



Grip op digitale afhankelijkheid

Van vendor lock-in naar digitale autonomie

Mr. dr. Mathieu Paapst

**Forum
Standaardisatie**

Standaard Samenwerken



</HTML>

Grip op digitale afhankelijkheid

Van vendor lock-in naar digitale autonomie

Mr. dr. Mathieu Paapst

**Forum
Standaardisatie**

Standaard Samenwerken

Titel: Grip op digitale afhankelijkheid
Subtitel: Van vendor lock-in naar digitale autonomie
Druk: 1^e druk
ISBN: 9789493134997
NUR: 820

Inhoud: Mathieu Paapst (Bureau Forum Standaardisatie / Rijksuniversiteit Groningen)

Opmaak en drukkerij: Osage en Xerox.

©2026 Dit werk is voor verdere verspreiding en gebruik beschikbaar gesteld onder een Creative Commons Naamsvermelding-GelijkDelen 4.0 licentie. De teksten uit de bijlage zijn voor hergebruik beschikbaar onder een Creative Commons Zero licentie.

Inhoud

1. Inleiding	5
1.1 Digitalisering van de overheid	5
1.2 Digitale autonomie en digitale soevereiniteit	6
1.3 ICT aanbestedingen als cruciale hefboom	10
1.4 Opzet van het boek	11
2. Vendor lock-in en vendor break-out	14
2.1 Inleiding	14
2.2 Lock-in: Technologische barrières	15
2.3 Lock-in: Financieel-economische barrières	16
2.4 Lock-in: Contractuele en juridische barrières	17
2.5 Lock-in: Organisatorische barrières	19
2.6 Lock-in: Cloud- en SaaS-ecosystemen	21
2.7 Break out: Analyse van afhankelijkheden	23
2.8 Break out: Technologische mogelijkheden	24
2.9 Break-out: Financiële mogelijkheden	27
2.10 Break out: Juridische mogelijkheden	28
2.11 Break out: Juridische verplichtingen	33
2.11.1 <i>Licenties van specifieke leveranciers</i>	33
2.11.2 <i>Uitbreidingen van licenties</i>	35
2.11.3 <i>Technische redenen</i>	35
2.12 Break out: Organisatorische mogelijkheden	36
2.13 Eerst volledig naar Microsoft?	38
2.14 Gefaseerde exit-strategie	38
3. Leveranciersonafhankelijkheid als ontwerp en contracteringsprincipe	40
3.1 Inleiding leveranciersonafhankelijkheid	40
3.2 Interoperabiliteit als uitgangspunt	40
3.3 Dataportabiliteit en controle over data	43
3.4 Open standaarden in aanbestedingen	45
3.5 Specifiek voorgeschreven standaarden	48
3.6 Belangrijke standaarden in het geval van cloud	50
3.7 Exit-clausules en migratieverplichtingen	51

3.8	Documentatie en transparantie	53
3.9	Eigenaarschap intellectueel eigendomsrecht	55
3.10	Open source software: Voorkeur bij gelijke geschiktheid	56
3.11	Open source software: Niet aanbesteden, maar downloaden	58
3.12	Open source software: Open, tenzij	61
4.	Digitale autonomie	65
4.1	Autonomie als handelingsvrijheid	65
4.2	Vrijheid om samen te werken	65
4.3	Vrijheid om te migreren	68
4.4	Vrijheid om publieke waarden te realiseren	71
4.5	Vrijheid om collectief te handelen	74
4.6	Vrijheid om een eigen koers te bepalen	78
5.	Digitale soevereiniteit	80
5.1	Inleiding	80
5.2	Aanbestedingsrechtelijke ruimte voor soevereiniteitseisen	81
5.3	Change of control bepalingen	85
5.4	Steward ownership als governance instrument	86
5.5	Invloed op (persoons)gegevens in de dataketen	87
5.6	Cloud Sovereignty Framework	89
5.7	Aanbesteden onder defensie en veiligheidsvoorwaarden	94
5.8	Zonder digitale autonomie geen soevereiniteit	96
Bijlage 1:	Voorbeeldclausules	98
A.	Open architectuur	99
B.	Exit, migratie en overstapbaarheid	100
C.	Rechten op software, maatwerk en open source	101
D.	Privacy, veiligheid en compliance	104
E.	Ketencontrole en toegang tot data	105
F.	Digitale soevereiniteit en zeggenschap	106
G.	Continuïteit, roadmap en wijzigingsbeheer	107
H.	Financiële transparantie	108

1. Inleiding

1.1 Digitalisering van de overheid

De overheid is in de afgelopen decennia ingrijpend gedigitaliseerd. Wat begon als automatisering van administratieve processen, is uitgegroeid tot een digitale infrastructuur waarop vrijwel alle publieke taken steunen. Die ontwikkeling heeft de verhouding tussen overheid, burger en markt veranderd. Digitale systemen bepalen in toenemende mate hoe publieke dienstverlening wordt ingericht, hoe gegevens worden verzameld en gedeeld, hoe besluiten worden voorbereid, hoe toezicht wordt gehouden en hoe verantwoording kan worden afgelegd. De kwaliteit van het openbaar bestuur is daardoor mede afhankelijk geworden van de kwaliteit van de digitale systemen waarop dit bestuur rust. Beschikbaarheid, betrouwbaarheid, veiligheid, toegankelijkheid, transparantie en aanpasbaarheid van ICT zijn niet langer zuiver technische eisen, maar zijn voorwaarden geworden voor behoorlijk bestuur.

Dat betekent ook dat digitalisering niet neutraal is: een digitaal systeem bevat impliciete keuzes over macht, verantwoordelijkheid, toegang en controle. Wanneer dergelijke keuzes worden gemaakt door externe leveranciers of sterk afhankelijk zijn van deze partijen, verschuift een deel van de feitelijke sturing over publieke processen naar partijen buiten de overheid.

Deze verschuiving is ook om een andere reden relevant. ICT bestaat immers steeds minder uit afzonderlijke, lokaal beheerde systemen, maar steeds vaker uit cloudplatformen en SaaS-oplossingen. Hierdoor is de overheid niet alleen afhankelijk van één applicatie of één leverancier, maar van een gelaagd ecosysteem van technologieën, contracten, standaarden, dataformaten, beheerders, onderaannemers en infrastructuurpartijen.

Die afhankelijkheid is op zichzelf niet problematisch. Geen enkele moderne overheid kan volledig zonder marktpartijen of zonder internationale technologieketens functioneren. Het probleem ontstaat wanneer afhankelijkheden zodanig worden ingericht dat overheidsorganisaties hun feitelijke keuzevrijheid verliezen. Dan wordt het moeilijk om systemen aan te passen, gegevens over te dragen, leveranciers te vervangen, publieke waarden af te dwingen of zelfstandig te bepalen welke digitale koers wordt gevolgd. De overheid blijft dan formeel verantwoordelijk voor haar publieke taken, maar beschikt niet langer volledig over de middelen om die verantwoordelijkheid waar te maken.

Dit boek vertrekt vanuit de gedachte dat die digitale afhankelijkheid voor een belangrijk deel wordt georganiseerd via ontwerp-, inkoop- en contracteringskeuzes. Afhangelijkheid ontstaat niet pas aan het einde van een contract, wanneer een organisatie ontdekt dat overstappen moeilijk is. Zij ontstaat al bij de keuze voor een bepaalde architectuur, bij het accepteren van gesloten standaarden, bij het uitvragen van specifieke merkproducten, bij het ontbreken van exitafspraken, bij het onvoldoende borgen van dataportabiliteit, en bij het verlies van eigen kennis over systemen en gegevens. Wat later vendor lock-in wordt genoemd, is vaak het resultaat van keuzes die op het moment zelf praktisch, goedkoop of risicomijdend leken.

Daarmee krijgt publieke ICT-inkoop een strategische betekenis. Aanbesteden is niet slechts het selecteren van een leverancier tegen een goede prijs-kwaliteitverhouding. Bij ICT bepaalt de aanbesteding mede welke afhankelijkheden voor jaren worden gecreëerd, welke alternatieven later nog beschikbaar zijn, welke publieke waarden technisch kunnen worden geborgd en hoeveel regie de overheid behoudt over haar eigen digitale infrastructuur.

1.2 Digitale autonomie en digitale soevereiniteit

Er wordt in beleidsstukken vaak gesproken over het willen bereiken van meer digitale soevereiniteit én digitale autonomie. Die begrippen worden soms door elkaar heen gebruikt, en tegenwoordig vooral besproken in relatie tot het willen overstappen van Amerikaanse cloudleveranciers naar Europese partijen. Minder vaak wordt de link gelegd met het streven naar

leveranciersafhankelijkheid en de invloed daarop van vendor lock-in. In deze inleidende beschouwing maak ik eerst de onderlinge samenhang duidelijk tussen deze vier begrippen.

Digitale soevereiniteit verwijst naar het juridische en politieke vermogen van staten of publieke instellingen om in de digitale omgeving hun eigen regels, waarden en strategische belangen effectief te kunnen handhaven. Het begrip heeft een geopolitiek karakter en ziet onder meer op de eigen controle over digitale infrastructuur, bescherming van persoonsgegevens en de mogelijkheid om digitale markten effectief te reguleren. En in het spiegelbeeld daarvan de controle die andere staten ongewenst kunnen uitoefenen op die leveranciers. Dit begrip dus gaat minder over individuele ICT-systemen, ICT-diensten of leveranciers, maar veel meer over de structurele machtsverhoudingen in de digitale economie.

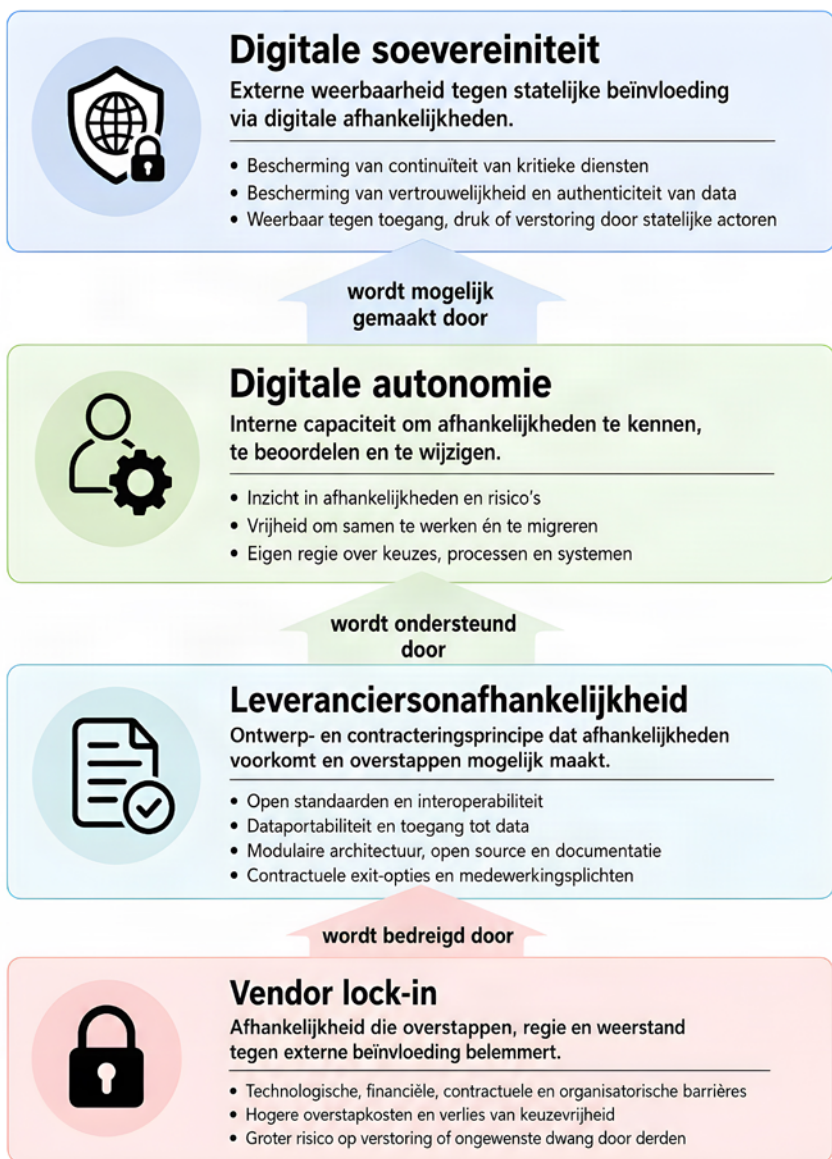
Digitale autonomie is het operationele en organisatorische vermogen van de eigen organisatie om digitale systemen, data en infrastructuur te gebruiken, te beheren en te wijzigen zonder onaanvaardbare afhankelijkheid van externe partijen. Het gaat daarbij om feitelijke handelingsvrijheid: de mogelijkheid om de systemen aan te passen, alternatieven te kiezen of van leverancier te wisselen, zonder dat daarbij disproportionele kosten, risico's of afhankelijkheden optreden. Maar bijvoorbeeld ook de mogelijkheid om de eigen software als open source beschikbaar te stellen. Digitale autonomie draagt bij aan het kunnen realiseren van volledige digitale soevereiniteit.

Leveranciersafhankelijkheid is een ontwerp- en contracteringsprincipe. Het beoogt de structurele afhankelijkheid van één specifieke ICT-leverancier te voorkomen, en tevens de structurele keuzevrijheid gedurende de levenscyclus van een specifiek ICT-systeem te behouden. Leveranciersafhankelijkheid betekent dus niet dat de overheid alles zelf moet gaan doen, zonder gebruik van leveranciers. Maar het betekent dat je desgewenst over kunt stappen naar een andere leverancier, of beheer en ontwikkeling weer zelf kunt gaan doen. Dit wordt onder meer gerealiseerd door in de architectuur, in projecten, bij aanbestedingen en in contracten uit te gaan van het gebruik en uitvragen van open standaarden, te kiezen voor bestaande open source software of het uitvragen van software geleverd onder ruime gebruiksvoorwaarden, rekening te houden met de

mogelijkheden voor dataportabiliteit, en door duidelijke en testbare exit- en migratiemechanismen. Leveranciersafhankelijkheid vormt daarmee een belangrijke onderliggende voorwaarde om digitaal autonoom te kunnen worden.

Vendor lock-in kan in algemene zin worden omschreven als de situatie waarin een organisatie zo afhankelijk is geworden van een specifieke leverancier, technologie of dienst, dat overstappen naar een beter alternatief gepaard gaat met substantieel hoge overstapkosten of aanzienlijke praktische belemmeringen. Lock-in betekent dus niet dat overstappen onmogelijk is, maar dat de drempels zodanig hoog zijn dat alternatieven feitelijk buiten bereik raken. Deze drempels kunnen voortkomen uit technische, contractuele, organisatorische, en financieel economische factoren, en manifesteren zich vaak pas ten volle op het moment dat verandering wenselijk of noodzakelijk wordt.

Vendor lock-in ondermijnt leveranciersafhankelijkheid doordat in het verleden afhankelijkheden zijn ontstaan die overstappen, concurrentie en effectieve regie juist bemoeilijken. Deze samenhang impliceert dat keuzes op het niveau van ICT-inkoop en systeemontwerp directe gevolgen hebben voor de mate waarin overheidsorganisaties hun autonomie kunnen behouden, en uiteindelijk zelfs voor de digitale soevereiniteit van staten. Conceptueel ziet dat er als volgt uit:



Figuur 1: Autonomie-kader: Conceptueel schema onderlinge relatie

In dit kader kan volledige digitale soevereiniteit slechts bereikt worden indien er tevens sprake is van digitale autonomie. Veel organisaties denken ten onrechte dat ze al volledig digitaal soeverein kunnen worden indien de leverancier zijn statutaire zetel in de EU/EER heeft, en alle opslag, verwerking en transport van data uitsluitend plaats zal vinden binnen de EU. Dat is echter alsof je een nieuwe dakkapel laat bouwen voor meer ruimte op zolder, maar je pakt de funderingsproblematiek van je woning niet aan. Je voorkomt dan bijvoorbeeld niet dat je in een nieuwe lock-in beland, maar dan bij een Europese partij. Bovendien bevat de technologiestack vrijwel altijd componenten die afkomstig zijn van niet-Europese partijen, en kan de leverancier zelf ook weer afhankelijk zijn van producten van niet-Europese toeleveranciers.

1.3 ICT aanbestedingen als cruciale hefboom

ICT-aanbestedingen vormen de cruciale hefboom waarmee overheidsorganisaties digitale autonomie en soevereiniteit kunnen nastreven en vestigen. In aanbestedingen en contractbepalingen formuleren zij, impliciet of expliciet, de keuzes die het vermogen om van leverancier te wisselen bepalen. Als deze aspecten onvoldoende worden behandeld in een aanbesteding, ontstaan er vanzelf afhankelijkheden die zich in de loop van de tijd opbouwen en verdiepen. ICT-aanbestedingen zijn dus veel meer dan een louter neutrale, administratieve inkoophandel; het is een van de weinige strategische instrumenten die overheidsorganisaties nog ter beschikking staan om te kunnen sturen richting digitale soevereiniteit.

Momenteel richten aanbestedingen zich echter vooral op “ontzorgt willen worden”, oftewel het willen worden ontlast van verantwoordelijkheid. Daarbij kiest men vaak bewust voor integratie van producten afkomstig van dezelfde leverancier in plaats van interoperabiliteit, korte termijn voordelen, en het mitigeren van risico's tijdens het aanbestedingsproces zelf. Kwesties van structurele afhankelijkheid en de langetermijnevolgen worden daarbij over het hoofd gezien. Bovendien schieten de juridische en organisatorische kaders er in tekort om in voldoende detail de verwachting vast te leggen dat leveranciers het vermogen voor de publieke sector om vrij van leverancier te kunnen wisselen, zullen faciliteren. Integendeel, de gebruikte kaders kunnen soms vendor lock-in versterken. Denk aan de

vele aanbestedingen waarbij een (aanbestedingsrechtelijk overigens veelal verboden) voorkeur wordt uitgesproken voor proprietary Office licenties van een specifieke Amerikaanse cloudleverancier.

Gezien deze context moet de aanbesteding van ICT in de publieke sector bewust en expliciet worden ontworpen en gebruikt als een instrument voor het waarborgen van digitale autonomie en soevereiniteit. De principes van leveranciersafhankelijkheid moeten daarbij verschuiven van de categorie “nice to have” naar die van “absoluut vereist”. Wie digitale soevereiniteit en autonomie wil bereiken, moet deze expliciet inkopen; wie dat nalaat, koopt afhankelijkheid in.

1.4 Opzet van het boek

Dit boek onderzoekt hoe overheidsorganisaties meer grip kunnen krijgen op hun digitale afhankelijkheden. De centrale vraag is hoe ICT-inkoop en contractering kunnen bijdragen aan het voorkomen en doorbreken van vendor lock-in, en hoe zij daarmee de digitale autonomie en digitale soevereiniteit van overheidsorganisaties kunnen versterken.

Het boek is naast deze inleiding opgebouwd uit vier hoofdstukken.

Hoofdstuk 2 analyseert vendor lock-in. Daarin wordt uiteengezet dat lock-in niet één oorzaak heeft, maar voortkomt uit een combinatie van technologische, financieel-economische, juridische, contractuele en organisatorische factoren. Bijzondere aandacht gaat uit naar Cloud- en SaaS-ecosystemen, omdat daarin verschillende vormen van afhankelijkheid samenkomen en elkaar versterken. Het hoofdstuk bespreekt vervolgens hoe een ‘vendor break-out’ kan worden voorbereid: door afhankelijkheden te analyseren, technische en financiële mogelijkheden te beoordelen, juridische aanknopingspunten te benutten, organisatorische belemmeringen weg te nemen en een gelijk speelveld voor alternatieve leveranciers te creëren.

Hoofdstuk 3 richt zich op leveranciersafhankelijkheid als ontwerp- en contracteringsprincipe. Dit hoofdstuk laat zien welke eisen overheidsorganisaties in architectuur, aanbesteding en contracten kunnen opnemen om mogelijke toekomstige afhankelijkheid te beperken.

Aan bod komen onder meer interoperabiliteit, dataportabiliteit, open standaarden, voorgeschreven verplichte standaarden, exitclausules, migratieverplichtingen, documentatie, transparantie, intellectuele eigendomsrechten en open source software. Daarbij wordt niet alleen gekeken naar juridische mogelijkheden, maar ook naar de praktische vraag hoe eisen zodanig kunnen worden geformuleerd dat zij na gunning daadwerkelijk afdwingbaar en controleerbaar blijven.

Hoofdstuk 4 werkt het begrip digitale autonomie uit. Autonomie wordt daar niet opgevat als volledige onafhankelijkheid, maar als feitelijke handelingsvrijheid. Een overheidsorganisatie is digitaal autonoom wanneer zij kan samenwerken, migreren, publieke waarden realiseren, collectief ontwikkelen en inkopen, en een eigen digitale koers bepalen zonder onevenredig afhankelijk te zijn van één leverancier of technologisch ecosysteem. Dit hoofdstuk verbindt daarmee de inhoud van de twee eerdere hoofdstukken met de veel bredere bestuurlijke vraag welke handelingsvrijheid de overheid nodig heeft om haar publieke taken zelfstandig en verantwoord uit te voeren.

Hoofdstuk 5 behandelt de digitale soevereiniteit. Waar digitale autonomie ziet op het interne handelingsvermogen van overheidsorganisaties, ziet digitale soevereiniteit op de externe beïnvloedbaarheid door buitenlandse statelijke actoren. Het hoofdstuk onderzoekt op welke wijze aanbestedingsrechtelijke instrumenten, change of control-bepalingen, steward ownership, grip op de dataketen, het Cloud Sovereignty Framework en de Aanbestedingswet op defensie- en veiligheidsgebied kunnen bijdragen aan het beperken van risico's voor continuïteit en vertrouwelijkheid. Daarbij wordt verdedigd dat volledige digitale soevereiniteit niet kan worden bereikt zonder digitale autonomie. Een organisatie die haar afhankelijkheden niet kent, niet kan migreren en geen alternatieven kan organiseren, kan statelijke beïnvloedbaarheid immers slechts beperkt beheersen.

