CONCEPT Risicoanalyse

MAPGOOD model

Inhoud

[Inleiding 2](#_Toc69977303)

[Quick scan MAPGOOD model 3](#_Toc69977304)

[Risicocomponenten 5](#_Toc69977306)

[Voorbeeldrisico’s 7](#_Toc69977307)

[Jurisprudentie zorgplicht leverancier 17](#_Toc69977308)

##

## Inleiding

In artikel 3 GIBIT komt de precontractuele zorgplicht van de Leverancier duidelijk naar voren. De GIBIT vult de zorgplicht voor wat betreft de voorfase van contracteren nader in. Leverancier moet zich namelijk niet alleen goed op de hoogte stellen van relevante informatie over Opdrachtgever en het voorgenomen project (artikel 3.2/3.3), maar daar vervolgens ook wat mee doen door deze informatie te vertalen in het aanbod en de risicoanalyse (artikel 3.4/3.5). Van Leverancier wordt in feite verwacht dat hij voldoet aan het “ken uw klant” en “ken uw product” principe. Doordat Leverancier de Opdrachtgever moet waarschuwen voor eventueel gesignaleerde risico’s, wordt bovendien bewerkstelligd dat Opdrachtgever vooraf weet met welke risico’s rekening gehouden moet worden.

De gedachte is dat de inventarisatie van risico’s zo meer naar voren wordt gehaald en beide partijen beter weten waar ze aan beginnen en vroegtijdig mitigerende maatregelen kunnen treffen.

De aard en omvang van de risicoanalyse zal per opdracht verschillen. Bij kleine opdrachten of projecten is denkbaar dat de inventarisatie nauwelijks iets om het lijf heeft en bij wijze van spreken beperkt blijft tot het door Leverancier uitdrukkelijk wijzen op de systeemeisen en navraag doen naar gebruik van bij Leverancier bekende incompatibele combinaties van hard- en software; bij grote opdrachten en projecten zal hier meer van beide partijen gevergd worden. Nuance en maatwerk blijven terugkerende thema’s ook hier. Het gaat inderdaad niet alleen om de grote van de opdracht maar ook de voorzienbaarheid en bekendheid van risico’s. Kleine opdrachten, waarvan bekend is dat zij veel risico in zich dragen, leidt ook tot een zwaardere plicht dit vooraf te melden.

Bij zeer risicovolle en complexe projecten ligt het voor de hand separaat advies in te winnen over de risico’s, hetzij bij Leverancier zelf als afzonderlijke (deel)opdracht, hetzij bij een derde partij. In dit soort gevallen is er echter geen sprake meer van een precontractuele verplichting. Het is nu een opdracht geworden waar een factuur tegenover staat. Dit kan zeker voor risicovolle en complexe projecten wenselijk zijn.

Steeds moet worden bedacht dat de risicoanalyse een invulling is van de precontractuele zorgplicht. Deze analyse gaat dus ook niet verder dan wat er redelijkerwijs precontractueel van een leverancier mag worden verwacht. Juist een Leverancier die zijn eigen product kent, kan in voorkomend geval er tijdig voor waarschuwen (en ook goed uitleggen) dat een goede risicoanalyse dusdanig veel tijd en moeite kost dat het in dat specifieke geval niet redelijk is dit te beschouwen als onderdeel van de offertefase. In de meeste gevallen zal deze precontractuele verplichting vallen binnen wat er redelijkerwijs van een Leverancier mag worden verwacht.

Hierbij moet ook benadrukt worden dat Opdrachtgever gehouden is om medewerking te verlenen aan de risicoanalyse, door redelijkerwijs gevraagde informatie aan te leveren (artikel 3.3).

Bij een gebrek aan medewerking door Opdrachtgever kan van Leverancier niet meer worden verwacht dan dat deze zijn aanbod doet op basis van de wel beschikbare informatie. Leveranciers doen er zodoende goed aan te documenteren, en liefst te expliciteren, op basis van welke informatie zij hun aanbod doen. Dit maakt voor beide partijen duidelijk wat de basis voor de samenwerking vormt.

Afhankelijk van de waarde van de opdracht en/of het eigen inkoopbeleid van gemeenten zal een opdracht aanbesteed moeten worden De aanbestedingswetgeving beperkt de ruimte voor leveranciers om zelf bij opdrachtgevers tijdens het aanbestedingsproces navraag te doen. Dit wordt erkend in artikel 3.5 van de GIBIT. In dit geval dient alle relevante informatie die nodig is voor de Leverancier in de aanbestedingsstukken te zijn opgenomen.

