GIBIT 2025

Toelichting per artikel

VNG Realisatie
Nassaulaan 12
2514 JS Den Haag

www.gibit.nl

12 februari 2026

Inhoud

I
Algemeen deel

Artikel 1. Begrippen

In dit artikel zijn de diverse centrale begrippen uit de GIBIT gedefinieerd. Deze begrippen worden niet afzonderlijk toegelicht, doch worden besproken bij de verschillende artikelen waar ze worden gebruikt.

In algemene zin kan worden opgemerkt dat gepoogd is de begrippen abstract en beschrijvend te houden en zeer terughoudend te zijn met het opnemen van inhoudelijke keuzes in de begrippen. De GIBIT-voorwaarden blijven generiek, abstract van karakter. Ze moeten immers op een veelheid aan situaties van toepassing kunnen zijn.

In de GIBIT wordt om de wederpartij van de Leverancier aangeduid als "Opdrachtgever". Hiervoor is gekozen omdat de GIBIT behalve door gemeenten zelf, ook gebruikt kan worden door gemeentelijke samenwerkingsverbanden of andere (al dan niet aan de gemeente gelieerde) instanties. Vandaar dat niet voor bijvoorbeeld "Gemeente" is gekozen. In deze toelichting wordt daarom ook steeds over "Opdrachtgever" gesproken. Met de keuze voor het woord "Opdrachtgever" is overigens niet bedoeld om de juridische relatie te kwalificeren. Overeenkomsten die onder de GIBIT worden gesloten kunnen kwalificeren als overeenkomst van opdracht, als koopovereenkomst, als gemengde overeenkomst met een opdrachtelement, of als een andersoortige overeenkomst. Het is goed denkbaar dat er geen enkel opdrachtelement in de Overeenkomst zit.

Overigens geldt voor alle definities: het enkele feit dat Partijen in de praktijk andere woorden gebruiken om een begrip aan te duiden (bijv. "projectplan" in plaats van "implementatieplan"), doet aan de betekenis, de duiding en de juridische gevolgen van die duiding in de Inkoopvoorwaarden niets af.

De inhoudelijke wijzigingen in de begrippen van de GIBIT-versie 2025 ten opzichte van de versie 2023 zijn de volgende:

- Acceptatie: Er is een scherper onderscheid gemaakt tussen definities en inhoudelijke eisen, omdat de eisen aan Acceptatie losstaan van de betekenis van Acceptatie.
- Acceptatieprocedure: Er is een strakker onderscheid gemaakt tussen definities en inhoudelijke eisen, omdat de eisen aan een Acceptatieprocedure losstaan van de betekenis van de Acceptatieprocedure.
- AI-systeem: Het begrip AI-systeem is toegevoegd. Dit is dezelfde definitie als die aan AI-systemen wordt gegeven in de AI Act (Verordening (EU) 2024/1689), en dient hetzelfde te worden geïnterpreteerd.
- Algoritmische toepassing: Het begrip Algoritmische toepassing is uitgebreid, om duidelijk te maken dat AI-systemen altijd algoritmische toepassingen zijn.
- Applicatielandschap: Deze definitie is ten opzichte van de versie 2023 tekstueel iets gewijzigd, zonder juridisch gevolg. Het gaat bij het Applicatielandschap om het "totaalplaatje" van de ICT binnen de organisatie van Opdrachtgever. In de Inkoopvoorwaarden wordt verder gesproken over de "relevante onderdelen van het Applicatielandschap".

- Bestek: Duidelijk is gemaakt dat het Bestek alle bij de aanbesteding gedeelde stukken betreft. Het gaat hierbij om stukken waarin bijvoorbeeld de organisatie van Opdrachtgever, de ICT Prestatie, de contract- en organisatiedoelen en het door Opdrachtgever beoogde gebruik van de ICT Prestatie, alsmede de aanbestedingsprocedure zijn beschreven en toegelicht.

- Conversie: Deze definitie is ten opzichte van de versie 2023 tekstueel iets gewijzigd, zonder juridisch gevolg. Soms zal Conversie immers nodig zijn zonder het bestaande systeem volledig te vervangen, of zal Conversie uit een ander systeem nodig zijn. Ook daar kan de GIBIT nu op zien. Ook zijn de definities van Conversie en Migratie uit elkaar gehaald, en is een scherper onderscheid gemaakt tussen definities en inhoudelijke eisen.

- CSIRT: Het begrip CSIRT is toegevoegd. Dit is in het geval van gemeenten de Informatiebeveiligingsdienst (IBD) van de VNG.

- Data: Het begrip Data is toegevoegd. Dit is dezelfde definitie als die aan Data wordt gegeven in de Data Act (Verordening (EU) 2023/2854), en dient hetzelfde te worden geïnterpreteerd. Overal waar in de versie 2023 “gegevens” stond terwijl het om Data ging, is deze definitie doorgevoerd.

- Documentatie: Deze definitie is aangescherpt ten opzichte van de versie 2023. Het gaat bij Documentatie om technische en gebruikersdocumentatie, zoals handleidingen, en beschrijvingen van de ICT Prestatie. Het is zaak voor Partijen om af te stemmen welke documentatie opgeleverd en bijgehouden moet worden. Voorstelbaar is dat de eisen aan Documentatie van Open Source-programmatuur bijvoorbeeld verder zullen strekken.

- Exit-plan: Het begrip Exit-plan is toegevoegd. Hoewel de term in de versie 2023 namelijk veel voorkwam, was dit nog niet gedefinieerd.

- Functieherstelttijd: Deze definitie is geschrapt. De term stond weliswaar in artikel 1 als definitie opgenomen, maar werd verder niet in de Inkoopvoorwaarden gebruikt. Zodoende heeft ze een plek gekregen in de Inkoopvoorwaarden (artikel 10), en is ze uit de definitielijst gehaald.

- Gebruikersondersteuning: Deze definitie stond in de versie 2023 in de tekst van de Inkoopvoorwaarden opgenomen (10.7), en is naar de definities verplaatst. Ook is toegevoegd dat Gebruikersondersteuning louter gaat om vragen over het gebruik van de ICT Prestatie; vragen die bijvoorbeeld gaan over een systeem waarmee gekoppeld is, vallen hier niet onder.

- GIBIT 2025: De definitie van GIBIT 2023 is vervangen door GIBIT 2025.

- Implementatie: Er is een strakker onderscheid gemaakt tussen definities en inhoudelijke eisen, omdat de eisen aan Implementatie losstaan van de betekenis van Implementatie.

- Inkoopvoorwaarden: De definitie van GIBIT 2023 is vervangen door GIBIT 2025.

- Jaarvergoeding: In deze bepaling was abusievelijk geen provisie opgenomen voor de situatie waarin de Overeenkomst langer voortduurt dan overeengekomen. Dan zou immers de (feitelijk betaalde) Vergoeding worden gedeeld door de initieel beoogde looptijd. Dit is dan echter geen realistische weergave van een Jaarvergoeding meer.

- Koppeling: Deze definitie is uitgebreid. In de versie 2023 ging het enkel om koppelingen tussen de ICT Prestatie en het Applicatielandschap, maar het is ook mogelijk dat een koppeling wordt gelegd met externe systemen. Het is vervolgens aan Partijen om af te stemmen welke koppelingen opgeleverd en bijgehouden moeten worden.

- Licentie: De term “gebruiksrecht” is vervangen door de term “licentie”. Dit is een tekstuele wijziging, zonder juridisch gevolg.

- Maatwerkprogrammatuur: In de markt bestond de vrees dat ook specifieke inrichtingen van Standaardprogrammatuur (bijv. het doorvoeren van de huisstijl van een gemeente) ook maatwerkprogrammatuur was. De definitie is verduidelijkt om helder te maken dat cosmetische aanpassingen niet zonder meer van Standaardprogrammatuur Maatwerkprogrammatuur maken. Ook bestond in de markt de vrees dat het onderscheid tussen Maatwerkprogrammatuur en Innovatief Onderhoud op verzoek niet duidelijk genoeg was. Dit is verhelderd. Duidelijk is gemaakt dat Partijen het ontwikkelen van Maatwerkprogrammatuur echt expliciet overeen moeten komen. Alsdan zullen Partijen ook afspraken kunnen maken over de (door)ontwikkeling van die Maatwerkprogrammatuur.

- Migratie: Het begrip Migratie is losgekoppeld van Conversie en toegevoegd.

- Opdrachtgever: In de versie 2023 werd over Opdrachtgever gesproken als de Partij "ten behoeve waarvan" de Overeenkomst wordt gesloten. De Overeenkomst wordt echter ten behoeve van beide Partijen gesloten. Een andere definitie is daarom zuiverder.

- Open Source-programmatuur: Omdat Open Source een nieuw thema in de Inkoopvoorwaarden is, is hiervoor een definitie opgesteld.

- Partij: De termen "partij" en "partijen" werden in eerdere versies door elkaar gebruikt met en zonder hoofdletter. In het kader van de eenduidigheid is overal de term "Partij" met een hoofdletter gebruikt, wanneer sprake is van Leverancier en/of Opdrachtgever.

- Programmatuur: Aan de definitie van Programmatuur is toegevoegd dat daaronder ook is te verstaan de te leveren Koppelingen.

- Reactietijd: Deze definitie is geschrapt. De term stond weliswaar in artikel 1 als definitie opgenomen, maar werd verder niet in de Inkoopvoorwaarden gebruikt. Zodoende heeft ze een plek gekregen in de Inkoopvoorwaarden (artikel 10), en is ze uit de definitielijst gehaald.

- Service Levels: De termen "functieherstelttijd" en "reactietijd" stonden weliswaar in artikel 1 als definities opgenomen, maar werden verder niet in de Inkoopvoorwaarden gebruikt. Zodoende hebben ze een plek gekregen in de Inkoopvoorwaarden (artikel 10), en zijn ze uit de definitielijst van artikel 1 gehaald.

- Upgrade: In de markt bestond de vrees dat het onderscheid tussen Maatwerkprogrammatuur en Innovatief Onderhoud op verzoek niet duidelijk genoeg was. Dit is verhelderd. Hierbij wordt opgemerkt dat het aan Partijen is om goede afspraken te maken over doorontwikkeling op opdracht versus het ontwikkelen van Maatwerkprogrammatuur. Het doel is dat gemeenten en leveranciers hier strategisch over afstemmen, bijvoorbeeld via gebruikersverenigingen die de roadmap voor nieuwe functionaliteiten opstellen.

- Vergoeding: De oude definitie ging nog uit van een looptijd, terwijl hiervoor juist de definitie "jaarvergoeding" in het leven is geroepen.

Artikel 2. Toepasselijkheid

Dit artikel geeft enkele algemene regels omtrent de toepasselijkheid van de GIBIT. Daarbij wordt onder ICT Prestatie verstaan de totale leveringsomvang van te leveren Producten en diensten en Licenties.

Artikel 2.1 bepaalt dat de GIBIT niet alleen van toepassing is op de ICT Prestaties uit de Overeenkomst, maar ook op daarmee – eventueel in de toekomst overeen te komen – samenhangende ICT Prestaties. Hiermee wordt beoogd te voorkomen dat op latere, aanvullende, overeenkomsten opeens een andere set voorwaarden van toepassing zou zijn. Hiervan kan uiteraard worden afgeweken; de voorwaarden zijn een vangnet.

Let wel: er is niet beoogd Leveranciers voor alle toekomstige opdrachten bij voorbaat aan de GIBIT te binden. Het beding heeft alleen betrekking op overeenkomsten die samenhangen met een overeenkomst waarbij de toepasselijkheid van de GIBIT reeds bedongen is. Een voorbeeld is dat op een later moment alsnog een onderhoudsovereenkomst wordt afgesloten terwijl die oorspronkelijk niet tot de Overeenkomst behoorde. Deze betreffende onderhoudsovereenkomst valt dan onder de voorwaarden van de GIBIT. Opdrachtgevers dienen er dus op bedacht te zijn voorafgaand aan het sluiten van een overeenkomst – dus al in de fase van een offerteaanvraag/aanbesteding – de GIBIT van toepassing te verklaren. Zodoende wordt geborgd dat vanaf het begin de GIBIT als voorwaarden geldt, ook voor aanvullende Overeenkomsten die op een later moment worden afgesloten.

Het vangnet-karakter van de GIBIT brengt ook met zich dat irrelevante bepalingen niet per definitie geschrapt hoeven te worden. Gaat de Overeenkomst bijvoorbeeld niet over Producten, dan kunnen de bepalingen omtrent Producten gewoon in stand blijven; ze zullen simpelweg niet van toepassing zijn. Dit vergemakkelijkt het tot stand brengen van Overeenkomsten; maatwerk is op dit punt niet nodig.

Artikel 2.2 ziet op de indeling van de GIBIT in vier hoofdstukken. Het algemene hoofdstuk I is altijd van toepassing; de overige hoofdstukken met bepalingen over privacy, beveiliging, archiefbeheer, Dienstverlening op Afstand en Open Source-programmatuur zijn van toepassing naar gelang de aard van de te leveren Producten/diensten (aanvullend).

Artikel 2.3 is opgenomen om algemene voorwaarden van Leveranciers van de hand te wijzen, ook wanneer daar later naar verwezen wordt. Doel van deze bepaling is te voorkomen dat de GIBIT niet van toepassing is in het geval Leveranciers eigen voorwaarden van toepassing verklaren. De bepaling hangt samen met het bepaalde in artikel 6:225 lid 3 BW. Daarin staat – in de kern – dat de algemene voorwaarden die als eerste van toepassing zijn verklaard van toepassing blijven, tenzij bij het van toepassing verklaren van een tweede set algemene voorwaarden de eerste set *uitdrukkelijk* van de hand is gewezen. Het is overigens de vraag of het bepaalde in dit artikel voldoet aan het uitdrukkelijkheidsvereiste als bedoeld in artikel 6:225 lid 3 BW. Opdrachtgevers dienen er dus altijd alert op te zijn dat Leveranciers in het aanbod geen eigen voorwaarden van toepassing verklaren.

Artikel 2.4 is opgenomen om bij eventuele ongeldigheid van een bepaling uit de GIBIT:
1. te voorkomen dat dit effect heeft op de overige bepalingen van de GIBIT; en
2. Partijen te verplichten nieuwe afspraken te maken waarbij doel en strekking van de oorspronkelijke bepaling in acht worden genomen.

Artikel 2.5 bepaalt dat de Overeenkomst prevaleert op hetgeen in de GIBIT is bepaald, terwijl de nadere Overeenkomst en eventuele voorwaarden voor Derdenprogrammatuur en Open Source-programmatuur dan weer prevaleren op deze documenten. Het is een zeer belangrijke bepaling. Dit hangt samen met het abstracte karakter van de GIBIT en het feit dat de GIBIT een vangnet is. Voor de goede orde: in de Overeenkomst tussen Opdrachtgever en Leverancier kan van iedere bepaling in de GIBIT worden afgeweken. Dat in de GIBIT bij sommige bepalingen uitdrukkelijk wordt verwezen naar de Overeenkomst en in andere bepalingen niet, is hiervoor niet relevant. De verwijzingen naar de Overeenkomst zijn in voorkomend geval louter opgenomen om extra aandacht te vestigen op de mogelijkheid om af te wijken.

Ook is in het lid bepaald dat de voorwaarden van Derdenprogrammatuur, mits deze op de goede wijze van toepassing zijn verklaard, prevaleren boven de afspraken tussen partijen. De gedachte hierachter is dat een derde updates kan doorvoeren, garanties kan weigeren, etc., zonder dat de leverancier daar invloed op heeft. Het gaat daarbij niet om licentie- en onderhoudsvoorwaarden in de tekstuele zin, maar in brede zin. Ook verkoopvoorwaarden en garantievoorwaarden van die toeleverancier vallen eronder. Dit geldt overigens alleen voor programmatuur, niet voor apparatuur.
Artikel 2.6 bepaalt dat de wet als vangnet van toepassing is. Het contractenrecht is in de kern nagenoeg volledig regelend recht. De wet geeft aldus de ‘default’, tenzij Partijen anders overeenkomen. In de rechtspraktijk blijkt evenwel verschillend geoordeeld te worden over wat het bestaan van een contract betekent voor die aspecten van het regelend recht waar Partijen geen

expliciete keuze hebben gemaakt: blijft dan de genoemde 'default' van kracht, of geldt juist slechts het contract? Om aan die onduidelijkheid een einde te maken bepalen de Inkoopvoorwaarden dat het regelend recht in beginsel van toepassing blijft.

Artikel 2.7 bepaalt ten slotte dat wijzigingen op de GIBIT schriftelijk overeengekomen moeten zijn. Ook is bepaald dat wijzigingen slechts voor de in artikel 2.1 bedoelde Overeenkomst gelden. De gedachte is dat voor ieder project opnieuw moet worden bezien welke bepalingen al dan niet relevant zijn.

Artikel 3. Totstandkoming Overeenkomst

In dit artikel komt de zorgplicht van de Leverancier duidelijk naar voren. Deze zorgplicht voor Leveranciers geldt hoe dan ook op grond van de wet en de rechtspraak (vgl. artikel 7:17 lid 5 BW in het kader van koop, artikel 7:401 BW bij opdrachten, de mededelingsplichten op grond van 6:228 BW, etc.). Vaak is echter niet duidelijk wat precies onder deze abstracte zorgplicht wordt verstaan. Die wordt daarom hier in artikel 3 nader ingevuld.

Zoals hierna nader zal worden toegelicht, probeert de GIBIT met de regeling omtrent de risicoanalyse een genuanceerde balans te zoeken in de belangen van Partijen. De regeling voorkomt dat Partijen hun heil moeten zoeken in niet heel scherp afgebakende begrippen als "zorgplichten" en geeft juist een heldere regeling met een in beginsel voorzienbaar risico.
De GIBIT vult de zorgplicht voor wat betreft de voorfase van contracteren nader in. De 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 de Leverancier wordt in feite verwacht dat hij voldoet aan het "ken uw klant" en "ken uw product"-principe. Doordat de 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. Als de Opdrachtgever bij zijn uitvraag expliciet heeft aangegeven wat er bij de inschrijving moet worden ingediend, dan kan van leverancier niet worden verwacht dat hij veel meer dan dat aanlevert, tenzij hij redenen heeft om Opdrachtgever "tegen zichzelf in bescherming te nemen".

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 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 de Leverancier uitdrukkelijk wijzen op de systeemeisen en navraag doen naar gebruik van bij de Leverancier bekende incompatibele combinaties van hard- en software; bij grote opdrachten en projecten zal hier meer van beide Partijen gevergd worden. Het is niet per se noodzakelijk dat er onderzoek bij Opdrachtgever op locatie plaatsvindt. Een Leverancier die zijn eigen Product kent en ervaring heeft met het implementeren daarvan, weet welke informatie vereist is voor het kunnen doen van een goed aanbod en welke valkuilen in dat aanbod dienen te worden geadresseerd (althans behoort dit te weten).

Bij zeer risicovolle en complexe projecten ligt het voor de hand separaat advies in te winnen over de risico's, hetzij bij de Leverancier zelf als afzonderlijke (deel)opdracht, hetzij bij een derde partij. 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.

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), zoals het verstrekken van een beschrijving van het Applicatielandschap. Laat Opdrachtgever dit na, dan komt zij voor die verplichting in (schuldeisers)verzuim. Dat zou overigens ook zonder expliciete tekst in

de GIBIT het geval zijn geweest. Bij een dergelijk gebrek aan medewerking door Opdrachtgever kan van de 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. Het belangrijkste gevolg van de schending van voornoemde "ken uw klant"- en "ken uw product"-principes is dat Opdrachtgever aanspraak kan maken op vergoeding van de tijdens de Implementatie noodzakelijke, maar niet vooraf kenbaar gemaakte aanpassingen aan de eigen ICT-omgeving.

In theorie zou een Opdrachtgever de Overeenkomst ook kunnen ontbinden zodra blijkt dat de Leverancier te kort is geschoten in het doen van een passend aanbod. Juist omdat de GIBIT al de hiervoor beschreven oplossing voor die situatie bevat, gericht op voortgang van het project, en Opdrachtgevers bij het uitoefenen van bevoegdheden ook steeds de redelijkheid en billijkheid in acht dienen te nemen, ligt ontbinding in die situatie echter niet voor de hand. Dit maakt de regeling in de GIBIT ook genuanceerd en zeker niet alleen in het belang van Opdrachtgevers.
Informatie en transparantie over Derdenprogrammatuur is essentieel, ook in de precontractuele fase. Daarom zijn in lid 5 diverse informatieverplichtingen rondom Derdenprogrammatuur opgenomen. De gedachte is dat Opdrachtgever zo een geïnformeerd besluit kan nemen over het al dan niet accepteren van het gebruiken van die Derdenprogrammatuur en de daaraan verbonden die voorwaarden. Die voorwaarden prevaleren namelijk op hetgeen elders in de Overeenkomst is bepaald (artikel 2.5).

Op grond van sub iv moet de Leverancier ook de eventuele afhankelijkheid van Derdenprogrammatuur in het aanbod specificeren. De ervaring leert dat bij discussies over bijvoorbeeld performance (te) snel wordt gewezen op programmatuur van derden. Door vooraf te worden geïnformeerd over die afhankelijkheid, kan Opdrachtgever ook op dit punt een geïnformeerde keuze maken. Bovendien wordt zo oneigenlijk gebruik van dit argument voorkomen.

