JURIDISCH UP TO DATE

Vaktijdschrift voor de juridische praktijk

Juridisch up to Date is een uitgave van Fiscaal up to Date – onderdeel van Rendement Uitgeverij BV
Conradstraat 18
3013 AP Rotterdam
E-mail: redactie@futd.nl

Hoofdredactie
Mr. dr. J. (Harry) van Drongelen
(emer.) universitair hoofddocent Sociaal Recht en Sociale Politiek, Universiteit van Tilburg &
(gepens.) senior wetgevingsjurist Ministerie SZW
Mr. A.D.M. (André) van Rijs
Docent bij de vakgroep Private, Business and Labour Law van de Universiteit van Tilburg

Uitgever
Drs. M.P. Hoogerwerf

Abonnementenadministratie
Rendement Uitgeverij BV
Postbus 27020
3003 LA Rotterdam
Telefoon: (010) 243 39 33
E-mail: info@rendement.nl

Abonnementen
Juridisch Up to Date verschijnt 12 keer per jaar. (Proef) abonnementen kunnen ieder moment ingaan, maar slechts worden beëindigd indien uiterlijk twee maanden voor het einde van de abonnementsperiode is opgezegd. Zonder of bij niet-tijdige opzegging wordt het abonnement automatisch verlengd met een jaar. Abonnementen worden geacht zakelijk te zijn. Wilt u een particulier abonnement, dan dient u dit binnen één maand na het aangaan van het abonnement aan ons door te geven. Rendement behoudt zich het recht voor om prijzen en inhoud van de algemene voorwaarden te wijzigen. U kunt de volledige algemene voorwaarden nalezen op www.rendement.nl/av

ISSN 0924-9451

ONDERNEMING EN BEDRIJF

Lauren Wendrich[1] en Frank Rutgers[2]

Nieuwe digitale wetgeving legt extra rechten én verplichtingen bij veel IT-afnemers

2026-0051

De digitale transformatie brengt waardevolle innovaties met zich, maar stelt organisaties onmiskenbaar voor nieuwe uitdagingen. In sectoren die als vitaal worden beschouwd voor het functioneren van onze samenleving – denk aan de zorg, energievoorziening, transport en de overheid – is de verwevenheid met digitale dienstverleners groter dan ooit. Hiermee is ook de kwetsbaarheid voor cyberdreigingen en de kans op ontwrichting van de toeleveringsketen exponentieel toegenomen: een incident bij één dienstverlener kan de continuïteit van een hele (vitale) dienst ontregelen.

Digitale ketenzorg onder druk

Tegen deze achtergrond zien en voorzien wij dat op IT-gebied twee Europese wetten de komende periode grote invloed gaan hebben:

- de NIS2-richtlijn (hierna: NIS2); en
- de Dataverordening.

Enerzijds stelt NIS2 sectoren verplicht tot aantoonbare ketenbeveiliging en risicobeheer; afnemers moeten partijen in hun IT-keten dus actiever gaan managen. Daar staat tegenover dat de Dataverordening het overstappen tussen IT-leveranciers die dataverwerkingsdiensten leveren eenvoudiger maakt, waardoor het managen van de keten ook effectief kan en 'vendor lock-in' wordt teruggedrongen.

In dit artikel staat het praktische samenspel tussen deze twee Europese kaders centraal, met een nadruk op de wijze waarop afnemers in de praktijk hun contractuele positie kunnen versterken, compliance kunnen afdwingen en daarmee hun digitale weerbaarheid kunnen vergroten.

Achtergrond: Dataverordening en NIS2 nader beschouwd

Dataverordening

De Dataverordening, formeel Verordening (EU) 2023/2854, is een reactie van de Europese Unie op de groeiende rol van data als strategisch bedrijfsmiddel. De verordening, die sinds september 2025 van toepassing is, faciliteert eerlijke toegang tot en het gebruik van data, zowel voor bedrijven als consumenten. Het doel is dat gebruikers meer zeggenschap krijgen over data die zij met verbonden producten genereren; dat zijn producten die op het internet zijn aangesloten, zoals een slimme thermostaat of koelkast.[3] De Dataverordening ziet niet alleen op data die wordt gegenereerd door verbonden producten (en gerelateerde diensten), maar bevat ook regels voor zogeheten dataverwerkingsdiensten. Dat zijn, kort gezegd, vrijwel alle digitale diensten die via cloud- of edgetechnologie worden aangeboden, waaronder de SaaS-, IaaS- en PaaS-diensten.[4] Zo kwalificeert een SaaS-platform dat een energieleverancier gebruikt om meterstanden en verbruiksdata te verwerken en te analyseren als een dataverwerkingsdienst in de zin van de Dataverordening en geldt de IT-leverancier als aanbieder van zo'n dataverwerkingsdienst.