Uiteraard moet de Leverancier in de nota van inlichtingen om aanvullende informatie vragen wanneer de aanbestedingstukken niet duidelijk genoeg antwoord geven op bepaalde vragen.

## Quick scan MAPGOOD model

### Deze risicoanalyse behelst een Quick scan aanpak die er voor zorgt dat op een pragmatische en effectieve manier de juiste zaken in kaart worden gebracht. Met behulp van de zeven componenten van het MAPGOOD model kan de Leverancier de risico’s omtrent de ICT-prestatie categoriseren. MAPGOOD staat voor:

* Mens, de mensen die nodig zijn om het informatiesysteem te beheren en gebruiken.
* Apparatuur, de apparatuur die nodig is om het informatiesysteem te laten functioneren.
* Programmatuur, de programmatuur waaruit het informatiesysteem bestaat.
* Gegevens, de gegevens die door het systeem worden verwerkt.
* Organisatie, de organisatie die nodig is om het informatiesysteem te laten functioneren.
* Omgeving, de omgeving waarbinnen het informatiesysteem functioneert.
* Diensten, de externe diensten die nodig zijn om het systeem te laten functioneren

Belangrijk is dat ieder MAPGOOD-component afgewogen moet worden wat het risico is, hoe zwaar deze weegt, welke beheersmaatregel hier op kan volgen en waar het eigenaarschap ligt.

Het gaat om de componenten in de hierna opgenomen tabel. In de bijlage bevinden zich voorbeeldrisico’s per component conform het MAPGOOD model. Met behulp van de zeven componenten van het MAPGOOD model kan de Leverancier de risico’s omtrent de ICT-prestatie categoriseren. Voeg waar nodig nieuwe rijen in. De tabel is niet limitatief en niet alle risico’s hoeven van toepassing te zijn op de ICT-prestatie. Van de Leverancier wordt verwacht dat hij bij een inschrijving of indiening van een offerte onderbouwd welke mitigerende maatregelen kunnen worden getroffen bij de aangegeven risico’s.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Risicocomponent** | **Eigenaar** | **Kans** | **Effect** | **Mogelijke gevolgen** | **Beheersmaatregel** |
| **OG** | **Gedeeld** | **ON** |
| **Mens** | **Wegvallen:** |  |  |  |  |  |  |  |
| **Onopzettelijk foutief handelen:** |  |  |  |  |  |  |  |
| **Opzettelijk foutief handelen:** |  |  |  |  |  |  |  |
| **Apparatuur**  | **Spontaan technisch falen:** |  |  |  |  |  |  |  |
| **Technisch falen door externe invloeden:** |  |  |  |  |  |  |  |
| **Menselijk handelen/falen:** |  |  |  |  |  |  |  |
| **Programmatuur** | **Nalatig menselijk handelen:** |  |  |  |  |  |  |  |
| **Onopzettelijk menselijk handelen:** |  |  |  |  |  |  |  |
| **Opzettelijk menselijk handelen:** |  |  |  |  |  |  |  |
| **Technische fouten/mankementen:** |  |  |  |  |  |  |  |
| **Organisatorische fouten:** |  |  |  |  |  |  |  |
| **Gegevens** | **Via gegevensdragers (CD/DVD/ USB-sticks/ Harddisk/ Back-ups/ mobiele apparaten):** |  |  |  |  |  |  |  |
| **Via Cloud voorzieningen:** |  |  |  |  |  |  |  |
| **Via apparatuur:** |  |  |  |  |  |  |  |
| **Via programmatuur:** |  |  |  |  |  |  |  |
| **Via personen:** |  |  |  |  |  |  |  |
| **Gebruikersorganisatie:** |  |  |  |  |  |  |  |
| **Beheerorganisatie:** |  |  |  |  |  |  |  |
| **Ontwikkelingsorganisatie:** |  |  |  |  |  |  |  |

## Risicocomponenten

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| **Omgeving** | **Huisvesting:** |  |  |  |  |  |  |  |
| **Nutsvoorzieningen:** |  |  |  |  |  |  |  |
| **Buitengebeuren:** |  |  |  |  |  |  |  |
| **Diensten** | **Diensten worden niet conform afspraak geleverd:** |  |  |  |  |  |  |  |
| **Diensten dienstverlener tijdelijk niet beschikbaar:** |  |  |  |  |  |  |  |
| **Diensten dienstverlener definitief niet meer te leveren:** |  |  |  |  |  |  |  |