Afhankelijk van de waarde van de opdracht en/of het eigen beleid van Opdrachtgevers kan het zijn dat een opdracht aanbesteed wordt. De aanbestedingswetgeving beperkt de ruimte voor Leveranciers om zelf bij Opdrachtgevers tijdens het aanbestedingsproces navraag te doen. Dit wordt erkend in artikel 3.6 van de GIBIT.

Met *"schriftelijk"* in artikel 3.7 is wordt bedoeld *"geschreven"*, niet *"op papier"*. Elektronische communicatie is dus ook toegestaan.

Artikel 4. Uitvoering Overeenkomst

Uitgangspunt van GIBIT is dat termijnen niet fataal zijn, behoudens:

a) overeengekomen einddata voor de primaire Implementatie; en
b) overeengekomen data voor Implementatie of levering van Updates/Upgrades in verband met de inwerkingtreding van wijzigingen in wet- en regelgeving.

Hiermee wordt aangesloten bij de systematiek van de wet. Het is belangrijk dat data voor Implementatie fataal zijn; vaak zal de Go Live-datum van een ICT Prestatie samenhangen met het uitfaseren van een oud systeem. In dit licht moet dit artikel overigens ook worden gelezen. Als nazorg ook als onderdeel van de Implementatie wordt beschouwd, moet deze nazorgfase niet worden meegenomen bij het bepalen van de fatale termijn.

Overigens ligt de ingangsdatum van (wijzigingen in) wet- en regelgeving ook vast als fatale termijn. Dit is slechts anders indien deze wet- en regelgeving niet voorzienbaar was of de termijn voor inwerkingtreding aantoonbaar te kort was. Hiervan zal niet snel sprake zijn. Gedacht kan bijvoorbeeld worden aan noodwetgeving of regelgeving met onmiddellijke ingang.

Artikel 4.4 biedt de ruimte om de in artikel 3 bedoelde risicoanalyse op een later moment uit te voeren, bijvoorbeeld in de proof-of-concept-fase (POC) of in de verificatiefase. Dit geeft Leveranciers de ruimte om niet al in de offertefase veel energie in de risicoanalyse te hoeven steken. Het risico dat in deze latere fase onacceptabele risico's naar voren komen, wordt afgedekt

door het recht van Opdrachtgever om in die situatie (tegen vergoeding van gemaakte kosten) de Overeenkomst te ontbinden. Leveranciers hebben dit recht niet. Hier is expliciet voor gekozen: immers, van een Leverancier mag verwacht worden dat hij reeds bij de eerste aanbieding (voordat de risicoanalyse is uitgevoerd) een goed beeld heeft van de risico's aan zijn kant ten aanzien van het leveren van de ICT Prestatie. Dit is ook de reden waarom is expliciet is opgenomen dat de Leverancier algemeen bekende risico's al bij het aanbod moet benoemen.

In artikel 4.5 is uitdrukkelijk bepaald dat Opdrachtgever alle verplichtingen die uit de Overeenkomst voortvloeien zal naleven. Strikt genomen is de bepaling overbodig, omdat dit ook al uit de wet en de Overeenkomst voortvloeit. De bepaling heeft vooral een belangrijke signaalfunctie, zowel richting Opdrachtgevers als Leveranciers. Voor Opdrachtgevers is van belang dat zij zich terdege realiseren dat het van belang is dat de – bijvoorbeeld in het Implementatieplan – gemaakte afspraken over de te verrichten werkzaamheden ook (tijdig) worden nagekomen.

Wij wijzen er volledigheidshalve op dat bij schending van deze medewerkingsplicht Leveranciers zich (ook eerst achteraf) kunnen beroepen op opschorting. In dit geval komt Opdrachtgever in schuldeisersverzuim en kan de Leverancier (dus) niet meer zelf in verzuim geraken. Adequate medewerking verlenen door Opdrachtgever is dus van cruciaal belang. Wel is het zo dat gelet op de wettelijke zorgplicht die op Leveranciers rust, waarschijnlijk van Leveranciers mag worden verwacht dat zij Opdrachtgever waar nodig tijdig aansporen tot het nakomen van de (medewerkings) verplichtingen.

Artikel 5. Transport, eigendom en risico van Producten

Artikel 5 bestaat veelal uit procedurele afspraken die voor zich spreken, de inhoud is grotendeels overgenomen van artikel 6 en 7 ARBIT.

In artikel 5.6 is bewust afgeweken van de ARBIT: waar de ARBIT veronderstelt dat sprake is van eigendomsoverdracht, geeft GIBIT slechts randvoorwaarden voor het geval eigendomsoverdracht is overeengekomen. Dit aangezien in de praktijk Producten steeds vaker niet worden verkocht, maar onder een andere titel ter beschikking worden gesteld.

Artikel 6. Implementatie ICT Prestatie

De GIBIT gaat ervan uit dat de Leverancier de Implementatie verzorgt. De Implementatie is daarbij bewust ruim gedefinieerd (zie artikel 1) en gaat uit van het beheerst en projectmatig inrichten en in gebruik nemen van de ICT Prestatie in de organisatie en het inpassen ervan binnen de bestaande informatievoorziening. Dit laatste uiteraard binnen de kaders van het Overeengekomen gebruik. De Implementatie leidt dus niet tot wijzigingen van de gemaakte afspraken over de te leveren functionaliteit. Uiteraard gelden de verplichtingen omtrent Implementatie niet, indien de ICT Prestatie niet geïmplementeerd wordt of geïmplementeerd kan worden.

Het maakt hierbij – in abstracto – niet uit of sprake is van de Implementatie van een on *premise*- of een SaaS-prestatie. In beide gevallen zullen immers – in meer of mindere mate – stappen moeten worden gezet om tot ingebruikname van de ICT Prestatie te (kunnen) komen. De aard van de implementatiewerkzaamheden zal uiteraard wel verschillen.

In artikel 6 komt het vroegtijdig adresseren van risico's aan de orde. Artikel 6.1 bepaalt dat de Implementatie overeenkomstig het Implementatieplan plaatsvindt en artikel 6.2 bepaalt welke elementen daarin terugkomen. In artikel 6.3 zijn de randvoorwaarden van de Conversie en de Migratie tijdens de Implementatie vastgelegd. Daarbij geldt dat Data intact moet blijven en één op één overgezet moet worden. Voor metadata (een gestructureerde beschrijving van de inhoud of het gebruik van data die het vinden en gebruiken van die data vergemakkelijkt) geldt in beginsel hetzelfde, maar dit zal in uitzonderingsgevallen niet mogelijk zijn. Bij een migratie naar een nieuw systeem wordt immers vaak gewerkt met andere metadata-structuren. Wel draagt Leverancier er zorg voor dat metadata (aantoonbaar) zo intact mogelijk wordt overgezet.

Artikel 6.4 bepaalt vervolgens dat het opstellen van een dergelijk plan altijd verlangd kan worden, en dat dit in beginsel binnen 3 maanden opgeleverd moet worden. Uiteraard kan daarbij niet van de

Leverancier worden verwacht dat hij in 3 maanden een plan opstelt, terwijl een van de andere betrokken partijen dit frustreert. Artikel 6.5 geeft bovendien aan welke onderwerpen in een dergelijk plan opgenomen moeten worden. Het idee is dat het in belang van beide Partijen is vooraf – en niet pas gaandeweg het project – goed na te denken over al datgene dat noodzakelijk is om de Implementatie tot een succes te maken. Overigens zullen in de praktijk niet alle in het artikel 6.5 genoemde onderwerpen voor ieder project van belang zijn. Om die reden staat tussen haakjes vermeld *"steeds voor zover van toepassing"*.

Artikel 6.6 geeft een regeling over de afhankelijkheid van derde partijen bij de ketentesten en bepaalt dat de regelingen over het tijdig betrekken van derde partijen van overeenkomstige toepassing voor de gehele Implementatie.
Nieuw in de versie 2025 is artikel 6.7. In de praktijk is te zien dat licenties soms al worden aangeboden, terwijl een (lange) Implementatie nog loopt. In zo'n situatie betaalt een Opdrachtgever al voor alles, terwijl hij daar nog geen profijt van heeft. Het is zodoende de plicht van Leverancier om slechts die Licenties aan te bieden die in de Implementatie nodig zijn, zoals testlicenties. Het is denkbaar dat sommige licenties tussen wal en schip vallen: ze zijn niet strikt noodzakelijk, maar wel handig. Ook bij deze licenties kan Leverancier niet eenzijdig de plicht opleggen om deze licenties af te nemen. Partijen zullen hier over moeten overleggen.

In artikel 6.8 komt de in artikel 3 en 4 bedoelde risicoanalyse terug. Hierin is opgenomen dat aanpassingen aan het Applicatielandschap van Opdrachtgever die noodzakelijk zijn maar vooraf niet-voorzien waren, doch gelet op de zorgplicht van Leverancier achteraf wel voorzienbaar waren geweest, voor rekening van de Leverancier komen. Het artikel vormt in zoverre de *"proof of the pudding"* van (de kwaliteit van) de eerdergenoemde risicoanalyse ten aanzien van de inpasbaarheid van de aangeboden oplossing bij Opdrachtgever. Het artikel is alleen van toepassing op aanpassingen aan het Applicatielandschap die de Leverancier had kunnen of behoren te voorzien. Het artikel probeert in zoverre te voorkomen dat Leveranciers die willens en wetens een onvolledig of ondoordacht aanbod doen bij de gunning voordeel halen en later "beloond" worden met meerwerkopdrachten.

Het artikel is bovendien alleen van toepassing op aanpassingen aan het Applicatielandschap die voor de Implementatie (en daarmee dus voor het Overeengekomen gebruik) noodzakelijk zijn. Het artikel vormt dus ook zeker geen vrijbrief voor Opdrachtgevers om op kosten van Leveranciers allerlei niet aan de Implementatie gerelateerde onderdelen van het Applicatielandschap te laten upgraden, of om verderstrekkende verbeteringen te verlangen dan die noodzakelijk zijn voor de Implementatie. Voor verdergaande aanpassingen maakt Opdrachtgever nieuwe/separate afspraken. Indien in de praktijk blijkt dat het voor Opdrachtgevers aantrekkelijk is om bij de aanpassing in het Applicatielandschap verder te gaan dan het voor de Overeenkomst strikt noodzakelijke, dan ligt het voor de hand dat Partijen daarover separate afspraken maken (bijv. een afzonderlijk Upgrade project met een korting).

Artikel 6.9 ziet op de bereidheid van de Leverancier om later alsnog of nogmaals aan de Implementatie gerelateerde werkzaamheden te verrichten. Te denken valt hierbij aan een na inbedrijfsstelling of livegang alsnog uit te voeren Conversie, het na livegang alsnog aanleggen van extra Koppelingen of het na livegang alsnog verzorgen van (aanvullende) trainingen. Bij aanbestede opdrachten is het overigens zaak te toetsen of een dergelijke aanvullende opdracht niet leidt tot een wezenlijke wijziging van de opdracht.

Artikel 7. Afhankelijkheid van en afstemming met derde partijen

In artikel 7 zijn de reeds bestaande regelingen over de afhankelijkheid van derde partijen verder uitgewerkt. Het artikel ziet op de afhankelijkheid van derde partijen die geen hulppersoon zijn van een van de Partijen (artikel 7.1). Partijen zijn immers zelf verantwoordelijk voor de door hen betrokken hulppersonen. Het gaat in dit artikel juist om van Partijen onafhankelijke derden, zoals leveranciers van andere ICT Prestaties die gekoppeld moeten worden aan de onderhavige ICT Prestatie of van eigenaren van gebouwen indien apparatuur daar geïnstalleerd moet worden (om twee uiteenlopende voorbeelden te noemen).

In artikel 7.2 wordt vastgelegd welke Partij in de basis moet vaststellen en aan de andere Partij moet melden ('aan de bel moet trekken') indien van dergelijke afhankelijkheid sprake is. Meer dan een signaleringsplicht is dit niet. De gedachte is dat bij Dienstverlening op Afstand het de Leverancier is die bij uitstek weet of sprake is van dergelijke afhankelijkheid, terwijl bij overige dienstverlening het meer voor de hand ligt die taak bij de Opdrachtgever te leggen nu de Opdrachtgever het eigen Applicatielandschap het best zal (behoren te) kennen. Dit laatste laat de plicht voor een Leverancier tot het in het primaire aanbod signaleren van risico's onverlet (zie artikel 3.4). Ook moeten Partijen elkaar – uiteraard – ook wijzen op de risico's die zij al kennen of horen te kennen, zelfs al ligt dit in de verantwoordelijkheidssfeer van de andere Partij. Voorkomen moet worden dat Partijen blind op de informatie van de ander varen.

In artikel 7.3 ligt vervolgens vast dat over een aantal genoemde onderwerpen nadere afspraken moeten worden gemaakt. Het doel van de bepaling is vooral om die afspraken zo vroegtijdig mogelijk te maken en verrassingen achteraf te voorkomen. Zie in dat kader ook artikel 7.5: uitgangspunt is dat de derde partij ook op voorhand al bij het overleg worden betrokken en dat ook met hen op voorhand al afspraken worden gemaakt.

Artikel 7.6 bevat een genuanceerde regeling over hoe om te gaan met blokkerende doch niet aan Leverancier maar aan een derde partij toerekenbare kwesties. In de kern ziet dit artikel op (i) een overlegplicht indien zich kwestie voordoen waarbij de ICT Prestatie niet conform werkt, terwijl de oorzaak daarvoor niet bij Leverancier ligt (maar bij derde partijen, of de Opdrachtgever zelf); en (ii) de erkenning dat Leverancier in een dergelijke situatie gewoon recht heeft op datgene dat is afgesproken omtrent de gevolgen van Acceptatie (in de praktijk veelal: betaling).

Artikel 8. Interoperabiliteitseisen, normen en standaarden

Een van de doelen van de GIBIT is te komen tot een hogere kwaliteit van de informatievoorziening van gemeenten en van de ICT-Producten en diensten die daar deel van uitmaken. Ook wenst de GIBIT gestandaardiseerde gegevensuitwisseling te stimuleren zodat informatie goed, veilig en betrouwbaar gedeeld kan worden en processen ketengericht kunnen worden uitgevoerd. Dit komt terug in artikel 8.

Artikel 8 schrijft voor dat de ICT Prestatie moet voldoen aan alle voorgeschreven normen. De Gemeentelijke ICT-kwaliteitsnormen (het document met verplichte normen) staan daarbij centraal: partijen worden aangemoedigd om deze van toepassing te verklaren en hiermee te werken. Nieuw in de versie 2025 is dat de normen niet meer altijd van toepassing zijn, maar enkel indien partijen daarvoor kiezen. Om te voorkomen dat normen botsen, zeker als het kernverplichtingen zijn, is het immers noodzakelijk om ze expliciet te noemen. Het zou indruisen tegen het transparantiebeginsel om kernverplichtingen als deze op te leggen via een enkele verwijzing in algemene inkoopvoorwaarden.

Ook nieuw is de mogelijkheid om, in plaats van de Gemeentelijke ICT-kwaliteitsnormen, standaarden die hiermee vergelijkbaar en erkend zijn als maatstaf te nemen. Daarbij kan worden gedacht aan ISO/ISAE/NEN-normen. Het doel van de bepaling is immers niet om slechts de Gemeentelijke ICT-kwaliteitsnormen naar voren te schuiven, maar om een hoog niveau van beveiliging te waarborgen. Als dat niveau geborgd kan worden zonder de Gemeentelijke ICT-kwaliteitsnormen, dan is dat ook acceptabel en proportioneel. De Leverancier zal moeten aantonen dat de normen vergelijkbaar én internationaal breed geaccepteerd zijn.

In de Gemeentelijke ICT-kwaliteitsnormen geeft VNG Realisatie aan voor bepaalde soorten/typen applicaties of ICT Producten/diensten welke normen gelden. Het is mogelijk om alle Gemeentelijke ICT-kwaliteitsnormen van toepassing te verklaren, maar het aan te raden om de te implementeren normen en standaarden specifiek te benoemen in de uitvraag en te bespreken met de Leverancier. Op dat moment kan ook worden gekeken naar de vraag of een alternatieve standaard ook voldoende is. Dit geldt zeker waar (juiste) implementatie van een norm of standaard belangrijk is voor het slagen van een verwervingstraject. Zowel Opdrachtgevers – die zo wordt gedwongen na te denken over (het belang van) normen en standaarden voor een specifiek project, en Leveranciers – die specifiek wordt gewezen op het belang daarvan, zijn hierbij gebaat.

De Gemeentelijke ICT-kwaliteitsnormen worden periodiek door VNG/VNG Realisatie gepubliceerd. Binnen de set vallen alleen normen en standaarden die verplicht zijn binnen het werkingsgebied van gemeenten, van gemeentelijke samenwerkingsverbanden of voor ketens waarin gemeenten opereren. Het betreft open standaarden en normen waarbij Leveranciers bij de vaststelling zijn betrokken.

Bij het beantwoorden van de vraag welke normen en standaarden relevant zijn en voorgeschreven kunnen worden, kan worden gekeken naar de lijst van open standaarden zoals vastgesteld en gepubliceerd door het bureau Forum Standaardisatie (ook wel de gangbare standaarden en/of standaarden op de pas-toe-of-leg-uit lijst) en standaarden die als landelijke gemeentelijke standaard of norm door VNG/VNG Realisatie zijn vastgesteld. Het betreft normen en standaarden die de volgende ICT-kwaliteitsgebieden afdekken (tussen haakjes staan ter verduidelijking voorbeelden van betreffende normen en standaarden, waarbij opvolgende versies ook onder de normen vallen):

- Architectuur (GEMMA);
- Interoperabiliteit (NEN3610, Stuf, SUWIML, Digikoppeling, iWMO);
- Beveiliging (Baseline Informatiebeveiliging Gemeenten);
- Dataportabiliteit;
- Metadatering (TMLO);
- Toegankelijkheid (Webrichtlijnen);
- Archivering (NEN-ISO 15489-1 NL, NEN-ISO 16175-1);
- Infrastructuur (Generieke Digitale Infrastructuur, aansluiten op Stelsel van Basisregistraties);
- Documentatie;
- E-facturering.

Veel normen en standaarden schrijven voor dat bepaalde preventieve testen worden uitgevoerd zodat aangetoond wordt dat aan de betreffende norm wordt voldaan. Artikel 8.2 bepaalt dat deze testen moeten worden uitgevoerd voorafgaand aan de Implementatie. Tevens bepaalt artikel 8.2 dat de Leverancier dit testrapport overlegt aan de Opdrachtgever, zodat beide Partijen over dezelfde informatie beschikken.

Waar in de versie 2023 uit werd gegaan van testen op een niet-productieve omgeving, is dat beginsel nu geschrapt. De praktijk leert dat dit lang niet altijd nodig en/of proportioneel is. Indien de Opdrachtgever dit in gegeven omstandigheden echter wel wenst, dan zal Leverancier deze omgeving alsnog aanbieden. Is die wens al aangegeven in het Bestek, dan maakt dit onderdeel uit van de opdracht. Is dit een latere wens, dan is het logisch dat Opdrachtgever hiervoor dient te betalen.

Overigens kan de gemeente niet verwachten dat een alternatieve omgeving precies hetzelfde werkt als de reële omgeving. Printen, e-mailen en koppelingen met andere applicaties zullen hun restricties kennen.

Op grond van artikel 8.4 is het opnieuw preventief testen niet noodzakelijk indien de testen onder vergelijkbare omstandigheden op dezelfde versie van het Product, van de norm en van de testset al eens succesvol zijn doorlopen. Dit maakt dat het artikel over de preventieve testen met name bij nieuwe Producten, nieuwe versies van Producten of Producten die nog niet in een vergelijkbare context zijn gebruikt relevant is.

Overigens is een aanvullende test niet verplicht als de Leverancier kan aantonen dat hij al degelijke tests heeft verricht. Van de Leverancier kan immers niet worden verwacht dat hij Standaardprogrammatuur maar blijft testen. Dit kan slechts anders zijn als aangetoond wordt dat een aanvullende test meer zekerheid biedt.

Artikel 8.6 benoemt (volledigheidshalve) dat gedurende de Acceptatieprocedure wordt getoetst in hoeverre de ICT Prestatie aan de normen voldoet. Strikt genomen volgt dit al uit het gegeven dat het voldoen aan de normen tot het “Overeengekomen gebruik” hoort.

Artikel 9. Acceptatie

In artikel 9 is de Acceptatieprocedure beschreven. Deze wordt gedefinieerd in artikel 9.1.
Het is in het belang van beide Partijen dat vooraf helder is op welke wijze de acceptatieprocedure zal verlopen. Vandaar ook dat reeds in artikel 6.4 sub ix is bepaald dat, als onderdeel van het Implementatieplan, moet worden vastgelegd op welke wijze de Acceptatieprocedure wordt uitgevoerd. Er zal echter niet altijd een Implementatieplan zijn. Ook is denkbaar dat het Implementatieplan ten aanzien van de Acceptatieproceduregeen of onvoldoende uitgewerkte afspraken bevat. Vandaar dat artikel 9.2 bepaalt dat op verzoek van Opdrachtgever alsnog een schriftelijk testprotocol wordt opgesteld. De verwijzing naar artikel 6.3 is bedoeld om aan te geven dat de Leverancier penvoerder is van het plan (als meest deskundige) en voor het opstellen van het plan geen afzonderlijke Vergoeding in rekening mag brengen.