Kernverplichtingen: dataportabiliteit, overstap en contractuele minimumafspraken

Alhoewel het faciliteren van eerlijke toegang tot en het gebruik van data de meest belichte kant van de Dataverordening is, bevat de verordening ook bepalingen die een brede impact hebben op IT-leveranciers die kwalificeren als aanbieder van dataverwerkingsdiensten. Dit komt doordat de Dataverordening het recht op dataportabiliteit en de mogelijkheid tot een overstap contractueel vastlegt. IT-leveranciers worden verplicht om data vlot en zonder technische of juridische hindernissen over te dragen wanneer een afnemer naar een andere aanbieder of eigen infrastructuur wil overstappen. Dit stimuleert concurrentie, voorkomt langdurige afhanke-

lijkheid van één IT-leverancier (vendor lock-in) en dient uiteindelijk het publieke belang van betrouwbare en toegankelijke digitale diensten.[5] Dit aspect wordt later nader toegelicht.

Tegelijkertijd verplicht de Dataverordening IT-leveranciers om nadere contractuele afspraken te maken met afnemers over hoe de IT-leverancier interoperabiliteit realiseert, haar dienstverlening voortzet bij migratie en hoe zij de bedrijfscontinuïteit van hun afnemers waarborgt. Voor afnemers betekent deze verordening dat IT-contracten niet alleen over prestaties of prijzen van de IT-leverancier moeten gaan, maar zij ook diepgaand aandacht moeten besteden aan data-eigendom, overdraagbaarheid en contractuele waarborgen.[6]

Worden in het contract geen expliciete afspraken gemaakt over interoperabiliteit, migratie of waarborgen van bedrijfscontinuïteit, zoals voorgeschreven in de Dataverordening, dan worden de dwingendrechtelijke bepalingen van de Dataverordening van rechtswege in het contract ingelezen. Dit leidt ertoe dat de wettelijke minimumverplichtingen – waaronder het waarborgen van overstapmogelijkheden, het voorkomen van overstapbelemmeringen en een maximale opzegtermijn – onverkort gelden. Deze aanvullende werking van de Dataverordening perkt in voorkomende gevallen in het bijzonder de contractvrijheid van de IT-leverancier in, nu van deze bepalingen niet ten nadele van de afnemer kan worden afgeweken en overtreding kan leiden tot aanzienlijke sancties.

NIS2-richtlijn
NIS2, formeel Richtlijn (EU) 2022/2555, borduurt voort op de eerdere NIS-richtlijn,[7] maar brengt deze naar een substantieel hoger niveau. NIS2 wordt op dit moment in Nederland geïmplementeerd middels de Cyberbeveiligingswet (hierna: CBW) en vergroot zowel de reikwijdte als de zwaarte van de bestaande verplichtingen.[8] Organisaties die als essentieel of belangrijk zijn gekwalificeerd, worden met ingang van de CBW nadrukkelijk verantwoordelijk voor de beveiliging van hun gehele netwerk- en informatiesysteem, inclusief de (IT-)toeleveringsketen.

Kernverplichtingen: zorg- en meldplicht
Niet alleen de beveiliging van de afnemer zelf moet op orde zijn, maar óók haar rechtstreekse IT-leveranciers en -dienstverleners dienen te werken in overeenstemming met de voorgeschreven (strengere) beveiligingsstandaarden. Het zwaartepunt verschuift zo van alleen interne governance naar een stelsel van ketenzorg. Deze bredere verantwoordelijkheid betekent overigens niet dat de afnemer álle uitvoering van de beveiligingsmaatregelen op zich moet nemen. Wel blijft de afnemer eindverantwoordelijk voor de governance, verantwoordelijkheden en controlemechanismen in de gehele keten, waarbij het contract met de IT-leveranciers als één van de belangrijkste instrumenten geldt.[9]