De bijlage bevat voorbeeldclausules die kunnen worden gebruikt bij aanbestedingen en contracten. Deze clausules zijn niet bedoeld als standaardoplossingen die zonder context kunnen worden overgenomen,

maar dienen als praktische vertaling van de uitgangspunten uit het boek. Zij maken zichtbaar hoe abstracte begrippen als leveranciersafhankelijkheid, interoperabiliteit, dataportabiliteit, exit, open source en soevereiniteit kunnen worden omgezet in concrete contractuele verplichtingen en aanbestedingseisen.

Het boek is geschreven voor juristen, inkopers, contractmanagers, beleidsmakers en bestuurders die binnen de overheid betrokken zijn bij het verwerven van ICT. Enige voorkennis van het proces van aanbesteden wordt verondersteld aanwezig te zijn. Het boek beoogt geen pleidooi te zijn voor volledige zelfvoorziening of afkeer van leveranciers. Overheidsorganisaties zullen altijd met marktpartijen blijven samenwerken. De kern is dat die samenwerking zodanig moet worden ingericht dat de overheid haar keuzevrijheid behoudt.

2. Vendor lock-in en vendor break-out

2.1 Inleiding

Vendor lock-in is de situatie waarin een afnemer niet kan overstappen naar een beter alternatief omdat de overstapkosten (switching costs) substantieel hoog zijn, of omdat een overstap gepaard gaat met aanzienlijke praktische bezwaren of ongemak.¹ Dat betekent niet dat dat overstappen onmogelijk is, maar dat de drempels zodanig hoog zijn dat alternatieven in de praktijk niet haalbaar lijken.

In de context van ICT-producten en diensten is vendor lock-in een structureel kenmerk van de wijze waarop digitale systemen worden ontworpen, ingekocht en beheerd. Keuzes voor bepaalde technologieën, standaarden of leveranciers werken door in latere fasen van gebruik en beheer, waardoor afhankelijkheden zich geleidelijk opbouwen en verdiepen. Wat begint als een rationele keuze op korte termijn, kan op langere termijn leiden tot een situatie waarin reële alternatieven ontbreken.

Een belangrijk kenmerk van vendor lock-in is het zelfversterkende karakter. Naarmate ICT systemen intensiever door een organisatie worden gebruikt, nemen de kosten en complexiteit van een toekomstige overstap toe. Data worden opgeslagen in specifieke leverancierseigen formaten of omgevingen, processen worden volledig afgestemd op de logica van een systeem, en kennis en expertise concentreren zich na verloop van tijd rond een bepaalde technologie of leverancier. Daarnaast spelen netwerkeffecten een rol: de waarde van een systeem neemt toe naarmate meer partijen ervan gebruikmaken, hetgeen de overstap naar alternatieven verder bemoeilijkt.

Wanneer de feitelijke keuzeruimte van overheidsorganisaties wordt beperkt door afhankelijkheden van leveranciers en technologieën, komt

¹ M.H. Paapst, *Barrières en doorwerking*, Diss. Groningen 2013, p. 21-22.

het sturingsvermogen en daarmee de digitale autonomie onder druk te staan. Deze bredere benadering van vendor lock-in vormt het uitgangspunt voor de analyse in dit boek. In de volgende paragrafen worden eerst de verschillende barrières die als gevolg van een lock-in worden opgeworpen nader onderscheiden en uitgewerkt. Vervolgens zal aandacht worden gegeven aan de vendor break-out, de mogelijkheden om los te breken en de barrières te slechten.

2.2 Lock-in: Technologische barrières

Technologische keuzes vormen een fundamentele bron van vendor lock-in. Waar de verderop te bespreken financiële of contractuele afhankelijkheden zich vaak expliciet manifesteren, zijn technologische afhankelijkheden veelal impliciet verankerd in de wijze waarop systemen zijn ontworpen en geïmplementeerd. Juist deze onderliggende technische structuren bepalen in belangrijke mate de feitelijke keuzeruimte van de afnemer.

Een eerste belangrijke factor betreft het gebruik van standaarden en van dataformaten. Indien systemen gebruikmaken van open, breed geaccepteerde standaarden, wordt uitwisseling van gegevens en integratie met andere systemen in beginsel vergemakkelijkt. Omgekeerd, als de gebruikte standaard een gesloten en propriëtaire standaard is van de betreffende leverancier, kunnen andere systemen die standaard veelal niet of enkel tegen betaling ondersteunen. Toegang tot gegevens is dan gebonden aan de technologieën van één enkele leverancier.

Bovendien communiceren systemen via interfaces, zoals Application Programming Interfaces (API's), waarmee het ene systeem de diensten van het andere systeem kan gebruiken. Wanneer het systeem van een leverancier een duidelijke en gestandaardiseerde interface biedt om andere systemen ermee te verbinden of om de functionaliteit ervan te gebruiken, neemt de integreerbaarheid toe en daarmee ook de vervangbaarheid. Daarentegen kunnen beperkte interface-toegang, slecht gedocumenteerde API's of het ontbreken van gestandaardiseerde API's de overdracht van diensten tussen systemen beperken en voorkomen, wat mogelijk leidt tot voortdurende aankopen bij een enkele leverancier. Dit omdat de kosten van vervanging of integratie met een andere dienstverlener veel hoger zouden worden.

Ook gemaakte architectuurkeuzes zijn een belangrijke factor van de technische lock-in. De afgelopen jaren is er een sterke tendens geweest naar integratie, waarbij verschillende producten en diensten van dezelfde producent worden verworven die in technische zin naadloos op elkaar aan kunnen sluiten. In dergelijke systemen zijn functionaliteiten vaak sterk met elkaar verweven, waardoor het vervangen van afzonderlijke onderdelen complex of onmogelijk wordt. Modulaire architecturen daarentegen maken het mogelijk om componenten onafhankelijk van elkaar te vervangen of aan te passen. Architecturale keuzes, zoals de overgang van een monolithische naar een modulaire of servicegerichte architectuur, zijn belangrijk om toekomstige zekerheid en flexibiliteit te waarborgen.

Een ander technologisch mechanisme betreft de wijze waarop data zijn opgeslagen en gestructureerd. Sommige opslagmechanismen, gegevensmodellen en semantische gegevensstructuren, indien slecht gedocumenteerd en niet-standaard, maken het moeilijk om gegevens te migreren. In dergelijke situaties ontstaat niet alleen afhankelijkheid van de technologie zelf, maar ook van de kennis van de leverancier die het systeem heeft ontwikkeld of beheert.

2.3 Lock-in: Financieel-economische barrières

Naast technologische factoren spelen financieel-economische barrières een belangrijke rol bij het ontstaan en voortbestaan van vendor lock-in. Waar technologische keuzes de feitelijke mogelijkheden tot overstap bepalen, beïnvloeden financieel-economische overwegingen in sterke mate de vraag of een overstap als haalbaar wordt beschouwd.

Een centraal element in dit verband betreft de zogenoemde switching costs: de kosten die gepaard gaan met het overstappen van de ene leverancier of technologie naar een andere. Deze kosten kunnen zowel direct als indirect van aard zijn. Directe kosten omvatten onder meer migratiekosten, implementatiekosten en investeringen in nieuwe systemen. Indirecte kosten hebben betrekking op verstoringen van processen, productiviteitsverlies en de inzet van personeel voor training en aanpassing. Hierbij speelt ook de informatie-asymmetrie een rol. Overheidsorganisaties beschikken niet altijd over volledige of betrouwbare informatie over de daadwerkelijke kosten, risico's en baten van een

overstap. Die onzekerheid over de migratiekosten, mogelijke verstoringen en de prestaties van alternatieve oplossingen kan leiden tot risicomijdend gedrag, waarbij wordt vastgehouden aan bestaande leveranciers, zelfs wanneer rationele gronden voor verandering aanwezig zijn.

In aanvulling hierop spelen zogenoemde *sunk costs* een rol. Deze verzonken kosten gaan over reeds in het huidige product gedane investeringen die bij een overstap naar een alternatief niet meer kunnen worden “terugverdiend”. Toch zijn die reeds gemaakte kosten in werkelijkheid niet relevant voor de beslissing om al dan niet door te gaan met het huidige product. De kosten zijn immers al gemaakt en kunnen niet meer ongedaan gemaakt worden, ook niet indien er voor gekozen zou worden om bij het oude product te blijven. Desondanks vormen ze samen met de overstapkosten de financiële verklaring waarmee het gevoelsmatig logischer lijkt om voort te borduren op het al in gebruik zijnde product.

Ook schaalvoordelen kunnen bijdragen aan het idee dat het economisch aantrekkelijk is om gebruik te blijven maken van het bestaande systeem. Naarmate een organisatie samen met andere organisaties een bepaald systeem of platform heeft ingekocht, kunnen de gemiddelde kosten per gebruiker of per functionaliteit afnemen. Denk aan de gezamenlijk collectieve overeenkomsten die er bijvoorbeeld door koepelorganisaties of andere inkoopverbanden met leveranciers zoals Microsoft worden afgesloten. Door de totstandkoming van deze soort van overeenkomsten te faciliteren, dragen deze partijen zelf bij aan het versterken van de financieel-economische vendor lock-in. Het verlaten van een dergelijke schaalvoordeelpositie kan leiden tot hogere kosten, althans op korte termijn.

De prijsstructuren en commerciële strategieën van de leveranciers kunnen verder bijdragen aan het versterken van de lock-in. De bundeling van producten en diensten, waaronder ook het achteraf toevoegen van extra diensten zoals AI ondersteuning of videobellen, en langdurige prijsafspraken met een recht om gratis te kunnen upgraden naar nieuwere versies, kunnen ertoe leiden dat het economisch onaantrekkelijk wordt om onderdelen van een oplossing afzonderlijk te vervangen.

2.4 Lock-in: Contractuele en juridische barrières

Waar technologische en financieel-economische factoren de feitelijke afhankelijkheden bepalen, geven de contractuele en juridische barrières deze afhankelijkheden een juridische structuur en afdwingbaarheid. De wijze waarop rechten en verplichtingen tussen partijen zijn vastgelegd, is daarmee van directe invloed op de mate waarin een afnemer in staat is om systemen te gebruiken, aan te passen of te vervangen.

Een eerste relevant aspect betreft de inrichting van licenties en gebruiksrechten. In veel gevallen verkrijgt de afnemer geen eigendom van software, maar slechts een gebruiksrecht onder specifieke voorwaarden. Deze licenties kunnen beperkingen bevatten ten aanzien van gebruik, reproductie, wijziging en overdracht. Met name wanneer aanpassing of integratie van software contractueel wordt beperkt, kan dit de mogelijkheid om systemen aan te passen aan veranderende behoeften of om alternatieven te implementeren aanzienlijk beperken. Eveneens kan het ontbreken van rechten op broncode, documentatie of specificaties de afhankelijkheid van de oorspronkelijke leverancier versterken.

Daarnaast is de toegang tot data en systemen juridisch en contractueel vormgegeven. Hoewel data in veel gevallen inhoudelijk afkomstig zijn van de afnemer, betekent dit niet zonder meer dat de afnemer ook volledige controle heeft over de opslag, toegang en overdraagbaarheid daarvan. Contractuele bepalingen kunnen de wijze waarop data kunnen worden geëxporteerd, gedeeld of gemigreerd beperken, bijvoorbeeld door het ontbreken van expliciete rechten op dataportabiliteit of door het verbinden van voorwaarden aan toegang tot interfaces en systemen. Dit speelt al helemaal indien er gecontracteerd is onder de algemene voorwaarden van de dominante leverancier of van een bepaalde branche vereniging. Daarin staat dan bijvoorbeeld opgenomen dat de leverancier bij of na het einde van de overeenkomst niet verplicht is om bijstand te verlenen met het oog op een door klant gewenste dataconversie.

Ook de looptijd van contracten en de voorwaarden waaronder een overeenkomst beëindigd kan worden, zijn belemmerende factoren. Vaak is er sprake van meerdere parallel lopende contracten, die echter niet allemaal op dezelfde momenten zijn gestart of zullen eindigen. Bijvoorbeeld de gebruiksovereenkomst die eerder is

afgesloten dan een onderhouds- en supportcontract. Of afzonderlijke gebruiksovereenkomsten voor verschillende elkaar aanvullende componenten. Daarbij is soms ook nog sprake van automatische verlengingsmechanismen. Contractueel overeengekomen beëindigingsvoorwaarden, zoals opzegtermijnen, beëindigingsvergoedingen of afhankelijkheid van medewerking van de leverancier beïnvloeden de feitelijke mogelijkheid tot overstap.

In het verlengde hiervan spelen contractuele bepalingen inzake exit en migratie een belangrijke rol. Indien dergelijke bepalingen ontbreken of beperkt zijn uitgewerkt, kan de afnemer bij beëindiging van de overeenkomst geconfronteerd worden met onzekerheid over de beschikbaarheid van data, documentatie en ondersteuning. Ook kan de leverancier voorwaarden stellen aan de wijze en het tempo van migratie, hetgeen de overstap naar alternatieven bemoeilijkt.

2.5 Lock-in: Organisatorische barrières

Naast technologische, economische en contractuele factoren spelen tot slot ook organisatorische barrières een belangrijke rol bij het ontstaan en voortbestaan van vendor lock-in. De afhankelijkheid is namelijk niet uitsluitend het gevolg van externe omstandigheden, maar het wordt ook in belangrijke mate gevormd en versterkt binnen de organisatie zelf.

Eindgebruikers vinden de technische compatibiliteit van producten en diensten van dezelfde producent doorgaans erg prettig. Bekend is de integratie van Microsoft tussen email, agenda, teams en documenten. Bovendien hebben ze meestal bepaalde ervaringen opgedaan met de al in gebruik zijnde producten en diensten. Men weet welke knop waar zit, en met welke functie. De eindgebruikers zijn in het product getraind, evenals het gros van de ICT-medewerkers die hier hun certificaten voor hebben behaald. Deze “subjectieve compatibiliteit” zorgt vrijwel altijd voor een bepaalde mate van weerstand indien men afscheid wil nemen van dergelijke producten en diensten. Men is dan sneller geneigd om alternatieven langs dezelfde meetlat te leggen, en daarbij op voorhand aan te nemen dat deze alternatieven niet schaalbaar zullen zijn, en hun functionaliteiten niet op korte termijn vergelijkbaar kunnen zijn.

Netwerk- en coördinatie-effecten versterken de bovengenoemde dynamiek. De gepercipieerde waarde van een systeem of platform neemt toe naarmate meer gebruikers, leveranciers of ketenpartners ervan gebruikmaken. Dit kan zich bijvoorbeeld manifesteren in de beschikbaarheid van aanvullende diensten, compatibiliteit met andere systemen of de aanwezigheid van een bredere gebruikersgemeenschap. Eventuele alternatieven die deze voordelen vanwege hun kleinere omvang nog niet bieden, worden daardoor op voorhand als minder aantrekkelijk beschouwd. Men geeft dan vaak aan dat het alternatief al snel vijf jaar in ontwikkeling achterloopt ten opzichte van het product of de dienst van de huidige leverancier. Het is echter de vraag of die vermeende achterstand en benodigde ontwikkeltijd daadwerkelijk goed ingeschat is. Daarvoor is namelijk ook diepgaande kennis en expertise nodig over de werking en de toekomstige ontwikkeling van de verschillende systemen, die zich in veel gevallen enkel nog bij de huidige leverancier bevindt. Wanneer deze kennis binnen de overheidsorganisatie niet (langer) breed beschikbaar of overdraagbaar is, ontstaat bovendien een afhankelijkheid die het vermogen om systemen zelfstandig te beheren, aan te passen of te vervangen beperkt. Dit geldt in het bijzonder wanneer documentatie ontbreekt of onvoldoende toegankelijk is.

Een andere factor waar we mee te maken hebben, is het feit dat werkprocessen vaak aangepast worden op basis van de mogelijkheden van de bestaande systemen. De software structureert vaak de wijze waarop taken worden uitgevoerd, informatie verwerkt, en beslissingen worden genomen. Wanneer een organisatie dergelijke systemen wil gaan vervangen, ontstaat tevens een weerstand tegen het daarvoor benodigde aanpassen van werkwijzen en processen.

Organisatorische traagheid en risicomijding vormt een verdere factor van belang. Overheidsorganisaties opereren binnen kaders van continuïteit, risicobeheersing en verantwoording, hetgeen kan leiden tot een voorkeur voor stabiliteit boven verandering. Onzekerheid over de uitkomsten van een overstap kan deze terughoudendheid verder versterken. Dit is ook de reden dat overheden het potentieel van samenwerken met andere overheidsorganisaties onvoldoende benutten. Men kijkt eerder naar het beschermen van de eigen belangen en de continuïteit van de eigen dienstverlening.

Ook langdurige samenwerkingsrelaties met een leverancier kunnen ervoor zorgen dat er een wederzijdse afhankelijkheid ontstaat door het vertrouwen in elkaar, de praktische samenwerking, en de gezamenlijk opgebouwde kennis. Er is daarbij dus sprake van een meer relationele afhankelijkheid, waarbij keuzemogelijkheden om minder afhankelijk te worden in de praktijk juist minder worden benut. Daarbij moet ook worden opgemerkt dat partijen zoals Microsoft uitermate goed in staat zijn door middel van marketing- en lobbystrategieën om het door de overheid inleveren van digitale autonomie te presenteren als efficiëntie en gemak.²

2.6 Lock-in: Cloud- en SaaS-ecosystemen

De opkomst van cloudcomputing en Software-as-a-Service (SaaS) heeft de aard en intensiteit van vendor lock-in ingrijpend verder veranderd. Waar afhankelijkheden in traditionele ICT-omgevingen vaak betrekking hadden op afzonderlijke systemen of applicaties, kenmerken cloud- en SaaS-omgevingen zich door geïntegreerde ecosystemen waarin infrastructuur, platform en applicaties in samenhang worden aangeboden. Deze ontwikkeling heeft geleid tot een verschuiving van geïsoleerde afhankelijkheden naar meer omvattende vormen van lock-in. In dergelijke omgevingen komen de in de voorgaande paragrafen beschreven barrières in versterkte vorm samen.

Een kenmerkend aspect van cloud-ecosystemen is de gelaagde opbouw van diensten, waarbij onderscheid kan worden gemaakt tussen infrastructuur (IaaS), platformdiensten (PaaS) en applicaties (SaaS). Deze lagen zijn in de praktijk vaak nauw met elkaar verweven en worden veelal door dezelfde leverancier aangeboden. Hierdoor ontstaat een vorm van verticale integratie, waarbij technische afhankelijkheid op het ene niveau doorwerkt naar andere niveaus. Het gebruik van specifieke platformdiensten kan bijvoorbeeld de keuzevrijheid op het niveau van applicaties beperken, en omgekeerd.

De technische lock-in wordt in het geval van clouddiensten vooral veroorzaakt door het gebruik van gesloten, of leveranciers-eigen

² J. de Groot, *Kolonisten van de cloud*, Amsterdam: de bezige bij 2025, p.134.

standaarden of architectuur (bijv. specifieke cloud-native functies zoals de serverless functies van een hyperscaler).

Ook data spelen in deze context een centrale rol. In cloud- en SaaS-omgevingen worden data doorgaans opgeslagen binnen de infrastructuur van de leverancier en zijn zij nauw verbonden met de gebruikte applicaties en diensten. De uitwisseling en migratie van data wordt daarmee afhankelijk van de technische en contractuele voorwaarden die door de leverancier worden gesteld. Naarmate meer systemen en processen binnen hetzelfde ecosysteem worden ondergebracht, neemt de complexiteit van datamigratie en systeemvervanging verder toe.

In de context van cloudcomputing is het vaak financieel onhaalbaar gebleken om de eigen data (inclusief de historie) te exporteren door hoge egress fees. Dat zijn de kosten die clouddaanbieders in rekening kunnen brengen voor het benodigde dataverkeer om data te kunnen verplaatsen vanaf een website, app of cloudopslag naar de eindgebruiker of naar een andere clouddaanbieder. Ze zijn het tegenovergestelde van ingress fees, de kosten om data naar de clouddaanbieder te importeren. Die ingress fees zijn meestal gratis of zeer laag om gebruikers over te halen om gebruik te gaan maken van de clouddienst.

Vanaf 12 januari 2027 is het clouddaanbieders op grond van de Data Act verboden om zogeheten *switching charges* in rekening te brengen. Dat verbod omvat ook kosten voor data-egress die noodzakelijk zijn om over te stappen naar een andere aanbieder of naar een on-premise omgeving.

Opvallend is dat overstapkosten bij het oorspronkelijke besluit om een clouddienst af te nemen vaak nauwelijks een rol lijken te hebben gespeeld. Indien deze kosten destijds wel expliciet in de afweging waren betrokken, zou de businesscase vermoedelijk aanzienlijk minder gunstig hebben uitgepakt. Dit is opmerkelijk, omdat bij clouddiensten één ontwikkeling vrijwel onvermijdelijk is: op enig moment zal de dienstverlening moeten worden overgedragen aan een andere leverancier, of weer door de organisatie zelf moeten worden uitgevoerd. In dat opzicht vertoont cloudgebruik duidelijke parallellen met klassieke outsourcing. Ook daar is een succesvolle overgang afhankelijk van de medewerking van de zittende leverancier, wat de positie van de afnemer kwetsbaar kan maken en het risico op vendor lock-in vergroot. Overigens is uit onderzoek gebleken

dat rond 2016, toen veel organisaties besloten om gebruik te maken van cloudcomputing, de meerderheid daarvan überhaupt niet op de hoogte was van de mogelijkheid dat er zich daarbij een probleem zou kunnen voordoen met vendor lock-in. Slechts 3% van die organisaties was daarvan uitermate goed op de hoogte.³

Ook contractuele en juridische factoren dragen bij aan de bestendiging van afhankelijkheden. Cloud- en SaaS-diensten worden veelal aangeboden via abonnementsmodellen, door bundeling van functionaliteiten en met gestandaardiseerde contractvoorwaarden. Deze kenmerken beperken de mogelijkheid tot maatwerk en kunnen ertoe leiden dat overstappen naar alternatieven gepaard gaat met aanzienlijke kosten en onzekerheden. Tegelijkertijd kunnen schaalvoordelen en integratievoordelen binnen het ecosysteem de aantrekkelijkheid van blijven verder vergroten. Daarbij is er vaak ook sprake van langlopende contracten, met onduidelijke exit-clausules of licentiestructuren die migratie bestraffen. Ook in dit geval kan sprake zijn van de uitoefening door de cloudaanbieder van een intellectueel eigendomsrecht, waardoor een technische lock-in in stand kan worden gehouden.