De overige bepalingen van artikel 9 moeten worden gezien zijn "vangnetbepalingen". Deze artikelen geven de kaders voor zover er in de Overeenkomst of in een ander bovenliggend document geen meer specifieke afspraken over de Acceptatieprocedure zijn gemaakt. Het geheel van deze bepalingen beschrijft de Acceptatieprocedure.

Artikel 9.3 geeft in de kern aan wat er tijdens testen gebeurt. We lichten de elementen puntsgewijs toe:

- Er wordt getest op Gebreken, dus op het niet voldoen aan het *Overeengekomen gebruik*. Er wordt uitdrukkelijk niet getest op aspecten van de ICT Prestatie die niet overeengekomen zijn (dat zou immers ook niet toerekenbaar zijn aan Leverancier). Wel wordt getest op het begrip *Overeengekomen gebruik* welke ruimer is dan sec datgene wat in een programma van eisen staat (o.a. vanwege de in artikel 3 verwoorde zorgplicht);
- De resultaten van de Acceptatieprocedure worden schriftelijk vastgelegd in een testverslag. Dit verslag zal door Partijen worden ondertekend. De gedachte is dat discussie achteraf over de uitkomsten van de Acceptatieprocedureop deze wijze tot een minimum wordt beperkt;
- Leverancier dient een planning af te geven voor het herstel van geconstateerde Gebreken. Die planning dient conform artikel 9.4 te passen binnen de algehele planning van het project;
- Na het herstel van de Gebreken legt de Leverancier de ICT Prestatie opnieuw ter Acceptatie voor. Er volgt dan wederom een Acceptatieprocedureconform de hiervoor beschreven uitgangspunten.

Artikel 9.4 is hiervoor al kort aangestipt. Het artikel bepaalt dat herstel van tijdens het testen geconstateerde Gebreken niet mag leiden tot vertraging. Het is dus aan de Leverancier – mede gelet op zijn rol als penvoerder van het aanbod (artikel 3), het Implementatieplan (artikel 6) en/of het testprotocol (artikel 9.2) – om op voorhand een realistische planning te hanteren met voldoende ruimte voor herstel van eventueel geconstateerde Gebreken. Het behoort overigens tot de zorgplicht van Leverancier om de voortgang van de Implementatie te bewaken en zo nodig de Opdrachtgever te waarschuwen of zelfs aan te manen. Deze aanmaning moet binnen 5 werkdagen gegeven worden. Deze zorgplicht is gebaseerd op bestaande rechtspraak (vgl. o.m. ECLI:NL:GHSHE:2015:4428, r.o. 3.8.4). Mocht een Opdrachtgever hier niet adequaat op reageren, dan ligt de bal weer bij hem (artikel 9.5). Een fatale termijn kan hier bijvoorbeeld door opgeschort worden.

Artikel 9.6 verklaart de eerdergenoemde genuanceerde regeling bij afhankelijkheid van derde partijen van overeenkomstige toepassing.

Artikel 9.7 bepaalt dat eventuele Koppelingen met andere systemen gedurende de Acceptatieprocedure moeten worden getest op correcte interoperabiliteit. Veel applicaties werken immers alleen goed in de context van Koppelingen met andere applicaties. Dat is voor de eindgebruiker echter vaak niet goed zichtbaar, maar wel essentieel voor veilige en betrouwbare informatieketens.

In artikel 9.8 staan de verschillende scenario's bij het niet slagen van de Acceptatieprocedure vermeld:
(1) ontbinding van de Overeenkomst; of
(2) het alsnog kosteloos laten herstellen van de Gebreken; of
(3) onder een nadere voorwaarde accepteren waarbij geldt dat indien niet aan de voorwaarde wordt voldaan alsnog direct kan worden ontbonden.

Deze drie smaken geven Opdrachtgevers veel flexibiliteit in hoe om te gaan met eventuele Gebreken:
(1) indien kernaspecten van de ICT Prestatie niet goed zijn dan ligt ontbinding voor de hand;
(2) bij kleine Gebreken ligt kosteloos herstel voor de hand; en
(3) bij het niet tijdig opleveren van onderdelen van de Prestatie die voor Opdrachtgever pas in de toekomst relevant worden, ligt voorwaardelijke Acceptatie voor de hand (namelijk Acceptatie onder de voorwaarde dat de ICT Prestatie wel correct is geïmplementeerd op de datum dat de nu ontbrekende onderdelen voor Opdrachtgever relevant worden).

In de GIBIT is er bewust voor gekozen na twee testrondes direct te kunnen ontbinden, zonder nadere ingebrekestelling. De gedachte is dat twee kansen om de overeengekomen prestatie te leveren in beginsel voldoende moet zijn. Bovendien wordt hiermee het preventief en zorgvuldig testen gestimuleerd.

Hierbij moet worden aangetekend dat van Opdrachtgever in een Acceptatieprocedure wordt verlangd dat hij zowel alle noodzakelijke medewerking verleent aan de Acceptatieprocedure, als zijn eigen verplichtingen nakomt (zoals vastgelegd in het Implementatieplan en/of testprotocol). Doet Opdrachtgever dat niet, dan kan de Leverancier zich op opschorting beroepen en komt Opdrachtgever in schuldeisersverzuim te verkeren. Zie ook de toelichting bij artikel 4.5. Verkeert Opdrachtgever in schuldeisersverzuim, dan komt hem uiteraard geen recht op ontbinding toe. Dit laatste volgt uit de wet en de GIBIT wijkt hier (bewust) niet vanaf.

In artikel 9.9 is bepaald dat er niet mag worden ontbonden wegens Gebreken die eerst in de tweede testronde worden geconstateerd, terwijl deze ook eerder in de Acceptatieprocedure geconstateerd hadden kunnen worden. Dit dwingt Opdrachtgevers om de Acceptatieprocedure serieus te nemen en de aandacht te geven die deze verdient.

Artikel 9.10 geeft Partijen de ruimte om eventueel overeen te komen dat bepaalde Gebreken buiten de staande planning worden hersteld.

Artikel 9.11 bepaalt uitdrukkelijk dat Gebreken die niet in de weg staan aan productieve ingebruikname, geen grond kunnen vormen voor niet-Acceptatie. De gedachte van de bepaling is dat een project niet op een formaliteit zou moeten worden afgekeurd, maar alleen op Gebreken die daadwerkelijk relevant/wezenlijk zijn voor Opdrachtgever. Dat laat overigens onverlet dat ook die minder relevante Gebreken alsnog moeten worden hersteld. De levering van die betreffende functionaliteit is immers wel overeengekomen.

Artikel 9.12 bepaalt dat, indien er deelleveringen hebben plaatsgevonden, dat dan na de laatste deellevering er ook nog een integrale Acceptatieprocedure plaatsvindt. Hiermee wordt uitdrukkelijk erkend dat bij ICT Prestaties de delen correct kunnen functioneren (voor zover te beoordelen als losstaand onderdeel), doch de som der delen niet, terwijl het Opdrachtgever uiteraard om de som der delen (de totale ICT Prestatie) te doen is.

Artikel 9.13 geeft ten slotte een vermoeden van Acceptatie aan indien de ICT Prestatie voor productieve doeleinden in gebruik is genomen, tenzij die vroegtijdige ingebruikname verband houdt met vertragingen of tekortschieten aan de zijde van Leverancier. Het is denkbaar dat een Opdrachtgever bij vertraagde levering de ICT Prestatie noodgedwongen wel in gebruik moet nemen (bijv. omdat er anders geen ICT in huis is om een nieuwe wet te ondersteunen), maar dat wil daarmee niet zeggen dat Opdrachtgever de ICT Prestatie (dus) ook geaccepteerd heeft. Als Opdrachtgever echter zelf op voorhand bewust afziet van het houden van een

Acceptatieprocedure en de ICT Prestatie vervolgens voor productieve doeleinden in gebruik neemt, dan aanvaardt ze daarmee impliciet dat de ICT Prestatie bij levering mogelijk nog Gebreken bevat, die vervolgens in het kader van Onderhoud (artikel 10) geadresseerd zullen (kunnen/moeten) worden.

Artikel 10. Onderhoud en ondersteuning

Uitgangspunt van de GIBIT is dat na de Acceptatie de onderhoudsfase volgt. De GIBIT biedt een (abstract) kader voor de onderhoudsfase. Dit kader wordt in de praktijk veelal nader uitgewerkt in de Overeenkomst of een afzonderlijke onderhoudsovereenkomst/SLA.

Vanwege het belang van blijvend goed functionerende ICT systemen is er bewust voor gekozen om standaard te bepalen dat de Leverancier Onderhoud verricht (artikel 10.1) en dat dit Onderhoud standaard alle in artikel 10.3 genoemde vormen van Onderhoud omvat. Uiteraard is het ook mogelijk dat in de Overeenkomst juist wordt bepaald dat Leverancier geen Onderhoud verricht, of slechts een deel van de in artikel 10.3 genoemde vormen van Onderhoud.

In artikel 10.2 wordt het “vangnet” karakter van de GIBIT wederom benadrukt. De bepalingen in de GIBIT gelden als basis, maar in de Overeenkomst of SLA kan hiervan worden afgeweken. De GIBIT bevat weinig concrete normen ter zake van Onderhoud, behoudens enkele abstracte eisen (die hierna worden toegelicht). De concrete door de Leverancier na te leven normen (Service Levels) zullen dan ook in de Overeenkomst of SLA moeten worden opgenomen. Bovendien zullen allerlei praktische aspecten rondom het verlenen van Onderhoud nader moeten worden ingevuld (zoals hoe en waar een Gebrek gemeld moet worden). In veel gevallen is een dergelijke onderhoudsovereenkomst of SLA dan ook noodzakelijk.

In artikel 10.4 is het uitgangspunt benoemd dat Onderhoud zo min mogelijk verstorend moet zijn voor de bedrijfsprocessen van Opdrachtgever. Er is bewust gekozen niets te bepalen over de precieze tijden waarop Onderhoud wel/niet mag plaatsvinden, aangezien dat te zeer afhankelijk is van de precieze aard van de ICT Prestatie en de processen waarin deze wordt gebruikt. Bij in bulk verricht Onderhoud is afstemming immers niet altijd even goed mogelijk.

Bij dit Onderhoud moet voorop staan dat Opdrachtgever er niet in functionaliteit op achteruit gaat (lid 5).

Artikel 10.6 bepaalt dat de Leverancier in ieder geval bereikbaar moet zijn op werkdagen tussen 09.00 en 17.00 uur. Er is bewust gekozen voor de term bereikbaar, zonder te specificeren welk kanaal of communicatiemiddel hierbij gebruikt moet worden. Dit laat Leveranciers voldoende ruimte om dit zelf in te richten (telefoon, e-mail, chat, etc.).Daarbij is ook een zekere wederkerigheid aangebracht: ook de gemeente moet bereikbaar zijn voor Onderhoud. Deze wederkerigheid is minder hard dan de plichten die op de Leverancier rusten, omdat gemeenten niet altijd kunnen garanderen dat er iemand met kennis van zaken aanwezig is om direct te reageren. Wat wel mogelijk is, en in dit lid onderkend wordt, is dat gemeenten de Leverancier in ieder geval te woord te kunnen staan binnen kantooruren.

Voor effectieve onderhoudswerkzaamheden is het soms ook essentieel dat de Opdrachtgever ook beschikbaar is, bijvoorbeeld voor afstemming, testen of communicatie tijdens het Onderhoud. Dat de Opdrachtgever hiervoor beschikbaar moet zijn, is aangegeven in lid 7.

Artikel 10.8 geeft aan dat alle storingen gemeld kunnen worden, ook niet-toerekenbare storingen.

Artikel 10.9 vult de hiervoor beschreven gedachte in: alle storingen (in brede zin) kunnen worden gemeld. Indien het gemelde niet kwalificeert als tekortkoming kunnen Partijen in overleg gaan over eventueel als meerwerk te verrichten aanvullende werkzaamheden. Te denken valt hierbij aan de situatie dat een medewerker van Opdrachtgever in strijd met instructies van de Leverancier belangrijke instellingen in de ICT Prestatie heeft gewijzigd, of dat door toedoen van een niet aan Leverancier toerekenbare virusuitbraak er allerlei herstelwerkzaamheden moeten worden verricht. Volledigheidshalve zij opgemerkt dat het hier een herstelpoging betreft (nu immers sprake is van een niet aan Leverancier toerekenbare situatie).

Artikel 10.10 hangt samen met het “vangnet”-karakter van de GIBIT. Het bepaalt dat Leverancier bereid moet zijn een nadere SLA te sluiten. Een specifieke eis aan die SLA is dat er Service Levels in kunnen worden opgenomen en dat aan het niet halen van Service Levels maatregelen zijn verbonden. Welke maatregelen dat zijn, zal van geval tot geval nader moeten worden ingevuld. Het is voor Opdrachtgever van belang dat de maatregel voldoende prikkel voor de Leverancier geeft tot nakoming en bovendien iets oplevert waar Opdrachtgever ook iets aan heeft. Omdat er geen model-SLA gegeven kan worden, zijn in de versie 2025 in ieder geval twee belangrijke KPI’s benoemd die als Service Level opgenomen moeten worden: de reactietijd en de functiehersteltijd. Het is immers belangrijk dat de Leverancier in ieder geval over deze twee punten duidelijkheid verschaft. Dit zijn zodoende ook resultaatsverbintenissen.

In artikel 10.11, 10.12 en 10.13 is bepaald dat ontbinding van de Overeenkomst(en) in ieder geval mogelijk is bij het herhaald niet halen van de Service Levels. Deze bepaling is opgenomen om uit de discussie te blijven of het niet halen van een Service Level altijd kwalificeert als tekortkoming en/of de discussie of dergelijke omissies altijd de ontbinding van de Overeenkomst rechtvaardigen. Bovendien is bepaald dat bedongen maatregelen de overige rechten van Opdrachtgevers onverlet laten. Dit om te voorkomen dat een in de SLA bedongen sanctie op grond van de wet zou gelden als gefixeerde schadevergoeding (artikel 6:92 lid 2 BW).

Ten opzichte van de versie 2023 is de escalatieladder tussen Partijen uitgebreid. Als de Leverancier de Service Levels niet haalt, zijn de opties voor Opdrachtgever normaliter om te ontbinden of om de wanprestatie te accepteren. Dit is in de praktijk vaak beide onwenselijk. In de vorige versie was zodoende al toegevoegd dat een verbeterplan en/of een directieoverleg tussenstappen kunnen vormen voordat overgegaan wordt tot ontbinding. Nieuw is de mogelijkheid om in het kader van het verbeterplan een malusregeling af te spreken, ter voorkoming van verdere escalatie. Hierbij kan bijvoorbeeld worden gedacht aan het verbeuren van service credits, of het verbeuren van boetes. Service credits zijn een vorm van compensatie die een Leverancier aan een opdrachtgever kan betalen als de leverancier de afgesproken prestatieniveaus in de SLA niet haalt. Dit kan bijvoorbeeld een percentage van de maandelijkse kosten zijn, of een andere vorm van creditering.

Bij het bepalen van de hoogte van de boete kan worden gekeken naar de EMVI-boete. Het niet voldoen aan Service Levels is immers aanbestedingsrechtelijk problematisch: als andere aanbieders wel in voldoende mate aan deze eisen hadden kunnen voldoen, is de opdracht wellicht aan de verkeerde partij gegund.

In artikel 10.14 zijn enkele eisen opgenomen ten aanzien van het Preventief Onderhoud. Het is voor Opdrachtgevers van groot belang dat blijvend wordt voldaan aan wet- en regelgeving en dat de interoperabiliteit gewaarborgd blijft. Ook veiligheidsadviezen uitgebracht door NCSC, zijn rechtsopvolger of anderszins publiekelijk uitgebracht moeten zo spoedig mogelijk worden opgevolgd en risico’s moeten zo spoedig mogelijk zullen worden gemitigeerd. De wijze waarop dit gebeurt is uitdrukkelijk aan Leverancier gelaten (zie ook woorden ‘of anderszins’). Voorop staat echter dat (het gebruik van) de ICT Prestatie veilig moet zijn, hetgeen bepaald geen onredelijke eis lijkt.

Voor Leveranciers is dit een zware eis, maar voor Opdrachtgevers is het een belangrijke eis. Vrijwel alle gemeentelijke producten, diensten, processen en informatieketens zijn immers op de een of andere manier gerelateerd aan het voldoen aan wet- en regelgeving. Door verdergaande digitalisering heeft dat effect op de kwaliteitseisen aan ICT-Producten en diensten. De GIBIT gaat er derhalve vanuit dat de Leverancier, als gespecialiseerde aanbieder van bepaalde Programmatuur om bepaalde wetgeving te ondersteunen, veel beter dan Opdrachtgever in staat is (zou moeten zijn) om wijzigingen in wetgeving tijdig te vertalen naar de benodigde (technische) aanpassingen in de ICT Prestatie. Volledigheidshalve is ook bepaald dat de verplichting ziet op de voor het Overeengekomen gebruik relevante Wet- en regelgeving (en dus niet alle denkbare wetgeving). De kosten voor die aanpassingen liggen in beginsel besloten in de onderhoudsvergoeding. Let op: het ondersteunen van volstrekt nieuwe wetgeving valt veelal niet onder het “Overeengekomen gebruik” (en daarmee het Onderhoud) en valt dus niet binnen de verplichting van dit artikel. Dit ligt vast in artikel 11.3, zie ook de toelichting aldaar.

Artikel 10.15 geeft het kader voor de installatie van Updates en Upgrades. Uitgangspunt is dat Opdrachtgever in beginsel zelf de installatie van Updates en Upgrades verzorgt. In het artikel is niettemin bepaald dat Leverancier dit op verzoek (en tegen vergoeding) kan doen. In dat geval zijn ook de bepalingen omtrent Implementatie en Acceptatie van toepassing.

In artikel 10.16 is getracht een genuanceerde regeling te treffen voor het weigeren van de installatie van nieuwe Updates of Upgrades. Enerzijds heeft Opdrachtgever het recht die installatie te weigeren, anderzijds worden de verplichtingen van de Leverancier in het kader van Onderhoud wat gerelativeerd indien Opdrachtgever besluit aangeboden Updates of Upgrades niet (direct) te installeren. In dit geval is Leverancier nog slechts gehouden is Gebruikersondersteuning te blijven verlenen (behoudens Gebreken die nog niet zijn verholpen in Updates of Upgrades). Als Opdrachtgever 18 maanden of meer achterloopt bij het installeren van Updates of Upgrades, mag Leverancier de (aantoonbare) meerkosten voor het Onderhoud doorberekenen aan Opdrachtgever.

In artikel 10.17 is opgenomen dat de Leverancier in beginsel standaard rapporteert over de nakoming van de Service Levels. Partijen kunnen hierover nadere afspraken maken. Artikel 10.18 bepaalt vervolgens dat Opdrachtgever na ontvangst van de rapportage zal beoordelen in hoeverre de Leverancier de gemaakte afspraken naleeft. Eventueel kan op grond van artikel 27 hierbij een derde partij (auditor) worden ingeschakeld.

In artikel 10.19 is bepaald dat voor Onderhoud van Derdenprogrammatuur afwijkende bepalingen van toepassing zijn, mits deze vooraf tijdig kenbaar zijn gemaakt. De afwijkende bepalingen zullen in veel gevallen worden bepaald door de voorwaarden van de rechthebbende op die Derdenprogrammatuur. De gedachte hierbij is dezelfde als die bij de hele regeling omtrent Derdenprogrammatuur: omdat op grond van de wet (Auteurswet) voor iedere wijziging in programmatuur (zoals bij Onderhoud) de toestemming van de rechthebbende nodig is, en dus de Leverancier bij gebreke van die toestemming helemaal geen Onderhoud kan en mag leveren, is het niet redelijk niettemin onderhoudsverplichtingen in de GIBIT op te nemen.

Artikel 10.20 vormt het sluitstuk van het vangnetkarakter van de GIBIT inzake Onderhoud. Het bepaalt namelijk dat indien er initieel geen of slechts deels Onderhoud is overeengekomen, dat Leverancier dan bereid moet zijn om op verzoek later alsnog Onderhoud te gaan verrichten of de bestaande Overeenkomst inzake Onderhoud uit te breiden. Uiteraard geschiedt dit alles tegen een nader overeen te komen Vergoeding. Het belang voor Opdrachtgever is er met name in gelegen dat hij zeker weet dat hij altijd alsnog tot het afnemen van Onderhoud kan overgaan.

Artikel 11. Vergoeding, facturatie en betaling

In artikel 11.2 is een iets andere benadering gekozen dan de ARBIT doet. Waar de ARBIT uitgaat van volledige voorfinanciering door de Leverancier, kiest de GIBIT ervoor een deel van de betalingen achter te houden tot na Acceptatie (doorgaans 30%). Over de resterende 70% moeten afspraken worden gemaakt in de Overeenkomst.

Dit in de gedachte dat het onredelijk is het gehele financiële risico van het project bij de Leverancier te leggen, doch tegelijkertijd voldoende (financiële) prikkel voor de Leverancier over te houden om tot correcte Implementatie te komen. Tegelijkertijd is het evenmin redelijk om als Opdrachtgever al te betalen voor diensten die nog niet kunnen worden gebruikt.

