsgegevens (Wbp). Als bijvoorbeeld een ICT-dienstverlener een applicatie aanbiedt (bijvoorbeeld door middel van SaaS[1]), en in die applicatie staan persoonsgegevens, dan is de leverancier ook de bewerker. Een leverancier hoeft niet direct te werken met persoonsgegevens om toch een bewerker te zijn in de zin van de Wbp.

2.3 Beveiligingseisen in Algemene Inkoopvoorwaarden

Op basis van de BIR-maatregelen is het aan te bevelen om de volgende beveiligingseisen op te nemen in algemene inkoopvoorwaarden. Hiermee kunnen relevante beveiligingsaspecten in een vroegtijdig stadium onderwerp zijn van het inkoopproces. Onderstaande tekstvoorstellen kunnen worden ingevoegd in algemene inkoopvoorwaarden.

- *Personeel van de contractant*

“Het is de leverancier verboden, zonder voorafgaande uitdrukkelijke schriftelijke toestemming van de organisatie, de uitvoering van een overeenkomst geheel of gedeeltelijk aan derden over te dragen of uit te besteden, dan wel gebruik te maken van ter beschikking gestelde of ingeleende arbeidskrachten.”

DOEL VAN DEZE BEPALING:

Het is noodzakelijk inzicht te hebben in welke medewerkers werkzaamheden verricht voor de organisatie. Het kan voorkomen dat een partij hiervoor derden inschakelt die mogelijkerwijs daarmee niet voldoen aan de alle beveiligingseisen die gesteld zijn. Hiervan moet een organisatie op de hoogte zijn.

- *Personeel van de contractant*

“Alle voorwaarden en eisen die gelden voor personeel van de leverancier zijn ook van toepassing op derden, die in opdracht van de leverancier diensten verrichten voor de organisatie.”

[1] Software as a Service (SaaS) is software die als een onlinedienst wordt aangeboden.

DOEL VAN DEZE BEPALING:
Als er inzicht is in het inzetten van derden door de leverancier, dienen alle voorwaarden en eisen ook van toepassing te zijn op die derden.

- *Geheimhouding*

“Leverancier zal het bestaan, de aard en de inhoud van de overeenkomst, evenals overige bedrijfsinformatie van de organisatie geheimhouden en niets daaromtrent openbaar maken zonder schriftelijke toestemming van de organisatie.

De leverancier staat er voor in dat personeel van de leverancier, overige personeelsleden en derden de bepalingen betreffende gedrag, vertrouwelijkheid en bescherming van gegevens naleven.”

DOEL VAN DEZE BEPALING:
De leverancier zal geen informatie van de organisatie openbaar maken zonder toestemming van de organisatie. Eventueel wordt een geheimhoudingsverklaring door de leverancier getekend. Als dit niet collectief kan, dient iedere ingehuurde medewerker apart een geheimhoudingsovereenkomst te tekenen.

- *Verklaring Omtrent het Gedrag (VOG)*

“Medewerkers van de leverancier overleggen voor aanvang van de werkzaamheden bij de organisatie een recente Verklaring Omtrent het Gedrag (VOG). De leverancier stemt voorafgaand aan de aanvraag de noodzaak, inhoud en aard hiervan af met de organisatie.”

DOEL VAN DEZE BEPALING:
Externe medewerkers dienen als deze in aanraking komt met gevoelige gegevens en/of systemen een VOG te kunnen overleggen bij aanvang van de werkzaamheden voor een organisatie.

In uitzonderlijke gevallen zal een VOG niet voldoen. Een veiligheidsonderzoek kan tot de mogelijkheden behoren.

- *Gedragsregels*

“De leverancier zal voor de prestaties voldoende personen inzetten met voldoende opleiding, vaardigheden en kennis van de bedrijfsvoering en van de overheidsorganisatie, om de prestaties te verrichten.

Wanneer de hierboven genoemde personen zich bij de organisatie bevinden, of in direct contact met de organisatie staan, zal het personeel van de leverancier de gedragsvoorschriften van de organisatie naleven. Hiermee zal gevolg gegeven worden aan redelijke verzoeken van de organisatie.”

DOEL VAN DEZE BEPALING:
De leverancier moet blijk geven van het hebben van personeel met voldoende kennis en kunde om de werkzaamheden binnen de organisatie te verrichten. Dit hangt samen met beveiligingseisen, die bijvoorbeeld door scholing en/of voldoende kennis en kunde

gebruikersfouten beperken. De gedragsregels voor medewerkers van de organisatie gelden tevens voor externe medewerkers.

- *Diensten en goederen*

"In het geval van af te nemen diensten met afgesproken serviceniveaus wordt tussen de leverancier en de organisatie een Service Level Agreement (SLA) afgesloten."