Tot slot hebben cloud- en SaaS-ecosystemen een belangrijke organisatorische impact. Naarmate digitale voorzieningen worden uitbesteed aan externe platforms, verschuift de rol van de organisatie van beheer naar regie. Dit vergt andere vormen van kennis, governance en sturing. Indien deze niet adequaat worden ingericht, kan de afhankelijkheid van leveranciers verder toenemen, doordat de organisatie onvoldoende in staat is om alternatieven te beoordelen of migraties te realiseren.

2.7 Break out: Analyse van afhankelijkheden

Het doorbreken of omkeren van vendor lock-in wordt ook wel een break-out genoemd. Het begint met het verkrijgen van inzicht in de aard en omvang van de bestaande afhankelijkheden. Zonder een dergelijke analyse is het moeilijk om gerichte maatregelen te nemen of om te beoordelen welke interventies haalbaar en effectief zijn. Een analyse van

³ J. Opara-Martins, R. Sahandi, & F. Tian, 'Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective'. *J Cloud Comp* 2016/5. p. 8-9.
<https://doi.org/10.1186/s13677-016-0054-z>

afhankelijkheden dient integraal van aard te zijn en alle relevante barrières te omvatten. Op technisch niveau kan bijvoorbeeld worden gekeken naar de integratie met andere producten, de gebruikte standaarden, dataformaten en architecturen. Op contractueel en juridisch niveau gaat het om de inhoud van licenties, gebruiksrechten en exit-bepalingen. Economische afhankelijkheden betreffen onder meer de verwachte kosten en risico's van een overstap, terwijl organisatorische afhankelijkheden betrekking hebben op kennis, processen en governance. Daarbij dient ook te worden gekeken naar de besluitvorming die ten grondslag heeft gelegen aan het ontstaan van de lock-in. Daardoor kunnen bepaalde patronen, voorkeuren, participanten en oorzaken vastgesteld worden.

Daarnaast is het van belang om de mate en aard van de afhankelijkheid te duiden. Beslissend is of de afhankelijkheid de feitelijke keuzeruimte van de organisatie zodanig beperkt dat een overstap naar alternatieven niet of slechts tegen disproportionele kosten en risico's mogelijk is. De analyse dient daarom niet alleen beschrijvend, maar ook beoordelend van aard te zijn. Vervolgens kan de analyse gebruikt worden om bepaalde prioriteiten te stellen, waarbij er een gefaseerde aanpak kan worden ontwikkeld om eerst die afhankelijkheden aan te pakken die het meest beperkend danwel risicovol zijn.

2.8 Break out: Technologische mogelijkheden

Bij het ontwikkelen van de gefaseerde aanpak kijken we allereerst naar technische migratiestrategieën die er op gericht moeten zijn om afscheid te gaan nemen van bestaande systemen en de technische afhankelijkheden. Dergelijke migraties zijn zelden eenvoudig en vinden doorgaans niet plaats via een volledige en onmiddellijke vervanging van systemen. Dat zou namelijk aanzienlijke risico's met zich mee brengen voor de continuïteit van de dienstverlening. In plaats daarvan ligt een aanpak voor de hand waarbij de technische afhankelijkheden stapsgewijs worden verminderd en onderdelen van het systeemlandschap stap voor stap geleidelijk worden vervangen.

Doorgaans vormen data het vertrekpunt van de beoogde migratie. Door eerst te zorgen voor toegang tot en controle over data, wordt de afhankelijkheid van het oorspronkelijke systeem direct verminderd en

ontstaat er ook ruimte om alternatieve oplossingen te implementeren. Onderzoek dus eerst of dataportabiliteit technisch gezien mogelijk is. Dataportabiliteit komt verderop in paragraaf 3.3 nog uitvoerig aan de orde. Kijk vervolgens ook of het mogelijk is om over te gaan tot het vervangen van afzonderlijke componenten binnen een systeem. Een belangrijk onderscheid doet zich daarbij voor tussen monolithische en modulaire systemen. In monolithische architecturen zijn functionaliteiten sterk geïntegreerd en onderling afhankelijk, waardoor het vervangen van afzonderlijke onderdelen complex of praktisch onmogelijk wordt. Deze verwevenheid leidt ertoe dat een organisatie bij een poging tot break-out vaak genoodzaakt is het gehele systeem te vervangen, hetgeen aanzienlijke kosten en risico's met zich meebrengt.

Modulaire architecturen daarentegen zijn gebaseerd op het principe dat systemen worden opgebouwd uit afzonderlijke, afgebakende componenten met duidelijk gedefinieerde functies. Deze componenten communiceren via gestandaardiseerde interfaces en kunnen in beginsel onafhankelijk van elkaar worden ontwikkeld, aangepast of vervangen. Door functionaliteiten waar mogelijk alsnog op te knippen in afzonderlijke modules, ontstaat er ruimte voor flexibiliteit en geleidelijke verandering. Mocht dat laatste niet mogelijk zijn, dan zal gekeken moeten worden naar het vervangen van volledige systemen. Het zal niet verbazen dat juist deze situatie zich vaak voordoet in geval van een vendor lock-in.

In de praktijk zullen bestaande en nieuwe systemen soms gedurende een langere periode naast elkaar moeten functioneren. Daarbij worden nieuwe oplossingen naast bestaande systemen opgebouwd en nemen zij geleidelijk de functionaliteiten over. Dat maakt het dus mogelijk om bij de vervanging van volledige systemen afhankelijkheden af te bouwen zonder de continuïteit van de dienstverlening in gevaar te brengen. Dergelijke hybride vormen vereisen echter expliciete regie en coördinatie. Ook laat de praktijk zien dat wanneer twee systemen naast elkaar blijven draaien met vergelijkbare functionaliteit, de eindgebruikers gebruik zullen blijven maken van datgene waar ze al mee werkten. Zo staan op de gemiddelde werkplek binnen de ministeries niet alleen Microsoft Word en Microsoft Edge, maar ook de open source alternatieven LibreOffice en Firefox. Toch zijn de Microsoft producten door toedoen van de ICT beheerder

als de default applicatie ingesteld, waardoor de eindgebruikers vrijwel altijd (bijvoorbeeld bij het openen van ontvangen documenten) bij die producten uitkomen. Het zou goed zijn om allereerst die alternatieve open source applicaties in te stellen als default, en om daarna de applicaties waar afscheid van moet worden genomen simpelweg te blokkeren of te verwijderen. Het technisch ingrijpen door een bepaalde applicatie te blokkeren wordt in de bestuurskunde ook wel het fysiek sturingsmodel genoemd. De reguliere weg wordt voor sluipverkeer geblokkeerd door in het midden van de weg een paaltje te zetten. Wat in dat kader ook goed werkt is het centraal aanbieden van een ICT voorziening waar men voortaan gebruik van kan gaan maken.

De overgang van het ene naar het andere systeem brengt sowieso onzekerheden met zich mee ten aanzien van continuïteit, functionaliteit, en de kwaliteit. Het is daarom van belang om te voorzien in fallback-mechanismen, testfasen en gecontroleerde overgangsmomenten. Door de migratie naar het alternatief als een beheerst en iteratief proces in te richten, kunnen deze risico's worden beperkt.

Migratiestrategieën die uitgaan van tijdelijke consolidatie binnen één leverancier brengen het risico met zich mee dat afhankelijkheden worden verdiept, hetgeen het latere doorbreken daarvan bemoeilijkt. Verderop in dit hoofdstuk bij 2.13 zal hierop verder worden ingegaan. In plaats daarvan kan beter een multi-vendor strategie worden gehanteerd, waarbij verschillende onderdelen van een ICT-landschap door verschillende leveranciers worden geleverd en beheerd. Dit versterkt de onderhandelingspositie van de afnemer en maakt het mogelijk om onderdelen afzonderlijk te vervangen of opnieuw aan te besteden.

Het toepassen van modulaire architecturen en multi-vendor strategieën brengt echter ook uitdagingen met zich mee. Het beheer van meerdere componenten en leveranciers vereist een hogere mate van coördinatie, governance en technische expertise. Daarnaast kunnen integratievraagstukken ontstaan, met name indien standaarden onvoldoende worden nageleefd of interfaces niet eenduidig zijn gedefinieerd. Het realiseren van modulariteit vraagt daarom om bewuste keuzes en consistente toepassing van architectuurprincipes.

2.9 Break-out: Financiële mogelijkheden

Het spreekt voor zich dat een break-out de nodige kosten met zich mee zal brengen. Zo is er een transitiebudget nodig omdat een oude omgeving meestal nog even blijft draaien, terwijl de nieuwe omgeving wordt opgebouwd, data geconverteerd moet worden, en de medewerkers moeten worden getraind. Ook worden er kosten gemaakt voor de aanpassing van koppelingen, templates, en werkwijzen.

Het grootste probleem daarbij is dat die kosten bij een break-out direct al zichtbaar zijn, terwijl de baten pas later zichtbaar zullen worden, en mogelijk zelfs vooral een voordeel zullen kunnen opleveren bij ketenpartners indien zij pas later overstappen. Dat betekent dus ook dat de kosten vaak binnen de termijn van de huidige bestuurder of CIO vallen, terwijl de baten pas bij een opvolger te zien zullen zijn. De voordelen kunnen op financieel gebied bestaan uit een betere onderhandelingspositie omdat je kunt wisselen van leverancier, delen zelf uit kunt voeren, en meerdere leveranciers gelijktijdig kunt inzetten. Daardoor ontstaat er meer concurrentie, lagere licentiekosten, en minder grote prijsstijgingen. De keuzevrijheid die na de break-out gaat ontstaan heeft daarom ook economische waarde. Die waarde verschijnt niet op de begroting, maar is wel degelijk financieel relevant.

Aan de ander kant registeren veel organisaties de bestaande afhankelijkheden ook niet als een financieel risico. Dat is opmerkelijk omdat de vendor lock-in kan leiden tot onverwachte gedwongen prijsstijgingen, hoge migratie kosten, kosten om de continuïteit te waarborgen van de leverancier en daarop regie te voeren, en de kosten van uitgestelde innovaties (omdat een leverancier daartoe geen incentive meer heeft). In het geval van een proprietary closed source systeem met leverancierseigen koppelingen en gesloten standaarden worden de kosten voor de overstap naar een alternatief weliswaar veroorzaakt door de huidige dominante leverancier, maar vrijwel altijd toegerekend aan (de leverancier van) het alternatief. Daarmee ontstaat een vertekend beeld ten gunste van de huidige dominante leverancier. De juiste vraag bij een break-out is dus niet alleen hoeveel het kost om over te stappen, maar ook hoeveel het gaat kosten om de bestaande afhankelijkheid nog tien jaar in stand te houden.

Het is dus voor een break-out noodzakelijk om de afhankelijkheid zichtbaar te maken als financieel risico, een transitiebudget te reserveren en bestuurlijk te accepteren dat kosten en baten in verschillende jaren zullen vallen.

Aanvullende kosten waar rekening mee moet worden gehouden dat is de tijdelijke terugval in productiviteit, en extra investeringen in kennis. Deze kosten doen zich weliswaar voor bij vrijwel elke migratie, maar in het geval van een break-out wordt het nog wel eens uitvergroot en oneigenlijk gebruikt als argument om toch gebruik te blijven maken van het bestaande systeem. De terugval in productiviteit ontstaat omdat gebruikers moeten wennen, werkprocessen moeten veranderen, en niet alles in het alternatieve systeem direct optimaal zal werken. De investeringen in kennis zijn nodig omdat de organisatie jarenlang afhankelijk is geweest van de dominante leverancier, en daardoor ook eigen kennis niet meer in huis heeft. Gedacht kan worden aan investeringen in eigen technische expertise, architectuurn kennis, contractmanagement, en leveranciersmanagement.

2.10 Break out: Juridische mogelijkheden

Het doorbreken van een vendor lock-in vindt in de praktijk vaak plaats binnen de kaders van bestaande contractuele relaties. Het zal niet verbazen dat veel ICT contracten zo zijn opgesteld dat de positie van de dominante leverancier erg sterk is, en er weinig mogelijkheden bestaan om de afhankelijkheid te doorbreken of te verminderen. Vooral wanneer er gecontracteerd is onder de algemene voorwaarden van de ICT leverancier. Er zal dus gestart moeten worden met een zorgvuldige juridische analyse van de oorspronkelijke aanbestedingsstukken, de daarna gesloten contracten, en tot slot de op het contract van toepassing zijnde relevante wetgeving.

Vaak blijken er in de oorspronkelijke aanbestedingsstukken bepaalde vereisten opgenomen die kunnen helpen om de lock-in te verminderen. In het volgende hoofdstuk zullen enige van deze vereisten aan bod komen en verder uitgewerkt worden. Zo is er in gemiddeld de helft van de ICT aanbestedingen wel een rechtstreekse verwijzing opgenomen naar de verplicht toe te passen open standaarden van het Forum Standaardisatie. Of we zien bijvoorbeeld een verwijzing naar de ICT-kwaliteitsnormen van

de VNG, die concreet eist van de leveranciers dat de te leveren producten of diensten moeten voldoen aan de wettelijke standaarden, de open standaarden van de 'Pas toe of leg uit' lijst en de landelijke gemeentelijke standaarden. Bij gunning blijkt dan vaak dat de leverancier weliswaar akkoord is gegaan met de gestelde eis, maar daar wordt dan na de gunning bijna nooit meer op gecontroleerd. Ook kan gedacht worden aan een eis om mee te werken aan een exitplan, of in het geval van maatwerk mee te werken aan de overdracht van auteursrechten, maar waarbij dit na de gunning niet meer door juristen of contractmanagers opgevolgd is. Het heeft daarbij vaak ook geen expliciete plaats gekregen in de na gunning gesloten overeenkomst. Dat is op zich ook geen probleem, omdat er vaak in de aanbestedingsdocumenten is opgenomen dat de inschrijving van de leverancier, het Programma van Eisen, de aanbestedingsleidraad en eventuele andere stukken onderdeel worden van de overeenkomst.

Ook zijn er in de overeenkomsten zelf vaak bepaalde rangordes opgenomen, waarbij bijvoorbeeld ook de inschrijving, de nota van inlichtingen of de aanbestedingsleidraad als onderdeel is opgenomen. Tot slot kunnen de aanbestedingsstukken ook nog een rol spelen bij de uitleg van de overeenkomst, zeker indien bepaalde eisen niet terug zijn gekomen in de letterlijke tekst van de overeenkomst.

Met betrekking tot het contract kan ook nog onderzocht worden of er ruimte aanwezig is voor wijzigingen. Binnen de kaders van het aanbestedingsrecht zijn wijzigingen van een bestaande overeenkomst toegestaan, mits de wijziging niet dusdanig groot is dat er sprake is van een wezenlijke wijziging van de aanbestede opdracht. Of sprake is van een dergelijke wijziging hangt af van de aard en omvang van de aanpassing, maar doorgaans hebben andere leveranciers dan de huidige dominante leverancier geen problemen met wijzigingen ten opzichte van de aanbestede opdracht indien dat voor hen weer nieuwe commerciële kansen kan gaan bieden na een break-out.

Soms is er ook sprake van wijzigingen in wetgeving of van nieuwe rechtspraak waardoor een contract kan worden opgebroken.

Ook beëindigingsmogelijkheden verdienen aandacht. Contracten bevatten vaak eigen bepalingen over opzegging, ontbinding of beëindiging bij

bepaalde omstandigheden. Denk bijvoorbeeld aan de ‘change of control’ bepaling waarin men aangeeft dat een afnemer tussentijds mag opzeggen indien de leverancier wordt overgenomen of fuseert met een andere partij. Verderop in 5.3 zal dit verder uitgewerkt worden.

Mocht er onverhoopt geen looptijd of opzegmogelijkheid zijn afgesproken, dan geldt als praktijkregel dat opzegging wegens een zwaarwegende grond altijd mogelijk moet zijn, mits een redelijke opzegtermijn in acht is genomen. Daarbij rekent men doorgaans met een maand voor ieder jaar dat de overeenkomst heeft gelopen.

Naast de meer formele juridische mogelijkheden en beperkingen kan ook gebruik worden gemaakt van de dynamiek achter de contractuele relatie. Dominante leveranciers hebben er in veel gevallen toch ook wel een zeker belang bij om reputatieschade te voorkomen. Dit gegeven kan daarom ruimte bieden voor heronderhandeling of aanpassing van de bestaande afspraken, bijvoorbeeld met betrekking tot gewenste dataportabiliteit, toegang tot interfaces of ondersteuning bij migratie. Een concreet en actueel voorbeeld daarvan is de situatie rond het bedrijf Archiefweb, die hoge kosten in rekening bracht aan overheidsklanten die hun webarchieven wilden overzetten naar een ander alternatief systeem, maar die bij het sluiten van het oorspronkelijke contract hadden nagelaten om direct een exitplan met Archiefweb overeen te komen.⁴ Hoewel het opnieuw overgaan tot onderhandelingen dus juridisch niet altijd afdwingbaar is, kan het beperken van mogelijke reputatieschade in de praktijk toch bijdragen aan het openbreken van een bestaand contract.

Tot slot kan ook nog worden gekeken naar wetgeving waar bepaalde rechten uit afgeleid kunnen worden, zoals de auteurswet, de Algemene Verordening Gegevensbescherming (AVG) en de Data Act.

De artikelen 45l en 45m van de Auteurswet geven bijvoorbeeld expliciet het recht om software te reverse engineeren of te decompileren. Bij reverse engineering is er sprake van het onderzoeken van de werking van de software, en bij het decompileren wordt getracht om de software terug te vertalen naar de broncodevorm. Deze handelingen zijn volgens de

⁴ <https://www.binnenlandsbestuur.nl/digitaal/archiefweb-maakt-plan-van-aanpak-voor-ontevreden-gemeenten>

Auteurswet toegestaan indien dat nodig is om interoperabiliteit tot stand te brengen met de producten of diensten van andere leveranciers.

In artikel 20 van de AVG wordt onder bepaalde omstandigheden aan betrokkenen, dat wil zeggen de natuurlijke personen wiens persoonsgegevens verwerkt worden, het recht gegeven op dataportabiliteit van hun eigen gegevens. Een leverancier zal in veel gevallen een verwerker zijn van die gegevens, en is op basis van art. 28 lid 3 sub e AVG verplicht om bijstand te verlenen aan de aanbesteder, die doorgaans heeft te gelden als de verwerkingsverantwoordelijke. Dat betekent in de praktijk dat als de verwerkingsverantwoordelijke gegevens nodig heeft om een dergelijk verzoek van een betrokkene af te handelen, de verwerker daaraan moet meewerken door het aanleveren van die gegevens in een gestructureerde, gangbare en machinaal leesbare vorm.

Ter afsluiting noem ik de Dataverordening, ook wel bekend als de Data Act. Die bevat twee verschillende regimes die in het kader van een break-out relevant zijn:

Het eerste regime geeft rechten voor gebruikers van zogeheten ‘verbonden producten’, slimme fysieke apparaten die data verzamelen, genereren, of digitaal kunnen verzenden zoals IoT-apparaten en sensoren, op toegang tot de door het product gegenereerde gegevens. De gebruiker kan dus verlangen dat die gegevens aan een derde partij beschikbaar worden gesteld waardoor het eenvoudiger kan worden om van dienstverlener te wisselen zonder de achterliggende data kwijt te raken. Dit regime lijkt enigszins op het hiervoor besproken artikel 20 AVG, maar is aanzienlijk breder omdat het niet beperkt is tot persoonsgegevens.

Vanuit het perspectief van een break-out is echter vooral het tweede regime veelbelovend. De artikelen 23 tot en met 31 van de Data Act verplichten de aanbieders van cloud-, SaaS-, PaaS- en IaaS-diensten om overstappen mogelijk te maken en eventuele obstakels weg te nemen.

De afnemer krijgt daarmee in feite een wettelijk recht om over te stappen naar een andere aanbieder of naar een eigen on-premise omgeving, en om meerdere aanbieders parallel te gebruiken (multi-cloud). Zo bepaalt artikel 23 expliciet dat de aanbieders geen technische, commerciële, contractuele

of organisatorische barrières mogen opwerpen die een overstap zouden belemmeren. Contracten moeten volgens artikel 25 expliciet een duidelijke overstapprocedure bevatten, inclusief een maximale opzegtermijn van twee maanden, het verlenen van redelijke ondersteuning in het overstapproces, inclusief het verstrekken van alle relevante informatie en het betrachten van de nodige zorgvuldigheid om de bedrijfscontinuïteit van de afnemer in stand te kunnen houden, het aanbieden van exportmogelijkheden waardoor exporteerbare data en digitale activa kunnen worden overgedragen, en verwijdering van de achterblijvende gegevens na een succesvolle voltooiing van het overstapproces. Al deze vereisten zijn tevens van toepassing op bestaande contracten.

Voor IaaS diensten is specifiek bepaald dat de aanbieders redelijke maatregelen moeten nemen om ervoor te zorgen dat de klant bij de nieuwe aanbieder een vergelijkbaar functioneel niveau kan bereiken. Daarbij moeten documentatie, hulpmiddelen en technische ondersteuning beschikbaar worden gesteld. Voor andere soorten diensten, zoals PaaS of SaaS, is bepaald dat er kosteloos open interfaces (API's) beschikbaar moeten worden gesteld om de migratie te vergemakkelijken.

Een van de meest ingrijpende onderdelen van de Data Act is het verbod op overstapkosten bij clouddiensten. De Data Act schrijft een geleidelijke afschaffing van switching charges voor. In de eindsituatie, vanaf 12 januari 2027, mogen de meeste leveranciers geen kosten meer rekenen voor het overstappen zelf of voor het exporteren van gegevens ten behoeve van die overstap. Hiervan uitgezonderd zijn systemen die volledig als maatwerk zijn ontwikkeld voor een individuele afnemer.