Deze afspraken leiden tot de volgende verdeling:

a) van eenmalige Vergoedingen wordt 30% achtergehouden tot Acceptatie (dus bijv. 30% van de eenmalige implementatiekosten), over de overige 70% worden afspraken gemaakt;
b) periodieke Vergoedingen zijn eerst verschuldigd vanaf Acceptatie van het betreffende deel van de ICT Prestatie, doch worden vanaf dan vooruitbetaald (dus bijv. jaarlijkse abonnementsvergoedingen);
c) de Vergoeding voor Derdenprogrammatuur wordt volledig betaald bij levering, mits is voldaan aan de vereisten van artikel 3.5.

Eenmalige Vergoedingen zijn alle Vergoedingen die niet periodiek zijn. Een eenmalige Vergoeding kan ook gespreid worden betaald. Veelal zal in de Overeenkomst nader zijn uitgewerkt op welke wijze betaling van de eenmalige Vergoedingen plaatsvindt. Zo kunnen Partijen bijvoorbeeld een betaalschema met elkaar afspraken. De GIBIT verplicht echter niet tot een dergelijke uitwerking. Periodieke Vergoedingen zijn Vergoedingen die op geregelde tijden en met een zekere regelmaat verschuldigd zijn. In de Overeenkomst zal zijn bepaald wat de overeengekomen betalingsfrequentie is. Te denken valt hierbij aan maandelijkse, driemaandelijkse of jaarlijkse Vergoedingen. In theorie kan de betaalfrequentie ook éénmalig zijn, bijvoorbeeld als er nog één keer wordt betaald in het kader van verlengd gebruik (artikel 29.11).

In de GIBIT is bepaald dat periodieke Vergoedingen bij vooruitbetaling verschuldigd zijn. Hiermee wordt aansluiting gezocht bij de gebruikelijke werkwijze van veel Leveranciers (de GIBIT is hier dus leveranciersvriendelijk). Tegelijkertijd ligt ook vast dat de periodieke Vergoeding eerst vanaf (deel) Acceptatie verschuldigd is.

De gedachte daarachter is eenvoudig: het is onredelijk om vooruit te betalen voor een prestatie terwijl nog onzeker is of deze voldoet aan de overeengekomen eisen (dan wel kan worden gebruikt). Dat zullen Leveranciers wellicht als minder vriendelijk ervaren, maar dat is niet terecht. Het is immers een normaal ondernemersrisico om als Leverancier eerst zelf in te kopen en later pas door eigen klanten betaald te worden.

Hierbij zij aangetekend dat artikel 9.4 (over het zonder vertraging doorlopen van de Acceptatieprocedure) voor beide Partijen geldt en dat ingebruikname voor productieve doeleinden Acceptatie impliceert (zie artikel 9.11). Dit zijn beide nuanceringen die de eventuele vrees van Leverancier voor langdurige voorfinanciering sterk kunnen temperen. Verder wordt aangetekend dat onderhoudsvergoedingen, die veelal periodiek zullen zijn, op grond van artikel 10.1 eerst na Acceptatie verschuldigd zijn nu het Onderhoud niet eerder start.

Er wordt vooruitbetaald voor de diensten in de komende periode (niet voor de gehele contracttermijn). Dat betekent dat uiterlijk op de in de Overeenkomst bepaalde datum, althans uiterlijk bij het intreden van die nieuwe periode, moet zijn betaald. Eerder kan de Leverancier ook geen betaling afdwingen (vgl. artikel 6:39 BW).

De GIBIT erkent voorts dat bij Derdenprogrammatuur de Leverancier veelal zelf direct moet betalen. Dat is een inkooprelatie waarbij de Leverancier, naar de aard van Derdenprogrammatuur (in feite monopolies), veelal geen enkele onderhandelingspositie heeft (anders dan bij de inkoop van andere Producten en diensten). Vandaar dat bij Derdenprogrammatuur geen sprake is van het achterhouden van een deel van de Vergoeding maar betaling na levering geschiedt. Overigens, dit geldt enkel voor Derdenprogrammatuur die conform artikel 3.5 vooraf aan Opdrachtgever kenbaar is gemaakt. De gedachte daarachter is dat zodoende verrassingen worden voorkomen, nu artikel 3.5 tot transparantie vooraf verplicht.

Het moment van levering van Derdenprogrammatuur is hierbij overigens het moment waarop de Opdrachtgever de feitelijke macht over die Derdenprogrammatuur zou kunnen uitoefenen (vgl. het Burgerlijk Wetboek). Of wat praktischer uitgedrukt: het moment waarop Opdrachtgever van de software gebruik kan maken. Uiteraard kan in de Overeenkomst een ander moment worden overeengekomen (zoals het moment van tenaamstelling van licenties).

De uitgestelde opeisbaarheid is niet van toepassing indien er geen Acceptatieprocedure wordt uitgevoerd. In samenhang met de regel dat ingebruikname voor productieve doeleinden in beginsel kwalificeert als Acceptatie, geeft dit Leveranciers zo in de praktijk voldoende houvast dat er tijdig betaald wordt. Zo nodig kan Leverancier de Opdrachtgever in gebreke stellen om alsnog tot het doorlopen van de Acceptatieprocedure over te gaan.

Een belangrijke tegemoetkoming is artikel 11.3. Zoals hiervoor beschreven wordt van de Leverancier als gespecialiseerde aanbieder verwacht dat zij in beginsel in staat moet zijn aan de gestelde eisen inzake het Onderhoud te kunnen voldoen. Onder omstandigheden kan dit echter onbillijk uitpakken.

De bewijslast hiervoor ligt bij Leverancier. Dit is een reactie op vragen over de kosten voor het verwerken van wijzigingen in wet- en regelgeving, met name in relatie tot ingrijpende stelstelwijzigingen of (te laat aangekondigde) ingrijpende wijzigingen in de eisen die aan de ICT Prestatie worden gesteld. Het komt daarbij mede aan op de vraag in hoeverre de Leverancier, als zorgvuldig en professioneel handelende partij, de wetswijzigingen had kunnen of althans behoren te voorzien. Die vraag is in abstracto in deze voorwaarden niet te beantwoorden; vandaar ook dat de GIBIT slechts een bewijsverdelingsregel bevat.

In artikel 11.4 wordt verhelderd dat de randvoorwaarden nog steeds gelden: meerwerk wordt gemeld, de Opdrachtgever moet akkoord geven, en de afgesproken tarieven gelden.

Artikel 11.5 geeft de mogelijkheid in de Overeenkomst nadere eisen te stellen ten aanzien van de factuur. Facturen dienen binnen drie maanden na het opeisbaar worden van de betreffende werkzaamheden te worden verstuurd. De gedachte is dat laat factureren moet worden voorkomen; dat is in het belang van beide Partijen. De termijn van drie maanden is echter niet haalbaar voor gemeentes die een fiscaal jaar moeten afsluiten. Daarom is bepaald dat het mogelijk is om af te spreken dat alle facturen voor werkzaamheden in een bepaald jaar vóór een bepaalde datum in het daarop volgende jaar naar de Opdrachtgever moet worden verstuurd. In de versie 2023 stond hier een harde datum van 6 januari voor, maar dit is ervaren als te strikt. Zodoende is deze concrete datum geschrapt. Aangezien dit moment niet voor alle Opdrachtgevers passend zal zijn, of een strikte vervaltermijn niet voor alle Opdrachtgevers noodzakelijk zal zijn, is het opnemen van een harde einddatum slechts optioneel.

Artikel 11.6 stelt als standaard betaaltermijn 30 dagen.

Artikel 11.7 bepaalt dat er standaard elektronisch moet worden gefactureerd conform de daarvoor geldende standaard.

In artikelen 11.8, 11.9 en 11.10 zijn regelingen omtrent prijsverhogingen doorgevoerd. Hoofdregel is dat alleen de prijsstijging uit de dienstenprijsindex, groep J62 (althans J6202) gevolgd mogen worden (artikel 11.8). Vanwege het begrotingsproces van gemeenten is opgenomen dat prijsindexaties ruim van tevoren (één maand) moeten worden aangekondigd, inclusief het specifieke indexatiecijfer. Om die reden ligt indexatie met terugwerkende kracht, bijvoorbeeld omdat Leverancier vergeten is een indexeringsbrief te sturen, niet voor de hand. Er wordt steeds vergeleken met de index van 12 maanden daarvoor. Zodoende wordt ook minder relevant dat op het moment van indexeren wellicht nog niet de jaarindexcijfers gepubliceerd zullen zijn. Opnieuw wordt hier de nuance gezocht ten aanzien van Derdenprogrammatuur: hier mogen niet voorzienbare prijsstijgingen aan Opdrachtgevers worden doorbelast mits deze aantoonbaar worden gemaakt. Overigens moeten Partijen hierbij wel in ogenschouw nemen dat wijzigingen van de prijs onder omstandigheden aanbestedingsrechtelijke gevolgen kunnen hebben.

Daarnaast kwam in de praktijk voor dat Leveranciers zeer snel na contracteren al de prijs verhoogden in het kader van indexatie. Dit is onwenselijk, omdat de Overeenkomst dan wordt gesloten onder een onrealistische voorstelling van de werkelijkheid. In het nieuwe artikel 11.9 wordt dit deels tegengehouden: bij een Overeenkomst die is gesloten aan het eind van een jaar, kan de prijs niet direct op 1 januari worden geïndexeerd. Hiervan kan wel worden afgeweken in de bovenliggende Overeenkomst.

Ten opzichte van de versie 2023 is de regeling over het doorvoeren van prijsverlagingen geschrapt. In de praktijk was namelijk te zien dat dit feitelijk zelden tot nooit gebeurde. Een van de redenen hiertoe is dat de Leverancier weinig reden heeft om kortingen af te dwingen bij zijn toeleverancier, als hij er toch niet aan kan verdienen. Ook is te zien dat staffelkorting wegens een bepaalde hoeveelheid licenties dermate ingewikkeld is om door te voeren (Leveranciers moeten immers berekeningen maken voor welke afnemers welk gedeelte van de korting horen te krijgen), dat het voor Leveranciers efficiënter is om af te zien van de staffelkorting. Dat is begrijpelijk, maar wel onwenselijk. De absolute plicht om prijsverlagingen door te voeren, is zodoende geschrapt. Dat betekent niet dat Leveranciers nooit prijsverlagingen hoeven door te voeren (dit is uiteraard nooit

onwenselijk), maar in ieder geval zijn ze hier niet toe verplicht. Leveranciers verdienen zodoende aan inspanningen om de prijs van Derdenprogrammatuur laag te houden, en tevens hebben nieuw gecontracteerde Opdrachtgevers wél profijt van de verlaagde prijs: de Leverancier zal in een nieuwe aanbesteding immers de verlaagde prijs offreren. Dit is ook een extra motivatie voor Opdrachtgevers om zorgvuldig aan te besteden, en contracten niet te lang door te laten lopen.

Artikel 11.11 bevat een bepaling over onvoorziene aanzienlijke kostprijsverhogende omstandigheden. Het artikel voorziet in een overlegverplichting en geeft daarbij op voorhand drie opties: (i) prijsverhoging betalen, (ii) ICT Prestatie beperken of (iii) Overeenkomst beëindigen tegen vergoeding van de daarmee gemoeide kosten (dat laatste gelet op de verwijzing naar artikel 24.6). Met het artikel wordt voorkomen dat bij onvoorziene omstandigheden de gang naar de rechter is vereist (vgl. artikel 6:258 BW).

De lat hierbij ligt vrij hoog; het gaat om excessen. Het gaat bij dit artikel bijvoorbeeld om dermate ingrijpende situaties dat continuïteit van dienstverlening en/of bedrijfsvoering aantoonbaar in het geding komt. Het toelaten van een grote prijsverhoging is weliswaar een discretionaire bevoegdheid van de Opdrachtgevers (en geen verplichting), maar gelet op de algemene beginselen van behoorlijk bestuur kan van een gemeente wel worden verwacht dat zij hier redelijk en behoorlijk in handelt.

Het artikel geeft bovendien op voorhand aan tot welk percentage een kostenstijging geacht wordt voor risico van Leverancier te zijn (<10%); dat geeft Partijen op voorhand al enige zekerheid. Het is immers niet de bedoeling om zaken als extra indexatie te regelen in dit artikel. Overigens gelden de vereisten uit de Aanbestedingswet hiervoor onverkort, en dan met name de regeling omtrent onvoorziene kosten uit artikel 2.163e Aanbestedingswet 2012. De mogelijkheid van substantiële prijsverhoging moet dan ook worden toegepast binnen de kaders die door de Aanbestedingswet worden gegeven.

Artikel 11.12 bepaalt dat Vergoedingen die gerelateerd zijn aan wijzigingen onderhevige getallen die zijn gerelateerd aan Opdrachtgever, slechts éénmaal per jaar worden bijgesteld en wel op 1 januari, tenzij anders overeengekomen. De gedachte is dat hierdoor prijsschommelingen gedurende de looptijd worden beperkt. Uiteraard kan in de Overeenkomst een andere afspraak worden gemaakt.

Artikel 11.13 bepaalt ten slotte dat hetgeen in dit artikel omtrent Derdenprogrammatuur is bepaald alleen geldt voor zover Leverancier heeft voldaan aan hetgeen in artikel 3.5 is bepaald. Artikel 3.5 bepaalt dat Leverancier de relevante Derdenprogrammatuur uitdrukkelijk in zijn aanbod moet specificeren. Met andere woorden: indien Leverancier verzaakt de relevante Derdenprogrammatuur te specificeren, dan geniet hij ook niet de voordelen van genuanceerde betalingsregeling zoals verwoord in dit artikel (en wordt dus ook bij die Programmatuur 70% bij ingebruikname en 30% bij integrale Acceptatie betaald).

Artikel 12. Garanties

In dit artikel worden in het eerste lid diverse garanties vermeld. Het is vaste rechtspraak dat wat Partijen beogen met garanties een kwestie is van uitleg. In het geval van de GIBIT is het belangrijkste beoogde gevolg vermeld in artikel 12.2, namelijk dat indien Opdrachtgever een garantie inroept, het dan aan Leverancier is om aan te tonen dat dit beroep onterecht is. Het artikel bevat in zoverre een bewijslastverdeling. Daarbij is ook in artikel 12.3 bepaald wat het geven van een garantie nu precies betekent. Dit is gedaan aangezien het vaste rechtspraak is dat wat onder een garantie is te verstaan afhangt van de partijbedoeling, terwijl die partijbedoeling regelmatig niet zal blijken bij het gebruik van de Inkoopvoorwaarden in formele inkoopprocessen als een aanbesteding. In de Inkoopvoorwaarden is met de begrippen slechts de resultaatsverbintenis met de genoemde bewijslastverdeling mee bedoeld, verder niets.

De meeste garanties spreken voor zich en zien er met name op dat de Leverancier ervoor instaat dat hij levert wat is overeengekomen. Ten opzichte van de versie 2023 is de garantie geschrapt dat de ICT Prestatie de overeengekomen eigenschappen zal bevatten en dat deze voldoet aan het Overeengekomen gebruik. Dit is nadrukkelijk niet geschrapt omdat Leverancier hier niet meer aan

hoeft te voldoen; uiteraard moet de ICT Prestatie voldoen aan de Overeenkomst. Door dit als garantie te formuleren, was echter onbedoeld de situatie ontstaan dat het aan de Leverancier was om te bewijzen dat hij met de ICT Prestatie géén wanprestatie pleegt. Dat is een onredelijke uitkomst, en is nooit de bedoeling geweest.

De garantie onder iv hangt samen met het belang van Opdrachtgevers om desnoods op een later moment alsnog Onderhoud af te kunnen nemen. Het is daarvoor noodzakelijk dat de geleverde ICT Prestatie daadwerkelijk nog onderhouden wordt. In dit artikel geeft de Leverancier de garantie dat dit in ieder geval twee jaar na Acceptatie nog het geval is.

Artikel 13. Algoritmische toepassingen

Gemeenten zien steeds meer gebruik van algoritmen en de maatschappelijk vragen over dergelijk gebruik neemt ook toe. Vandaar dat de GIBIT enkele (minimale) eisen stelt aan dergelijke toepassingen. Het is denkbaar – en onder omstandigheden ook wenselijk – dat in het bovenliggende contract de eisen nader worden uitgewerkt. De eisen beperken zich vooralsnog tot de volgende basis-/kerneisen.

In het eerste lid zijn eisen gesteld aan (de kwaliteit van) de Algoritmische toepassing: een rechtmatige dataverwerking, gestructureerde en neutrale dataverwerking en nauwkeurigheid.
In het tweede lid is een gebruiksbeperking op de verwerkte Data opgenomen: geen gebruik voor eigen doeleinden, tenzij volledig geanonimiseerd en niet-herleidbaar. Zijn de Data persoonsgegevens, dan moet de Verwerkersovereenkomst ruimte bieden voor anonimisering. Zijn de Data geen persoonsgegevens, dan dienen de Data alsnog niet-herleidbaar te zijn. Hiermee wordt enerzijds bedrijfsvertrouwelijke en privacygevoelige informatie beschermd, doch anderzijds erkend dat een algoritme 'input' nodig heeft om verrijkt te worden.

Aangezien een algoritme in de praktijk regelmatig een 'black box' is, terwijl de gemeente als actor in een democratische rechtstaat het eigen handelen juist zal moeten kunnen verantwoorden is aan lid 3 toegevoegd dat Leverancier zowel in algemene zin als in een specifiek geval moet kunnen uitleggen/verantwoorden hoe het algoritme werkt of waarom het tot een bepaalde beslissing is gekomen. Dit gaat zowel over traceerbaarheid als over verklaarbaarheid. Dat hoeft niet zo ver te gaan dat Leverancier het algoritme prijs hoeft te geven (het belang van bescherming van bedrijfsvertrouwelijke informatie wordt onderkend), maar wel zo ver dat in voorkomend geval de beslissing in rechte toetsbaar wordt. Dat laatste is immers een basisbeginsel van de democratische rechtstaat. Het is daarom belangrijk om in ieder geval betekenisvolle kwantitatieve en kwalitatieve informatie te verschaffen. Dat betekent dat niet het model niet uitgelegd moet worden in technische getallen (zoals nauwkeurigheid of foutpercentages), maar (ook) moet worden uitgelegd in begrijpelijke taal over hoe het model werkt en wat de beperkingen zijn. Bij mogelijkheden om te voldoen aan deze bepaling kan bijvoorbeeld gedacht worden aan technische mogelijkheden van controleerbaarheid, reproduceerbaarheid en verslaglegging en aan het beschrijven en minimaliseren van potentiële negatieve gevolgen. Ook kan worden gedacht aan het ombuigen van deze plicht van reactief naar proactief, bijvoorbeeld in de vorm van model cards.

Gelet op de eerdergenoemde beginselen van de democratische rechtstaat is ook in lid 4 opgenomen dat de Opdrachtgever de informatie over de werking met derden (zoals de rechtbank) mag delen. Om diezelfde reden is ook in artikel 13.5 opgenomen dat het bestaande controle-/ auditrecht ook van toepassing is op de Algoritmische toepassing (strikt genomen is de bepaling welhaast overbodig, want dat controlerecht zag toch al op nakoming van alle verplichtingen).

Artikel 14. AI-systemen

Nieuw in de Inkoopvoorwaarden is de bepaling omtrent AI-systemen. Vooropgesteld moet worden dat dit een specificering vormt van artikel 13: alle AI-systemen zijn Algoritmische toepassingen, maar niet alle Algoritmische toepassingen zijn AI-systemen. Daarom is voor AI-systemen een los artikel in het leven geroepen.

Bij het opstellen van het artikel is voornamelijk gekeken naar de AI Act (Verordening (EU) 2024/1689), de EU-modellen voor de inkoop van AI en enkele reeds bestaande inkoopvoorwaarden in de gemeente- en zorgmarkt.

In het eerste lid zijn eisen gesteld aan (de kwaliteit van) het AI-systeem: een nauwkeurig, robuust en veilig Product, waarvan de werking kan worden gecontroleerd en de output kan worden begrepen. Dit dient hetzelfde te worden uitgelegd als de bepalingen hieromtrent in de AI Act. Principes als rechtmatigheid, non-bias en transparantie zijn afkomstig uit de AI Act expliciet. Mocht Leverancier slechts de toeleverancier zijn en niet de aanbieder, dan zal Leverancier de oorspronkelijk aanbieder moeten aanspreken als die niet voldoet aan de AI Act. Dit doet geen afbreuk aan de plicht van Leverancier om een ICT Prestatie te leveren die voldoet aan de gestelde eisen. Het feit dat veiligheid als expliciete eis is opgenomen voor AI-systemen betekent overigens niet dat voor ICT Prestaties die geen AI-systeem zijn, deze eis niet geldt. Het is louter opgenomen om de tekst van de AI Act te reflecteren.

De AI Act schrijft voor dat passende en doelgerichte risicobeheersingsmaatregelen doorgevoerd moeten worden in het AI-systeem. Het is denkbaar dat dit op een specifieke afnemer afgestemd moet worden. In lid 2 is bepaald dat de Leverancier hiervoor open moet staan. In overleg zal moeten worden bekeken hoe dit precies doorgevoerd zal worden.

Wanneer gebruik wordt gemaakt van AI-systemen met een hoog risico, rusten de voornaamste verplichtingen op de aanbieder. De gebruiksverantwoordelijke kan ingevolge artikel 25 AI Act echter ook worden beschouwd als aanbieder, bijvoorbeeld wanneer zijn naam of merk op het AI-systeem wordt aangebracht of wanneer hij een substantiële wijziging in het AI-systeem aanbrengt. Het is onwenselijk om gemeenten op deze wijze te laten “verschieten van kleur”. Om deze reden is in lid 3 bepaald dat Leverancier de zorgplicht heeft om dit verschieten van kleur, voor zover mogelijk, te voorkomen.