## Voorbeeldrisico’s

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Nr.** | **Risico** | **Eigenaar** | **Kans** | **Effect** | **Mogelijke gevolgen** | **Beheersmaatregel** |
| **OG** | **Gedeeld** | **ON** |
| **Mens** | **Wegvallen:** |
| 1 | Voorzienbaar (ontslag, vakantie) |   |   |   |   |   |   |   |
| 2 | Onvoorzienbaar (ziekten, overlijden, ongeval, staking) |   |   |   |   |   |   |   |
| **Onopzettelijk foutief handelen:** |
| 3 | Onkunde, slordigheid |   |   |   |   |   |   |   |
| 4 | Foutieve procedures |   |   |   |   |   |   |   |
| 5 | Complexe foutgevoelige bediening |   |   |   |   |   |   |   |
| 6 | Onzorgvuldige omgang met wachtwoorden |   |   |   |   |   |   |   |
| 7 | Onvoldoende kennis/training |   |   |   |   |   |   |   |
| **Opzettelijk foutief handelen:** |
| 8 | Niet werken volgens voorschriften/procedures |   |   |   |   |   |   |   |
| 9a | Diefstal |   |   |   |   |   |   |   |
| 9b | Fraude |   |   |   |   |   |   |   |
| 9c | Lekken van informatie |   |   |   |   |   |   |   |
| 10 | Ongeautoriseerde toegang met account van medewerker met hogere autorisaties |   |   |   |   |   |   |   |
| **Apparatuur**  | **Spontaan technisch falen:** |
| 11 | Veroudering/slijtage |   |   |   |   |   |   |   |
| 12 | Storing |   |   |   |   |   |   |   |
| 13 | Ontwerp/fabricage/installatie/onderhoud fouten |   |   |   |   |   |   |   |
| **Technisch falen door externe invloeden:** |
| 14 | Stroomuitval |   |   |   |   |   |   |   |
| 15 | Slechte klimaatbeheersing |   |   |   |   |   |   |   |
| 16 | Nalatig onderhoud door schoonmaak |   |   |   |   |   |   |   |
| 17 | Elektromagnetische straling |   |   |   |   |   |   |   |
| 18 | Elektrostatische lading |   |   |   |   |   |   |   |
| 19 | Natuurgeweld |   |   |   |   |   |   |   |
| 20 | Diefstal/schade |   |   |   |   |   |   |   |
| **Menselijk handelen/falen:** |
| 21 | Installatiefout |   |   |   |   |   |   |   |
| 22 | Verkeerde instellingen |   |   |   |   |   |   |   |
| 23 | Bedieningsfouten |   |   |   |   |   |   |   |
| 24 | Opzettelijke aanpassingen/sabotage |   |   |   |   |   |   |   |
| 25 | Beschadiging/vernieling |   |   |   |   |   |   |   |
| 26 | Verlies/diefstal (onder andere USB-sticks of andere gegevensdragers) |   |   |   |   |   |   |   |
| 27 | Verwijdering van onderdelen waardoor storingen ontstaan |   |   |   |   |   |   |   |
|  |  |  |  |  |  |  |  |  |  |
| **Programmatuur** | **Nalatig menselijk handelen:** |
| 28 | Ontwerp-, programmeer-, invoering, beheer/onderhoudsfouten |   |   |   |   |   |   |   |
| 29 | Introductie van virus en dergelijke door gebruik van niet gescreende programma's |   |   |   |   |   |   |   |
| 30 | Gebruik van de verkeerde versie van programmatuur |   |   |   |   |   |   |   |
| 31 | Slechte documentatie |   |   |   |   |   |   |   |
| **Onopzettelijk menselijk handelen:** |
| 32 | Fouten door niet juist volgen van procedures |   |   |   |   |   |   |   |
| 33 | Installatie van malware en virussen door gebruik van onjuist/hoge autorisaties bijvoorbeeld gebruik admin-account tijdens browsen websites |   |   |   |   |   |   |   |
| **Opzettelijk menselijk handelen:** |
| 34 | Manipulatie voor of na ingebruikname |   |   |   |   |   |   |   |
| 35 | (Ongeautoriseerde) functieverandering en/of toevoeging |   |   |   |   |   |   |   |
| 36 | Installatie van virussen, Trojaanse paarden en dergelijke |   |   |   |   |   |   |   |
| 37 | Kapen van autorisaties van collega's |   |   |   |   |   |   |   |
| 38 | Illegaal kopiëren van programmatuur |   |   |   |   |   |   |   |
| 39 | Oneigenlijk gebruik of privégebruik van bedrijfs-programmatuur |   |   |   |   |   |   |   |