De Data Act vermindert dus vooral de technische, financiële en juridische barrières, maar lost niet alle lock-in problemen op. Zij verplicht bijvoorbeeld niet dat SaaS-applicaties volledig interoperabel zijn, noch dat broncode wordt vrijgegeven. Organisatorische afhankelijkheden, maatwerkconfiguraties, kennisconcentratie en applicatie specifieke functionaliteit kunnen dus nog steeds tot substantiële lock-in leiden. De Data Act alleen is dus ook geen vervanging voor goede aanbestedingseisen op het gebied van interoperabiliteit en leveranciersafhankelijkheid.

2.11 Break out: Juridische verplichtingen

Het centrale uitgangspunt van het Europese aanbestedingsrecht wordt gevormd door de beginselen van gelijke behandeling, non-discriminatie, transparantie en proportionaliteit. Deze beginselen zijn gericht op het waarborgen van eerlijke concurrentie en gelijke toegang tot overheidsopdrachten voor marktpartijen. Vrije concurrentie is noodzakelijk om daadwerkelijk concurrerende aanbiedingen te kunnen krijgen, en daarmee ‘value for money’. Alleen dan komt een optimale prijs-kwaliteit verhouding voor de overheid tot stand. De specificaties dienen in dat licht zodanig te worden geformuleerd dat zij de mededinging niet onnodig beperken. Volgens art. 1.10a Aanbestedingswet is de mededinging kunstmatig beperkt indien de opdracht is ontworpen met het doel om bepaalde ondernemers ten onrechte te bevoordelen of te benadelen. Door op de voorgeschreven wijze het aanbestedingsrecht te hanteren, kan dit bijdragen aan een break-out.

2.11.1 Licenties van specifieke leveranciers

Bij de inkoop van ICT-producten en ICT-diensten hanteert de Nederlandse overheid al sinds 2007 expliciet het uitgangspunt dat er bij inkoopprocedures geen onderscheid gemaakt mag worden tussen leveranciers die hun software willen leveren onder een open source licentie, en leveranciers die vast willen blijven houden aan meer traditionele licentievormen. Dat laatste betreft dan vaak licenties voor closed source software die enkel tegen betaling via tussenpersonen, zoals brokers of resellers, verkrijgbaar zijn. In de praktijk is te zien dat er door allerlei ondoordachte keuzes juist toch de nodige voorkeuren worden gegeven aan leveranciers in die laatste categorie, waardoor leveranciers die mogelijk met een open source licentie willen aanbieden al op voorhand worden buitengesloten.

Dat kan heel concreet bijvoorbeeld gaan om aanbestedingen waarbij er rechtstreeks gevraagd wordt om een bij naam genoemd product, of een licentie van dat product. Ook kan het gaan om raamovereenkomsten met resellers of brokers van de bij naam genoemde producten of diensten. Hoewel het hanteren van dergelijke inkoopmethodieken bijna volledig lijkt te zijn ingeburgerd, is het klip en klaar dat daarmee in strijd met het

aanbestedingsrecht bepaalde ondernemers worden bevoordeeld, en andere benadeeld. Door bijvoorbeeld te vragen om licenties Microsoft Office 365, kan immers alleen Microsoft en het door Microsoft opgetuigde partnernetwerk van resellers een inschrijving doen. Alle andere leveranciers van office software worden bij voorbaat uitgesloten. In plaats van het uitvragen van Microsoft licenties had de aanbesteding door middel van prestatie eisen en functionele eisen moeten aangeven dat de organisatie op zoek is naar een officepakket. Het noemen van merknamen is slechts bij uitzondering toegestaan indien op die wijze een begrijpelijke beschrijving niet mogelijk is.⁵ In zo'n uitzonderlijk geval dient men bij de gevraagde merknaam gebruik te maken van de toevoeging "of gelijkwaardig". Het gebruik van de toevoeging heeft als consequentie dat de aanbestedende dienst bij de uiteindelijke beoordeling van de offertes de gelijkwaardigheid ook daadwerkelijk moet controleren en beargumenteren. Uit het verplichte gebruik van die toevoeging kan overigens ook worden afgeleid dat er met het aanbestedingsrecht juist concurrentie tussen merken (intra-brand) wordt beoogd, in plaats van concurrentie binnen één merk (inter-brand) zoals bij software resellers het geval is.

Die toevoeging "of gelijkwaardig" hoeft natuurlijk niet gebruikt te worden indien het merk in het aanbestedingsdocument gebruikt wordt om de huidige architectuur te beschrijven, of indien men van het nieuwe product compatibiliteit eist met software X van leverancier Y. Dat laatste geeft dan weer een verboden voorkeur indien de voor compatibiliteit vereiste technische specificaties niet publiekelijk beschikbaar zijn, en zonder kosten bruikbaar zijn.⁶

Naast het expliciet en zonder rechtvaardiging vragen om bepaalde (licenties van) producten zijn er ook allerlei andere voorbeelden waarbij er sprake is van een functionele omschrijving, maar er toch sprake is van een ongelijke behandeling. Denk aan een functioneel omschreven aanbesteding voor een tekstverwerkingspakket, waarbij er dan ergens een eis is opgenomen dat de medewerkers van de beoogde leverancier in het bezit moeten zijn van bepaalde certificaten van Microsoft. Of een aanbesteding voor een functioneel omschreven videoconferencing tool,

⁵ HvJ EG 24 januari 1995, C-359/93, ECLI:EU:C:1995:14 (Commissie/Nederland), ook bekend als het Unix arrest.

⁶ GvEA EG 12 maart 2008, T-345/03.

waarbij men vervolgens wel eist dat de leverancier in staat is om ook heel specifieke opleidingen en trainingen te geven op het gebied van Cisco. Niet geheel toevallig is Cisco vervolgens de winnaar geworden met haar Webex product.

2.11.2 Uitbreidingen van licenties

In sommige gevallen is het zo dat een organisatie al eerder licenties heeft verworven voor bepaalde software, waarna zich een situatie voordoet dat er extra licenties nodig blijken te zijn. Dan is het uiteraard niet wenselijk dat de nieuwe licenties gebruiksrechten geven op een ander alternatief product. Temeer als aannemelijk is dat de technische eigenschappen van het andere product niet verenigbaar zijn met het al in gebruik zijnde product of als zich dan bij het gebruik of onderhoud onevenredige technische moeilijkheden kunnen voordoen. Mede vanwege de inkoop van softwarelicenties is in art. 2.33 Aanbestedingswet een procedure opgenomen voor beperkte uitbreidingen van eerder rechtmatig verworven licenties.⁷ Die opdracht mag daarbij rechtstreeks gegund worden aan de oorspronkelijke leverancier. Wel is het zo dat de maximale looptijd 3 jaar is, en dat de levering ondergeschikt moet zijn aan de oorspronkelijke levering. Ook het op deze wijze overgaan naar een nieuwe versie van een software programma voldoet hier niet aan, omdat er dan al snel sprake kan zijn van een wezenlijke wijziging van de oorspronkelijke aanbesteding.

Voor herhalende contracten op het gebied van support en onderhoud biedt art 2.36 Aanbestedingswet uitkomst. Daarbij mag er gedurende een periode van drie jaar na de eerste opdracht rechtstreeks gegund worden aan de oorspronkelijke dienstverlener. De voorwaarde is wel dat de mogelijk toekomstige herhaling al bekend is gemaakt tijdens de aanbesteding van de oorspronkelijke opdracht.

2.11.3 Technische redenen

Er zijn dus in het aanbestedingsrecht concrete mogelijkheden aanwezig om een voorkeur aan te geven voor specifieke producten en diensten die al in gebruik zijn. Omdat organisaties echter vaak niet voldoen aan de daarvoor gestelde voorwaarden, kiest men er regelmatig voor om nieuwe en herhalingsopdrachten rechtstreeks aan de zittende leverancier te gunnen

⁷ Dit volgt uit de toelichting van het met deze bepaling corresponderende artikel XV lid 1 d GPA dat aangeeft dat ook softwarelicenties hieronder vallen.

met een beroep op de in artikel 2.32 lid 1 Aanbestedingswet genoemde uitzonderingsgrond “technische redenen”, of de uitzonderingsgrond “redenen van bescherming van alleenrechten”. Met de term ‘alleenrechten’ gaat het om rechten van intellectueel eigendom, zoals het auteursrecht en het octrooirecht. Een beroep op deze uitzondering is mogelijk indien het product of de dienst vanwege technische redenen of een intellectueel eigendomsrecht enkel geleverd kan worden door één specifieke leverancier, en er voor dat product of dienst geen redelijk alternatief of vervanging bestaat. Het is daarvoor niet voldoende dat één leverancier de voorkeur geniet of dat een overstap complex of kostbaar is. Beslissend is of andere partijen in staat zijn de opdracht uit te voeren. Het Europese Hof van Justitie heeft in het verleden al aangegeven dat aan dit vereiste enkel kan worden voldaan indien er op de markt geen enkele concurrentie bestaat.⁸

Een dergelijk beroep op exclusiviteit dient dus met grote terughoudendheid te worden toegepast. Uit recente rechtspraak van het Hof van Justitie volgt bovendien dat een aanbestedende dienst zich niet op technische exclusiviteit kan beroepen wanneer hij zelf de omstandigheden heeft gecreëerd die tot deze afhankelijkheid hebben geleid.⁹ De aanbestedende dienst zal moeten kunnen aantonen dat bij de oorspronkelijke verwerving daadwerkelijk maatregelen zijn genomen om vendor lock-in te voorkomen en dat er nadien geen redelijke economische mogelijkheden bestonden om de ontstane exclusiviteit te doorbreken. Met andere woorden: wie de lock-in zelf heeft laten ontstaan, en deze daarna heeft laten voortduren, kan zich in beginsel niet op diezelfde lock-in beroepen om bij een vervolgoedracht verdere concurrentie uit te sluiten.

2.12 Break out: Organisatorische mogelijkheden

Een noodzakelijke conditie voor een succesvolle break-out is de aanwezigheid of in ieder geval de ontwikkeling van een alternatief. Zonder zicht op een beschikbaar alternatief zal de organisatie geen echte noodzaak voelen om afscheid te nemen van het product van de dominante leverancier. Overigens moet opgemerkt worden dat de enkele opkomst van een alternatief, zelfs als dat technisch superieur is ten opzichte van

⁸ HvJ EG 3 mei 1994, C-328/92, ECLI:EU:C:1994:178 (Commissie/Spanje), rechtsoverweging 17.

⁹ HvJ EU 9 januari 2025, C-578/23, ECLI:EU:C:2025:4

het bestaande product, ook niet dat gevoel van noodzaak zal laten ontstaan. Daartoe dient er in de meeste gevallen sprake te zijn van een geplande of toevallige interventie van buiten af. Bijvoorbeeld vanwege politieke druk, of vanwege andere organisaties. De bereidheid van een organisatie om over te stappen is namelijk vele malen groter indien er ook andere organisaties zijn die willen overstappen naar het alternatief. In een dergelijk geval kunnen de netwerk- en coördinatie effecten, die meestal enkel ten gunste werken van de dominante leverancier, omgedraaid worden ten gunste van het alternatief.

Binnen een organisatie moet verder inzichtelijk worden gemaakt op welke wijze de keuze voor de huidige dominante leverancier tot stand is gekomen, wie daar bij betrokken is geweest en welke voorkeuren de aanleiding zijn geweest voor de eerdere besluitvorming. Dit omdat deze eerdere keuzes hebben bijgedragen aan een verdieping van de lock-in, en het werken aan een break-out bij sommige personen al dan niet terecht kan overkomen als een diskwalificatie van hun eerdere besluiten. Daardoor ontstaat een risico dat het alternatief geen eerlijke kans krijgt, of dat er juist een lobby ontstaat ten gunste van het huidige product. Het is dus noodzakelijk dat dergelijke personen ook de nut en noodzaak onderschrijven van een break-out, en met een open blik aan boord zijn bij het verkennen van alternatieven. Belangrijk te onthouden is dat een alternatief niet altijd dezelfde functionaliteit hoeft te hebben, maar dat het juist op andere gebieden zoals kosten of handelingsvrijheid kan excelleren. Er moet onder beslissers een gedeeld vertrouwen ontstaan dat het alternatief voordelen gaat opleveren zodra de markt rondom dat alternatief volwassen is geworden.

In veel organisaties is tegenwoordig ook een Open Source Program Office, ook wel een OSPO genoemd, ingericht. Een OSPO dient op bestuurlijk niveau te zorgen voor voldoende aandacht en middelen voor de overstap naar open source alternatieven, en biedt op uitvoerend niveau praktische hulp en ondersteuning. Ook het organiseren van cursussen of trainingen valt onder het takenpakket. Om het werken met open source software mogelijk te maken zet een OSPO intern ook in op het wegnemen van mogelijke barrières en het opzetten van een ecosysteem en een inkoopstructuur waarbij leveranciers van open source producten een eerlijke kans krijgen ten opzichte van de dominante leverancier.

2.13 Eerst volledig naar Microsoft?

In de praktijk wordt soms betoogd dat het wenselijk is om eerst bestaande, versnipperde ICT-oplossingen te consolideren binnen één geïntegreerd ecosysteem van een enkele leverancier, met het oog op een latere migratie naar een meer open en flexibele situatie. Deze redenering verdient echter een zeer kritische beschouwing. Het concentreren van voorheen elders af te nemen systemen en data bij één al dominante leverancier leidt in de praktijk veelal juist tot een versterking van de bestaande afhankelijkheden. Dit omdat de al bestaande technische, financiële, juridische en organisatorische barrières zich verder zullen verbreden. Er ontstaan dan nieuwe integraties, nieuwe werkprocessen, nieuwe opleidingen en nieuwe contracten waardoor deze tussenstap vaak ook het eindstation blijkt te zijn. De altijd optimistisch veronderstelde vervolgstap, het losmaken van deze geconsolideerde omgeving, blijkt vervolgens complex, kostbaar en risicovol, waardoor deze in veel gevallen niet of slechts gedeeltelijk wordt gerealiseerd. De strategie “eerst volledig naar Microsoft, en daarna weer weg” komt daarom regelmatig langs als beleidsvoornemen, maar komt relatief weinig voorbij als succesvol afgerond traject.

Bovendien is een dergelijke tussenstap meestal ook niet noodzakelijk. In veel gevallen is het gewoon mogelijk om rechtstreeks te migreren naar oplossingen die beter aansluiten bij de uitgangspunten van interoperabiliteit en leveranciersafhankelijkheid. Ook kan er bijvoorbeeld geconsolideerd worden op basis van open standaarden, gestandaardiseerde API's, gemeenschappelijke gegevensmodellen, open source middleware en containerisatie. Het bewust vergroten van afhankelijkheid als tussenstap naar meer autonomie is daarmee niet alleen risicovol, maar ook conceptueel moeilijk te rechtvaardigen.

2.14 Gefaseerde exit-strategie

De mogelijkheid om tot een break-out te komen en over te kunnen stappen naar alternatieve oplossingen, vormt een essentiële voorwaarde waardoor het mogelijk gaat worden om voortaan leveranciersafhankelijk te gaan inkopen. In de praktijk blijkt echter dat een break-out zelden in één keer kan worden gerealiseerd. Het

vereist daarom een gefaseerde exit-strategie, waarin de verschillende afhankelijkheden planmatig en stapsgewijs worden afgebouwd.

Een belangrijk onderdeel van een dergelijke strategie is het stellen van prioriteiten. Niet alle afhankelijkheden zijn even kritisch of even moeilijk te doorbreken. Door inzicht te verkrijgen in welke afhankelijkheden de grootste risico's vormen, kan vervolgens ook worden bepaald waar interventies het meest effectief zullen zijn.

De effectiviteit van een exit-strategie is sterk afhankelijk van de samenhang tussen technische, juridische en organisatorische maatregelen. Technische break-out strategieën, zoals besproken in paragraaf 2.8, dienen te worden ondersteund door contractuele mogelijkheden tot beëindiging en wijziging, zoals behandeld in paragraaf 2.10. Zonder deze samenhang bestaat het risico dat migratie technisch mogelijk is, maar juridisch of organisatorisch wordt belemmerd. Daarnaast is er coördinatie nodig tussen de verschillende onderdelen van de organisatie en tussen betrokken disciplines. Zonder duidelijke sturing en financiering bestaat het risico dat initiatieven versnipperd raken of dat afhankelijkheden in stand blijven door gebrek aan besluitvorming.

Het uitvoeren van een gefaseerde exit strategie moet ook niet worden gezien als iets wat slechts tijdelijk is. Het verminderen en het voorkomen van afhankelijkheden blijft namelijk de voortdurende aandacht opeisen, omdat er vooral in grote organisaties ondanks de goede voornemens nog steeds nieuwe systemen zullen worden ingekocht die onbedoeld weer extra afhankelijkheden kunnen introduceren.

3. Leveranciersonafhankelijkheid als ontwerp en contracteringsprincipe

3.1 Inleiding leveranciersonafhankelijkheid

Het vorige hoofdstuk liet zien hoe vendor lock-in ontstaat en waarom overstappen naar alternatieven via een vendor break-out vaak moeilijk is. Dit hoofdstuk richt zich op de vraag hoe overheidsorganisaties zulke afhankelijkheden kunnen voorkomen bij het ontwerpen, aanbesteden en contracteren van ICT.

Leveranciersonafhankelijkheid betekent niet dat de overheid zonder leveranciers moet werken. Het betekent dat samenwerking met leveranciers zodanig wordt ingericht dat toekomstige keuzevrijheid behouden blijft. Daarvoor moet leveranciersonafhankelijkheid niet als beleidswens, maar als ontwerp- en contracteringsprincipe worden behandeld. Zij moet terugkomen in architectuurkeuzes, technische specificaties, aanbestedingseisen, contractuele verplichtingen en contractmanagement. Dit hoofdstuk werkt de daarvoor noodzakelijke voorwaarden uit. Eerst komen interoperabiliteit, dataportabiliteit en open standaarden aan bod. Daarna volgen exit, migratie, documentatie, transparantie en intellectuele-eigendomsrechten. Tot slot wordt besproken hoe open source software kan bijdragen aan leveranciersonafhankelijkheid, hergebruik en doorontwikkeling van publieke ICT.

3.2 Interoperabiliteit als uitgangspunt

Interoperabiliteit verwijst naar het vermogen van (informatie)systemen om gegevens en informatie elektronisch uit te wisselen, zowel binnen als tussen organisaties.¹⁰ Ten onrechte wordt nog wel eens gedacht dat interoperabiliteit niet relevant is voor de uitwisseling die enkel plaats

¹⁰ Kamerstukken II 2007/2008, 26643, nr. 108. De Nederlandse overheid volgt met deze specifieke definitie onder andere het ISO, en kiest dus niet voor sommige andere definities die zich beperken tot organisatie overstijgende gegevensuitwisseling.

heeft ‘binnen’ een organisatie. Dat is een misvatting. Interoperabiliteit vereist een open-einde-aanpak omdat het ook de samenwerking mogelijk moet maken tussen nieuwe en onvoorziene systemen. Het is bovendien zeer goed mogelijk dat er in de toekomst vanuit een andere organisatie koppelingen nodig zullen blijken te zijn met nu nog enkel interne systemen. Daarnaast is het binnen de overheid ook goed denkbaar dat organisatieonderdelen volledig verhuizen naar een nieuwe moederorganisatie.

Ook dan moeten soms systemen, gegevens en informatie mee verhuizen en gekoppeld kunnen worden aan de systemen van de ontvangende organisatie.

Wanneer systemen niet zijn ontworpen om gegevens op een gestandaardiseerde wijze met elkaar uit te wisselen, of wanneer de toegang tot interfaces en data wordt beperkt, dan wordt het vervangen of het combineren van systemen bemoeilijkt. Om deze reden dient interoperabiliteit vanaf het begin expliciet te worden meegenomen in het ontwerp en de aanbesteding van ICT-producten en diensten. Dit vergt dat eisen ten aanzien van gegevensuitwisseling, open standaarden en toegang tot interfaces niet worden beschouwd als aanvullende wensen, maar als kernvereisten.

Hierbij zijn vijf soorten van interoperabiliteit te onderscheiden:

- **Technische interoperabiliteit:** Dit betreft de infrastructuur en protocollen voor datatransmissie. Kunnen systemen fysiek en digitaal verbinding met elkaar maken (bijv. via TCP/IP)?
- **Syntactische interoperabiliteit:** Dit gaat over het formaat van de data. Als Systeem A gegevens stuurt in XML-formaat, kan Systeem B dat dan verwerken? Er wordt afgesproken hoe de data eruitziet (grammatica), maar niet wat het betekent.
- **Semantische interoperabiliteit:** Begrijpen beide systemen de betekenis van de data op dezelfde manier? Als Systeem A een veld ‘Klant’ heeft en Systeem B een veld ‘Opdrachtgever’, betekenen die dan juridisch hetzelfde? Ook kan hierbij gedacht worden aan dezelfde woorden die meerdere betekenissen kunnen hebben. Zonder semantische standaarden (zoals datamodellen, gegevenswoordenboeken of ontologieën) leidt uitwisseling van informatie tot corruptie van de betekenis.

- **Organisatorische interoperabiliteit:** Hierbij gaat het erom dat bedrijfsprocessen en de bijbehorende gegevensuitwisseling met behulp van algemeen aanvaarde modelleringstechnieken gedocumenteerd en geïntegreerd of afgestemd moeten worden.
- **Juridische interoperabiliteit:** Hierbij gaat het om de afstemming van juridische kaders op de beoogde gegevensuitwisseling. Zijn er bijvoorbeeld geografische of sectorale restricties voor het gebruik en de opslag van de data? Mogen de data überhaupt wel uitgewisseld worden, bijvoorbeeld vanwege de Algemene Verordening Gegevensbescherming (AVG)? En zijn de eventuele licentievoorwaarden wel onderling compatibel?