In lid 4 is bepaald dat de classificatie van het AI-systeem (onaanvaardbaar risico, hoog risico, AI-model voor algemene doeleinden, etc.) aan de Leverancier is, en dat hij hier desgevraagd bewijs c.q. een onderbouwing van overlegt. Indien de classificatie “hoog” is, dan garandeert Leverancier dat hij voldoet aan de eisen die daaraan worden gesteld in de AI Act (lid 5). Ook zonder deze bepaling had deze verplichting bestaan, maar door het uit te schrijven wordt dit een punt van aandacht bij het contracteren.

Hetzelfde geldt voor de loggingsplicht uit lid 6 en lid 7: deze verplichtingen vloeien voort uit de wet, maar door het uit te schrijven weten Partijen waar ze aan toe zijn.
Verder rusten twee medewerkingsverplichtingen op de Leverancier. Gemeenten zullen regelmatig een beoordeling van de gevolgen voor de grondrechten (FRIA) moeten verrichten, waarvoor ze over kennis van het AI-systeem moeten beschikken. De Leverancier zal hierbij assisteren. Daarnaast is bepaald dat vragen over de werking van het AI-systeem en de interpretatie van output tot de Gebruikersondersteuning (helpdesk) behoort.

Afsluitend wordt van de Opdrachtgever ook verwacht dat hij de Leverancier helpt. De AI Act verplicht soms tot het informeren van gebruikers over het AI-systeem, dus de Opdrachtgever zal dit op aangeven van de Leverancier ook moeten doen. Verder kan de Opdrachtgever Leverancier helpen door feedback te verstrekken over de werking van het AI-systeem.

Uiteraard kan het aanbieden van een AI-systeem niet los worden gezien van het gebruik daarvan. De Leverancier kan niet verantwoordelijk gehouden worden voor (verkeerde) toepassingen die de Opdrachtgever zelf aan het AI-systeem geeft. Hiertoe biedt artikel 36 een grondslag.

Artikel 15. Documentatie en informatie

Het eerste lid van dit artikel bepaalt dat Leverancier Documentatie dient te leveren. Ook stelt het artikel enkele eisen aan de Documentatie, zowel in lid 1, lid 2 als lid 3.

Documentatie wordt hier in brede zin gebruikt: het artikel ziet zowel op het gebruik van de geleverde ICT Prestatie (sub i, sub iii), op het documenteren van de door Leverancier gemaakte instellingen (sub ii), op het kunnen uitvoeren van de acceptatietesten (sub iv) en op het beheren van de ICT Prestatie (sub v). Daarbij kan voor het nakomen van sub v de GEMMA Softwarecatalogus (www.softwarecatalogus.nl) deels worden gebruikt.

Om Leveranciers voldoende flexibiliteit te geven, is bepaald dat alleen de Documentatie gericht op eindgebruikers in het Nederlands gesteld dient te zijn. Overige Documentatie mag ook in het Engels zijn opgesteld.

Artikel 15.4 ziet op het tijdig aanleveren van de Documentatie. Het artikel bepaalt in algemene zin dat Leverancier de Documentatie moet updaten zodra blijkt dat deze niet langer juist is. Het initiatief tot een Update kan zowel bij de Leverancier zelf liggen als bij Opdrachtgever.

Artikel 16. Productmanagement

Het is voor Opdrachtgevers van belang tijdig op de hoogte te zijn en blijven omtrent de ontwikkelingen van de ICT Prestatie. Vandaar dat in dit artikel is opgenomen dat Opdrachtgever tijdig over de roadmap wordt geïnformeerd (artikel 16.1) en toegang krijgt tot organen/platformen waar ervaringen met en informatie over de ICT Prestatie wordt uitgewisseld (artikel 16.2). Beide aspecten staan los van eventueel overeengekomen Onderhoud.

Artikel 17. Aansprakelijkheid

Het onderwerp aansprakelijkheid leidt vaak tot verhitte discussies tussen Opdrachtgevers en Leveranciers. De ervaring leert echter ook dat die discussies niet altijd terecht zijn:

a) Enerzijds dienen Opdrachtgevers zich te realiseren dat het aan hen als publiekrechtelijke organen is om een proportioneel contractueel kader te hanteren. Met de GIBIT is gepoogd hiertoe een aanzet te geven, door een aansprakelijkheidsmaximum te hanteren dat in relatie staat tot de opdrachtwaarde (idem ARBIT). Dit laat onverlet dat het in voorkomend geval passend kan zijn van dit kader af te wijken.
b) Anderzijds dienen Leveranciers zich te realiseren dat hun tekortschieten kan leiden tot grote schades bij Opdrachtgevers en dat het zodoende niet onredelijk is dat Opdrachtgevers verlangen dat Leveranciers die – door hen veroorzaakte – schade te vergoeden en dat Leveranciers hiervoor over passende verzekeringen beschikken. Ook mag van Leveranciers worden verwacht dat zij hun bedrijfsvoering zo hebben ingericht dat een incident niet direct tot disproportioneel grote schades of schades onder een groot deel of alle klanten van die Leveranciers leidt.
c) Beide Partijen dienen zich verder te realiseren dat naast de bepalingen in de GIBIT het Burgerlijk Wetboek (en andere wetgeving) onverkort van toepassing is, tenzij daar in de GIBIT uitdrukkelijk van is afgeweken. Dit houdt o.m. in dat de regels uit boek 6 titel 1 afdeling 10 (over schadevergoeding) van toepassing zijn, waaronder begrepen de daarin opgenomen regels omtrent schadebegroting, causaliteit, eigen schuld, etc. Zo kan Opdrachtgever pas schade claimen als er sprake is van een tekortkoming of onrechtmatig handelen van de Leverancier en geen schade claimen voor zover zij daar zelf debet aan is of voor zover de schade in onvoldoende causaal verband staat tot de tekortkoming van de Leverancier. Anders dan dus wel eens wordt geroepen in onderhandelingen is van onbeperkte aansprakelijkheid zeker geen sprake (maar beperkt door de kaders van het BW).

In de aansprakelijkheidsclausule wordt onderscheid gemaakt tussen enerzijds persoons- en zaakschade en anderzijds overige schade. Het onderscheid tussen deze twee schadesoorten sluit aan bij verzekeringen die in de markt worden aangeboden. Er wordt zodoende uitdrukkelijk ook geen onderscheid gemaakt tussen directe en indirecte schade. Dit onderscheid komt in de Nederlandse wet niet voor en het is (daarmee) vaak onduidelijk wat er precies met het onderscheid wordt bedoeld. Bij onduidelijkheid is geen van de Partijen gebaat. Soms wordt met indirecte schade gedoeld op schade die in onvoldoende causaal verband staat tot de tekortkoming; de eis van causaal verband is echter al een algemene regel van Nederlands schadevergoedingsrecht (zie hiervoor).

De overige schade staat in relatie tot de omvang van de Jaarvergoeding. Het begrip Jaarvergoeding is gedefinieerd in artikel 1. Het gaat in de kern om een jaargemiddelde van de (oorspronkelijke voorziene) totale vergoeding gezien over de (oorspronkelijk beoogde) duur van het project. In de praktijk zal die totale prijs veelal deels zijn gebaseerd op eenmalige vergoedingen, periodieke vergoedingen of vergoedingen op nacalculatiebasis. Om voor beide Partijen helderheid te bieden is bepaald dat de hoogte van die vergoedingen moet worden berekend aan de hand van de initieel beoogde looptijd en de initiële begrotingen. Beide Partijen weten zo – voorafgaand aan het sluiten van het contract – wat de omvang van de maximale aansprakelijkheid in voorkomend geval zal zijn. Er is bewust niet gekozen voor een dynamischer definitie, aangezien dat in de praktijk alleen maar tot onzekerheid zou leiden. Partijen dienen er aldus wel op bedacht te zijn dat bij majeure wijzigingen onder een bestaande Overeenkomst (voor zover aanbestedingsrechtelijk toegestaan), het waarschijnlijk passend is het aansprakelijkheidsregime bij te stellen.

De maximale aansprakelijkheid is tweemaal de Jaarvergoeding per gebeurtenis en de maximale totale aansprakelijkheid per jaar is viermaal de Jaarvergoeding. Uiteraard blijft onverlet – ongeacht dit 'vangnet' – dat Partijen altijd proportionele afspraken zullen moeten maken. Andere afspraken zijn dus ook denkbaar.

Vaak wordt de discussie gestart om, naast een beperking van aansprakelijkheid per gebeurtenis, ook een algehele beperking van aansprakelijkheid op te nemen. De werkgroep is kritisch op deze verzoeken. Dergelijke afspraken kunnen namelijk tot effect hebben dat er in bepaalde situaties voor de Leverancier weinig prikkel tot nakoming meer is (bij een absoluut maximum is de Leverancier immers niet meer aansprakelijk zodra door eerdere claims dat maximum al is 'volgelopen'). Vandaar dat ervoor is gekozen om de maximale aansprakelijkheid te beperken voor steeds de periode van één jaar. Het daaropvolgende jaar staat de spreekwoordelijke teller weer op nul (een schone lei). Dit sluit ook aan bij de systematiek die verzekeraars hanteren. Het belang van Leveranciers is bovendien gediend met de bepaling dat samenhangende gebeurtenissen worden aangemerkt als één gebeurtenis. De werkgroep meent dat hiermee een gebalanceerde benadering is gekozen die beide belangen dient: enerzijds voor Opdrachtgevers een reëel en voldoende hoog maximum waar voldoende prikkel tot nakoming vanuit gaat en anderzijds voor Leveranciers een absoluut jaarlijks maximum dat daarmee ook beter voorzienbaar en verzekerbaar is.

In het vijfde lid is een genuanceerde regeling getroffen over uitzonderingen op de aansprakelijkheidsregeling, waarbij oog wordt gehouden voor de Gids Proportionaliteit. In de kern zijn hier alle gebruikelijke uitzonderingen op de beperking van aansprakelijkheid samengebracht. Het beperken voor dood of letsel (sub i) en bij opzet of grove schuld (sub ii) wordt algemeen onaanvaardbaar geacht. Het schenden van IE-rechten (sub iii) ligt naar zijn aard volledig in de risicosfeer van de Leverancier, aangezien Opdrachtgever (die slechts objectcode geleverd krijgt) niet in de positie is om te kunnen controleren of de Leverancier enige rechten schendt. Daarbij komt dat de Leverancier al gerechtigd is zelf in te grijpen om die schade te beperken (zie artikel 21). De uitzondering op de beperking voor de verwerking van persoonsgegevens in sub iv is genuanceerd. In de ARBIT is gekozen voor een onbeperkte aansprakelijkheid bij tekortkomingen in verband met de verwerking van persoonsgegevens. Dat lijkt in veel gevallen echter niet proportioneel. Daarom is in de GIBIT in sub iv opgenomen dat er slechts geen beperking geldt voor boetes die ook aan verwerker hadden kunnen worden opgelegd (om zo te benadrukken dat de boete moet zien op handelingen in de risicosfeer van Leverancier liggen) en onder de voorwaarde dat Leverancier tijdig wordt geïnformeerd over onderzoek door de toezichthouder en wordt betrokken bij het voeren van verweer tegen de boete. Daarbij kan bijvoorbeeld worden gedacht aan de situatie waarin Leverancier een slechte beveiliging heeft en de Opdrachtgever daardoor een datalek ondervindt: de Opdrachtgever kan beboet worden voor het datalek, maar dat ligt buiten haar macht. Het is in zo'n geval onbillijk als de Leverancier zich vervolgens kan beroepen op het aansprakelijkheidsmaximum.

Er staat overigens uitdrukkelijk "wordt betrokken bij" het verweer voeren tegen de boete en niet iets als "afstemmen". Het is immers in ultimo aan Opdrachtgever zelf om te bepalen of en zo ja hoe verweer tegen een aan Opdrachtgever opgelegde boete wordt gevoerd. Tegenover die partijautonomie staat wel dat het naar maatstaven van redelijkheid en billijkheid onaanvaardbaar zou zijn om enerzijds wel de boete op de Leverancier te willen verhalen doch anderzijds niet

diezelfde Leverancier in staat stellen verweer te voeren tegen (het aan Leverancier toe te rekenen deel van) die boete. Dat zou een soort 'blanco cheque'-situatie zijn en dat is niet de bedoeling. In dat licht moet deze genuanceerde set aan randvoorwaarden dan ook worden gezien.

Opgemerkt wordt dat ervoor gekozen is om de hoeveelheid uitzonderingen op de aansprakelijkheidsregeling beperkt te houden. In andere inkoopvoorwaarden is bijvoorbeeld terug te vinden dat de beperking van de aansprakelijkheid wordt doorbroken bij datalekken. In de GIBIT is ervoor gekozen om dit geen (generieke) uitzondering te maken. Dit betekent niet dat de werkgroep de mening is toegestaan dat het niet uitzonderen van datalekken altijd een gepaste route is. Het is raadzaam om per overeenkomst te bekijken of een uitzondering voor datalekken proportioneel is.

Artikel 18. Verzekering

In artikel 18 is bepaald dat Leverancier voldoende zekerheid moet bieden voor verhaal, hetzij via een verzekering, hetzij anderszins. Er is bewust voor gekozen een verzekering niet dwingend voor te schrijven. Er zijn immers legio manieren denkbaar waarop het risico voor Opdrachtgevers dat de Leverancier in voorkomend geval geen verhaal biedt, afgedekt kan worden (moedergarantie, bankgarantie, derdenrekening, etc.). De verzekering dient in ieder geval passend en gebruikelijk te zijn. Soms betekent dit dat de Leverancier verzekerd dient te zijn voor beroeps- en bedrijfsaansprakelijkheid, maar in voorkomend geval kan het ook passend en gebruikelijk zijn dat de Leverancier een cyberverzekering heeft.

In het tweede lid is een minimumdekking opgenomen, voor zowel de uit te keren bedragen als de hoeveelheid *events* per jaar. Deze dekking correspondeert met de maximale aansprakelijkheid zoals dit in het vorige artikel is bepaald.

Artikel 19. Geheimhouding

Artikel 19 regelt een wederkerige geheimhoudingsverplichting. In het eerste lid is bepaald dat beide Partijen alle informatie waarvan zij het vertrouwelijke karakter (behoren te) kennen geheim zullen houden, met een uitzondering voor onderaannemers, aandeelhouders, accountants, professionele adviseurs, en dergelijke. Partijen worden ook uit de geheimhouding ontheven voor zover dit noodzakelijk is op grond van een wettelijk voorschrift, onderzoek van een toezichthouder of gerechtelijke procedures.

In het tweede lid is de minimale geheimhoudingstermijn opgenomen. In voorkomend geval zal deze moeten worden verlengd, naar gelang de aard van de gegevens. Voor persoonsgegevens geldt hoe dan ook de termijn die in de Verwerkersovereenkomst is opgenomen.
In het derde lid is opgenomen dat beide Partijen de geheimhouding ook zullen opleggen aan door hen ingeschakeld Personeel en hulppersonen.

Voor transparantie binnen de overheid is in het vierde lid toegevoegd dat de inhoud van Overeenkomsten gedeeld mag worden binnen gemeenten, tussen gemeenten en met relevante samenwerkingspartners. De GIBIT is zodoende meer in lijn met bijvoorbeeld wetgeving omtrent openbaarheid van bestuur.

Artikel 19.5 bepaalt dat vertrouwelijke gegevens op verzoek moeten worden teruggeven. Deze plicht staat, evenals de andere plichten uit dit artikel, los van de verplichtingen die op de Leverancier rusten uit hoofde van de Verwerkersovereenkomst. Overigens kan van Leverancier natuurlijk niet worden verwacht dat hij gegevens verwijdert in dien dit in strijd komt met de wet, zoals wettelijke bewaartermijnen.

Het zesde lid ten slotte stelt voor alle Partijen een boete op het schenden van de geheimhoudingsplicht. Er is een boete opgenomen omdat het begroten van de schade bij schending van de geheimhouding in de praktijk veelal niet eenvoudig is. Zodoende zou iedere prikkel tot het geheim houden van vertrouwelijke informatie zonder boetebeding kunnen ontbreken (bij niet te begroten schade volgt immers toch geen schadeclaim).

Artikel 20. Overmacht

Het eerste lid van dit artikel herhaalt in feite wat er in de wet omtrent overmacht staat.
Het tweede lid expliceert dat bepaalde omstandigheden in ieder geval niet als overmacht worden gekwalificeerd. De in dit lid genoemde omstandigheden komen dus voor risico van de Leverancier. Dit geschiedt uiteraard wel naar redelijkheid en billijkheid: hoewel ziekte geen overmacht is, betekent dit niet dat de Opdrachtgever het conflict met de Leverancier kan opzoeken wanneer een personeelslid incidenteel griep heeft.

Ten aanzien van uitval van nuts- en telecomvoorzieningen is een genuanceerde regeling getroffen. In beginsel kwalificeert uitval van dergelijke diensten als overmacht. De GIBIT erkent daarmee dat Leveranciers dergelijke diensten zelf ook inkopen en daarbij veelal niet in de positie zijn om een bepaald niveau van dienstverlening af te dwingen. Van overmacht is echter geen sprake indien de storing door Leverancier zelf is veroorzaakt of wanneer is overeengekomen dat Leverancier de nuts- of telecomvoorzieningen beschikbaar diende te houden. Ter illustratie van dit laatste: voor een cloud-/ASP-dienst betekent dit veelal dat het de Leverancier wel kan worden aangerekend als zijn eigen verbinding naar het publieke internet toe uitvalt (dit is dan geen overmacht), maar niet indien er op het publieke internet of bij de provider van Opdrachtgever storingen zijn die maken dat er geen gebruik kan worden gemaakt van de cloud-/ASP-dienst.

In artikel 20.3 is bepaald dat Leverancier enig door overmacht genoten voordeel dient te vergoeden, met inachtneming van de beperking van aansprakelijkheid. De gedachte is eenvoudig: Leverancier zou niet rijker moeten worden van een overmachtssituatie. De bepaling is overgenomen uit de ARBIT.

Artikel 21. Intellectuele eigendom

De GIBIT sluit aan bij het in de markt gebruikelijke onderscheid tussen standaard en maatwerk: in beginsel rusten de rechten op standaardprestaties bij de Leverancier, en de rechten op Maatwerkprogrammatuur bij de Opdrachtgever. Dit geldt ook voor de rechten op Data. In artikel 21.2 is dit vastgelegd, om te garanderen dat auteursrechten en databankrechten toekomen aan de Opdrachtgever. Overigens geeft artikel 13.2 Leverancier vervolgens het recht om die Data, ondanks die IE-rechten, te gebruiken (mits deze geanonimiseerd zijn).

Bij Maatwerkprogrammatuur wordt specifiek voor Opdrachtgever iets ontwikkeld. Het ligt dan voor de hand dat Opdrachtgever ook de beschikking krijgt over de rechten en de broncodes van dat werk. Dat is dan ook in artikel 21.4 bepaald.

Voor de overige ICT Prestaties geldt dat daarop een Licentie wordt verleend. Dit komt in artikel 21.3 naar voren. De duur van de Licenties verschilt naar gelang de aard van de Vergoeding: bij periodieke Vergoedingen is de duur van de Licentie gelijk aan de looptijd van de Overeenkomst, bij overige Vergoedingen is sprake van een eeuwigdurende Licentie. De koppeling aan de duur van de Overeenkomst (en niet: aan de betaalfrequentie) bij periodieke Vergoedingen is bewust; voorkomen moet worden dat het niet tijdig betalen automatisch tot verval van de Licentie leidt. Deze abstracte omschrijving sluit zodoende ook aan bij een veelheid aan licentiemodellen die in de praktijk voorkomt. Welk licentiemodel in concrete gevallen wordt gehanteerd, zal volgen uit de (bovenliggende) Overeenkomst die Partijen sluiten. Wel ligt – mede op verzoek van Leveranciers – op voorhand vast dat een licentie in principe niet het recht omvat om zelf exploitatiehandelingen te verrichten. Het woord ‘exploitatiehandelingen’ is zeer breed en is in de IE-literatuur ook gebruikelijk.

In lid 4 is de oplevering en eigendomsoverdracht bij Maatwerkprogrammatuur vastgelegd. Ten opzichte van de versie 2023 geldt hier een nieuw uitgangspunt: open source, tenzij (lid 5). Dit wordt uitgewerkt in hoofdstuk IV.

Denkbaar is ook dat meerdere gemeenten gezamenlijk de Leverancier vragen om Maatwerkprogrammatuur te ontwikkelen. De wet schrijft voor dat dan een gedeeld IE-recht ontstaat. Denkbaar is dat dit helemaal niet wenselijk is, omdat het handiger is om het bijvoorbeeld aan één gemeente (de kartrekker) toe te kennen. Dit is expliciet opgeschreven in lid 6.

Lid 7 bepaalt dat de Leverancier een vrijwaring afgeeft voor aanspraken die voortvloeien uit inbreuken op IE-rechten en daarmee verwante rechten (zoals persoonlijkheidsrechten en portretrechten).

In lid 8 en 9 is geborgd dat Opdrachtgever gebruik kan blijven maken van de voor hem relevante functionaliteit bij claims van derden dat de gebruikte ICT Prestatie inbreuk maakt op hun rechten. Leverancier moet bij inbreuk zo snel mogelijk een oplossing bieden, waarbij hij kan kiezen tussen ten minste één van de opties die genoemd worden in lid 8.