Daarnaast legt NIS2 aan alle essentiële en belangrijke organisaties meld- en informatieverplichtingen op. Doet zich bij de desbetreffende organisatie een significant incident voor dat (onder meer) leidt tot een operationele verstoring van haar dienstverlening, dan moet de organisatie haar klanten tijdig informeren en uiterlijk binnen 24 uur een eerste melding doen bij Nationaal Cyber Security Centrum (NCSC).[10]

Ketenverantwoordelijkheid voor afnemers

Met de komst van NIS2 staan afnemers voor de uitdaging om niet alleen bij hun eigen processen en systemen het beveiligingsniveau te bepalen, maar ook af te dwingen dat hun externe (IT-)leveranciers dit doen. Vervolgens moet dit worden vastgelegd in een robuust contractueel fundament.

Risicoanalyse, contracteisen en naleving
Artikel 21 van NIS2 (en de CBW) schrijft afnemers expliciet voor om passende en evenredige technische, operationele en organisatorische maatregelen te nemen om ketenrisico's te beheersen.[11] Dat vraagt niet alleen om het vastleggen van maatregelen, maar ook om beleid en procedures waarmee de afnemer de effectiviteit van die maatregelen regelmatig toetst. Om te waarborgen dat de effectiviteitstoets daadwerkelijk aansluit bij de praktijk, is het verstandig om de onderliggende risico's eveneens regelmatig te analyseren, in ieder geval bij relevante wijzigingen binnen de afnemer (bijvoorbeeld een gewijzigde IT-leverancier of intern systeem) en na incidenten. In die analyse moeten niet alleen IT-leveranciers en onderaannemers van de afnemer worden betrokken, maar ook ketenpartners van partners waar de dienstverlening van afhankelijk is.[12] De uitkomsten van deze analyse vormen de basis voor nieuwe of gewijzigde contractuele afspraken over onder meer toegangsbeheer, dataopslag, authenticatie en monitoring. De afnemer mag dus niet vertrouwen op loze garanties of 'standaard' beveiligingscertificaten, maar moet concrete eisen stellen en naleving hiervan aantoonbaar contractueel borgen.

Governance en handhaving
Ook het toezicht op naleving en de expliciete bevoegdheid om in te grijpen als een IT-leverancier niet aan de eisen voldoet, maken integraal onderdeel uit van de NIS2 regelgeving. Zo wordt het mogelijk om in te spelen op incidenten of nieuwe dreigingen, zonder telkens de afhankelijkheid van één leverancier te hoeven accepteren. Het opstellen van auditrechten, tussentijdse controlemomenten en het recht om verplichtingen aan te scherpen waarborgen dat ketenbeveili-

ging geen eenmalig of reactief thema blijft.[13] Belangrijk is ook dat de bestuurlijke verantwoordelijkheid binnen de organisatie van de afnemer duidelijk wordt toegewezen. Onder NIS2 rusten er immers aanvullende verantwoordelijkheden op bestuurders: zij dienen risico's op het gebied van informatiebeveiliging actief te beoordelen en de bijbehorende beveiligingsmaatregelen van de organisatie goed te keuren zodat aan artikel 21 NIS2 wordt voldaan. Het voorgaande betekent ook dat bestuurders verplichte opleidingen moeten volgen over cyberbeveiliging. Door het volgen van deze opleidingen kunnen organisaties aantonen dat zij beschikken over voldoende kennis en vaardigheden om voornoemde beoordelingen en keuzes te maken.[14] De gevolgen van het negeren van deze verplichting zijn niet gering: boetes, reputatieschade of zelfs bestuurdersaansprakelijkheid zijn reële risico's bij nalatigheid.[15] Een passieve rol in risicomanagement en contractbeheer is dus niet meer acceptabel, zeker nu de RDI samen met acht sectorale toezichthouders duidelijke verwachtingen formuleren en actief op handhaving sturen.[16]

Al met al brengt NIS2 voor bedrijven in kritieke en belangrijke sectoren niet alleen zwaarwegende interne, maar vooral ook externe, contractueel afdwingbare verplichtingen met zich mee. Het afdwingen van naleving binnen de keten vraagt om een juridisch gedetailleerde contractpraktijk, actieve governance, en consistente handhaving richting leveranciers. In de praktijk kunnen conflict en weerstand ontstaan bij IT-leveranciers, hetgeen des te meer het belang benadrukt van duidelijke wettelijke en contractuele instrumenten en het benutten van juridische middelen die naleving kunnen afdwingen.