DOEL VAN DEZE BEPALING:
Als diensten worden afgenomen, dan horen daar serviceniveaus betrokken te worden over beveiligingsaspecten, zoals bijvoorbeeld beschikbaarheid, melden van incidenten, doorvoeren van wijzigingen en escalatie.

- *Informatieveiligheid*

"De leverancier accepteert de maatregelen uit de Baseline Informatiebeveiliging Rijksdienst (BIR), voor zover van toepassing verklaard door de organisatie, en past deze toe op de geleverde producten en/of diensten."

DOEL VAN DEZE BEPALING:
Als een leverancier producten en/of diensten levert aan een organisatie, dan dient de leverancier uit te gaan van het basisbeveiligingsniveau van de organisatie, dat gebaseerd is op de BIR. Eventueel wordt een link toegevoegd of de BIR is onderdeel van de eisen en wensen.

- *Persoonsgegevens*

"De leverancier accepteert dat, wanneer persoonsgegevens worden bewerkt in systemen van de leverancier buiten de organisatie, een bewerkersovereenkomst wordt afgesloten als onderdeel van het contract. Tevens worden in het contract afspraken vastgelegd betreffende aansprakelijkheid en schade in geval van incidenten."

DOEL VAN DEZE BEPALING:
Als persoonsgegevens van de overheidsorganisatie worden gehost bij een externe partij, dan is deze derde partij volgens de Wet bescherming persoonsgegevens (Wbp) in juridische zin een bewerker. Of deze derde partij zelf iets aanpast of niet, is voor de Wbp niet relevant. De organisatie is en blijft eigenaar en verantwoordelijk voor alle persoonsgegevens. Daarmee is de organisatie verplicht om beveiligingsmaatregelen te laten uitvoeren door deze derde partij en deze ook jaarlijks te (laten) toetsen. Deze beveiligingsmaatregelen en verantwoordelijkheden worden in een bewerkersovereenkomst vastgelegd.

- *Melden van (beveiligings)incidenten*

"In het geval van afnemen van producten en/of diensten accepteert de leverancier dat (beveiligings)incidenten direct worden gemeld aan de organisatie, en als dat wettelijk noodzakelijk is ook aan het College Bescherming Persoonsgegevens (CBP). Bij niet gemelde incidenten waar persoonsgegevens bij betrokken zijn, zal de organisatie een ontvangen boete en ontstane schade verhalen op de leverancier."

DOEL VAN DEZE BEPALING:
Als de leverancier informatie van de organisatie host op haar systemen, dienen (beveiligings)incidenten direct te worden gemeld aan de betrokken contactpersoon van de organisatie. De organisatie dient te kunnen reageren op (beveiligings)incidenten.

- *Incidenten met persoonsgegevens*

"Als de leverancier informatie van de organisatie host op haar systemen, dienen (beveiligings)incidenten direct gemeld te worden aan de betrokken contactpersoon van de organisatie."

Vanaf 1 januari 2015, dient een verantwoordelijke overheidsorganisatie, bij een inbreuk op beveiliging met aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens, onverwijld het CBP daarvan in kennis te stellen. Het niet (of niet tijdig) melden kan leiden tot een boete van 450.000 euro.

- *Controle en toezicht*

"De organisatie kan een (broncode)audit laten uitvoeren om te controleren dat aan beveiligingseisen die van toepassing zijn wordt voldaan. Een Third Party Mededeling (TPM) kan als vervanging van de gevraagde audit worden gebruikt om aan te tonen dat aan beveiligingseisen voldaan is."

DOEL VAN DEZE BEPALING:
De leverancier kan te maken krijgen met beveiligingseisen in bijvoorbeeld de bewerkersovereenkomst, de organisatie moet dan controleren dat die beveiligingseisen ook worden nageleefd. Om te voorkomen dat bij een leverancier door iedere klant jaarlijks audits worden uitgevoerd, kan de leverancier ook volstaan met een Third Party Mededeling (TPM) waardoor de auditlast verminderd.

- *Escrow*

"De leverancier draagt zorg voor een Escrow. Zo heeft de organisatie in voorkomend geval de mogelijkheid om bij het in vervulling gaan van één of meer in de Escrow genoemde voorwaarden, software die onderdeel is van het contract, eigenmachtig te (laten) gebruiken voor het herstellen van fouten en anderszins het onderhouden en beheren van de standaardprogrammatuur."

DOEL VAN DEZE BEPALING:
De organisatie die software gebruikt van een leverancier op haar eigen ICT-infrastructuur of in een Cloud-achtige toepassing, moet de mogelijkheid hebben om bijvoorbeeld in het geval dat de software leverancier failliet gaat, kunnen waarborgen dat de software onderhouden en gebruikt kan blijven worden. Dit wordt overeengekomen is een Escrow waarbij een derde partij de broncode van het product aan de organisatie vrijgeeft in dergelijke specifieke gevallen.