In lid 10 is bepaald dat bij een aansprakelijkstelling door de betreffende derde, Opdrachtgever de Overeenkomst ook moet kunnen ontbinden. Deze laatste bepaling is met name bedoeld om de schade voor Opdrachtgever te kunnen beperken. Opdrachtgever moet een aansprakelijkstelling immers in de administratie opnemen en heeft zodoende een (boekhoudkundige) prikkel om de (vermeende) inbreuk zo snel mogelijk te (kunnen) staken. In de praktijk zal vermoedelijk weinig een beroep worden gedaan op lid 10 en zal met name de (meer praktisch gerichte) benadering van lid 8 en 9 relevant zijn.

De mogelijkheid de Overeenkomst te ontbinden na een beweerde schending van intellectuele eigendomsrechten door derden in lid 10 (zie ook 17.5) is opgenomen vanwege de potentieel grote gevolgen van zo'n claim. Opdrachtgever kan als gevolg daarvan worden geconfronteerd met onder andere beslaglegging op alle inbreukmakende zaken, waaronder computers waarop inbreukmakende software is geïnstalleerd. De (beweerde) rechthebbende kan bovendien schade claimen voor gederfde licentievergoedingen. Dat voor ontbinding een bewering volstaat, en geen in rechte vastgestelde schending het intellectueel eigendom (IE) nodig is, heeft ermee te maken dat de kosten (zie hierboven) bij een voortdurende schending van IE-rechten zeer snel kunnen oplopen, terwijl juridische procedures om de schending definitief vast te stellen zeer lang kunnen lopen.

Artikel 21.11 bepaalt ten slotte dat de garanties en vrijwaringen wegens IE-inbreuken niet van toepassing zijn indien deze betrekking hebben op werken die de Opdrachtgever aan de Leverancier ter beschikking heeft gesteld of door de Opdrachtgever zelf doorgevoerde wijzigingen in de Programmatuur van de Leverancier.

Artikel 22. Toegang tot Data en autorisaties

Ten opzichte van de versie 2023 is het artikel over Data ingrijpend veranderd. Met het oog op nieuwe en hernieuwde aandacht voor de rol die data speelt binnen de overheid, spelen de Inkoopvoorwaarden in op ontwikkelingen in de markt. Het doel is om met de bepalingen omtrent Data tegemoet te komen aan de Wet open overheid, de Wet hergebruik overheidsinformatie, de Data Act (2023/2854), de Data Governance Act (2022/868) en andere nieuwe ontwikkelingen. Het is voor Opdrachtgevers immers van groot belang dat zij toegang blijven houden tot de met de ICT Prestatie verwerkte Data (hun eigen Data). Opdrachtgevers wensen de betreffende gegevens ook buiten de door de Leverancier geleverde prestatie en/of voor andere doeleinden en in andere processen en systemen te kunnen gebruiken, zoals business intelligence toepassingen of big data analyses voor managementinformatie en/of in bedrijfssystemen die deel uitmaken van de proces- en informatieketen. Ook moeten zij voldoen aan wettelijke (transparatie)verplichtingen.

Dit artikel ziet niet enkel op persoonsgegevens, maar ook op niet-persoonsgebonden gegevens. Daarnaast ziet dit artikel niet alleen op de "klassieke" gegevensverwerkingen (SaaS-diensten), maar op alle fysieke en digitale Producten en diensten waarmee Data wordt gegenereerd en verwerkt. Denk bijvoorbeeld niet enkel aan slimme camera's en burgerzakenapplicaties, maar ook aan stoplichten die meten hoeveel auto's er passeren, en speeltoestellen die gebruik meten.

In dat licht bepaalt lid 1 van artikel 22 dat Leverancier de Opdrachtgever op de hoogte stelt van het feit dat er Data worden verwerkt. Het mag niet de bedoeling zijn dat Leveranciers Data genereren (en zelf gebruiken c.q. verkopen), zonder dat de Opdrachtgever hiervan op de hoogte is.

Lid 2 bepaalt dat deze Data in beginsel ook met de Opdrachtgever gedeeld moeten worden. Het is aan Partijen zelf om hier afspraken over te maken. Toegang tot een portaal is een optie, maar het is

ook een mogelijkheid dat Leverancier periodiek een Product uitleest en de Data overhandigt aan de Opdrachtgever. Het ligt bij Data met een dynamisch karakter (zoals sensordata) bijvoorbeeld voor de hand om de Data te ontsluiten via een API. Bij het bepalen van de wijze van verstrekking kunnen partijen ook denken aan het overeenkomen van een licentiemodel voor de Data. CC BY of CC0 zijn hiervoor opties.

Deze gegevensverstrekking dient vervolgens op gangbare en uitgelegde wijze te geschieden (22.3). Het is aan de Leverancier om deugdelijke datastructuren te hanteren waarmee Opdrachtgever kan voldoen aan zijn wettelijke plichten. Dit laat uiteraard onverlet dat de Opdrachtgever hierbij kan helpen, bijvoorbeeld door inzichtelijk te maken welke datastructuren voor hem het beste werken. Het kan voorkomen dat Data niet te duiden is zonder inzage in het onderliggende model of metadatamodel. Als dit model geopenbaard wordt, kan het echter voorkomen dat bedrijfsgeheimen openbaar worden. Het is expliciet niet het doel van de GIBIT om Leveranciers te dwingen tot het opgeven van haar bedrijfsgeheimen. Daarom kan Leverancier eisen dat een NDA wordt getekend door iedereen die inzage krijgt in de beschrijving van het datamodel. Dit moet wel vooraf kenbaar zijn gemaakt; het kan niet zo zijn dat de Opdrachtgever hier bijvoorbeeld middenin een Woo-traject achter komt.

Opdrachtgever is vervolgens vrij om de Data naar eigen goeddunken te gebruiken, tenzij er IE-rechten van de Leverancier op rusten (22.5). Overigens moeten onjuiste Data worden gecorrigeerd (22.6) en helpt de Leverancier bij de wijze van interpretatie van de Data (22.7). Het recht op correctie is bedoeld voor de situatie waarin de Data technisch onvolledig of onjuist is, bijvoorbeeld doordat de Data verkeerd geconverteerd zijn. De bedoeling is niet dat van de Leverancier wordt verwacht dat hij kosteloos Data zelf aanvult en fouten van de Opdrachtgever corrigeert.

Lid 8 bepaalt dat de Data, net als geldt bij persoonsgegevens onder de AVG, worden verwerkt in opdracht van de Opdrachtgever. Zodoende gebruikt Leverancier de Data uitsluitend voor de uitvoering van de Overeenkomst, verwijdert hij de Data niet zonder opdracht daartoe en verwijdert hij de Data wel zodra hij de opdracht daartoe krijgt. Bij het einde van de Overeenkomst treden Partijen in contact over wat de gevolgen van de beëindiging zijn voor de verwerking van de Data. Overigens kan van dit lid, net als van alle andere bepalingen in de Inkoopvoorwaarden, worden afgeweken. Dat betekent dat Partijen bijvoorbeeld kunnen afspreken dat Leverancier de Data (niet zijnde persoonsgegevens) wel voor eigen doeleinden mag gebruiken, of dat Data automatisch worden gewist c.q. overschreven.

Lid 9 bepaalt dat het voorgaande niet geldt in vier gevallen. Ten eerste geldt dit niet als het nakomen van de verplichting technisch onmogelijk is, bijvoorbeeld omdat de Data bij een derde wordt opgeslagen en Leverancier daar ook geen toegang toe heeft. Het moet wel te allen tijde onmogelijk zijn; het enkele feit dat Leverancier de Data bijvoorbeeld verwijdert, doet niet af aan de werking van artikel 22. Ten tweede hoeven de Data niet in strijd met de wet te worden gedeeld of verwijderd. Ten derde hoeft Leverancier zijn bedrijfsgeheimen niet prijs te geven. Het is dan wel aan Leverancier om te bewijzen dat hier sprake van is. Ten slotte hoeft de Leverancier niets met de Data te doen indien de Opdrachtgever heeft aangegeven dat hij de Data niet hoeft te ontvangen.

De laatste leden bepalen dat het gebruik van de Data door Opdrachtgever voor eigen rekening en risico is. Wel moet de Leverancier Opdrachtgever waarschuwen indien het verlenen van toegang ertoe leidt dat bepaalde beveiligingen worden omzeild (lid 10). Opdrachtgever kan zo een geïnformeerde keuze maken over het gebruik van de Data.

Artikel 23. Derdenprogrammatuur

In de GIBIT is een afzonderlijke regeling opgenomen voor Derdenprogrammatuur. Dit begrip is gedefinieerd in artikel 1. Er wordt gedoeld op programmatuur van externe leveranciers die niet gelieerd zijn aan de Leverancier en op de ontwikkeling waarvan de Leverancier verder ook geen invloed heeft. Er kan worden gedacht aan programmatuur van partijen als Microsoft, Oracle, Adobe, Google, IBM, HP, SAP, etc. Overigens zou ook bepaalde Open Source-programmatuur onder deze definitie kunnen vallen.

De regeling van artikel 23 is opgenomen omdat erkend wordt dat Leveranciers veelal geen invloed hebben op de kwaliteit/functionaliteit van deze Derdenprogrammatuur, noch op de voorwaarden waaronder deze Derdenprogrammatuur op de markt wordt gebracht. Dit hangt samen met de wettelijke regeling omtrent het auteursrecht, waaruit (in de kern) volgt dat het exclusief aan de rechthebbende is om te bepalen of, en zo ja onder welke voorwaarden, software op de markt komt en onder welke voorwaarden deze software vervolgens mag worden gebruikt.

Om diezelfde reden is er uitdrukkelijk geen regeling opgenomen omtrent 'derdenapparatuur' of iets dergelijks. Het wettelijke regime bij fysieke zaken (zoals hardware) is namelijk anders dan bij software. Uitgangspunt bij de koop van roerende zaken is immers dat de verkrijger vrij is die zaken te gebruiken en weer door te verkopen, terwijl die vrijheid wettelijk gezien niet bestaat bij software. Een verkoper van gebrekkige zaken zal normaalgesproken ook de achterliggende toeleverancier daar in rechte op kunnen aanspreken (regres hebben op zijn leverancier).

Hoewel de ervaring leert dat veel Derdenprogrammatuur ook bij andere Leveranciers te krijgen is, of wellicht al eerder door Opdrachtgever is aangeschaft, acht de werkgroep het geen onderdeel van de zorgplicht van Leverancier om Opdrachtgever actief te informeren over de mogelijkheid om Derdenprogrammatuur elders te betrekken.

In het eerste lid is bepaald dat de Leverancier tijdig Updates en Upgrades moet uitbrengen teneinde de compatibiliteit met Derdenprogrammatuur te blijven borgen. Hierbij kan bijvoorbeeld gedacht worden aan de situatie dat de ICT Prestatie niet meer functioneert na een Update van de Derdenprogrammatuur, of de situatie dat de Derdenprogrammatuur zelf (om wat voor reden dan ook) niet langer functioneert.

Het bepaalde in lid 2 en 3 vormt het sluitstuk van de afhankelijkheid van Derdenprogrammatuur. Vrij vertaald staat hier dat een Leverancier vrijuit gaat indien een Gebrek in de door hemzelfde geleverde prestatie (veelal: software) wordt veroorzaakt door een fout in de Derdenprogrammatuur, tenzij hij die laatstgenoemde fout had behoren te kennen en eromheen had kunnen werken. Eventueel overeengekomen Service Levels e.d. gelden dus in dat geval ook niet. Wel moet de Leverancier er dan alsnog zo snel mogelijk alles aan doen om het probleem zo snel mogelijk op te lossen (lid 3).

De Leverancier kan niet van deze (royale) uitzondering op de onderhoudsverplichtingen profiteren indien hij niet de hiervoor gespecificeerde informatie heeft gegeven De Leverancier schiet in dat geval in beginsel bovendien tekort in de nakoming van de betreffende verplichtingen. Dat zou in principe een ontbinding of mogelijk vernietiging (wegens dwaling) van de Overeenkomst kunnen rechtvaardigen. Wel moet dan steeds van geval tot geval bezien worden hoe zwaar dat achterhouden van de betreffende informatie door de Leverancier in concreto heeft meegewogen.

In lid 4 wordt een uitzondering op dit regime gemaakt voor Dienstverlening op Afstand. Bij een *on premise*-situatie wordt de software geïnstalleerd op lokale apparatuur en is het uitvoeren van het programma al een auteursrechtelijk relevante handeling waarvoor een licentie is vereist (vgl. artikel 45i Auteurswet). In die situatie wordt dus zowel de software van de Leverancier als de Derdenprogrammatuur (bijv. een SQL-server) geïnstalleerd en heeft de Opdrachtgever voor beide pakketten een licentie nodig. Aangezien die licentie in de praktijk niet onderhandelbaar is (noch voor Leverancier, noch voor Opdrachtgever), onderkennen de Inkoopvoorwaarden dat die licentievoorwaarden dan prevaleren. Leverancier mag deze dan direct doorzetten naar de Opdrachtgever. Bovendien erkent artikel 23 dat Gebreken die worden veroorzaakt door bugs in die Derdenprogrammatuur geen (toerekenbare) Gebreken zijn, doch dat Leverancier dan wel zo snel mogelijk een oplossing moet bedenken.

Bij Dienstverlening op Afstand (cloud, SaaS) is de situatie een hele andere. De software wordt dan geïnstalleerd op de server van de Leverancier. Het is de Leverancier die (door het uitvoeren ervan) verveelvoudigingshandelingen verricht en die (dus) een licentie nodig heeft. Waar bij de *on premise*-situatie het de Opdrachtgever zelf is die een licentie nodig heeft op die Derdenprogrammatuur (zoals een SQL-server), is het bij Dienstverlening op Afstand een interne

kwestie voor de Leverancier geworden om over de juiste licenties te beschikken. De Opdrachtgever koopt eenvoudigweg een totaalpakket als dienst. De Opdrachtgever ziet niet welke Derdenprogrammatuur wordt gebruikt, en gebruikt deze software zelf ook niet. Zij gebruikt immers alleen het pakket van de Leverancier.

In leden 5 en 6 wordt ingespeeld op de situatie waarin de inzet van de Derdenprogrammatuur wijzigt, bijvoorbeeld wanneer de licentievoorwaarden wijzigen (lid 5) of wanneer aanvullende Derdenprogrammatuur in gebruik wordt genomen (lid 6). Het kan immers voorkomen dat een Leverancier gedurende de Overeenkomst extra Producten gaat aanbieden, bijvoorbeeld bij koop op afroep of bij het aanbieden van een aanvullende module.

In beide situaties is het aan de Leverancier om transparant te zijn en de (nieuwe versie van) de licentievoorwaarden ter beschikking te stellen en uit te leggen. De administratie van de Opdrachtgever moet immers volledig blijven, dus als de voorwaarden van derden wijzigen, moet zij deze ook tot haar beschikking hebben.

Lid 7 behandelt de rol van de broker. Gemeenten maken immers steeds vaker gebruik van brokers. Dit is efficiënt, maar ligt aanbestedingsrechtelijk ingewikkeld. Daarnaast ontstaat in die driehoeksrelatie het risico dat de Inkoopvoorwaarden weliswaar gelden tussen Opdrachtgever en broker, maar niet jegens de uiteindelijke toeleverancier. Dat is problematisch nu de feitelijke risico's zich vooral zullen voordoen in de risicosfeer van de uiteindelijke toeleverancier (datalekken, aansprakelijkheid, wanprestatie, etc.). In dit lid wordt duidelijk gemaakt dat de broker ervoor moet zorgen dat de GIBIT gelden tussen Opdrachtgever en toeleverancier. Lukt dat niet of is dat niet opportuun, dan moet de broker eerst met de Opdrachtgever in overleg. De Opdrachtgever kan vervolgens ook toestemming geven om altijd van bepaalde bepalingen af te wijken (bijv. altijd een lagere aansprakelijkheid te accepteren) of om bij bepaalde toeleveranciers of bepaalde ICT Prestaties de GIBIT niet van toepassing te verklaren, maar dit moet wel eerst worden besproken en schriftelijk worden vastgelegd.

Artikel 24. Vervanging Personeel

Het artikel over vervanging van Personeel is overgenomen uit de ARBIT, met dien verstande dat het verbod om Personeel te vervangen behoudens toestemming niet is overgenomen. De bepalingen zijn procedureel van aard, en spreken veelal voor zich.

Artikel 25. Software Bill of Materials

Nieuw in de Inkoopvoorwaarden is de Software Bill of Materials (SBOM). Eisen omtrent cyberveiligheid en de toeleveringsketen worden steeds strenger, bijvoorbeeld vanuit de Cyber Resilience Act (Verordening (EU) 2024/2847). De Leverancier wordt daarom verplicht om duidelijk te zijn over zijn keten en afhankelijkheden. Dit wordt gedaan in de vorm van een Software Bill of Materials. In dit artikel is zoveel mogelijk aangesloten bij de voorschriften van het NCSC. De Leverancier wordt verplicht om transparant te zijn over het gebruik en de herkomst van Derdenprogrammatuur, de toeleveringsketen en de ontvangers van de Data. De werkgroep onderkent dat de SBOM niet in iedere situatie noodzakelijk is. Net als bij alle andere voorschriften uit de Inkoopvoorwaarden is het mogelijk om in de Overeenkomst van deze bepaling af te wijken of deze buiten toepassing te verklaren. Aan Opdrachtgever is de taak om proportioneel om te gaan met de SBOM-verplichting. Maakt iets geen onderdeel uit van een essentiële keten, dan zal de SBOM-verplichting niet altijd voor de hand liggen. Zo ligt het voor de hand om een uitgebreide SBOM te eisen bij kritieke infrastructuur (zoals burgerzakenapplicaties en financiële pakketten), applicaties die lang in gebruik blijven, ICT Prestaties met veel integraties en koppelingen en systemen met hoge compliance-eisen. Een uitgebreide SBOM ligt minder voor de hand bij bijvoorbeeld kleine ICT Prestaties (zoals een plug-in), niet-kritieke diensten (zoals een vertaal-tool) en publiek beschikbare open source software.

Anno 2025 is de SBOM een relatief nieuw fenomeen, waardoor er nog geen legio marktstandaarden zijn. Een van de marktstandaarden die wel bestaat, is ISO/IEC-norm 5230:2020. Om geen overbodige complianceverplichtingen in het leven te roepen, is aangegeven dat het voldoen aan deze norm afdoende is (lid 2). De Leverancier kan er zodoende voor kiezen om een SBOM als

bedoeld in lid 1 aan te leveren, of gecertificeerd te worden onder de ISO/IEC-norm en daar bewijs van aan te leveren. Omdat deze norm zelfcertificering kent, is dit een relatief laagdrempelige manier om een uniforme SBOM te ontwikkelen. Daarbij is het doel van de SBOM dat de Opdrachtgever kan controleren waar de afhankelijkheden, licentieproblemen, *bottlenecks* en overige risico's liggen. Velden uit de norm leeglaten, is dus niet acceptabel.

Het doel van de SBOM is om cyberbeveiliging te stimuleren. Zou er juist een risico voor de cyberveiligheid ontstaan door het delen van een deel van de SBOM, wordt dit doel ongedaan gemaakt. Dit is dus niet de bedoeling, zo bepaalt lid 3. Het verstrekken van een volledige SBOM kan indirect inzicht geven in toegepaste architectuur- en leverancierskeuzes (zoals strategische afhankelijkheden) en componenten of versies die, hoewel niet publiek kwetsbaar, gevoelig kunnen zijn voor misbruik of reverse engineering. Een Leverancier is niet verplicht om dit te delen, tenzij dit naar aanleiding van een incident noodzakelijk is (bijvoorbeeld om effectieve maatregelen te nemen tegen (verdere) schade). Overigens wordt opgemerkt dat hier bijna nooit sprake van zal zijn: onderzoek wijst uit dat SBOM's in de praktijk geen beveiligingsrisico vormen. Dit geldt temeer omdat de SBOM strikt vertrouwelijk is (lid 4).

Ten slotte wordt de rol van de IBD als CSIRT benoemd in lid 5. Denkbaar is dat communicatie over cyberveiligheid in de toekomst (veel) meer via de IBD zal lopen. Dit is positief voor beide partijen: gemeenten kunnen gebruik maken van de expertise van een zeer gespecialiseerde organisatie, en Leveranciers hoeven nog maar met één partij te spreken over cyberveiligheid, in plaats van met al hun klanten.

Artikel 26. Overname van onderneming

In de markt ontstaat nogal eens onrust wanneer sprake is van een overname van onderneming van de Leverancier. Vaak is er weinig reden tot zorg, maar is er wel veel onduidelijkheid omtrent de gevolgen van deze overname. Om deze onrust te verminderen, is dit artikel toegevoegd. Dit betreffen geen nieuwe vereisten (voldoen aan de wet en aan het contract geldt altijd), maar biedt houvast in overleg over de overname van onderneming.

Artikel 27.Opschorting, opzegging en ontbinding

De GIBIT geeft enkele aanvullende regels op de wettelijke regels omtrent opschorting, opzegging en ontbinding. De overige wettelijke regels blijven dus bestaan.