| **Technische fouten/mankementen:** |
| 40 | Fouten in code programmatuur die de werking verstoren |   |   |   |   |   |   |   |
| 41 | Achterdeuren in programmatuur voor (onbevoegde) toegang |   |   |   |   |   |   |   |
| 42 | Bugs/fouten in code die tot exploits kunnen leiden |   |   |   |   |   |   |   |
| **Organisatorische fouten:** |
| 43 | Leverancier gaat failliet |   |   |   |   |   |   |   |
| 44 | Geen goede afspraken met leverancier |   |   |   |   |   |   |   |
| **Gegevens** | **Via gegevensdragers (CD/DVD/ USB-sticks/ Harddisk/ Back-ups/ mobiele apparaten):** |
| 45a | Diefstal/zoekraken |   |   |   |   |   |   |   |
| 45b | Lekken |   |   |   |   |   |   |   |
| 46 | Beschadiging door verkeerde behandeling |   |   |   |   |   |   |   |
| 47 | Niet overeenkomende bestandformaten |   |   |   |   |   |   |   |
| 48 | Foutieve of geen versleuteling |   |   |   |   |   |   |   |
| 49 | Foutieve of vervalste identificatie van ontvangers om aan gegevens te komen |   |   |   |   |   |   |   |
| **Via Cloud voorzieningen:** |
| 50 | Ongeautoriseerde toegang door onbevoegden (hackers/hosters) |   |   |   |   |   |   |   |
| 51a | Ongeautoriseerde wijziging van gegevens (hacking) |   |   |   |   |   |   |   |
| 51b | Ongeautoriseerde verwijdering van gegevens (hacking) |   |   |   |   |   |   |   |
| **Via apparatuur:** |
| 52 | Fysieke schrijf- of leesfouten |   |   |   |   |   |   |   |
| 53 | Onvoldoende toegangsbeperking tot apparatuur |   |   |   |   |   |   |   |
| 54 | Fouten in interne geheugens |   |   |   |   |   |   |   |
| 55 | Aftappen van gegevens |   |   |   |   |   |   |   |
| **Via programmatuur:** |
| 56 | Foutieve of gemanipuleerde programmatuur |   |   |   |   |   |   |   |
| 57 | Doorwerking van virussen/malware |   |   |   |   |   |   |   |
| 58 | Afbreken van verwerking |   |   |   |   |   |   |   |
| **Via personen:** |
| 59a | (On)opzettelijke foutieve gegevensinvoer en -verandering van data |   |   |   |   |   |   |   |
| 59b | (On)opzettelijke foutieve gegevensverwijdering van data |   |   |   |   |   |   |   |
| 60 | Onbevoegde toegang door onbevoegden bijvoorbeeld hackers en dergelijke via malware |   |   |   |   |   |   |   |
| 61 | Onbevoegd kopiëren van gegevens  |   |   |   |   |   |   |   |
| 62 | Meekijken over de schouder door onbevoegden |   |   |   |   |   |   |   |
| 63 | Onzorgvuldig vernietigen van gegevens bijvoorbeeld laten liggen op printer |   |   |   |   |   |   |   |
| 64 | Niet toepassen clear screen/clear desk |   |   |   |   |   |   |   |
| 65 | Aftappen (draadloos) netwerk door onbevoegden (telewerk situaties) |   |   |   |   |   |   |   |
| 66 | Oneigenlijk gebruik van autorisaties |   |   |   |   |   |   |   |
| 67 | Toegang verschaffen tot gegevens door middel van identiteitsfraude of social engineering |   |   |   |   |   |   |   |
| **Gebruikersorganisatie:** |
| 68 | Mismanagement |   |   |   |   |   |   |   |
| 69 | Gebrekkige toedeling taken, bevoegdheden en verantwoordelijkheden |   |   |   |   |   |   |   |
| 70 | Onduidelijke of ontbrekende gedragscodes |   |   |   |   |   |   |   |
| 71 | Afwezige, verouderde of onduidelijke handboeken/ systeemdocumentatie/ werkprocedures/ gebruiksinstructies |   |   |   |   |   |   |   |
| 72 | Onvoldoende interne controle |   |   |   |   |   |   |   |
| 73 | Onvoldoende toetsing op richtlijnen |   |   |   |   |   |   |   |
| 74 | Onvoldoende of geen contractbeheer |   |   |   |   |   |   |   |
| 75 | Ontbrekende of onduidelijke SLA’s  |   |   |   |   |   |   |   |
| 76 | Gebrekkige doel/middelen beheersing |   |   |   |   |   |   |   |
| **Beheerorganisatie:** |