In de aanbestedingsfase kunnen eisen worden gesteld op het gebied van interoperabiliteit. Het contract bepaalt vervolgens of deze interoperabiliteit daadwerkelijk kan worden gerealiseerd en behouden gedurende de looptijd van de overeenkomst.

Voor contractuele definities is het daarom cruciaal om te weten welke bovengenoemde soort interoperabiliteit er van toepassing is. In inkoopprocedures en in contracten moet daarom niet simpelweg geëist worden dat een oplossing ‘interoperabel’ is, maar moet bijvoorbeeld zijn opgenomen dat deze ‘semantische interoperabiliteit ondersteunt op basis van standaard [X].’

Een ander aandachtspunt in dit verband is de toegang tot interfaces, in het bijzonder Application Programming Interfaces (API's). API's vormen de technische toegangspunten waarmee systemen gegevens uitwisselen en functionaliteiten met elkaar verbinden. Wanneer toegang tot deze interfaces afhankelijk is van de medewerking van de leverancier, wordt het moeilijk om systemen te integreren met alternatieve oplossingen, of om onderdelen van het ICT-landschap te vervangen. Het contract dient daarom expliciet te voorzien in rechten op toegang tot en gebruik van relevante interfaces. Dit omvat in dat geval niet alleen de technische toegang, maar bijvoorbeeld ook de beschikbaarheid van de volledige en actuele documentatie.

Daarnaast is van belang dat die interfaces zonder eenzijdige voorwaarden gebruikt kunnen worden en dat die voorwaarden stabiel en voorspelbaar zijn. Indien leveranciers eenzijdig wijzigingen kunnen doorvoeren in interfaces of de toegang daartoe kunnen beperken, dan kan dit de interoperabiliteit ondermijnen en nieuwe afhankelijkheden creëren. Contractuele afspraken dienen daarom ook betrekking te hebben op de continuïteit en de betrouwbaarheid van te gebruiken interfaces.

3.3 Dataportabiliteit en controle over data

Waar interoperabiliteit zich richt op de onderlinge uitwisselbaarheid van gegevens tussen meerdere systemen, betreft portabiliteit de mogelijkheid om data en systemen daadwerkelijk tussen verschillende aanbieders te verplaatsen, te hergebruiken en onder eigen regie te beheren. In de context van de cloud gaat het daarbij niet om IaaS (omdat er doorgaans geen sprake is van de verplaatsing van infrastructuur) maar enkel om PaaS en SaaS.

Die portabiliteit valt op haar beurt uiteen in systeemportabiliteit en dataportabiliteit.

Bij systeemportabiliteit gaat het om het kunnen verplaatsen van applicaties van het ene platform naar het andere. Er is inmiddels de nodige opensource-software beschikbaar die een dergelijke verplaatsing mogelijk kan maken. Een bekend voorbeeld is Kubernetes, waarbij een applicatie in zogeheten containers draait (meestal Docker), en je deze applicaties zowel lokaal, alsook in verschillende cloudomgevingen kunt draaien. Daarvoor is binnen de Nederlandse gemeenten de HAVEN standaard ontwikkeld. Door in aanbestedingen te eisen dat te leveren applicaties “HAVEN compliant” zijn, wordt afgedwongen dat de software in een container wordt geleverd die op elk HAVEN-platform kan draaien. Hierdoor wordt de gemeente onafhankelijk van de hosting partij.

Dataportabiliteit is het vermogen om gegevens van de ene IT-omgeving naar de andere te verplaatsen zonder dat de bruikbaarheid van die gegevens verloren gaat. Het is daarbij belangrijk om onderscheid te maken tussen dataportabiliteit en datamigratie. Bij het recht op dataportabiliteit gaat het om de mogelijkheid voor de gebruiker om zijn data te ontvangen

in een gestructureerd, gangbaar en machineleesbaar formaat, met als doel hergebruik van die data in een andere context of bij een andere dienstverlener. Dit veronderstelt niet alleen toegang tot de data zelf, maar ook tot de structuur, betekenis en samenhang daarvan.

Als het gaat om datamigratie, dan doelen we op het bredere, vaak eenmalige proces van het volledig overzetten van data en applicatielogica naar een nieuw systeem (de exit).

Zonder effectieve controle over data verliest een organisatie in de praktijk de mogelijkheid om systemen te vervangen of alternatieven te implementeren. Naarmate er meer gegevens binnen een systeem of platform worden opgeslagen en verwerkt, neemt ook de afhankelijkheid van dat systeem toe. Migratie wordt steeds complexer, niet alleen vanwege de omvang van de data, maar ook vanwege de samenhang met applicaties, processen en andere systemen. Zonder adequate waarborgen voor dataportabiliteit kan deze afhankelijkheid zich in de loop der tijd verdiepen.

Dataportabiliteit en toegang tot data dienen daarom in de contractfase expliciet en juridisch afdwingbaar te worden vastgelegd. Waar in de aanbestedingsfase eisen worden geformuleerd ten aanzien van dataportabiliteit, bepaalt het contract in hoeverre deze eisen daadwerkelijk kunnen worden geëffectueerd gedurende de looptijd van de overeenkomst en bij beëindiging daarvan.

Een belangrijk uitgangspunt daarbij is dat juridisch eigenaarschap van data niet zonder meer samenvalt met feitelijke controle. In veel ICT-relaties blijven data formeel toebehoren aan de afnemer, terwijl de leverancier de technische en operationele controle uitoefent over opslag, toegang en verwerking. Zonder nadere contractuele afspraken kan dit ertoe leiden dat de afnemer in de praktijk afhankelijk is van de leverancier voor toegang tot en gebruik van de eigen data.

Het contract dient daarom niet alleen te bevestigen dat de afnemer gerechtigd is tot de data, maar ook te bepalen op welke wijze deze data toegankelijk, overdraagbaar en herbruikbaar zijn. Dit omvat onder meer afspraken over formaten, interfaces, documentatie en ondersteuning bij migratie. Daarbij is van belang dat deze verplichtingen niet uitsluitend

gelden bij beëindiging van de overeenkomst, maar gedurende de gehele looptijd daarvan.

3.4 Open standaarden in aanbestedingen

Open standaarden vormen een essentieel instrument voor het bevorderen van interoperabiliteit, een toekomstbestendige gegevensopslag, en het voorkomen van leveranciersafhankelijkheid. Het gebruik van open standaarden maakt het mogelijk om de interoperabiliteit en portabiliteit van systemen, data en processen zodanig vorm te geven dat zij niet afhankelijk zijn van één specifieke leverancier, maar toegankelijk blijven voor meerdere partijen.

Hoewel de termen ‘standaard’, ‘specificatie’ en ‘norm’ in het dagelijks spraakgebruik onderling uitwisselbaar lijken, bestaat er in juridische zin een hiërarchisch en procedureel onderscheid.

Een standaard kan gezien worden als een regel, een richtlijn of een kenmerk dat een bepaald (beweerdelijk) doel dient en die een technische implementatie kan hebben. De term wordt zowel gebruikt in de betekenis van een bepaalde mate van uniformiteit, alsook om te verwijzen naar het specificatiedocument waarin deze regels, richtlijnen of kenmerken zijn beschreven. Volgens Verordening (EU) 1025/2012 is een technische ICT-specificatie een document dat de technische eisen beschrijft waaraan een product, proces of dienst moet voldoen. In de context van cloud-computing kan dit bijvoorbeeld gaan om koppelvlakdocumentatie die beschrijft hoe verschillende applicaties met elkaar kunnen communiceren, maar bijvoorbeeld ook om de REST-API Design Rules, die een uniforme manier voorschrijven van structuur en naamgeving voor de documentatie van de koppelingen.

Niet iedere standaard is echter ook een norm. Het onderscheid tussen een standaard en een norm heeft te maken met de opsteller van de standaard. Een norm is namelijk een standaard die afkomstig is van een erkende normalisatie-instelling, zoals ISO op mondiaal niveau, CEN, ETSI en CENELEC op Europees niveau of NEN op nationaal niveau. In het Engels noemt men een dergelijke norm een *formal standard*. Juridisch gezien biedt conformiteit aan een norm vaak een vermoeden van overeenstemming

met wettelijke eisen (bijvoorbeeld in het kader van de Algemene Verordening Gegevensbescherming of de NIS2-richtlijn). Het is bovendien bij een norm vaak mogelijk om je daartegen te laten certificeren.

In de IT-sector en cloudmarkt komen veel standaarden echter niet voort uit normalisatie-instellingen, maar uit consortia of samenwerkingsverbanden (zoals het W3C, IETF of OASIS). Bekende internetstandaarden zijn HTTPS en IPv6. Hoewel deze standaarden formeel dus geen ‘normen’ zijn, hebben ze vaak een zeer grote marktimpact.

Daarnaast bestaan er ook geharmoniseerde normen. Dat zijn Europese technische specificaties ontwikkeld door CEN, CENELEC en ETSI op verzoek van de Europese Commissie. Die specificaties vertalen een bestaande wettelijke eis naar meer concrete (technische) regels. Het opvolgen van zo’n specificatie zorgt voor een ‘vermoeden van overeenstemming’ met de na te leven wettelijke verplichting, waardoor de bewijslast af zal nemen.

Dus alle geharmoniseerde normen zijn te beschouwen als een norm, en alle normen zijn te beschouwen als een standaard. Maar het omgekeerde is dus niet waar: niet alle standaarden zijn ook normen, en niet alle normen zijn geharmoniseerde normen.

Een bijzondere categorie vormt de open standaard. In Nederland hanteert het Forum Standaardisatie daarvoor een strikte definitie. Een standaard is pas ‘open’ indien:

- er voldoende inspraakmogelijkheden zijn voor stakeholders tijdens de (door)ontwikkeling van de standaard;
- het feitelijke gebruik van de standaard niet onderworpen is aan een (octrooi)vergoeding of aan andere contractuele beperkingen;
- de benodigde documentatie zoals het specificatiedocument laagdrempelig beschikbaar is, dat wil zeggen gratis, of tegen een redelijke vergoeding.

Door deze voorwaarden kan voorkomen worden dat gebruikers afhankelijk zijn of worden van één specifieke partij voor het kunnen gebruiken van (software bevattende) een *proprietary* standaard. In contracten is de eis voor open standaarden daarom een van de maatregelen om vendor lock-in te kunnen voorkomen. Voor de overheid is dit onderscheid cruciaal:

conformiteit met een zogeheten *proprietary* standaard (zoals een specifieke API van een hyperscaler) kan de lock-in juist vergroten, terwijl open standaarden deze beogen te doorbreken.

Doordat meerdere leveranciers systemen kunnen ontwikkelen die dezelfde standaarden ondersteunen, ontstaat uitwisselbaarheid van componenten en wordt de afhankelijkheid van individuele aanbieders verminderd. Open standaarden maken het mogelijk om gegevens over te dragen, systemen te integreren en onderdelen te vervangen zonder dat daarbij fundamentele technische barrières optreden.

Open standaarden vormen bovendien de meest concrete invulling van interoperabiliteit als uitgangspunt. Waar interoperabiliteit een abstracte doelstelling kan blijven, operationaliseren open standaarden deze doelstelling in specifieke eisen ten aanzien van gegevensformaten, protocollen en interfaces. Het expliciet voorschrijven van open standaarden in aanbestedingen maakt interoperabiliteit toetsbaar en afdwingbaar, en voorkomt dat deze afhankelijk wordt van interpretatie of goodwill van leveranciers.

De vraag om open standaarden in aanbestedingen past ook binnen het juridische kader van het aanbestedingsrecht. Aanbestedende diensten zijn gehouden technische specificaties zodanig te formuleren dat gelijke toegang tot de opdracht wordt gewaarborgd en mededinging niet onnodig wordt beperkt. Het verwijzen naar open standaarden is daarbij toegestaan, omdat zij juist zijn ontworpen om door meerdere partijen te worden geïmplementeerd. Sterker nog, het voorschrijven van open standaarden kan ook bijdragen aan het realiseren van de doelstellingen van het aanbestedingsrecht.

Door te kiezen voor standaarden die vrij toegankelijk en breed implementeerbaar zijn, wordt de markttoegang voor verschillende leveranciers vergroot en wordt een gelijk speelveld bevorderd. Dit voorkomt dat aanbestedingen feitelijk worden toegeschreven naar specifieke technologieën of leveranciers.

Open standaarden dienen daarom niet te worden beschouwd als een optionele voorkeur, maar als een structureel uitgangspunt bij alle publieke

ICT-inkoop. Alleen door het systematisch toepassen van open standaarden kan worden gewaarborgd dat interoperabiliteit daadwerkelijk wordt gerealiseerd en dat afhankelijkheden van leveranciers worden beperkt.

3.5 Specifiek voorgeschreven standaarden

Waar in de voorgaande paragraaf de algemene uitvraag van open standaarden is besproken, ziet deze paragraaf op situaties waarin het gebruik van specifieke open standaarden expliciet wordt voorgeschreven. In dergelijke gevallen gaat het niet langer om de eis dat open standaarden moeten worden toegepast, maar tevens welke open standaarden concreet moeten worden gebruikt.

Binnen het aanbestedingsrecht geldt als uitgangspunt dat technische specificaties zodanig moeten worden geformuleerd dat gelijke toegang voor marktpartijen wordt gewaarborgd. Dit brengt doorgaans met zich dat bij verwijzing naar specifieke standaarden ook “of gelijkwaardig” moet worden toegestaan. Indien het gebruik van specifieke standaarden echter voortvloeit uit wettelijke verplichtingen of uit beleidskaders met een bindend karakter, dan kan volgens artikel 60 lid 3 van de Aanbestedingsrichtlijn de ruimte voor het accepteren van gelijkwaardige alternatieven worden beperkt of geheel ontbreken.¹¹ In Nederland is het uitgangspunt van het Forum Standaardisatie dat enkel open standaarden kunnen worden aangewezen als verplichte standaard. Aangezien die standaarden namelijk zonder belemmeringen door alle marktpartijen kunnen worden geïmplementeerd, is er geen sprake van dat bepaalde ondernemingen of producten worden voorgetrokken of uitgesloten.

Als voorbeeld kan de Wet digitale overheid (Wdo) worden genoemd. Op grond van die wet kunnen bij Algemene Maatregel van Bestuur (AMvB) standaarden worden aangewezen die verplicht moeten worden toegepast door in de AMvB aangewezen overheidsorganisaties. Zo zijn op basis van het ‘Besluit beveiligde verbinding met overheidswebsites en -webapplicaties’ de open standaarden HTTPS en HSTS, bekend van

¹¹ De richtlijn noemt in artikel 60 lid 3 specifiek dat de regels over verwijzingen naar technische specificaties geen afbreuk doen aan dwingende nationale technische voorschriften, voor zover die verenigbaar zijn met het recht van de Unie. Deze uitzondering lijkt ten onrechte niet te zijn opgenomen in de Nederlandse Aanbestedingswet 2012.

het groene slotje bovenin in de webbrowser, wettelijk verplicht voor een groot deel van de overheidswebsites. In die context is er geen ruimte om inschrijvingen te accepteren waarbij de inschrijver beweert dat de website op een andere ‘gelijkwaardige manier’, of met een ‘gelijkwaardig protocol’ veilig is.

Naast wettelijk verplichte standaarden speelt in Nederland ook de ‘pas toe of leg uit’- lijst een belangrijke rol. Standaarden worden op deze lijst geplaatst indien een standaard bevorderend werkt voor de interoperabiliteit, een toekomstbestendige gegevensopslag, of voor leveranciersonafhankelijkheid. De lijst komt tot stand op advies van het Forum Standaardisatie, en bevat diverse open standaarden die door de overheid uitgevraagd moeten worden bij aanbestedingen, of die moeten worden gehanteerd in het geval de overheid zelf software ontwikkelt. Indien hiervan wordt afgeweken, dient dit in het aanbestedingsdossier of het projectdossier, en in de bedrijfsvoering paragraaf van het jaarverslag gemotiveerd te worden. Afwijken mag alleen indien er sprake is van een reden die van ‘bijzonder gewicht’ is. Het kabinet heeft aangegeven dat eventuele extra kosten, of het ontbreken van capaciteit geen geldige reden is. De verplichting is voor de Rijksoverheid vastgelegd in de ‘Instructie Rijksdienst bij van aanschaf ICT-diensten en ICT-producten’, en in de Rijksbegrotingsvoorschriften.¹² Ook Zelfstandige bestuursorganen worden geacht dit beleid te volgen.¹³ De gemeenten, provincies en waterschappen hebben zichzelf bestuurlijk verbonden aan het hanteren van deze standaarden conform het ‘Pas toe of leg uit’ principe, en hebben in het verleden ook financiering ontvangen voor het inrichten van deze procedure.

Vanuit aanbestedingsrechtelijk perspectief zijn deze vormen van standaardisatie goed te rechtvaardigen. Het voorschrijven van standaarden die voortvloeien uit wettelijke verplichtingen of breed gedragen beleidskaders beperkt de mededinging niet op ongeoorloofde wijze, maar draagt juist bij aan een gelijk speelveld. Doordat alle marktpartijen zich dienen te conformeren aan dezelfde standaarden, wordt voorkomen dat

¹² <https://wetten.overheid.nl/BWBR0024717/2008-11-23> en <https://rbv.rijksfinancien.nl/modellen/2022/verantwoording/3-24>

¹³ Het gaat hier om “ter zake voor de Rijksdienst geldende voorschriften” als bedoeld in artikel 41.1 Kaderwet Zelfstandige Bestuursorganen.

opdrachten impliciet worden toegeschreven op specifieke technologieën of leveranciers. Bovendien wordt de ruimte voor leveranciers om afhankelijkheden te creëren door middel van leverancierseigen protocollen, aanzienlijk beperkt.

3.6 Belangrijke standaarden in het geval van cloud

Voor juristen of inkopers die belast zijn met het opstellen of beoordelen van cloudovereenkomsten, is kennis van enkele specifieke standaarden onmisbaar. Een verwijzing in een contract of in aanbestedingsdocumenten naar iets als ‘leverancier dient te voldoen aan gangbare industriestandaarden’ is in een juridisch geschil immers vrijwel altijd te vaag. Deze paragraaf categoriseert een aantal cloudgerelateerde standaarden die de huidige marktpraktijk domineren. Hierbij ligt de nadruk op standaarden die invulling geven aan de drie pijlers van een solide cloudcontract: informatiebeveiliging, transparantie van dienstverlening (SLA’s), en portabiliteit en interoperabiliteit.

In het kader van mitigatie van leveranciersafhankelijkheid zijn de standaarden bedoeld voor portabiliteit het meest relevant. De NEN-ISO/IEC 19941:2017 (Cloud computing – Interoperability and portability) is de belangrijkste basisstandaard voor dit thema. De norm maakt onderscheid tussen de verschillende facetten van portabiliteit en interoperabiliteit, en dwingt de gebruiker om na te denken over vragen als: kan de klant zijn data eruithalen, kan de applicatie (code) gemigreerd worden naar een ander platform, kunnen verschillende platforms samenwerken, en is de fysieke verplaatsing van data gestandaardiseerd? Door in een contract of in een Programma van Eisen te verwijzen naar ISO/IEC 19941, wordt voorkomen dat een leverancier claimt ‘portabel’ te zijn enkel omdat er bijvoorbeeld een CSV-export mogelijk is, terwijl de applicatielogica vastzit in propriëtaire code.

Een ander veelvoorkomend juridisch probleem bij cloudcontracten is de definitie van metrics in een Service Level Agreement (SLA). Wat betekenen bijvoorbeeld de in een SLA gebruikte termen zoals ‘beschikbaarheid’ of ‘responstijd’? De ISO/IEC 19086-serie biedt een gestandaardiseerd raamwerk en taxonomie voor cloud-SLA’s. Het dwingt de partijen om in hun SLA ondubbelzinnige definities te hanteren. Een contract dat voor deze

termen verwijst naar ISO 19086 voorkomt discussie achteraf over of een verstoring wel of niet als ‘downtime’ telt.

Het hebben van een goede informatiebeveiliging bevordert de interoperabiliteit tussen partijen. In de juridische praktijk is de NEN-ISO/IEC 27001-norm de belangrijkste basisstandaard voor Information Security Management Systems. Toepassing van deze norm is samen met de ISO 27002-norm voor veel organisaties recentelijk wettelijk verplicht geworden op grond van de NIS2-richtlijn. Deze Europese wet voor netwerk- en informatiebeveiliging verplicht organisaties om gestandaardiseerde beveiligingsmaatregelen te nemen. Met een certificering voor deze norm tonen organisaties aan dat ze passende beheersmaatregelen hebben genomen. Voor cloudspectifieke contracten is die basis echter vaak onvoldoende gedetailleerd. Juristen en inkoopers dienen daarom ook bekend te zijn met de specifieke extensies 27017 en 27018. NEN-ISO/IEC 27017 geeft specifieke beheersmaatregelen voor cloudleveranciers én cloudafnemers. Het verduidelijkt de verdeling van verantwoordelijkheid tussen leverancier en afnemer, wat essentieel is voor wederkerige of evenwichtige aansprakelijkheidsclausules. NEN-ISO/IEC 27018 richt zich specifiek op een situatie waarbij de cloudleverancier als verwerker van de persoonsgegevens gezien wordt. Conformiteit met de beheersmaatregelen in deze norm kan worden gebruikt als bewijsstuk in het kader van AVG-compliance voor een verwerker.

3.7 Exit-clausules en migratieverplichtingen

De mogelijkheid om een ICT-relatie te beëindigen en over te stappen naar een alternatief vormt een essentieel onderdeel van digitale autonomie. Deze mogelijkheid dient echter niet te worden beschouwd als een vanzelfsprekend gevolg van het aflopen van een contract, maar als een aspect dat juist bij het afsluiten van het contract expliciet en zorgvuldig moet worden geregeld. Vaak is er op zo'n moment de neiging om over dit onderwerp niet al te stevig met elkaar het gesprek aan te gaan. Het is misschien het beste vergelijkbaar met het moment dat je gaat trouwen, en dan net voor het geven van het ja-woord nog met elkaar afspraken moet maken over hoe je weer uit elkaar zult gaan. Maar toch moet helder zijn dat zonder adequate contractuele bepalingen de beëindiging van

een overeenkomst gepaard kan gaan met aanzienlijke belemmeringen, waardoor afhankelijkheden in stand blijven.