Het gaat hier om drie juridisch onderscheiden middelen/situaties, die in de kern hier op neerkomen:

- opschorten = pauzeren. De Overeenkomst blijft bestaan, maar een der Partijen pauzeert het eigen werk, in reactie op gedrag van de andere Partij. De meest bekende situatie is die waarbij eerst de ene Partij verplichtingen niet nakomt, in reactie waarop de andere Partij daarmee samenhangende verplichtingen pauzeert (vgl. artikel 6:262 BW). Denk hierbij aan het pauzeren van het werk in reactie op het uitblijven van tijdige betaling.

- opzegging = stoppen. De Overeenkomst wordt opgezegd en Partijen gaan uit elkaar, zonder schadeclaims. Dit kan alleen tegen het einde van de looptijd. Vroegtijdige opzegging leidt tot schadeplichtigheid. Bij duurrelaties of zeer grote afhankelijkheid is het denkbaar dat een extra lange opzegtermijn in acht moet worden genomen.

- ontbinding = terugdraaien + schadevergoeding. De Overeenkomst komt ten einde en de gevolgen van de Overeenkomst worden zoveel mogelijk ongedaan gemaakt. Dat betekent praktisch dat de geleverde goederen weer terug worden geleverd en dat het geld terug wordt betaald. Waar teruglevering onmogelijk is, wordt gekeken wat de waarde van de prestatie was voor de ontvanger. Die waarde kan uiteenlopen van de betaalde vergoedingen tot 0. Bij een ontbinding kan de schade die wordt geleden wegens het tekortschieten en wegens het ontbinden op de wederpartij worden verhaald. Ontbinden kan alleen indien de wederpartij tekortschiet in de nakoming of indien zich een andere ontbindingsgrond voordoet. Ontbinden kan ook gedeeltelijk.

De aanvullingen zijn opgenomen in het belang van Opdrachtgever. Zo is een beroep van de Leverancier op opschorting aan banden gelegd (artikel 27.1). Opdrachtgever is immers veelal in grote mate afhankelijk van de Leverancier, terwijl het normale wettelijke systeem de Leverancier vrij laagdrempelig toestaat zich op opschorting te beroepen. Bij een mogelijk beroep op opschorting moet Leverancier voorafgaand waarschuwen voor de consequenties daarvan. Dit is een nadere invulling van de (toch al geldende) zorgplicht en overigens vooral ook fatsoenlijk.

In artikel 27.2 is bepaald dat Overeenkomsten voor bepaalde tijd in beginsel niet tussentijds kunnen worden opgezegd en dat Overeenkomsten voor onbepaalde tijd in beginsel altijd kunnen worden opgezegd met inachtneming van de vermelde opzegtermijnen. De bepaling houdt verband met het bepaalde in artikel 7:408 BW.

In artikel 27.3 is bepaald dat samenhangende Overeenkomsten – ondanks die samenhang – selectief kunnen worden opgezegd tegen het einde van de actuele looptijd. Hierbij kan bijvoorbeeld gedacht worden aan het opzeggen van de onderhoudsovereenkomst, terwijl de overeenkomst voor Dienstverlening op Afstand doorloopt. De bepaling kan overigens ook worden gelezen als selectief verlengen. Het artikel is vooral bedoeld om eventuele twijfel weg te nemen over de vraag of de Overeenkomsten vanwege die samenhang per se gelijktijdig verlengd dan wel opgezegd zouden moeten worden. Het artikel ziet uitdrukkelijk niet op vroegtijdige opzegging.

In de artikelen 27.4 en 27.5 is bepaald dat Opdrachtgever de Overeenkomst(en) moet kunnen opzeggen bij fusie, uitbesteding en de verplichte overstap naar landelijke voorzieningen. De gedachte bij al deze bepalingen is dat Opdrachtgever zonder een dergelijke bevoegdheid in voorkomend geval niet van bestaande Overeenkomsten af zou kunnen en aldus zou moeten blijven betalen voor dienstverlening die voor hem van geen waarde meer is. In artikel 27.6 is bepaald dat de Leverancier gerechtigd is om – kort samengevat – de daardoor geleden schade bij Opdrachtgever in rekening te brengen. Bij die schadeberekening moet rekening worden gehouden met mogelijke hernieuwde inzet van productiemiddelen door Leverancier. Dit om te voorkomen dat Leverancier voor hetzelfde productiemiddel zowel een schadevergoeding van Opdrachtgever ontvangt, als (bij een andere klant) daarmee opnieuw winst realiseert.

In de artikelen 27.9-27.13 zijn de verschillende ontbindingsgronden nader uitgewerkt. Naast de wettelijke gronden voor ontbinding, zijn hier ook de gebruikelijke gronden (zoals faillissement van de Leverancier) aan toegevoegd. Verder is voorzien in ontbinding bij een vernietiging van een Overeenkomst op grond van de Aanbestedingswet en bij langdurige overmacht. Ook is voorzien in de situatie dat er een wens bestaat om te ontbinden indien voortzetten van de Overeenkomst in strijd komt met grondrechten en de rechtsstaat. Hiermee wordt tegemoetgekomen aan de Agenda Digitale Grondrechten en aan de uitgangspunten van MVO. Om willekeur en rechtsonzekerheid ten aanzien van de laatste ontbindingsgrond te voorkomen, ligt de bewijslast dat voortzetting van de Overeenkomst onaanvaardbaar zou zijn bij de Opdrachtgever. Deze ontbindingsgrond is slechts bedoeld voor de meest extreme gevallen.

Het gaat hier stuk voor stuk om situaties waarbij het in redelijkheid niet van Opdrachtgever kan worden gevergd om de Overeenkomst voort te zetten. Uiteraard is het bij inroepen van al deze ontbindingsgronden aan Opdrachtgever om te bewijzen dat deze gronden zich daadwerkelijk voordoen. Opdrachtgevers die zich ten onrechte op ontbinding beroepen zijn bovendien aansprakelijk jegens de Leverancier. Van de door sommige Leveranciers gevreesde “gemakkelijke escape” is dan ook bepaald geen sprake.

In alle gevallen is rondom ontbinding niet afgeweken van het wettelijk uitgangspunt dat in beginsel ongedaan making van geleverde prestaties plaatsvindt (waaronder terugbetaling van betaalde Vergoedingen). Dat is gedaan omdat diezelfde wet ook als uitgangspunt kent dat voor zover de geleverde prestaties van waarde zijn geweest, de vergoeding ter hoogte van die waarde verschuldigd blijft. De wet is zodoende al (zeer) genuanceerd. Zo zal het bijvoorbeeld bij ontbinding wegens faillissement van de Leverancier bepaald niet voor de hand liggen om ook Vergoedingen uit het verleden terugbetaald te krijgen, nu daar immers prestaties tegenover hebben gestaan die van waarde zullen zijn geweest.

Verder is ook niet afgeweken van het normale wettelijke uitgangspunt dat ontbinding niet mogelijk is bij schuldeisersverzuim aan de zijde van Opdrachtgever.

Artikel 28. Controlerecht en medewerking audits bij Opdrachtgever

Dit artikel ziet op twee verschillende (en niet-gerelateerde) soorten controles/audits: enerzijds het door Opdrachtgever controleren van Leverancier (lid 1-5) en anderzijds het medewerking verlenen van Leverancier aan audits die bij Opdrachtgever worden uitgevoerd (lid 6).

Opdrachtgever is gerechtigd om een onafhankelijke (niet-concurrerende) derde te laten controleren of Leverancier de overeengekomen verplichtingen nakomt (lid 1). Ook mag de juistheid van de factureren worden onderzocht (lid 1).

Er is in het kader van de redelijkheid toegevoegd dat de controle moet zien op de nakoming van wezenlijke verplichtingen. Om diezelfde reden is ook toegevoegd dat een controle alleen gerechtvaardigd is indien er gerede twijfel is over de nakoming door de Leverancier, of indien er een ander gerechtvaardigd belang voor Opdrachtgever is. Ook moet de aanleiding voor een controle kenbaar worden gemaakt. Dit stelt Leverancier in staat om informatie ter beschikking te stellen en zodoende mogelijk de aanleiding voor de controle weg te nemen. Ook is in lid 2 opgenomen dat eerst om de generieke TPM moet worden gevraagd, alvorens een controle mag plaatsvinden. Ten slotte dient de controle binnen een redelijke termijn plaats te vinden en is de auditor aan geheimhouding gebonden.

De Leverancier moet aan de controle alle redelijkerwijs te verwachten medewerking verlenen (lid 3). De kosten voor de controle zijn voor Opdrachtgever, tenzij de deskundige relevante tekortkomingen van Leverancier constateert (lid 4). Deze laatste regel maakt dat een Opdrachtgever terughoudend en prudent zal omspringen met het aantal uit te voeren controles.

De rol van de IBD als CSIRT wordt ook in dit artikel benoemd, namelijk in lid 7. Denkbaar is dat communicatie over cyberveiligheid in de toekomst (veel) meer via de IBD zal lopen. Ook de controle hierop kan gecentraliseerd worden Dit is positief voor beide partijen: gemeenten kunnen gebruik maken van de expertise van een zeer gespecialiseerde organisatie, en Leveranciers hoeven nog maar één controle te ondergaan, in plaats van een controle door al hun klanten. Bij een controle door de IBD is het niet verplicht om eerst gerede twijfel vast te stellen, deze controle is naar haar aard immers minder incidentgericht.

Opdrachtgever zelf kan ook onderworpen zijn aan audits. Het kan in dat kader relevant zijn om meer informatie te kunnen verschaffen over de gebruikte ICT-prestaties. Veelal zal Opdrachtgever die informatie zonder medewerking van de Leverancier kunnen verschaffen. Er zijn echter omstandigheden denkbaar waarbij medewerking van de Leverancier noodzakelijk is. Voor die omstandigheden bepaalt lid 8 dat de Leverancier alle medewerking zal verlenen aan een dergelijke audit.

Artikel 29. Exit-plan, overstap, beperkte voortzetting, overdracht en verlengd gebruik

Artikel 29 vormt het sluitstuk op de “life cycle” benadering van de GIBIT. Dit artikel beschrijft diverse situaties waarbij Opdrachtgever de ICT Prestatie niet langer gebruikt en wat er (in voorbereiding daarop) in dat geval dient te gebeuren voor een soepele overstap.

In artikel 29.1 is vastgelegd dat Partijen op verzoek van een van de Partijen over zullen gaan tot het opstellen van een Exit-plan, en er kan verlangd worden om een bestaand plan bij te werken. In beginsel gebeurt dit één keer per jaar, maar Partijen kunnen hiervan afwijken. Een actueel plan is immers in het belang van beide Partijen. Overigens is het niet de bedoeling dat de Leverancier als verdienmodel onnodig veel overleggen over het Exit-plan bijeenroept. Als uitgangspunt kan worden aangenomen dat de Opdrachtgever uren van de Leverancier vergoedt als hij het overleg bijeenroept, maar de Leverancier het overleg gratis aanbiedt als de Leverancier degene is die het overleg bijeenroept.

Het artikel ziet louter op het opstellen van het plan als zodanig. In het plan kunnen één of meer van de in de volgende artikelleden beschreven opties nader worden uitgewerkt. Duidelijk is dat het bepaalde in de Inkoopvoorwaarden als vangnet is bedoeld; idealiter stellen Partijen een specifieker plan op.

De eerste optie die in dit kader wordt beschreven is dat van de overstap naar een soortgelijke ICT-Prestatie (artikel 29.5-29.7). Dit scenario ziet op de overstap op een ander systeem, of de overdracht van het beheer van het bestaande systeem aan een ander. De Leverancier wordt verplicht om daaraan mee te werken. Doel is een *vendor lock-in* situatie te voorkomen. Een exit kan onder omstandigheden complex zijn. Het verdient dan aanbeveling om de exit voorafgaand eens te evalueren/testen. Dit om te voorkomen dat zodra het moment werkelijk daar is er opeens onvoorziene omstandigheden opduiken. Leverancier kan voor het evalueren vergoedingen in rekening brengen.

De tweede optie die wordt beschreven is het verkrijgen van nieuwe licenties voor beperkt gebruik (artikel 29.8-29.9). De gedachte is dat de bestaande (ruime) licenties niet langer nodig zijn, maar Opdrachtgever door middel van beperktere versies van (nieuwe) software of beperkte licenties op de bestaande software (bijv. alleen inzagerechten, geen gebruik van de software) in ieder geval nog een basis kan borgen om bij bepaalde Data te kunnen. Overigens is hier opgenomen dat in ieder geval de administratieplicht nageleefd moet kunnen worden; ook hier zal in iedere instantie proportioneel mee omgegaan moeten worden. Als Opdrachtgever bijvoorbeeld van Leverancier verlangt dat zij gedurende de volledige fiscale bewaartermijn van 7 jaar het beperkte gebruik blijft aanbieden, kan in bepaalde gevallen wel van Opdrachtgever verwacht worden dat hij open staat voor alternatieve wijzen van het bieden van inzage in de administratie.

De derde optie die wordt geboden is dat de ICT Prestatie wordt overgedragen aan een gemeenschappelijke regeling of andere publieke entiteit (artikel 29.10). Dit artikel geldt in aanvulling op het bepaalde in artikel 27.4. Laatstgenoemde artikel biedt een grond om de Overeenkomst op te zeggen, artikel 29.10 biedt een grond om de Overeenkomst over te dragen. Dit maakt immers dat het Exit-plan van artikel 29.1 van toepassing is op deze werkzaamheden. Wat dit betekent voor de prijzen van de ICT Prestatie zal, net als alles omtrent prijzen, afhangen van hetgeen Partijen daarover hebben afgesproken in de Overeenkomst en/of het Prijzenblad. Is daarin een fixed fee afgesproken, dan zal die gelden. Is daarin een variabele opgenomen, dan zal dat gelden.

De Inkoopvoorwaarden onderkennen dat overdracht niet altijd mogelijk is bij Derdenprogrammatuur. Dat dit benoemd wordt, is slechts een verheldering; een verbod tot overdracht staat veelal toch al in de betreffende licentievoorwaarden en die voorwaarden prevaleerden reeds boven andere afspraken. Ook is overdracht niet mogelijk als dit technisch onmogelijk is.

Ten slotte wordt in algemene zin bepaald dat (kort gezegd) gedurende de uitvoering van de exit-werkzaamheden de Overeenkomst van kracht blijft c.q. verlengd wordt onder gelijke voorwaarden (artikel 29.11). Dit om te voorkomen dat Opdrachtgever in een situatie terechtkomt waarbij hij tijdelijk geen enkel systeem heeft (geen oud systeem meer, maar ook nog geen nieuw systeem). Dit kan bijvoorbeeld het geval zijn als een verliezende inschrijver in de nieuwe aanbesteding een kortgedingprocedure aanhangig maakt, als de inhoud van een rechtelijke uitspraak over de nieuwe aanbesteding leidt tot herbeoordeling of heraanbesteding of als Opdrachtgever tijdig is gestart met de voorbereidingen van een nieuwe aanbesteding, maar zij door onvoorziene omstandigheden meer tijd nodig heeft om de aanbesteding af te ronden. Ook kan een nieuwe Implementatie simpelweg meer tijd nodig hebben dan initieel ingeschat.

Ook hier is op voorhand de situatie rondom de verlenging van het gebruik van Derdenprogrammatuur geadresseerd.

In de basis geldt voor alle exit-werkzaamheden dat deze tegen betaling worden verricht (zie artikel 29.4 en toelichting hiervoor). In afwijking daarop bepaalt artikel 29.11 dat bij een beëindiging wegens toerekenbaar tekortschieten de diensten kosteloos worden verricht. Indien de

Overeenkomst is beëindigd wegens toerekenbaar tekortschieten van Leverancier, staat vast dat sprake is van aansprakelijkheid van Leverancier. Zodoende is deze bepaling in feite een vorm van schadevergoeding in natura. Ook de eenmalige vernietiging van gegevens dient zonder kosten te worden verricht. Dit is niet onredelijk, nu Leverancier de gegevens toch al zou moeten vernietigen. Leverancier heeft immers geen grond meer de gegevens na beëindiging onder zich te houden en zou mogelijk aansprakelijk zijn indien de gegevens wel langer worden bewaard.

Artikel 30. Toepasselijk recht en geschillen

In artikel 30 is bepaald dat de Overeenkomst wordt beheerst door Nederlands Recht, dat het Weens Koopverdrag niet van toepassing is en dat geschillen zullen worden beslecht door de rechter in het arrondissement van de Opdrachtgever.

Er is bewust gekozen voor de overheidsrechter en niet voor arbitrage. Afwegingen hierbij zijn o.m. kosten en de openbaarheid van de zitting. Het is voor overheidsorganen van belang dat publiekelijk verantwoording wordt afgelegd over de besteding van belastinggeld. Het past in dat kader niet om geschillen standaard door middel van (in beginsel) geheime en veelal kostbare arbitrageprocedures af te doen.

Het is wel denkbaar dat in voorkomend geval (alsnog) voor arbitrage gekozen wordt. Partijen zullen daar dan – bij contractering of achteraf – overeenstemming over moeten zien te bereiken. Met name de specifieke deskundigheid van de arbiters kan in dat kader een relevante afweging zijn.

II
Privacy, beveiliging en archivering

In dit hoofdstuk zijn enkele specifieke artikelen opgenomen over privacy, beveiliging en archivering. Het hoofdstuk is van toepassing zodra er gegevens met de ICT Prestatie worden verwerkt. Dat zal heel vaak het geval zijn, maar zeker niet altijd (bijv. niet bij verkoop hardware).

Artikel 31. Verwerkersrelatie

De GIBIT gaat uit van de Standaardverwerkersovereenkomst voor Opdrachtgevers van de VNG, althans een tussen Partijen specifiek overeengekomen verwerkersovereenkomst. Deze wordt in artikel 31 van toepassing verklaard. In de definitie van Verwerkersovereenkomst (zie artikel 1) ligt vast over welk document het gaat.

Artikel 32. Informatiebeveiliging

Artikel 32 ziet specifiek op beveiliging. Het artikel heeft enerzijds het karakter van een garantie, in de zin dat Leverancier er op grond van het eerste lid voor in moet staan dat de Opdrachtgever met de ICT Prestatie kan voldoen aan in de Overeenkomst opgenomen beveiligingsnorm (lid 1). De wijze waarop wordt voldaan aan de normen voor informatiebeveiliging is bewust niet toegevoegd; het is aan Partijen zelf om hier afspraken over te maken.

Ook in dit artikel is de rol van de IBD als CSIRT vastgelegd (lid 2). Als de Leverancier haar contactgegevens met de IBD deelt, kan deze organisatie alle communicatie over incidenten overnemen. Dit is positief voor beide partijen: gemeenten kunnen gebruik maken van de expertise van een zeer gespecialiseerde organisatie, en Leveranciers hoeven nog maar met één partij te spreken over cyberveiligheid, in plaats van met al hun klanten.

Anderzijds bevat het artikel ook een verplichting in die zin dat als de ICT Prestatie door de Leverancier beheerd of verricht wordt, dat de Leverancier er dan voor moet zorgen dat de ICT Prestatie feitelijk aan die norm voldoet (lid 3). Om praktische redenen is ervoor gekozen (in beginsel) dezelfde beveiligingsnorm te hanteren als die van toepassing is op de verwerking van persoonsgegevens.

Het vierde lid bepaalt dat de Leverancier ervoor in staat dat ingeschakeld Personeel zich aan de normen houdt. Hier is ruimte opgenomen voor het hanteren van normen van gelijkwaardig beschermingsniveau, om zodoende meer ruimte te beien voor situaties van uitbesteding.
Op de Leverancier rust een verplichting tot het maken van back-ups (lid 5), en er is een rapportageplicht voor beveiligingsincidenten (lid 6). Een dergelijke plicht bestaat reeds onder de Verwerkersovereenkomst; het is voor Opdrachtgevers echter van belang ook over andersoortige veiligheidsincidenten geïnformeerd te worden. Ter verduidelijking zijn hier de termen Recovery Point Objective (RPO) en Recovery Time Objective (RTO) benoemd, aangezien dit de termen zijn die vaak in SLA's worden gebruikt.

In lid 7 wordt de rol van de IBD andermaal uitgewerkt.

In het achtste lid is uitdrukkelijk bepaald dat informatie over de getroffen beveiligingsmaatregelen vertrouwelijk is. Uiteraard moet dit artikel niet zo worden gelezen dat het de Leverancier verbiedt om haar algemene beveiligingsmaatregelen kenbaar te maken aan anderen, zoals andere klanten. Hiervoor is een uitzondering gemaakt. De specifiek voor de Opdrachtgever aangebrachte beveiligingsmaatregelen vallen wel onder de geheimhoudingsplicht.

Voor de versie 2025 zijn de NIS2-richtlijn en de concepten voor de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit ook meegenomen.

Artikel 33. Archivering

Typerend voor de overheidsmarkt is de gebondenheid aan de Archiefwet. In dit artikel zijn daarom enkele randvoorwaarden opgenomen. Het eerste lid bepaalt dat de Leverancier zorg moet dragen voor het aantoonbaar beheren en beschermen van de bewaarde gegevens overeenkomstig daartoe in de Overeenkomst gestelde eisen, zoals die uit de Gemeentelijke ICT-kwaliteitsnormen. Het tweede lid bepaalt dat de Leverancier gegevens overeenkomstig de in die normen gestelde termijnen moet bewaren. Het derde lid bepaalt dat de Leverancier de archiefbescheiden moet kunnen migreren naar archiefsystemen van Opdrachtgever, overeenkomstig de Overeenkomst (zoals de Gemeentelijke ICT-kwaliteitsnormen). Het artikel zal in de praktijk enige overlap (kunnen) vertonen met het in artikel 29 beschreven deel van het Exit-scenario. Het vierde lid is opgenomen omdat denkbaar is dat de Leverancier de enige Partij is die feitelijk over de archiefbescheiden beschikt. Het artikel stelt buiten alle twijfel dat Leverancier die gegevens moet (terug)leveren aan Opdrachtgever bij opschorting, opzegging of ontbinding van de Overeenkomst. Het is de Leverancier dus niet toegestaan die gegevens te “gijzelen”. Ook hier geldt dat er enige overlap is met het in artikel 29 beschreven Exit-scenario.