Dataportabiliteit als hefboom in contractonderhandelingen

Het unieke karakter van de Dataverordening komt duidelijk naar voren in hoofdstuk VI: dataverwerkingsdiensten (onder welke beschrijving veel IT-leveranciers vallen) zijn verplicht afnemers altijd de mogelijkheid te bieden om hun data zonder belemmeringen over te dragen naar een alternatieve aanbieder van een dataverwerkingsdienst of een dienst in eigen beheer (on-prem). Daarbij moeten IT-leveranciers actief meewerken aan de data-export, het behoud van functionaliteit tijdens de migratie, het verstrekken van technische documentatie en het ondersteunen van het migratieproces. De migratie dient bovendien te kunnen plaatsvinden zonder buitensporige kosten of onnodig tijdverlies – eisen die juridisch afdwingbaar zijn onder de Dataverordening.[17]

Dit recht op dataportabiliteit versterkt de positie van organisaties die dataverwerkingsdiensten afnemen. Daarnaast biedt het organisaties die moeten voldoen aan de NIS2 vereisten een krachtig instrument wanneer aanbieders van dataverwerkingsdiensten onvoldoende bereid zijn mee te bewegen op het gebied van cyberbeveiliging. In sectoren waar ketenverantwoordelijkheid en compliance zwaar meewegen – zoals de zorg, energie en financiële dienstverlening – kunnen afnemers zo IT-leveranciers gericht tot actie aansporen. Wanneer een IT-leverancier de gevraagde beveiligingsmaatregelen uit artikel 21 NIS2 niet kan of wil implementeren, biedt het recht op overstap een daadwerkelijk uitvoerbaar alternatief om vaak langlopende contracten open te breken. In de praktijk blijkt bovendien dat de bereidheid van IT-leveranciers om extra te investeren in cyberbeveiliging toeneemt zodra het verlies van klanten een realistische optie wordt.

Praktische tips voor de praktijk

Wat opvalt is dat steeds meer organisaties zelf het initiatief nemen om hun contracten en leveranciersmanagement te herzien in plaats van te wachten op incidenten of overheidsingrijpen. Zij erkennen dat NIS2 niet alleen een juridische verplichting met zich meebrengt, maar vooral een kans biedt om operationele risico's, afhankelijkheden en compliance-kosten te verminderen.

Contracten: maak beveiliging, wijzigingen en overstap afdwingbaar

Organisaties die het komende jaar moeten voldoen aan de eisen van NIS2 doen er verstandig aan om zowel bestaande als nieuwe IT-contracten grondig te screenen op expliciete, meetbare en afdwingbare afspraken met betrekking tot (systeem)beveiliging, periodieke risico-evaluatie, de mogelijkheid tot tussentijdse aanpassingen, een doordachte exit-strategie, en bovendien een meldplicht van de IT-leverancier met betrekking tot significante incidenten die invloed (kunnen) hebben op de dienstverlening van de afnemer, aan de afnemer. Daarnaast dienen organisaties zich bewust te zijn dat overige wetgeving, waaronder de AVG, niet altijd volledig parallel loopt met de Dataverordening of NIS2. Consistente contractanalyse en juridische toetsing op deze parallelle wetgeving zijn cruciaal om risico's te beheersen en daadwerkelijke naleving te waarborgen.

Organisatie: borg governance en ga in gesprek

Zorg ervoor dat het bestuur structureel betrokken is bij compliance en dat er duidelijke procedures zijn voor incidenten, wijzigingen en overstapscenario's. Faciliteer regelmatig overleg tussen inkoop, IT, juridische zaken en security officers om de contractuele afspraken actueel te houden en continu af te stemmen op veranderende risico's. Voer daarnaast het gesprek met IT-leveranciers over de concrete eisen uit NIS2 en de Data-

verordening. Daarbij dienen vragen te worden gesteld zoals: zijn de vereisten bekend, kunnen data daadwerkelijk tijdig, veilig en volledig worden overgedragen, zijn migratiemogelijkheden voorbereid en zijn aansprakelijkheden, sancties en meldverplichtingen voldoende geregeld?