Exit-clausules en migratieverplichtingen vervullen in dit verband een cruciale functie. Deze bepalingen dienen niet alleen betrekking te hebben op de formele beëindiging van de overeenkomst, maar moeten vooral ook aandacht hebben voor de praktische uitvoerbaarheid van de exit. Daarbij is allereerst van belang om de leverancier daadwerkelijk te kunnen verplichten om mee te werken aan een migratie. Daarbij gaat het ondermeer om ondersteuning bij de overdracht, en het beschikbaar stellen van (toegang tot) data, systemen en interfaces. Maak van tevoren heel duidelijk wat er wel van de leverancier verwacht wordt en wat juist niet, wie er verantwoordelijk is voor bepaalde taken, welke kosten eventueel vergoed gaan worden, en binnen welke termijn de medewerking geboden dient te worden. De praktijk laat zien dat dergelijke voorwaarden vaak ontbreken of in ieder geval onvoldoende zijn uitgewerkt.

Tevens dient van tevoren al aandacht te zijn gegeven aan het waarborgen van de continuïteit van de dienstverlening gedurende de overgangsfase. Of naar de eerdere analogie van het trouwen: tijdens de afwikkeling van de scheiding moet de vertrekkende partner nog wel een tijdje in de gezamenlijke woning kunnen blijven. De migratie van ICT systemen brengt namelijk altijd risico's met zich mee rond de beschikbaarheid en betrouwbaarheid van de nieuwe systemen. In de overeenkomst moet daarom een bepaling zijn opgenomen waarmee men kan waarborgen dat de dienstverlening ook tijdens de overgangsfase op peil kan blijven. Bijvoorbeeld door een tijdelijke voortzetting van de ondersteuning.

Tijdens de exploitatiefase moet de organisatie periodiek toetsen of een migratie nog steeds uitvoerbaar is. Een exitplan dat alleen bij contractsluiting bestaat en daarna in een la verdwijnt, verliest snel zijn waarde. Een belangrijk onderdeel daarvan is het uitvoeren van periodieke exit- of migratietests. Organisaties testen vaak beschikbaarheid, beveiliging en performance, maar veel minder vaak hun vermogen om daadwerkelijk te vertrekken. Daardoor worden afhankelijkheden pas zichtbaar op het moment dat de migratie al moet plaatsvinden. Vanuit het perspectief van digitale autonomie is dat te laat. Een organisatie die pas bij beëindiging ontdekt dat data niet volledig exporteerbaar zijn, dat

koppelingen onvoldoende zijn gedocumenteerd of dat configuraties niet overdraagbaar zijn, heeft haar autonomie feitelijk al eerder verloren. Neem daarom in de contracten op dat de leverancier bijvoorbeeld jaarlijks moet meewerken aan een exit drill (een uitstapoefening) waarbij er in een simulatie wordt getest of systemen en data succesvol kunnen worden losgekoppeld, en kunnen worden overgedragen.

3.8 Documentatie en transparantie

In veel gevallen beschikt de leverancier over een kennisvoorsprong met betrekking tot de werking, inrichting en samenhang van systemen. Niet altijd is deze kennis volledig of systematisch vastgelegd in documentatie die toegankelijk is voor de afnemer. Hierdoor ontstaat een situatie waarin de afnemer weliswaar formeel bepaalde rechten kan hebben ten aanzien van systemen en data, maar waarbij deze voor het begrijpen en gebruiken daarvan nog steeds afhankelijk blijft van de leverancier.

Het contract dient daarom expliciet te voorzien in verplichtingen ten aanzien van het beschikbaar stellen en bijhouden van documentatie, die actueel, volledig en toegankelijk dient te zijn, en die zodanig is opgesteld dat deze ook door derden kan worden gebruikt. Die bepalingen moeten voldoende concreet zijn, en ook afdwingbaar worden opgesteld. Algemene verplichtingen tot het verstrekken van “redelijke informatie” of “benodigde documentatie” bieden daarvoor in de praktijk onvoldoende houvast. Specificeer daarom van tevoren om welke documentatie het gaat, in welke vorm deze beschikbaar gesteld moet worden (bijvoorbeeld via een webpagina of als bewerkbaar document), welke standaarden daarbij gevolgd moeten worden, of het digitoegankelijk moet zijn, en met welke frequentie de documentatie bijgewerkt moet worden.

Een voorbeeld van een hierbij te gebruiken standaard is de OpenAPI Specification (OAS). Door deze standaard te volgen wordt de documentatie van een API volgens een vaste werkwijze beschreven, waardoor het zowel leesbaar is voor machines alsook begrijpelijk is voor mensen. Ontwikkelaars kunnen de API dan bekijken en gebruiken zonder aanvullende documentatie en zonder toegang tot de programmatuur.

Daarnaast is transparantie van belang met betrekking tot de wijze waarop de systemen functioneren en worden beheerd. Het gaat daarbij ondermeer om het verkrijgen van inzicht in gebruikte (versies van) standaarden, afhankelijkheden van externe componenten en software libraries, en de inzet van onderaannemers of subverwerkers. Zonder dergelijke transparantie is het voor de afnemer moeilijk om de risico's van afhankelijkheid te beoordelen of om alternatieven te ontwikkelen.

Om inzicht te verkrijgen in componenten van derden, kan gebruik worden gemaakt van een zogeheten Software Bill of Materials (SBOM). Daarmee kan niet alleen worden gecontroleerd of een implementatievoorstel aan alle (niet-) functionele eisen voldoet, maar kan tevens sneller worden geacteerd op kwetsbaarheden in de componenten, kan sturingsinformatie worden verkregen over de aard en de opbouw van het softwareportfolio, en kan inzicht worden verkregen in de opbouw van door de overheid zelf ontwikkelde software. Bovendien kan een SBOM ook inzicht geven in de voor de eindgebruiker relevante gebruikslicenties die van toepassing zijn op de in een product of dienst gebruikte derdenprogrammatuur, zoals open source componenten.

SBOMs kunnen daarbij op twee manieren worden verkregen:

1. De SBOM wordt aangeleverd door de softwareleverancier. Dit kan zowel een commerciële softwareleverancier zijn als een open-source community. De leverancier of ontwikkelaar onderhoudt een SBOM en stelt deze periodiek en op afroep aan de opdrachtgever (al dan niet onder een geheimhoudingsbeding) beschikbaar. Indien levering of ontwikkeling onder open-sourcevoorwaarden is overeengekomen of beoogd dan maakt een SBOM onderdeel uit van de bij de software behorende (openbaar toegankelijke) documentatie.
2. De SBOM wordt door de overheidsorganisatie zelf gegenereerd. Dit is nodig voor zelfontwikkelde software of voor software waar (nog) geen SBOM voor beschikbaar is.

Het gebruik van de twee SBOM standaarden CycloneDX en SPDX ondersteunt de interoperabiliteit en de herbruikbaarheid van een SBOM en van software.

Eerlijkheidshalve moet opgemerkt worden dat onder SaaS- en cloudleveranciers de grotere leveranciers al vaak akkoord gaan met deze eis omdat zij hun ontwikkelstraten al hebben uitgerust met tools die doorlopend SBOM's genereren. Bij kleinere partijen is er nog wel eens weerstand omdat ze bang zijn dat een met de afnemer gedeelde SBOM direct verouderd is vanwege doorlopende ontwikkeling, of omdat ze bang zijn dat de opbouw van hun dienst op straat komt te liggen. Hoewel een discussie mogelijk is over zaken als de frequentie van updates, en over de diepgang van het overzicht, lijkt het er toch ook op dat het eisen en leveren van een SBOM meer en meer een standaard onderdeel is van het leveranciersmanagement.

3.9 Eigenaarschap intellectueel eigendomsrecht

In de context van ICT-contracten dient het begrip 'eigenaarschap' primair te worden begrepen als betrekking hebbend op intellectuele eigendomsrechten op de software, documentatie en andere relevante componenten. De wijze waarop deze rechten van te voren zijn verdeeld tussen opdrachtgever en leverancier heeft directe gevolgen voor de mate waarin de opdrachtgever systemen kan gebruiken, aanpassen en overdragen.

Wanneer er geen afspraken worden gemaakt over het intellectueel eigendomsrecht, behoudt de leverancier deze rechten, terwijl de opdrachtgever een gebruiksrecht verkrijgt in de vorm van een licentie. Deze licenties zijn in het geval van Commercial off-the-shelf (COTS) software vaak beperkt in omvang en reikwijdte, bijvoorbeeld ten aanzien van wijziging, reproductie of overdracht. Hierdoor blijft de afnemer juridisch afhankelijk van de leverancier voor bijvoorbeeld het doorvoeren van aanpassingen of het inschakelen van derden.

Deze afhankelijkheid wordt verder versterkt indien het gebruiksrecht geen toegang omvat tot de broncode of andere essentiële onderdelen van de software. Zonder toegang tot de broncode is het in de praktijk moeilijk om software zelfstandig te onderhouden, te verbeteren of te migreren naar een andere omgeving. In dergelijke gevallen is de leverancier zelfs in het geval van on-premise software feitelijk de enige partij die in staat is om de software aan te passen of door te ontwikkelen.

De aanbesteding en het contract dienen daarom expliciet te voorzien in een adequate verdeling van intellectuele eigendomsrechten of gebruiksrechten. Dit kan op verschillende manieren worden vormgegeven. Zo is er in het geval van maatwerkontwikkeling vaak behoefte aan volledige overdracht van rechten aan de opdrachtgever. Weliswaar is, in het geval van maatwerk, de toekomstige medewerking aan een dergelijke overdracht vaak als vereiste opgenomen in de door de overheid gebruikte algemene voorwaarden, maar komt het ook nog regelmatig voor dat na de uiteindelijke oplevering of beschikbaarstelling van het product of de dienst, de daadwerkelijke schriftelijke overdracht van de auteursrechten vergeten wordt. Bovendien bestaat, ook in het geval van maatwerk, het ontwikkelde product vaak gedeeltelijk uit al bestaande open source componenten waar het auteursrecht niet van kan worden overgedragen. Een overdracht zou in dat geval slechts gedeeltelijk kunnen plaatsvinden.

Nu is het zo dat de overdracht van auteursrechten enkel zinvol is indien de overheidsorganisatie ook daadwerkelijk van plan is om in de toekomst iets met die rechten te gaan doen. De praktijk laat echter zien dat er inmiddels een soort virtueel pakhuis met auteursrechten bestaat waarvan binnen de overheid niemand meer weet dat de rechten ooit aan hen zijn overgedragen en voor welk product dat is geweest. Het ligt daarom meer voor de hand om in plaats van een overdracht van auteursrecht aan te geven dat levering dient plaats te vinden onder een open source licentie.

3.10 Open source software: Voorkeur bij gelijke geschiktheid

Open source software dient te worden beschouwd als een essentieel instrument voor het realiseren van digitale autonomie. Onder open source software wordt in deze context verstaan software waarvan de broncode beschikbaar is gesteld onder een licentie met ruime gebruiksvoorwaarden die het gebruik, de bestudering, aanpassing en hergebruik toestaan. Deze kenmerken maken het mogelijk dat meerdere partijen bijdragen aan, of diensten leveren rond, dezelfde software, hetgeen de afhankelijkheid van individuele leveranciers vermindert. Open source software adresseert daarmee direct verschillende mechanismen van de vendor lock-in. Doordat de broncode beschikbaar is kan een organisatie ervoor kiezen om het beheer of de doorontwikkeling bij een andere partij onder te brengen.

Tevens maakt open source het mogelijk om functionaliteiten aan te passen zonder afhankelijk te zijn van de prioriteiten of de voorwaarden van een leverancier. In combinatie met open standaarden en dataportabiliteit ontstaat hierdoor een digitale infrastructuur die in beginsel vervangbaar en aanpasbaar blijft.

In Nederland hanteren we bij aanbestedingen van standaard software de beleidsregel dat er bij gelijke geschiktheid een voorkeur zal worden gegeven aan producten geleverd onder een open source licentie. Die term ‘gelijke geschiktheid’ is oorspronkelijk afkomstig uit het arbeidsrecht waarbij soms bij de vervulling van een vacature sprake is van positieve discriminatie. Het begrip betekent niet dat de software dezelfde functionaliteiten, dezelfde gebruikerservaring of dezelfde mate van ondersteuning moet bieden. Het gaat om de vraag of de software in voldoende mate geschikt is om dezelfde werkzaamheden mee uit te voeren en hetzelfde resultaat te bereiken. In dat geval dient er dus bij de beoordeling in ieder geval extra gewicht te worden toegekend aan inschrijvers die leveren onder een open source licentie. Omdat van tevoren natuurlijk onbekend is welke leveranciers zullen gaan inschrijven, is het wenselijk om als organisatie een strategie te hebben waarin is opgenomen of de levering onder een open source licentie een knock out criterium is, of in het geval van een wens hoeveel punten er voor de leverancier extra te verdienen zijn indien deze inschrijft met een licentie die ruime gebruiksvoorwaarden geeft. Overigens hebben de regering en de Tweede Kamer al eerder een oproep gedaan aan de departementen, de mede-overheden, en de instellingen op het gebied van onderwijs, zorg en sociale zekerheid, om dit voorkeursbeleid uiterlijk in 2010 (!) vast te leggen in een implementatiestrategie voor de aanbesteding, de inkoop en het gebruik van open source software.¹⁴

Voor de duidelijkheid: het slechts vermelden in een bestek van de tekst ‘Bij gelijke geschiktheid heeft open source de voorkeur’ creëert in de gunningsmethodiek geen enkele daadwerkelijke voorkeur en is meer een vorm van ‘open source beleid whitewashing’. Dus bij gebruik van deze tekst moet altijd in het bestek duidelijk worden gemaakt aan de gegadigden op welke wijze die voorkeur geëffectueerd gaat worden.

¹⁴ *Kamerstukken II 2007/2008, 26643, nr. 108*

En ook een tekst als “Opdrachtnemer wil graag dat de leverancier gebruik maakt van open source” is onvoldoende onderscheidend. Vrijwel alle software bestaat tegenwoordig uit een of meerdere open source componenten, en sommige licenties geven zelfs de vrijheid om de componenten te gebruiken in een closed source product of dienst. Vandaar dus dat zelfs gegadigden die met een closed source product willen inschrijven, naar eer en geweten akkoord kunnen gaan met deze nietszeggende eis. En desgevraagd zou men het ook nog zo kunnen interpreteren dat er voldaan is aan de eis omdat hun ontwikkelaars gebruik hebben gemaakt van open source ontwikkeltools.

Tegen de achtergrond van meer digitale autonomie verdient open source software een meer prominente plaats binnen aanbestedingen. In plaats van een uitzonderingspositie, waarbij open source software slechts wordt overwogen indien dit vanuit de organisatie expliciet gewenst is, zou het uitgangspunt moeten zijn dat open source wordt toegepast waar dit redelijkerwijs mogelijk is. Afwijking van dit uitgangspunt vereist dan een expliciete motivering, bijvoorbeeld op grond van aantoonbare technische of organisatorische beperkingen.

3.11 Open source software: Niet aanbesteden, maar downloaden

Soms wordt onder inkopers nog wel eens de vraag opgeworpen of het is toegestaan om open source software direct zonder aanbesteding te downloaden en in gebruik te nemen, en of het daarbij is toegestaan de eventueel benodigde aanvullende diensten afzonderlijk aan te besteden.

Het uitgangspunt vanuit het aanbestedingsrecht is eenvoudig: als aanbestedende dienst hoeft men alleen aan te besteden indien men iets inkoopt tegen betaling of een andere tegenprestatie. Bij open source software is dat vaak niet het geval. Als de overheid open source software gratis downloadt en ook mag gebruiken zonder tegenprestatie, dan is er geen sprake van een inkoop. Er wordt immers geen prijs betaald en er is geen sprake van een wederkerige, op geld waardeerbare verplichting. In die situatie hoeft de verwerving van de software niet te worden aanbesteed.

Dat neemt niet weg dat zorgvuldig moet worden beoordeeld of daadwerkelijk sprake is van een zuivere situatie zonder tegenprestatie. Ook “andersoortige” verplichtingen kunnen relevant zijn, bijvoorbeeld wanneer specifieke verplichtingen richting een leverancier voortvloeien uit de licentiestructuren of wanneer feitelijk toch sprake is van een vorm van vergoeding. Denk aan een situatie waarbij de software om te kunnen functioneren bepaalde externe data of andere geavanceerde functies nodig heeft, en er daarbij betaald moet worden aan de oorspronkelijk rechthebbende(n). In dergelijke gevallen kan alsnog sprake zijn van een overheidsopdracht, waardoor het aanbestedingsrecht van toepassing wordt. Ook doet zich soms de situatie voor dat onderhoud en support alleen beschikbaar zijn in combinatie met een enterprise variant van de software. In dergelijke gevallen vormt de door de leverancier aangeboden open source component slechts een onderdeel van een bredere commerciële aanbieding. De software en de diensten zijn dan feitelijk onlosmakelijk met elkaar verbonden.

Men kan zich de vraag stellen of productkeuze vooraf niet te veel de keuze beperkt voor de aanbieders van aanvullende diensten? In de praktijk bestaat immers vrijwel altijd behoefte aan aanvullende diensten, zoals implementatie, configuratie, onderhoud en support. Deze diensten kunnen in beginsel als separate dienstverlening worden beschouwd en worden verworven nadat een keuze is gemaakt voor een open source softwareproduct. De software fungeert dan als gegeven uitgangspunt voor de inkoop van de diensten. Deze benadering is juridisch houdbaar, mits zij niet wordt gebruikt om aanbestedingsregels te ontwijken. Een afzonderlijke aanbesteding van aanvullende diensten is met name goed verdedigbaar wanneer er een reële markt bestaat voor die diensten. Dat betekent dat meerdere aanbieders in staat zijn om implementatie, onderhoud of support te leveren. In dat geval kan de aanbestedende dienst de diensten uitvragen met verwijzing naar de reeds gekozen open source software, bijvoorbeeld vanuit het oogpunt van continuïteit of interoperabiliteit. En omdat het open source software is, is iedere marktpartij ook daadwerkelijk vrij en in staat om dergelijke diensten te ontwikkelen. Die mogelijkheid staat overigens in schril contrast tot proprietary closed source software waarbij support en onderhoud slechts bij een beperkt aantal leveranciers uit het partnernetwerk van de

licentiegever kan worden afgenomen. Juist in die gevallen is er voor de aanbestedende dienst weinig tot geen onderhandelingsruimte.

Heel soms komt het bij een open source product voor dat de markt voor de diensten nog in ontwikkeling is. Denk aan de situatie waarbij een leverancier haar eigen proprietary en voorheen gesloten software net enige weken als gratis download beschikbaar heeft gesteld onder een open source licentie, en er vrij snel daarna al een aanbesteding voor aanvullende diensten volgt. Dan is er in de meeste gevallen toch nog sprake van een exclusieve positie van die leverancier (bijvoorbeeld een kennisvoorsprong) die niet op een natuurlijke wijze tot stand is gekomen. In dat geval dient de aanbestedende dienst in haar aanbestedingsproces voldoende tijd in te bouwen zodat overige leveranciers de software kunnen bestuderen en de gevraagde diensten desgewenst kunnen ontwikkelen. Als er vervolgens toch maar één aanbieder is, dan is dat klaarblijkelijk een eigen keuze van de andere leveranciers geweest.

Voordat een overheidsorganisatie kiest voor het zogeheten “verwerven via download” scenario, moet er bijvoorbeeld via een marktconsultatie goed gekeken worden of er meerdere partijen zijn die implementatie, support en onderhoud kunnen leveren, en of er echte concurrentie mogelijk is. Als dat niet zo is, dan creëert men al snel afhankelijkheid van één leverancier, en daarmee ook aanbestedingsrisico’s.

Kort samengevat: Is er sprake van gratis te downloaden open source software die bruikbaar is zonder op geld waardeerbare verplichtingen? Dan is er geen aanbesteding nodig. Gaat het om diensten eromheen? Dan meestal wel aanbesteden, waarbij verwezen mag worden naar het open source product. Maar is er geen echte keuze tussen leveranciers van de diensten? Pas in dat geval op, want waarschijnlijk moet men dan toch integraal aanbesteden. In dat laatste geval is het uiteraard toegestaan om in het bestek een voorkeur op te nemen voor software die geleverd wordt onder ruime licentievoorwaarden, zoals bij open source software het geval is.

Binnen de Nederlandse overheid is dit vraagstuk in de loop der jaren uitgewerkt in meerdere handreikingen, waarvan de oudste “Het verwerven van (open source) software” in 2007 mede namens de Chief Procurement Officer Rijksoverheid is uitgebracht. In 2008 is deze verwervingsstrategie

ook als toegestane mogelijkheid besproken in een EU procurement guideline (OSOR Guidelines Public procurement and Open Source Software), en sindsdien is deze ook toegepast door diverse Nederlandse overheidspartijen en ook door de Europese Commissie. Naar aanleiding van een klacht van een closed source ondernemer tegen de Europese Commissie heeft de Europese ombudsman in 2010 uitgesproken dat aanbesteding inderdaad niet nodig is wanneer het gekozen systeem open source software betreft en deze software bovendien kosteloos is. Omdat het in die zaak echter ging om een betaalde “enterprise” versie waar licentiekosten voor moesten worden betaald, werd de commissie in het ongelijk gesteld. Wie het downloaden van open source dus enkel inzet om aanbesteding te vermijden, begeeft zich op glad ijs; wie het echter inzet binnen de juiste voorwaarden, benut juist de ruimte binnen het aanbestedingsrecht.