| 77 | Gebrekkig beleid betreffende beheer |   |   |   |   |   |   |   |
| 78 | Onvoldoende kennis of capaciteit |   |   |   |   |   |   |   |
| 79 | Onvoldoende kwaliteitsborging |   |   |   |   |   |   |   |
| 80 | Onvoldoende beheer van systemen en middelen |   |   |   |   |   |   |   |
| **Ontwikkelingsorganisatie:** |
| 81 | Slecht projectmanagement |   |   |   |   |   |   |   |
| 82 | Niet volgen van projectenkalender of PPM |   |   |   |   |   |   |   |
| 83 | Geen ontwikkelrichtlijnen en/of – procedures |   |   |   |   |   |   |   |
| 84 | Er worden geen methoden/technieken gebruikt |   |   |   |   |   |   |   |
| 85 | Gebrek aan planmatig werken |   |   |   |   |   |   |   |
| **Omgeving** | **Huisvesting:** |
| 86 | Ongeautoriseerde toegang tot gebouw(en) |   |   |   |   |   |   |   |
| 87 | Diefstal op werkplekken |   |   |   |   |   |   |   |
| 88 | Gebreken in ruimtes, waardoor kans op insluiping/inbraak |   |   |   |   |   |   |   |
| 89 | Onvoldoende fysieke voorzieningen om te vluchten of in te grijpen tijdens geweldsdreigingen/conflicten met klanten |   |   |   |   |   |   |   |
| **Nutsvoorzieningen:** |
| 90 | Uitval van elektriciteit, water, telefoon |   |   |   |   |   |   |   |
| 91 | Wateroverlast door lekkage, bluswater |   |   |   |   |   |   |   |
| 92 | Uitval van licht-, klimaat- en/of sprinklerinstallatie |   |   |   |   |   |   |   |
| **Buitengebeuren:** |
| 93 | Natuurgeweld (overstroming, blikseminslag, storm, aardbeving et cetera) |   |   |   |   |   |   |   |
| 94a | Overig geweld bijvoorbeeld oorlog, terrorisme, brandstichting en neerstortend vliegtuig |   |   |   |   |   |   |   |
| 94b | Overig geweld bijvoorbeeld inbraak |   |   |   |   |   |   |   |
| 95 | Blokkade/staking |   |   |   |   |   |   |   |
| 96 | Onveilige, geblokkeerde, vluchtwegen bij brand |   |   |   |   |   |   |   |
| **Diensten** | **Diensten worden niet conform afspraak geleverd:** |
| 97 | Slecht opgeleid personeel |   |   |   |   |   |   |   |
| 98 | Groot personeelsverloop |   |   |   |   |   |   |   |
| 99 | Onvoldoende capaciteit in personeel |   |   |   |   |   |   |   |
| 100 | Valse verklaringen over certificeringen |   |   |   |   |   |   |   |
| 101 | Onvoldoende of geen kwaliteitsborging |   |   |   |   |   |   |   |
| 102 | Personeel voldoet niet aan eisen zoals een geldige VOG en getekende geheimhoudingsverklaringen |   |   |   |   |   |   |   |
| 103 | Voert wanbeheer, slordigheden in beheersactiviteiten, |   |   |   |   |   |   |   |
| 104 | Werkt niet conform ITIL of BiSL-principes |   |   |   |   |   |   |   |
| 105 | Maakt misbruik van toevertrouwde gegevens, applicaties en documentatie |   |   |   |   |   |   |   |
| 106 | Houdt zich niet aan functiescheiding |   |   |   |   |   |   |   |
| 107 | Maakt gebruik van te zware autorisatie, niet functie gebonden |   |   |   |   |   |   |   |
| **Diensten dienstverlener tijdelijk niet beschikbaar:** |
| 108 | Levert diensten niet conform overeenkomst |   |   |   |   |   |   |   |
| 109 | Onderbreking dienstverlening door overname dienstverlener |   |   |   |   |   |   |   |
| 110 | Kan diensten tijdelijk niet uitvoeren door zaken buiten de eigen controle bijvoorbeeld stakingen en dergelijke |   |   |   |   |   |   |   |
| 111 | Past verkeerde prioriteiten toe in klantbejegening |   |   |   |   |   |   |   |
| 112 | Levert onvoldoende capaciteit voor een goede dienstverlening |   |   |   |   |   |   |   |
| **Diensten dienstverlener definitief niet meer te leveren:** |
| 113 | Een dienstverlener gaat failliet |   |   |   |   |   |   |   |
| 114 | Opzegging diensten door dienstverlener |   |   |   |   |   |   |   |