Leveranciers: stuur op ketenrisico's en beveiligingsstandaarden

Selecteer leveranciers bij voorkeur op hun bereidheid en vermogen om te voldoen aan de meest actuele beveiligingsstandaarden waarbij de basis vaak ISO27001 is, eventueel aangevuld met specifieke sectorale normen (zoals NEN7510 voor zorg). Besteed bij internationale samenwerkingen extra aandacht aan de extraterritoriale aspecten van data-opslag, overdracht en compliance. Passiviteit is het grootste risico: organisaties die nu investeren in robuuste contracten, effectieve samenwerking tussen disciplines en ketengerichte governance, zijn beter bestand tegen toekomstige incidenten, audits en veranderingen in de markt.

Vooruitblik: ketenweerbaarheid begint nu

NIS2 en de Dataverordening zetten een nieuwe marktstandaard. NIS2 stelt harde eisen aan ketenverantwoordelijkheid, terwijl de Dataverordening een tool is waarmee de keten ook makkelijker kan worden beheerst. Organisaties moeten investeren in ketengerichte governance, robuuste contracten en effectieve samenwerkingen tussen afdelingen én IT-leveranciers, simpelweg om te voldoen aan de standaarden die wettelijk worden opgelegd.

Noten:

1. Advocaat bij Louwers IP&Tech Advocaten.
2. Advocaat en partner bij Louwers IP&Tech Advocaten.
3. C.A. Janssen, "Lexplicatie, commentaar op Uitvoeringswet dataverordening", InView; Europese Commissie, "Uitleg over de dataverordening", https://digital-strategy.ec.europa.eu/nl/factpages/data-act-explained.
4. IaaS is een infrastructuur als dienst (Infrastructure-as-a-Service), een PaaS is een platform als dienst (Platform-as-a-Service) en een SaaS is een software als dienst (Software-as-a-Service). Deze opsomming van clouddiensten is niet-limitatief; zie randnummers 80 en 81 van de Dataverordening; Artikel 2 onderdeel 8 Dataverordening; zie ook randnummers 80 en 81 van de Dataverordening.
5. Hoofdstuk VI Dataverordening, "Overstappen naar een andere Dataverwerkingsdienst"; Europese Commissie, "Uitleg over de dataverordening", https://digital-strategy.ec.europa.eu/nl/factpages/data-act-explained.
6. C.A. Janssen, "Lexplicatie, commentaar op Uitvoeringswet dataverordening", InView; Europese Commissie, "Uitleg over de dataverordening", https://digital-strategy.ec.europa.eu/nl/factpages/data-act-explained. Zie randnummers 90, 96 en 99 van de Dataverordening.
7. Richtlijn (EU) 2016/1148 is niet meer van kracht sinds 17/10/2024.
8. Naar verwachting treedt de Cyberbeveiligingswet in Q2 van 2026 in werking.
9. Hoofdstuk IV NIS2, "Risicobeheersmaatregelen en rapportageverplichtingen op het gebied van cyberbeveiliging". Zie ook: randnummers 83 en 85 van NIS2.
10. Artikel 23 NIS2; randnummer 102 NIS2; artikelen 16, 26 en 27 CBW; NCSC, "Meldplicht", ncsc.nl.
11. Artikel 21 lid 1 en lid 2 onderdeel d NIS2.
12. Artikel 21 lid 2 onderdeel f NIS2; artikel 21 lid 3 onderdeel f CBW; NCSC, "Zorgplicht", ncsc.nl.
13. "Toeleveringsketen en cyberbeveiliging", rdi.nl.
14. Artikel 24 Cyberbeveiligingswet; artikel 20 NIS2; "De aandacht voor digitale dreigingen verschuift richting de bestuurder", ncsc.nl.
15. Artikel 92 en 93 Cyberbeveiligingswet.
16. Rijksinspectie Digitale Infrastructuur; "Sectoren die onder toezicht RDI vallen", rdi.nl; "Toezicht RDI op de Cyberbeveiligingswet (Cbw)", rdi.nl.
17. Artikel 23 en 25 Dataverordening; *Kamerstukken II* 2024/25, 36733, nr. 3, p. 16 (MvT).