3.12 Open source software: Open, tenzij

De Wet hergebruik overheidsinformatie (Who) bevat sinds 2024 een nieuwe bepaling: artikel 2a. Daarin staat dat publieke instellingen en overheidsondernemingen zich moeten inspannen om hun software geschikt te maken voor hergebruik, bij voorkeur als open source. Het gaat hier dus niet om een harde verplichting (“je moet”), maar om een inspanningsverplichting: de overheid moet in redelijkheid haar best doen om dit mogelijk te maken. Dat betekent bijvoorbeeld dat overheidsorganisaties nieuw te ontwikkelen software zoveel mogelijk als open source moeten ontwikkelen of moeten laten ontwikkelen. Maar ook dat ze bij bestaande (gesloten) software gaan onderzoeken of die alsnog open source kan worden gemaakt, en dat ze waar nodig open source communities gaan faciliteren en stimuleren.

Voor software die ná juni 2024 in gebruik is genomen, geldt bovendien een aanvullende regel (artikel 5d): die moet, tenzij dat onevenredig veel moeite of kosten vergt, zoveel mogelijk ook actief beschikbaar worden gesteld voor hergebruik. Denk dan aan het actief, dus niet enkel op verzoek, delen van broncode, documentatie of componenten met andere overheden of burgers.

De wet stelt ook eisen aan hoe de overheid software aanbesteedt of inkoopt. In artikel 2a, lid 2, staat dat aanbestedende diensten zich moeten inspannen om bij aanbestedingen minimaal de volgende twee dingen te regelen:

Allereerst moet de geleverde software geschikt zijn om openheid en hergebruik mogelijk te maken. En daarnaast moeten de auteursrechten worden overgedragen aan de overheid, of moet de software worden geleverd onder ruime licentievoorwaarden. Daarbij kan gedacht worden aan licenties die voldoen aan de vrijheden en randvoorwaarden die door het Open Source Initiative (OSI) zijn vastgelegd in de Open Source Definition.¹⁵

Met andere woorden: als een overheidsorganisatie software door derden laat bouwen, dan moet de organisatie er ook voor zorgen dat deze juridisch én technisch geschikt zijn voor hergebruik, bijvoorbeeld door andere overheidsorganisaties. Als dat niet direct in de aanbestedingsdocumenten staat, dan ontstaat er afhankelijk van de goede wil van de leverancier, en dat is nu precies wat dit artikel in de wet wil voorkomen.

De verplichtingen gelden in de eerste plaats voor software die sinds juni 2024 is gebouwd of in gebruik genomen. Maar dat betekent niet dat oudere software volledig buiten beeld blijft. De Wet open overheid (Woo) bevat al langere tijd een bredere inspanningsverplichting om software en broncode openbaar te maken. Samen laten deze twee wetten zien dat openbaarheid en hergebruik steeds meer de norm worden. Voor het juridische lezerspubliek merk ik nog op dat bovenstaande interpretatie van de bepalingen in de Who gebaseerd is op paragraaf 7.4 van de Memorie van Toelichting bij de Wet implementatie Open data richtlijn.

¹⁵ <https://opensource.org/osd>

Natuurlijk is het de overheid toegestaan om verdere voorwaarden te verbinden aan het hergebruik van software. In artikel 6 van de Who staat bijvoorbeeld dat de overheid aansprakelijkheid mag uitsluiten, of het hergebruik alleen mag toestaan onder bepaalde open source-licenties. Denk daarbij aan de European Union Public Licence (EUPL), waarin als voorwaarde staat opgenomen dat hergebruikers eventuele wijzigingen aan de broncode bij verdere verspreiding ook weer openbaar moeten maken onder dezelfde licentie.

Een praktisch instrument om de inzet van open source software te structureren is de zogenoemde ambitieladder, ontwikkeld door het ministerie van Volksgezondheid, Welzijn en Sport (VWS).¹⁶ Deze ladder onderscheidt verschillende niveaus van volwassenheid in het gebruik van open source, variërend van het incidenteel toepassen van open source oplossingen tot het actief ontwikkelen, delen en hergebruiken van software binnen en tussen overheidsorganisaties.

De ambitieladder maakt inzichtelijk dat de keuze voor open source geen binaire beslissing is, maar een ontwikkelpad. Organisaties kunnen stapsgewijs toewerken naar een situatie waarin open source niet alleen wordt gebruikt, maar ook actief wordt ontwikkeld en gedeeld. Dit sluit aan bij bredere beleidsdoelstellingen gericht op samenwerking, hergebruik en het voorkomen van dubbele ontwikkeling binnen de overheid. Bij de ambitieladder zijn ook diverse voorbeeld clausules opgenomen die goed gebruikt kunnen worden in aanbestedingstrajecten.

¹⁶ <https://minvws.opensourcewerken.nl/open-source-ambitieladder-voor-maatwerk-aanbesteding-of-opdracht/>



Figuur 2: Vendor break-out in zes stappen.

4. Digitale autonomie

4.1 Autonomie als handelingsvrijheid

In het vorige hoofdstuk is leveranciersafhankelijkheid uitgewerkt als ontwerp- en contracteringsprincipe. Dit hoofdstuk plaatst die instrumenten in een bredere bestuurlijke context. Digitale autonomie gaat niet alleen over het kunnen wisselen van leverancier, maar over de feitelijke handelingsvrijheid van publieke organisaties in een digitale omgeving.

Een overheidsorganisatie is digitaal autonoom wanneer zij voldoende grip heeft op haar systemen, data, kennis, contracten en leveranciers om haar publieke taken zelfstandig en verantwoord te kunnen uitvoeren. Vanuit dat perspectief kan digitale autonomie worden beschouwd als een verzameling van vrijheden die een organisatie in staat stellen om haar publieke of organisatorische doelen te realiseren zonder feitelijk gebonden te zijn aan één leverancier, technologie of ecosysteem.

Dit hoofdstuk werkt deze vormen van handelingsvrijheid uit. Daarbij wordt achtereenvolgens besproken wat het betekent om vrij te kunnen samenwerken, te kunnen migreren, publieke waarden te kunnen realiseren, collectief te kunnen ontwikkelen en inkopen, en een eigen digitale koers te kunnen bepalen. Daarmee vormt dit hoofdstuk ook de schakel tussen de meer technische en contractuele benadering van leveranciersafhankelijkheid en de bredere vraag naar digitale soevereiniteit in het volgende hoofdstuk.

4.2 Vrijheid om samen te werken

Digitale autonomie wordt vaak voorgesteld als een vorm van zelfstandigheid. Dat betekent echter niet dat de organisatie alles ook zelfstandig hoeft te doen. Integendeel, autonomie geeft juist de mogelijkheid om samen te werken met een of meerdere partijen naar keuze. Een organisatie die slechts kan communiceren, gegevens uitwisselen of diensten afnemen binnen één leveranciers-ecosysteem is niet autonoom, maar afhankelijk van de kaders en de grenzen die

dat ecosysteem stelt. Omdat overheidsorganisaties moeten kunnen samenwerken met andere overheden, maatschappelijke instellingen, bedrijven en burgers is deze vrijheid van het grootste belang. Het gaat daarbij dus om de mogelijkheid om onderling gegevens uit te wisselen, processen op elkaar aan te sluiten, diensten te kunnen combineren, gezamenlijke ketens te ondersteunen en nieuwe samenwerkingsvormen mogelijk te maken. Wanneer een organisatie daarvoor afhankelijk is van het handelen of de prioritering door een leverancier, dan wordt zij in de vrijheid tot samenwerking beperkt. Deze vorm van afhankelijkheid ontstaat meestal heel subtiel en in een heel vroeg stadium van gebruik. Zij manifesteert zich namelijk niet alleen bij beëindiging van de overeenkomst, maar juist al veel eerder tijdens het normaal gebruik. Een organisatie merkt dan bijvoorbeeld dat bepaalde koppelingen niet worden ondersteund, of dat de toegang voor derden extra licenties vereist, en dat gegevensuitwisseling alleen via leveranciersspecifieke interfaces kan plaatsvinden. De samenwerking lijkt formeel mogelijk, maar wordt praktisch gestuurd door de architectuur en voorwaarden van de leverancier.

De lijst met open standaarden van het Forum Standaardisatie bevat standaarden die interoperabiliteit, de toekomstbestendige gegevensopslag, en de leveranciersafhankelijkheid kunnen bevorderen binnen en tussen overheidsorganisaties, en tussen overheidsorganisaties, bedrijven en burgers. Deze standaarden voorkomen dat samenwerking afhankelijk wordt van leveranciersspecifieke formaten of protocollen. Een open standaard maakt het mogelijk dat verschillende partijen met verschillende systemen toch gegevens kunnen uitwisselen en processen op elkaar kunnen aansluiten. De waarde van open standaarden ligt in deze context niet alleen in technische interoperabiliteit, maar ook in het behoud van keuzevrijheid. Zij zorgen ervoor dat samenwerking niet hoeft te worden georganiseerd binnen één gesloten ecosysteem.

Daarbij is niet alleen syntactische interoperabiliteit van belang, maar bijvoorbeeld ook de semantische en organisatorische interoperabiliteit. Systemen kunnen technisch wellicht berichten uitwisselen, maar de samenwerking blijft beperkt wanneer partijen verschillende begrippen, datadefinities, verantwoordelijkheden of procesafspraken hanteren. De vrijheid om samen te werken vraagt daarom om een gemeenschappelijke

taal, duidelijke governance en afspraken over gegevenskwaliteit en gebruik. Digitale autonomie is in ketens dus niet uitsluitend een technisch vraagstuk, maar ook een bestuurlijk en juridisch vraagstuk.

De vrijheid om samen te werken heeft daarnaast een innovatieve dimensie. Nieuwe publieke diensten ontstaan vaak op het snijvlak van organisaties. Dat vereist dat systemen op nieuwe manieren kunnen worden gecombineerd. Wanneer digitale voorzieningen alleen bruikbaar zijn binnen vooraf bepaalde leveranciersscenario's, wordt innovatie beperkt tot wat het bestaande ecosysteem ondersteunt. Een organisatie die vrij kan koppelen en gegevens verantwoord kan delen, heeft meer ruimte om nieuwe maatschappelijke opgaven digitaal te ondersteunen.

Deze vrijheid vraagt ook om keuzes in architectuur. Een modulaire inrichting, goed beschreven koppelvlakken, open standaarden en duidelijke scheiding tussen data, functionaliteit en toegang vergroten de mogelijkheid om met verschillende partijen samen te werken. Daartegenover beperken gesloten suites, proprietary interfaces en ondoorzichtige integraties de ruimte om relaties met derden zelfstandig vorm te geven. De architectuur van een systeem bepaalt daarmee niet alleen hoe efficiënt een organisatie intern werkt, maar ook hoe vrij zij extern kan opereren.

Voor overheidsorganisaties betekent dit dat samenwerkingsvrijheid al in de strategische en aanbestedingsfase moet worden meegenomen. Bij de selectie van software moet niet alleen worden gevraagd of de oplossing de eigen functie ondersteunt, maar ook of zij deelname aan publieke ketens mogelijk maakt. En daarbij gaat het ook om nu nog onvoorziene toekomstige samenwerking of uitwisseling. Relevante vragen zijn bijvoorbeeld of de oplossing open standaarden ondersteunt, of koppelingen met derden mogelijk zijn, of documentatie in ODF formaat beschikbaar is, of autorisaties fijnmazig kunnen worden ingericht, of gegevensuitwisseling controleerbaar is en of integratie niet afhankelijk is van exclusieve dienstverlening door één leverancier.

Het Open Document Formaat (ODF) is een heel concreet voorbeeld van een standaard die onvoorziene samenwerking en uitwisseling mogelijk maakt. ODF is een bestandsformaat dat gebruikt kan worden voor het

bewaren en/of uitwisselen van bewerkbare tekstbestanden, rekenbladen en presentaties. Het kan door vrijwel alle tekstverwerkers geopend worden en is duurzaam toegankelijk zodat ze ook in de toekomst leesbaar en bewerkbaar zullen zijn, ongeacht de gebruikte office applicatie. Daarom is al in 2007 door het kabinet voor organisaties behorende tot de Rijksoverheid in een beleidsregel vastgelegd dat die organisaties het gebruik van ODF voor het lezen, schrijven en uitwisselen van documenten ondersteunen, en dat burgers, ondernemingen en andere overheden vanaf december 2008 het recht hebben om documenten in ODF aan te leveren, en in ODF terug te krijgen.¹⁷ Een jaar later hebben de medeoverheden zichzelf ook bestuurlijk verbonden aan dit voorrecht voor burgers en de plicht voor de overheid om desgewenst terug te leveren in dat formaat. Natuurlijk kan hieraan voldaan worden door alles default op te slaan in bijvoorbeeld het leverancierseigen Microsoft formaat docx, en dan desgevraagd de documenten om te zetten naar ODF. De ervaring laat echter zien dat er bij zo'n conversie van alles mis kan gaan in de opmaak vanwege leverancierseigen lettertypes, macro's en andere functies in docx die niet een-op-een overeenkomen. Het is dus verstandig om intern als default formaat direct gebruik te gaan maken van ODF in plaats van de leverancierseigen formaten. Daarnaast is het verstandig om in aanbestedingen ook te vragen om ondersteuning van het ODF formaat. Dat al helemaal indien er, bijvoorbeeld voor het maken van rapportages, ook bestandsformaten aan geïnteresseerde leveranciers worden voorgeschreven zoals docx, xlsx of ppt, of wanneer de aanbesteding meer in het algemeen een verwijzing bevat in de trant van "U dient gebruik te maken van Word, Excel, of Powerpoint".

4.3 Vrijheid om te migreren

Digitale autonomie veronderstelt dat een organisatie haar digitale omgeving kan verlaten wanneer dat bestuurlijk, financieel, juridisch of strategisch noodzakelijk is. Het gaat om het vermogen om een bestaande relatie met een leverancier te beëindigen zonder dat de continuïteit van de dienstverlening, de toegankelijkheid van gegevens, de uitvoerbaarheid van

¹⁷ Deze beleidsregel is opgenomen in het Actieplan Nederland Open in Verbinding. *Kamerstukken II 2007/2008, 26643, nr. 108*. Zie ook M.H. Paapst, *Barrières en doorwerking*, Diss. Groningen 2013, p. 140

publieke taken of de financiële positie van de organisatie onevenredig in gevaar komt.

De vrijheid om te migreren moet daarom worden beoordeeld aan de hand van de feitelijke overstapbaarheid van de gehele digitale functie. Daarbij gaat het om ten minste vier onderdelen. Als eerste wordt gekeken naar de overdraagbaarheid van data. Gegevens moeten daarbij volledig, actueel, gestructureerd en machineleesbaar beschikbaar zijn. Ten tweede kan worden gekeken naar de overdraagbaarheid van functionaliteit. Een nieuwe alternatieve ICT omgeving hoeft absoluut niet identiek te zijn aan de oude, maar moet wel in staat zijn de meest relevante processen voort te zetten. Als derde moet gekeken worden naar de overdraagbaarheid van integraties. Veel systemen staan immers niet op zichzelf, maar zijn verbonden met andere applicaties, databanken, authenticatiediensten, of archiefvoorzieningen. Tot slot moet gekeken worden naar de organisatorische uitvoerbaarheid. Een migratie kan juridisch en technisch mogelijk zijn, maar alsnog mislukken wanneer kennis, capaciteit, governance of budget ontbreken.

Deze benadering laat zien dat migratievrijheid meer is dan dataportabiliteit. Dataportabiliteit is noodzakelijk, maar onvoldoende. Zij biedt slechts toegang tot de gegevenslaag. Digitale autonomie vereist ook inzicht in de technische inrichting, de gebruikte standaarden, de beschikbare interfaces, de afhankelijkheden van derden en de voorwaarden waaronder de oude leverancier ondersteuning moet bieden bij de overgang. Zonder die bredere context kan een exportbestand vooral een symbolisch recht opleveren: de organisatie beschikt dan wel over haar gegevens, maar kan haar digitale functie niet daadwerkelijk elders voortzetten.

De vrijheid om te migreren heeft daarnaast een belangrijke markt ordenende functie. De mogelijkheid om weg te gaan disciplineert leveranciers. Een leverancier die weet dat een afnemer feitelijk niet kan overstappen, heeft meer ruimte om prijzen te verhogen, voorwaarden te wijzigen, ondersteuning te beperken of klanten richting een nieuwe productstrategie te dwingen. Omgekeerd versterkt een geloofwaardige exit de onderhandelingspositie van de afnemer. Migratievrijheid is daarmee niet alleen relevant op het moment van beëindiging van een contract, maar gedurende de gehele contractuele relatie.

Zij beïnvloedt de machtsbalans tussen afnemer en leverancier. Wanneer een overheidsorganisatie feitelijk niet meer kan migreren, wordt zij kwetsbaar voor private sturing. De leverancier bepaalt dan niet alleen de prijs en de technische mogelijkheden, maar indirect ook het tempo en de richting van publieke digitalisering. De vraag of een overheidsorganisatie kan migreren is daarom niet louter operationeel. Zij raakt aan de vraag of de overheid zelfstandig richting kan blijven geven aan haar digitale infrastructuur.

De Data Act bevestigt het belang van deze overstapbaarheid, vooral voor data processing services zoals cloud-, platform- en softwarediensten. De Data Act verplicht aanbieders om belemmeringen voor overstappen weg te nemen en bevat bepalingen over contractuele overstap-rechten, informatieplichten, samenwerking te goeder trouw, technische ondersteuning en de (geleidelijke) afschaffing van in rekening gebrachte overstapkosten.

Toch moet de impact en de reikwijdte van de Data Act niet worden overschat. Zij biedt een belangrijke minimumstructuur, maar garandeert niet dat iedere migratie eenvoudig, goedkoop of volledig probleemloos zal gaan verlopen. De verplichtingen zijn mede afhankelijk van het soort dienst, de aard van de functionaliteit en de technische mogelijkheden. Bovendien kan wetgeving niet achteraf alle afhankelijkheden herstellen die eerder door architectuurkeuzes, maatwerk, gesloten standaarden of gebrekkige contractering zijn ontstaan. De Data Act versterkt dus de positie van de afnemer, maar neemt de verantwoordelijkheid voor goed opdrachtgeverschap niet weg.

Ook financieel moet migratievrijheid expliciet worden gewaardeerd. Een oplossing met lage instapkosten kan op langere termijn duur blijken wanneer de exitkosten hoog zijn. Omgekeerd kan een oplossing die in aanschaf duurder lijkt aantrekkelijker zijn wanneer zij de toekomstige overstapbaarheid beter waarborgt. Digitale autonomie vereist daarom een beoordeling op basis van total cost of ownership, inclusief verwachte exitkosten, kosten van dubbele exploitatie, conversiekosten, kosten van herbouw van integraties en kosten van organisatorische transitie. De relevante vraag is niet alleen wat het systeem kost zolang het wordt gebruikt, maar ook wat het kost om het te verlaten.

Daarbij moet worden voorkomen dat het denken over migratievrijheid wordt gereduceerd tot een eenmalige exit aan het einde van een contract. Het blijkt vaak wenselijk dat organisaties bepaalde onderdelen gefaseerd kunnen vervangen, meerdere leveranciers naast elkaar kunnen gebruiken of bepaalde functionaliteiten kunnen ontbundelen. Migratievrijheid omvat daarom ook de mogelijkheid tot gedeeltelijke migratie en parallel gebruik van verschillende diensten. Een organisatie die alleen in één grote eindmigratie kan vertrekken, loopt een aanzienlijk groter risico dan een organisatie die haar digitale omgeving modulair kan aanpassen.

Zonder migratievrijheid blijft autonomie afhankelijk van de bereidwilligheid van de zittende leverancier. Met migratievrijheid ontstaat daarentegen een reële keuze: blijven wanneer de dienstverlening passend is, onderhandelen wanneer voorwaarden verslechteren, en vertrekken wanneer de eigen belangen dat vereisen.

4.4 Vrijheid om publieke waarden te realiseren

De vrijheid om bij het gebruik van digitale systemen ook publieke waarden te realiseren kan concreet worden gemaakt aan de hand van afwegingskaders die door ethische commissies worden gehanteerd. Een bruikbaar voorbeeld is het ethisch afwegingskader van de gemeente Groningen.¹⁸ Daarin worden publieke waarden niet opgevat als abstracte beginselen naast de technologie, maar als inhoudelijke maatstaven voor de beoordeling van digitale toepassingen. Een overheid is pas digitaal autonoom wanneer zij technologie kan inzetten op een wijze die verenigbaar is met de publieke waarden waarvoor zij verantwoordelijkheid draagt.

Een eerste waarde in dat Groningse voorbeeld is nuchterheid. Overheidsorganisaties moeten zich niet laten meeslepen door technologische hypes, maar kritisch beoordelen welk probleem daadwerkelijk moet worden opgelost en of de inzet van technologie daarvoor überhaupt het juiste middel is. Niet iedere innovatie is namelijk een verbetering. Digitale autonomie vraagt daarom om het vermogen van de overheidsorganisatie om afstand te houden tot leveranciersretoriek en innovatieclaims.

¹⁸ <https://gemeente.groningen.nl/ethische-commissie-data-en-technologie>

Een autonome overheid kan beoordelen of een digitale oplossing noodzakelijk, proportioneel, veilig, duurzaam en maatschappelijk verantwoord is. Zij kan ook besluiten om een technologische oplossing niet te gebruiken, of te kiezen voor een eenvoudiger, niet-technisch alternatief wanneer dat beter past bij het publieke doel.

De tweede waarde is autonomie voor de burgers zelf. Digitale technologie mag burgers niet onnodig beperken in hun vermogen om vrij, onbevangen en zonder ongepaste beïnvloeding hun leven vorm te geven. Systemen die gedrag sturen, bewegingen volgen, of keuzes voorspellen, kunnen invloed hebben op de feitelijke vrijheid van burgers. Dat geldt niet alleen wanneer rechten formeel worden beperkt, maar ook wanneer mensen zich anders gaan gedragen omdat zij weten of vermoeden dat zij worden gemonitord, geprofileerd of beoordeeld. Digitale autonomie van de overheid moet daarom mede worden beoordeeld aan de hand van de autonomie van burgers: publieke technologie mag de burger niet reduceren tot object van sturing, classificatie of gedragsbeïnvloeding.