## Jurisprudentie zorgplicht leverancier

De Risicoanalyse is een invulling van de precontractuele zorgplicht. Deze zorgplicht gaat niet verder dan wat er redelijkerwijs precontractueel mag worden verwacht. Er zijn verschillende zorgplichten die in jurisprudentie zijn aangenomen:

* In geval van projectleiding dient een IT-leverancier de voortgang proactief te bewaken en een klant aan te spreken indien deze niet voortvarend genoeg mee werkt (Kwetters/Profuse)
* Een adviseur die weet dat de implementatie van een bepaald pakket grote risico's met zich meebrengt, dient de klant daarop te wijzen (Breikant)
* Een leverancier van een IT-systeem die bekend is met het gebruik dat de klant daarvan wil maken, dient de klant te waarschuwen voor bijkomende kosten van derden bij onvoldoende voortgang (Set/Triple Ace)
* Een IT-leverancier die meent dat voor het welslagen van een project een bepaald traject noodzakelijk is, dient de klant daar vooraf op te wijzen en te waarschuwen voor de risico's van het achterwege laten daarvan (SGOA, softwareapplicatie en website).
* Overeengekomen budget- en resultaatverantwoordelijkheid van de IT-leverancier brengt een waarschuwingsplicht voor de leverancier mee indien wijzigingen die de klant verlangt het budget of resultaat in gevaar brengen (SGOA, maximumbedrag en wijzigen specificaties).
* Bij de aanschaf van software mag de klant in ieder geval de functionaliteit verlangen waarvan hij aan de leverancier heeft aangegeven dat die voor hem van belang is en die ook benodigd is voor het normaal gebruik van de software, tenzij hij is gewaarschuwd dat de functionaliteit in de software ontbreekt (Exact/Brandmeester's)
* Een IT-Leverancier dient de klant te behoeden voor te hoog gespannen verwachtingen (Dolmans/Burroughs)
* Een IT Leverancier dient de klant te weerhouden van ongefaseerde ingebruikneming als hij behoort te voorzien dat dit voor problemen leidt (Dolmans/Burroughs).
* Een adviseur dient onnodige maatwerkopdrachten te voorkomen c.q. in te dammen (Breikant).

In de volgende voorbeelden was geen sprake van schending van een precontractuele zorgplicht:

* "De enkele omstandigheid dat problemen zijn gerezen, brengt niet automatisch met zich mee dat de leverancier zijn zorgplicht heeft veronachtzaamd (Rb. Noord-Nederland 9 maart 2016, ECLI:NL:RBNNE:2016:997 (Agion/Almedo), r.o. 5.5)"
* Een leverancier van standaardsoftware die zelf niet verantwoordelijk is voor implementatie en integratie, schiet niet te kort in de leverplicht als die software uiteindelijk niet blijkt te werken in de beoogde doelomgeving waarvoor de leverancier geen verantwoordelijkheid draagt (Hof ’s-Hertogenbosch 13 februari 2018, ECLI:NL:GHSHE:2018:570 (Ziekenhuissoftware)
* "Op een leverancier van hardware die geen bijzondere informatie heeft ontvangen over het gebruik van de hardware, rust geen dermate grote zorgplicht dat hij de klant moet waarschuwen over het feit dat de hardware in de toekomst wellicht niet meer geschikt zal zijn. (Rb. Arnhem 19 november 2003, ECLI:NL:RBARN:2003:AN8897 (Tip Top),r.o. 3.6)"
* "Op een IT-leverancier rust op grond van een algemene zorgplicht geen verplichting om een back-up te maken van alle volledige bestanden van de klant (Hof Amsterdam 28 april 2015, ECLI:NL:GHAMS:2015:1635 (Staalbouw/X),r.o. 3.12.)"De Leverancier is afhankelijk van de informatie van de aanbestedende dienst om zijn precontractuele zorgplicht goed te kunnen uitvoeren.