Voor de volledigheid zij er op gewezen dat de bewaarplicht voor de Leverancier alleen geldt gedurende de looptijd van de Overeenkomst (artikel lid 2). Van Leverancier kan (en mag) immers niet gevergd worden archiefbescheiden te bewaren, zonder dat daar een Overeenkomst aan ten grondslag ligt. Opdrachtgever dient er wel op bedacht te zijn dat de bewaartermijnen onder de Archiefwet mogelijk langer zijn dan de looptijd van de Overeenkomst. Zij zal dan ook tijdig vooraf, bijvoorbeeld door middel van het hiervoor beschreven Exit-scenario of via de regeling omtrent toegang tot Data als beschreven in artikel 22, de nodige maatregelen moeten treffen om zodoende naleving van de Archiefwet te borgen. Na afloop van de looptijd van de Overeenkomst kan dat niet langer van de Leverancier worden gevergd.

De werkgroep heeft voor de versie 2025 gekeken naar de gevolgen die de aanstaande wijziging van de Archiefwet zal hebben. De conclusie is getrokken dat de nieuwe Archiefwet geen inhoudelijke wijzigingen in de Inkoopvoorwaarden vereist.

III
Dienstverlening op Afstand

In dit hoofdstuk zijn enkele specifieke artikelen opgenomen voor het geval de ICT Prestatie (mede) Dienstverlening op Afstand omvat. Het begrip “Dienstverlening op Afstand” is bewust abstract en vrij breed gedefinieerd (zie artikel 1). Het omvat niet alleen de dienstverlening die klassiek onder “hosting” wordt verstaan, maar alle dienstverlening op afstand (zoals Cloud, SaaS, etc.).

Artikel 34. Algemeen

In het eerste lid is de verplichting opgenomen om alle voor Dienstverlening op Afstand noodzakelijke gegevens aan Opdrachtgever ter beschikking te stellen.

Indien voor gebruik van de ICT Prestatie een webbrowser is vereist, bepaalt artikel 34.2 dat de ICT Prestatie correct dient te functioneren in recente en nog ondersteunde versies van gangbare webbrowsers. Daarnaast moet de ICT Prestatie zo zijn ingericht dat er geen single-point-of-failure is bij meerdere klanten. Het gaat hierbij om de gevallen waarin de applicatie zo is ingericht dat er automatisch een link tussen verschillende klanten is. Denk bijvoorbeeld aan de situatie waarin voor meerdere klanten dezelfde server wordt gebruikt, een klant deze server overbelast, en de andere klanten hun applicatie vervolgens niet kunnen gebruiken. Dit is in reactie op situaties waarbij Leverancier (veel te) lichtvaardig denken over het echt veilig en verantwoord inrichten van een multi-tenant omgeving.

In het vierde lid is het recht op opschorting verder aan banden gelegd. In artikel 27.1 is al bepaald dat opschorting eerst is toegestaan na het sturen van een ingebrekestelling. De afhankelijkheid van Opdrachtgever van de Leverancier bij Dienstverlening op Afstand is veelal niettemin zo groot, dat die waarborg nog onvoldoende kan zijn. Een beroep op opschorting bij Dienstverlening op Afstand betekent immers veelal de facto het volledig frustreren van de bedrijfsvoering van Opdrachtgever (hij kan dan immers niet meer bij zijn gegevens en/of zijn software). Vandaar dat de norm voor een beroep op opschorting bij Dienstverlening op Afstand is aangescherpt.

In het vijfde lid is de eigen verantwoordelijkheid van Opdrachtgever geadresseerd: het is aan hem om inloggegevens geheim te houden.

Artikel 35. Acceptatieprocedure

Acceptatie van een SaaS-dienst loopt net anders dan de Acceptatie van andere ICT Prestaties. Lid 1 bepaalt dat de Acceptatie in een van de productieomgeving afgescheiden omgeving plaatsvindt. Dat zal in veel on premise situaties overigens ook zo zijn, bij Dienstverlening op Afstand is op voorhand duidelijk dat werken met afzonderlijke omgevingen een must is.

In lid 2 wordt onderkend dat een testomgeving niet altijd volledig vergelijkbaar hoeft te zijn met de productieomgeving. Vrij vertaald: het is denkbaar dat de testomgeving ‘lichter’ is, zolang dat maar geen afbreuk doet aan het nut van de Acceptatieprocedure.

Typerend aan Dienstverlening op Afstand is dat deze via internet wordt verleend. Het is zodoende begrijpelijk dat Leveranciers zich gedwongen zien bepaalde vormen van Onderhoud voortdurend, en ook al tijdens de fase van Implementatie, te verrichten. Bij dienstverlening via internet zullen veiligheidsupdates e.d. immers geïnstalleerd moeten worden. In de praktijk ontstaat er dan evenwel soms ruis of daarmee dan (dus) de volledige onderhoudsfase al begonnen is of niet. Vandaar het bepaalde in het derde lid: dergelijk Onderhoud dat noodzakelijk is gelet op de aard van de dienstverlening valt onder de Implementatie, niet onder het Onderhoud.

Artikel 36. Opgeslagen Data

Dit artikel houdt verband met de aansprakelijkheid van Leverancier voor gehoste gegevens en de wettelijke vrijwaring (artikel 6:196c BW). Uit de wet zou kunnen worden afgeleid dat de Leverancier gerechtigd is gehoste gegevens prompt te verwijderen indien er een claim komt dat bepaalde informatie onrechtmatig is opgeslagen. Het artikel regelt dat het uitgangspunt is dat Opdrachtgever eerst over dergelijke claims wordt geïnformeerd (lid 2) en over dergelijke claims altijd overleg met Opdrachtgever plaatsvindt, tenzij de spoedeisendheid maakt dat dergelijk overleg niet kan worden afgewacht (lid 3).

Artikel 37. Onderhoud en Beschikbaarheid

Dit artikel geeft enige aanvullende bepalingen over het Onderhoud van de via Dienstverlening op Afstand aangeboden ICT Prestatie. Het artikel geeft een basis beschikbaarheidslevel van 98% per maand op werkdagen tussen 09.00 en 17.00 uur (lid 2). In alle gevallen geldt uiteraard dat het basisniveaus zijn; de Inkoopvoorwaarden zijn immers bedoeld als vangnet. In de praktijk zullen veelal andere afspraken over bereikbaarheid en Beschikbaarheid worden gemaakt.

In lid 3 is bepaald dat bij Dienstverlening op Afstand de installatie van Upgrades en Updates door de Leverancier wordt verzorgd. Dit zal bij Dienstverlening op Afstand veelal eigen zijn aan de aard van dienstverlening. Het artikel moet dan ook vooral worden gezien in samenhang met het bepaalde in artikel 10, waar juist stond dat Opdrachtgever in beginsel zelf de installatie verzorgt (hetgeen bij Dienstverlening op Afstand veelal niet mogelijk zal zijn).

In lid 4 is bepaald dat Opdrachtgever bij gestandaardiseerde Dienstverlening op Afstand niet het recht heeft de installatie van Updates en Upgrades te weigeren. Hiermee wordt erkend dat die diensten veelal op gelijke wijze voor een veelvoud aan klanten wordt aangeboden en dat het aldus noodzakelijk is steeds mee te gaan in de ontwikkelingen die voor alle klanten gelden. Veroorzaakt een Update of Upgrade downtime, dan moet de Leverancier hierover communiceren. Gedacht kan worden aan een webpagina waarop updates over het Onderhoud worden verstrekt. Bij acuut onderhoud hoeft dit niet voorafgaand te gebeuren, maar moet de Leverancier de Opdrachtgever wel op de hoogte houden van ontwikkelingen.

Artikel 38. Periodieke derdenverklaring

Van Leveranciers kan het verstrekken van een periodieke derdenverklaring (TPM) worden verwacht. Dit wordt in de praktijk ook wel eens een RSO genoemd. Die TPM ziet uitdrukkelijk slechts op de generieke aspecten van de dienstverlening, niet op klantspecifieke afspraken (zie lid 2). De Inkoopvoorwaarden sluiten met deze eis aan bij diverse normen en aanbevelingen waaruit volgt dat bij Dienstverlening op Afstand een dergelijke TPM vereist is. Dat dergelijke TPM's ook in Nederland veel voorkomen blijkt bijvoorbeeld wel uit een site als www.isae3402.nl. Een Leverancier wordt niet verplicht om zowel een TPM als een certificering te overleggen.

Artikel 39. Waarborgen continuïteit

Bij Dienstverlening op Afstand gelden er specifieke continuïteitsrisico's. De via de Dienstverlening op Afstand aangeboden software en de daarmee verwerkte gegevens staan immers buiten de deur. Dat betekent dat bij faillissement van de Leverancier en/of diens toeleverancier(s), Opdrachtgever zowel in juridische als in praktische zin niet (onverkort) meer bij zijn eigen Data kan. Artikel 39 erkent dit risico en bepaalt dat Partijen daarover preventief, dus voordat de feitelijke faillissementssituatie zich voordoet(!), aanvullende afspraken kunnen maken. Het artikel geeft enkele voorbeelden van mogelijke afspraken die in dat kader gemaakt kunnen worden. Opdrachtgevers worden er met klem op gewezen dat deze afspraken alleen zin hebben indien daar ook voor faillissement daadwerkelijk uitvoering aan wordt gegeven.

IV
Open Source

In dit hoofdstuk zijn enkele specifieke artikelen opgenomen voor het geval de ICT Prestatie (mede) het ontwikkelen van Open Source-programmatuur omvat. In artikel 21.5 is reeds het nieuwe uitgangspunt van Maatwerkprogrammatuur gepresenteerd: open source, tenzij. Partijen kunnen ervoor kiezen om de Maatwerkprogrammatuur niet als open source ter beschikking te stellen, maar daar moeten zij expliciet voor kiezen.

Open source is een breed begrip. De werkgroep heeft dan ook niet de intentie om met dit hoofdstuk ieder raakvlak tussen ICT-inkoop en open source te reguleren. Dit hoofdstuk ziet daarom enkel op de situatie waarin een Opdrachtgever Maatwerkprogrammatuur van de Leverancier ontvangt, en deze graag ter beschikking wil stellen aan anderen. Hiermee wordt tegemoet gekomen aan de praktijk, waarin Maatwerkprogrammatuur vaak te duur is om te ontwikkelen, en/of Opdrachtgevers het intellectueel eigendom op Maatwerkprogrammatuur “op de plank laten liggen” omdat zij de capaciteit niet hebben om de rechten optimaal te benutten. Door Maatwerkprogrammatuur te laten ontwikkelen en deze vervolgens als Open Source-programmatuur te laten publiceren, wordt het voor andere gemeenten mogelijk om ook gebruik te maken van deze Programmatuur, en wordt het goedkoper om vervolgens verder te bouwen op deze Programmatuur.

Het is hierbij belangrijk om onderscheid te maken tussen de verschillende termen die binnen de digitale overheid worden gebruikt in het kader van Open Source-programmatuur: open source, open standaarden en Common Ground. Hoewel deze begrippen nauw met elkaar samenhangen, verwijzen ze ieder naar een ander aspect van digitale samenwerking en ontwikkeling.

Open source verwijst naar software waarvan de broncode vrij beschikbaar is. Dit betekent dat overheden deze software kunnen gebruiken, aanpassen en doorontwikkelen zonder afhankelijk te zijn van één Leverancier. Het bevordert transparantie, stimuleert samenwerking tussen organisaties en maakt hergebruik mogelijk, wat leidt tot efficiëntere en duurzamere oplossingen.

Open standaarden vormen de technische spelregels voor gegevensuitwisseling tussen systemen. Het zijn publiek toegankelijke en vrij toepasbare specificaties die ervoor zorgen dat digitale systemen van verschillende Leveranciers goed met elkaar kunnen communiceren. Door het hanteren van open standaarden wordt interoperabiliteit bevorderd en wordt samenwerking tussen overheden eenvoudiger.

Common Ground is een samenwerkingsprogramma van Nederlandse overheden met als doel gezamenlijk digitale voorzieningen te ontwikkelen. De kern van Common Ground is het werken op basis van gedeelde principes, zoals open source software, open standaarden en een gemeenschappelijke informatiearchitectuur. Door deze aanpak kunnen overheden sneller innoveren, gegevens beter uitwisselen en *vendor lock-in* voorkomen.

Artikel 40. Algemeen

Overheidsorganen hechten er belang aan dat de principes van Common Ground worden gevolgd. Lid 1 bepaalt dat het aan de Leverancier is om hieraan te voldoen. Opdrachtgevers hebben de mogelijkheid om aan de Leverancier te vragen om uit te leggen op welke wijze zij uiting geeft aan de principes van Common Ground.

Artikel 41. Oplevering en rechten

Het intellectueel eigendom op de Open Source-programmatuur komt toe aan de Opdrachtgever. Artikel 41.1 bepaalt nog eens expliciet dat het de bedoeling is dat de publicatie als Open Source-programmatuur geschiedt in opdracht van de Opdrachtgever, waarbij ook zaken als Documentatie, plaatjes, bouwinstructies en overige bestanden worden opgeleverd.

Lid 2 bepaalt de wijze van oplevering: deze geschiedt onvoorwaardelijk door publicatie.

Lid 3 bepaalt ten slotte dat de Leverancier volledig gerechtigd en in staat dient te zijn om de Programmatuur te publiceren. Dat houdt in dat er geen intellectuele eigendomsrechten van anderen in de weg mogen staan aan publicatie, en dat er geen gebruik gemaakt mag worden van open source-programmatuur met een zogeheten “viraal effect”. Dat viraal effect heeft te maken met het copyleft-principe dat in sommige open sourcelicenties voorkomt. Copyleft houdt in dat wanneer iemand bestaande open source-software gebruikt, aanpast of combineert met eigen software, de nieuwe of afgeleide software onder dezelfde open-sourcelicentie beschikbaar moet worden gesteld.

Zo’n copyleft-principe bestaat in twee varianten: strong copyleft (zoals de GNU General Public License (GPL)), welke eist dat de gehele software die gebruikmaakt van GPL-componenten onder dezelfde licentie wordt vrijgegeven, en weak copyleft (zoals de EUPL) welke die verplichting beperkt tot de specifieke componenten die onder die licentie vallen. Bij strong copyleft kan Leverancier verplicht worden zijn eigen, mogelijk bedrijfsgevoelige broncode openbaar te maken, terwijl dit bij weak copyleft niet vereist is.

Met lid 3 wordt beoogd te voorkomen dat de Leverancier software oplevert die door het gebruik van strong copyleft-componenten of andere beperkingen niet vrij kan worden gepubliceerd of onderhouden door de opdrachtgever. De Leverancier dient dus zorgvuldig na te gaan welke open source-componenten in de software zijn verwerkt en ervoor te zorgen dat de gekozen licenties verenigbaar zijn met de verplichtingen uit de GIBIT.

Artikel 42. Repository

De publicatie van de Open Source-programmatuur geschiedt op een platform zoals GitHub, GitLab, of Bitbucket (artikel 42.1). Hiervoor wordt de term “repository” gebruikt. Een repository is een plek waar de broncode van een open source-project wordt opgeslagen, beheerd en gedeeld. Dit is een soort digitale map waarin alles staat wat men nodig heeft om het project te begrijpen, te gebruiken of eraan bij te dragen.

Er is bewust voor een platform-neutrale formulering gekozen; het is aan Partijen onderling om te bepalen welk platform zij kiezen. Leverancier zal in ieder geval wel een hyperlink naar de uiteindelijke broncode toesturen.

Het intellectueel eigendom op de Programmatuur komt toe aan de Opdrachtgever. De Leverancier mag de Open Source-programmatuur niet zonder opdracht van de Opdrachtgever publiceren. Daarom wordt de repository pas na Acceptatie publiek toegankelijk (lid 2), en bespreken Partijen hoe zij het openbaar maken (lid 3). Ten overvloede wordt bepaald dat inloggegevens vertrouwelijk zijn.

Databeheer kan onderdeel zijn van de ICT Prestatie (lid 4). Het is niet de bedoeling dat de Leverancier dit gratis hoeft te doen, maar hij dient er wel beschikbaar voor te zijn. Een gangbare vergoeding mag gevraagd worden.

Om problemen met versiebeheer te voorkomen, is in lid 5 vastgelegd dat wijzigingen altijd in de repository worden vastgelegd. Zo blijft de openbaarheid van de Programmatuur geborgd.

Artikel 43. Open source licentie

Wanneer Programmatuur open source beschikbaar wordt gesteld, moet worden bepaald onder welke voorwaarden. Lid 1 bepaalt dat dit in beginsel onder de European Union Public Licence (EUPL) geschiedt. Dit is een open source-licentie die is ontwikkeld en wordt beheerd door de Europese Commissie. Deze licentie is speciaal ontworpen voor gebruik door overheden binnen de EU, en houdt daarbij rekening met Europese wet- en regelgeving.

De EUPL maakt het mogelijk om software vrij te gebruiken, te bestuderen, aan te passen en te verspreiden. Organisaties die software onder de EUPL beschikbaar stellen, geven anderen daarmee

expliciet het recht om de broncode te hergebruiken en eventueel door te ontwikkelen – zolang zij zich houden aan de voorwaarden van de licentie. Hiermee voldoet Programmatuur die onder deze voorwaarden beschikbaar wordt gesteld aan de uitgangspunten van de Wet hergebruik overheidsinformatie. Het is mogelijk om hiervan af te wijken, maar hier zal in de regel vaak geen noodzaak toe zijn.

De bedoeling is een beschikbaarstelling aan het algemene publiek, niet louter aan andere overheden.

Het kan mogelijk zijn dat een leverancier gebruik maakt van bestaande (onderdelen van) open source-software, of verder werkt aan bestaande (onderdelen van) open source-software. Die software zal dan reeds een licentie hebben. Als deze onverenigbaar is met de EUPL, bijvoorbeeld vanwege copyleft-elementen, is het niet mogelijk om het uiteindelijke resultaat onder de EUPL te publiceren. In dit geval biedt lid 2 de mogelijkheid om niet voor de EUPL, maar voor een andere licentie te kiezen. Dit moet dan wel al van tevoren worden aangegeven, zodat de opdrachtgever niet voor verrassingen komt te staan. Het is ook mogelijk om in deze situatie de programmatuur op te splitsen, waardoor het ene deel wel, en het andere deel niet onder de EUPL wordt gepubliceerd (lid 3).

Lid 4 bepaalt, in samenhang met artikel 41.3, dat de Programmatuur onder de gekozen licentie ter beschikking gesteld mag worden.

Artikel 44. Beheer en Onderhoud

Onderhoud op de Open Source-programmatuur is ook mogelijk (artikel 44.1), conform het gebruikelijke regime daarvoor in artikel 10. Tegelijkertijd wordt onderkend dat Onderhoud bij open source soms anders verloopt dan bij “reguliere” software, al was het maar omdat (bij openbare repositories) ook de buitenwereld kan meedoen en meekijken. Ook is het financieringsmodel bij open source vaak anders. Zodoende geldt dat Partijen voor Correctief en Innovatief Onderhoud gezamenlijk de prioritering bepalen, met een doorslaggevende stem voor Opdrachtgever (lid 2 en lid 3). Uiteraard is het niet de bedoeling dat Leverancier dit gratis hoeft aan te bieden, of dat de Leverancier verplicht kan worden om verslechteringen van de programmatuur door te voeren.

Ten overvloede is bepaald dat ook Updates en Upgrades van Open Source-programmatuur open source gepubliceerd dienen te worden (lid 4).

Artikel 45. Aanvullende financiële afspraken

Artikel 45 spreekt grotendeels voor zich: het ter beschikking stellen van de Programmatuur is inbegrepen in de Vergoeding, maar aanvullende taken niet. Zo zijn de beheer- en onderhoudsverplichtingen (artikel 44) niet gratis.

Artikel 46. Beëindiging

Artikel 46.1 bepaalt dat het vroegtijdige einde van de Overeenkomst geen reden is om publicatie van de Programmatuur achterwege te laten. Een verdere exit is niet nodig (lid 2), omdat geen sprake is van een *vendor lock-in* situatie, waar artikel 29 tegen waakt.

Colofon

Auteur
mr. T.O. van Hoorn Dirkzwager legal & tax

Samenstelling en redactie
mr. T Maassen, VNG Realisatie

Kerngroep
C.M. Pelster, Shared Service Centrum Ons
H. Schröder, gemeente Apeldoorn
H.I. Kaynak MSc., VNG Realisatie

Advies Open Source
drs. M.J.C. Hendriks, Open source expert Ministerie van Volksgezondheid, Welzijn en Sport

Vereniging van
Nederlandse Gemeenten

Nassaulaan 12
2514 JS Den Haag
+31 70 373 83 93

info@vng.nl

februari 2026