Privacy vormt een derde kernwaarde. Burgers moeten erop kunnen vertrouwen dat hun persoonlijke levenssfeer wordt gerespecteerd. Dat vereist meer dan formele naleving van gegevensbeschermingsregels uit de AVG. Privacy moet vanaf het eerste ontwerp van digitale systemen worden meegenomen. Dat betekent dat gegevensverwerking wordt beperkt tot wat noodzakelijk is, dat persoonsgegevens zo min mogelijk herleidbaar zijn, dat bewaartermijnen en toegangsrechten worden begrensd, en dat de inrichting van systemen voorkomt dat gegevens later voor andere doeleinden worden gebruikt zonder behoorlijke rechtvaardiging. Digitale autonomie betekent in dit verband dat een overheidsorganisatie voldoende zeggenschap heeft over haar gegevensverwerking om privacy daadwerkelijk technisch, organisatorisch en juridisch te borgen.

Een vierde waarde is controle op technologie. Burgers mogen erop vertrouwen dat de overheid grip heeft op de technologie die zij gebruikt. Die grip vereist inzicht in datastromen, opslaglocaties, toegangsrechten, gebruikte algoritmen, koppelingen met derden en de wijze waarop gegevens binnen samenwerkingsverbanden worden gebruikt. Controle op technologie betekent ook dat de overheid zelf kan bijsturen wanneer een systeem onbedoelde effecten heeft, wanneer gegevens verkeerd worden

gebruikt of wanneer publieke belangen onvoldoende zijn geborgd. Een overheid die afhankelijk is van een leverancier voor basaal inzicht in de werking van haar systemen heeft onvoldoende controle op technologie.

Veiligheid is eveneens een zelfstandige publieke waarde. Digitale technologie kan bijdragen aan fysieke veiligheid, openbare orde en bescherming van burgers, maar kan ook nieuwe risico's introduceren. Daarbij gaat het niet alleen om cybersecurity, maar ook om het gevoel van veiligheid, de betrouwbaarheid van digitale voorzieningen en de bescherming van vertrouwelijke informatie. Digitale autonomie veronderstelt dat de overheid veiligheidseisen kan stellen aan haar leveranciers, kan controleren of daaraan wordt voldaan, en voldoende handelingsruimte heeft om eventuele kwetsbaarheden te verhelpen.

Gelijkwaardigheid vereist dat burgers in gelijke mate kunnen deelnemen, dat digitale dienstverlening toegankelijk is en dat mensen niet feitelijk worden uitgesloten doordat zij niet beschikken over de juiste vaardigheden, middelen, taalvaardigheid of digitale toegang. Ook moet ruimte blijven bestaan om niet of niet volledig digitaal mee te doen wanneer dat uit oogpunt van inclusiviteit noodzakelijk is. Digitale autonomie betekent hier dat de overheid haar digitale inrichting kan aanpassen aan burgers, in plaats van burgers te dwingen zich volledig aan te passen aan de logica van het systeem.

Rechtvaardigheid vraagt vervolgens om aandacht voor de verdeling van baten en lasten van technologie. Een digitale oplossing kan voor sommige groepen waardevol zijn, maar voor andere groepen juist nadelig, stigmatiserend of discriminerend uitwerken. Publieke technologie moet daarom worden beoordeeld op haar gevolgen voor verschillende groepen burgers. Wanneer mensen verschillend worden behandeld door een technologische toepassing, moet daarvoor een inhoudelijke en rechtmatige verantwoording bestaan. Rechtvaardigheid vereist bovendien dat overheidsorganisaties niet alleen kijken naar gemiddelde efficiëntiewinst, maar ook naar de positie van kwetsbare groepen, foutgevoeligheid, herstelmogelijkheden en de vraag wie de risico's van digitalisering draagt.

Tot slot is duurzaamheid een publieke waarde die nadrukkelijk onderdeel moet zijn van digitale autonomie. Digitale oplossingen hebben gevolgen voor energiegebruik, hardwareverbruik, grondstoffen, datacentercapaciteit, levensduur van apparatuur en de bredere leefomgeving. Een autonome overheid moet daarom kunnen kiezen voor digitale voorzieningen die passen binnen klimaatdoelen, circulaire principes en verantwoord gebruik van schaarse middelen. Dat vergt aandacht voor energie-efficiëntie, hergebruik (ook van broncode), levensduurverlenging, repareerbaarheid, vermindering van onnodige dataverwerking en beperking van technologische verspilling. Ook hier geldt dat de goedkoopste of meest gangbare oplossing niet vanzelfsprekend de meest duurzame oplossing is.

De vrijheid om publieke waarden te realiseren beschermt de mogelijkheid van de overheid om zelf richting te geven aan de digitale inrichting van publieke taken. Dat betekent niet dat overheidsorganisaties alles zelf moeten ontwikkelen of beheren. Het betekent wel dat zij niet afhankelijk mogen worden van leveranciers op een wijze die publieke waarden feitelijk ondergeschikt maakt aan commerciële productstrategieën. De overheid moet kunnen bepalen welke waarden leidend zijn, welke risico's aanvaardbaar zijn en welke waarborgen noodzakelijk zijn.

4.5 Vrijheid om collectief te handelen

Digitale autonomie is niet uitsluitend een individuele eigenschap van afzonderlijke organisaties. Zeker binnen de publieke sector ontstaat autonomie vaak pas wanneer organisaties gezamenlijk optreden. Veel digitale afhankelijkheden worden namelijk versterkt doordat overheidsorganisaties afzonderlijk inkopen, afzonderlijk ontwikkelen en afzonderlijk onderhandelen met dezelfde leveranciers. Die versnippering aan de vraagzijde vergroot de marktmacht van aanbieders. Iedere organisatie lijkt dan zelfstandig te kiezen, maar de gezamenlijke uitkomst is dat publieke middelen worden besteed aan grotendeels vergelijkbare oplossingen, zonder dat de overheid als geheel meer grip krijgt op de onderliggende technologie, data of doorontwikkeling.

Collectieve ontwikkeling en inkoop kan dit patroon doorbreken. Wanneer overheidsorganisaties gezamenlijk gaan investeren in software,

standaarden, documentatie en beheer, ontstaat er een andere verhouding tussen de opdrachtgever en leveranciers. De publieke sector wordt dan niet uitsluitend afnemer van kant-en-klare producten, maar mede vormgever van digitale voorzieningen. Dat betekent niet dat de overheid alle software zelf moet bouwen. Het betekent wel dat zij strategische zeggenschap behoudt over de eisen, de architectuur, de ontwikkelrichting en de voorwaarden waaronder derden kunnen bijdragen.

Open source software speelt daarbij een bijzondere rol. Niet omdat open source automatisch goedkoper of beter is, maar omdat zij direct geschikt is voor gedeelde ontwikkeling. Broncode kan door meerdere organisaties worden gebruikt, gecontroleerd, verbeterd en hergebruikt. Investerings van één organisatie kunnen daardoor ten goede komen aan andere organisaties. De waarde van open source ligt in deze context niet alleen in de beschikbaarheid van de code, maar vooral in het feit dat exclusieve controle door één leverancier wordt voorkomen. Een overheidsorganisatie kan een leverancier inschakelen voor ontwikkeling, beheer of ondersteuning, zonder dat die leverancier noodzakelijkerwijs eigenaar wordt.

Daarmee verschuift ook de betekenis van inkoop. In een traditioneel inkoopmodel koopt een organisatie een product of dienst in bij een leverancier. In een collectief model kan de overheid ook sturen op de ontwikkeling van een gemeenschappelijke voorziening of publieke gemeenschapsgoederen.¹⁹ De opdracht aan de markt wordt dan niet slechts: lever een oplossing voor deze organisatie. De opdracht wordt: draag bij aan een voorziening die herbruikbaar, controleerbaar en overdraagbaar is binnen een bredere publieke context.

Collectieve inkoop kan daarnaast de onderhandelingspositie van overheidsorganisaties versterken. Door vraagbundeling kunnen zij betere voorwaarden stellen aan prijs, kwaliteit, documentatie, interoperabiliteit, beveiliging, ondersteuning en continuïteit. Ook kan collectieve inkoop voorkomen dat verschillende overheidsorganisaties tegen uiteenlopende voorwaarden afhankelijk worden van dezelfde leverancier. Vanuit het perspectief van digitale autonomie is dat relevant omdat afhankelijkheden

¹⁹ <https://www.commonsnetwork.org/nl/digitale-gemeenschapsgoederen-uitleggen/>

niet alleen op organisatieniveau ontstaan, maar ook op stelselniveau. Wanneer een groot deel van de publieke sector afzonderlijk afhankelijk wordt van dezelfde leverancier, ontstaat een collectieve afhankelijkheid die moeilijker te corrigeren is dan een individueel contractueel probleem.

Daar staat tegenover dat collectieve inkoop niet zonder risico is. Vraagbundeling kan ook leiden tot grootschalige raamcontracten die juist dominante marktpartijen bevoordelen. Wanneer de gezamenlijke vraag te omvangrijk, te gesloten of te productspecifiek wordt geformuleerd, kunnen kleinere aanbieders, open source dienstverleners en gespecialiseerde marktpartijen juist moeilijker meedingen. Collectieve inkoop versterkt de digitale autonomie dus alleen wanneer zij zorgvuldig wordt ingericht. Dat vraagt om modulariteit, functionele specificaties, ruimte voor meerdere leveranciers en het vermijden van het onnodig noemen of toeschrijven naar producten of merken van dominante leveranciers.

Gezamenlijke digitale voorzieningen vragen om duidelijke governance. Er moet worden bepaald wie eigenaar is van de roadmap, wie prioriteiten stelt, wie wijzigingen goedkeurt, wie verantwoordelijk is voor beveiliging, wie beheer financiert en hoe deelnemende organisaties invloed kunnen uitoefenen. Zonder zulke afspraken ontstaat het gevaar dat niemand werkelijk verantwoordelijk is, terwijl iedereen afhankelijk wordt van de uitkomst. Digitale autonomie vereist daarom niet alleen technische herbruikbaarheid, maar ook bestuurlijke organiseerbaarheid.

In Nederland is er bijvoorbeeld voor gekozen om samenwerking te organiseren binnen de Generieke Digitale Infrastructuur (GDI). Die infrastructuur bestaat uit afspraken, standaarden, en landelijke voorzieningen die alle publieke dienstverleners gebruiken voor hun dienstverlening aan burgers en ondernemers. Voorbeelden zijn DigiD, Digipoort, of MijnOverheid.nl.

Collectieve ontwikkeling vraagt om een ander financieel model dan afzonderlijke aanschaf. De baten liggen vaak verspreid over meerdere organisaties, terwijl de kosten in eerste instantie bij een beperkt aantal initiatiefnemers terechtkomen. Organisaties wachten af totdat anderen betalen voor ontwikkeling, waarna zij later willen aansluiten. Een duurzaam

collectief model vraagt daarom om afspraken over bijdragen, onderhoud, doorontwikkeling, beheer en risicodeling. Zonder structurele financiering verandert een gezamenlijke voorziening al snel in een tijdelijk project.

Ook juridisch moet collectieve ontwikkeling zorgvuldig worden vormgegeven. Overheidsorganisaties kunnen samenwerken, gezamenlijk inkopen of gemeenschappelijke voorzieningen organiseren, maar moeten daarbij rekening houden met aanbestedingsrechtelijke, staatssteunrechtelijke, mededingingsrechtelijke en governancevragen. De juridische vormgeving moet aansluiten bij de feitelijke bedoeling. Gaat het om gezamenlijke opdrachtverlening aan de markt, om samenwerking tussen overheidsorganisaties, om financiering van een gemeenschappelijke voorziening, om subsidiering, of om deelname aan een open source gemeenschap?

Een goed voorbeeld van een succesvolle interbestuurlijke open source gemeenschap is de Stichting Pleio. Plein Overheid (Pleio) is rond 2009 gestart als Nederlands open source alternatief voor een Amerikaans proprietary online samenwerkingsplatform. Het eigenaarschap en het beheer van de software is in 2012 als publiek gemeenschaps-goed belegd bij een daarvoor opgerichte stichting. Deze stichting heeft in 2026 de beschikking over een pool van ongeveer 30 ontwikkelaars die op verzoek van de deelnemers nieuwe toepassingen en applicaties ontwikkelen. Deze komen vervolgens open source ter beschikking voor alle deelnemers. Pleio's positie is bijzonder omdat de stichting specifiek bedoeld is voor publiek-publieke samenwerking waarbij de Rijksoverheid en medeoverheden Pleio via quasi inbesteding opdrachten kunnen verlenen als zijnde een "verlengstuk van samenwerkende overheidsorganisaties". Daarom hoeven opdrachten aan Pleio niet aanbesteed te worden. Om tegemoet te komen aan aanbestedingsrechtelijke regels, houden de ruim 120 deelnemers gezamenlijk toezicht op de strategie en de belangrijke besluiten van de stichting via een Vergadering van Deelnemers. Zij werken daarin op gelijke voet met elkaar samen. Een deelnemende gemeente of een deelnemende provincie is in die zin gelijkwaardig aan een deelnemend departement. Inmiddels is het gebruik van Pleio ook overgenomen door diverse Duitse deelstaten, waaronder Sleeswijk-Holstein, waarmee duidelijk is dat collectieve ontwikkeling niet bij de landsgrenzen hoeft te stoppen.

4.6 Vrijheid om een eigen koers te bepalen

Digitale autonomie veronderstelt dat een organisatie in staat is om haar digitale ontwikkeling in overeenstemming te brengen met haar eigen doelen, prioriteiten en verantwoordelijkheden. Het gaat daarbij niet alleen om de vraag of een organisatie een leverancier kan kiezen of verlaten, maar ook om de vraag of zij gedurende de looptijd van een digitale voorziening nog zelfstandig richting kan geven aan haar eigen digitale toekomst. Een organisatie die haar koers voortdurend moet aanpassen aan de productstrategie, licentiemodellen of technologische roadmap van een leverancier, beschikt slechts beperkt over digitale autonomie.

Dit type van autonomie wordt vaak onderschat. Veel digitale afhankelijkheden ontstaan namelijk niet doordat een leverancier expliciet verbiedt om een andere richting te kiezen, maar doordat de feitelijke ontwikkelruimte van de afnemer gedurende de tijd steeds nauwer wordt. Leveranciers bepalen welke functionaliteiten worden doorontwikkeld, welke versies worden ondersteund, welke interfaces beschikbaar blijven, welke producten worden uitgefaseerd en welke migratiepaden worden aangeboden.

Denk aan de verplichte overgang naar cloudvarianten door het beëindigen van ondersteuning voor lokale installaties, wijzigingen in licentiemodellen, bundeling van producten, de ongevraagde introductie van AI-functionaliteiten zoals Copilot, of het uitfasen van bepaalde open koppelvlakken. Zulke veranderingen worden problematisch wanneer de afnemer daarbij geen realistische ruimte heeft om de gevolgen daarvan zelfstandig te wegen. Zij moeten zelf kunnen bepalen of een cloudmigratie gewenst is, of bepaalde functionaliteit noodzakelijk is, of gegevensverwerking onder aanvaardbare voorwaarden plaatsvindt, en of de voorgestelde technische richting past bij bredere beleidsdoelen. De leverancier kan daarbij adviseren en uitvoeren, maar mag niet de feitelijke eigenaar worden van de strategische afweging. Een belangrijk risico is namelijk dat leveranciers hun klanten meenemen in een ontwikkelrichting die commercieel logisch is voor de leverancier, maar niet noodzakelijk aansluit bij de publieke of organisatorische belangen van de afnemer. Vooral bij grootschalige platformen en cloudomgevingen

is dit zichtbaar. Leveranciers bieden daarin niet alleen afzonderlijke producten aan, maar complete ecosystemen met eigen architectuurkeuzes, beveiligingsmodellen, ontwikkeltools, identiteitsvoorzieningen, opslagdiensten en integratiemogelijkheden. Wie eenmaal diep in zo'n ecosysteem opereert, gaat toekomstige keuzes vaak formuleren binnen de grenzen van dat ecosysteem. Nieuwe beleidswensen, organisatorische veranderingen of technologische innovaties worden dan beoordeeld aan de hand van de vraag of zij passen binnen de bestaande omgeving. De leverancier levert daarmee niet alleen technologie, maar structureert ook de denkruimte van de afnemer.

De vrijheid om een eigen koers te bepalen vereist dus dat een organisatie haar architectuur, kennispositie en besluitvorming zo inricht dat strategische keuzes niet vooraf worden ingesloten door één technologisch pad. Dat betekent dat de organisatie moet kunnen beoordelen welke ontwikkelingen zij zelf wenselijk vindt, welke innovaties zij wil volgen, welke risico's zij aanvaardbaar acht en welke afhankelijkheden zij bewust wil aangaan. Ook vraagt dit om een periodieke reflectie. Afhankelijkheden ontstaan immers geleidelijk. Wat bij de aanschaf nog een rationele keuze was, kan na verloop van tijd een strategische beperking zijn geworden. Organisaties moeten daarom niet alleen bij nieuwe investeringen, maar ook steeds tijdens het gebruik beoordelen of hun digitale omgeving nog wel volledig past bij hun eigen koers.

Deze vrijheid betekent overigens niet dat organisaties zich moeten afsluiten voor technologische ontwikkelingen. Een eigen koers bepalen veronderstelt juist dat een organisatie actief kan kiezen welke ontwikkelingen zij wil benutten. Een overheidsorganisatie moet nieuwe technologie kunnen adopteren wanneer dat past bij haar doelen, maar zij moet ook kunnen weigeren, vertragen, aanpassen of alternatieven onderzoeken wanneer dat nodig is.

5. Digitale soevereiniteit

5.1 Inleiding

In het vorige hoofdstuk is digitale autonomie benaderd als de feitelijke handelingsvrijheid van overheidsorganisaties. Dit hoofdstuk richt zich op digitale soevereiniteit: de vraag in hoeverre organisaties hun digitale infrastructuur, data en continuïteit kunnen beschermen tegen ongewenste bemoeienis van andere staten. Digitale soevereiniteit gaat daarmee niet alleen over de vestigingsplaats van een leverancier of de locatie van datacenters. Relevant is ook wie feitelijke zeggenschap heeft over de leverancier, welke rechtsmacht van toepassing is, welke partijen toegang hebben tot data en beheerlagen, hoe de onderliggende technologieketen is opgebouwd en of de dienstverlening kan worden voortgezet wanneer politieke, juridische of economische omstandigheden veranderen.

Voor publieke ICT-inkoop betekent dit dat aanbestedende diensten soevereiniteitsrisico's niet pas na gunning moeten beoordelen. Zij moeten al bij de voorbereiding van de aanbesteding bepalen welke eisen nodig zijn ten aanzien van eigendom, zeggenschap, datatoegang, onderaannemers, rechtsmacht, continuïteit en exit. Tegelijkertijd kent het aanbestedingsrecht grenzen: niet iedere wens om Europese of nationale leveranciers te bevoordelen is juridisch toegestaan. Daarbij is van belang dat het aanbestedingsrecht onderscheid maakt tussen enerzijds ondernemers uit de EU en uit landen met gedekte toegang tot de Europese aanbestedingsmarkt, en anderzijds ondernemers uit zogenoemde niet-gedekte derde landen.

Ondernemers uit deze niet gedekte landen hebben niet dezelfde aanspraak op gelijke behandeling als ondernemers uit de EU of uit gedekte landen. Een voorbeeld van zo'n land is China. Dat opent geen algemene vrijbrief voor willekeur, maar maakt wel duidelijk dat de Europese aanbestedingsmarkt niet volledig open hoeft te staan voor iedere derde-landpartij onder dezelfde voorwaarden. Dat is anders voor de landen met gedekte toegang. Daartoe behoren ondermeer Israël, de VS, Japan, Australië en Canada. Ondernemers uit deze landen hebben op grond van

het WTO Government Procurement Agreement (GPA) toegang tot bepaalde Europese aanbestedingen, waarbij zij niet ongunstiger mag worden behandeld dan de Europese leveranciers. Soevereiniteitseisen moeten daarom verband houden met de opdracht, objectief te rechtvaardigen zijn en proportioneel worden geformuleerd.

Dit hoofdstuk bespreekt welke aanbestedingsrechtelijke ruimte daarvoor bestaat. Achtereenvolgens komen aan de orde: eisen aan leveranciers en ketenpartijen, change of control-bepalingen, steward ownership, grip op de dataketen, het Cloud Sovereignty Framework en de mogelijkheden van aanbesteding onder defensie- en veiligheidsvoorwaarden.

5.2 Aanbestedingsrechtelijke ruimte voor soevereiniteitseisen

In het publieke debat wordt digitale soevereiniteit vaak vereenzelvigd met de locatie van data. De vraag is dan of gegevens binnen Nederland of binnen de Europese Unie worden opgeslagen.

Die vraag is relevant, maar onvoldoende. Dataopslag binnen de EU biedt geen volledige bescherming wanneer beheer, sleutelbeheer, support, eigendom, technische updates of besluitvorming over de continuïteit van de dienst buiten de EU liggen of onder invloed staan van een derde staat. Soevereiniteit betreft daarom niet alleen data residency, maar vooral feitelijke zeggenschap over de voorwaarden waaronder digitale diensten blijven functioneren en gegevens vertrouwelijk blijven. Deze benadering maakt digitale soevereiniteit tot een risicobegrip dat beter aansluit bij het aanbestedingsrecht dan enkel een algemene voorkeur voor een nationale of Europese leverancier.

Naast de opslagplaats van de data wordt ook vaak gevraagd of een leverancier in de Europese Unie is gevestigd. Die vraag is begrijpelijk, maar niet voldoende. Een leverancier kan formeel in de EU zijn gevestigd en toch onder beslissende invloed staan van een moedermaatschappij buiten de EU. Omgekeerd kan een Europese leverancier voor kritieke onderdelen afhankelijk zijn van niet-Europese infrastructuur, softwarecomponenten, supportteams of cloudplatformen. Vestiging is dus een belangrijk signaal, maar geen sluitend criterium.

Relevanter is de vraag waar de feitelijke zeggenschap ligt. Die zeggenschap kan juridisch, economisch, organisatorisch of technisch van aard zijn. Juridische zeggenschap betreft de vraag onder welke rechtsmacht de leverancier, groepsmaatschappijen en onderaannemers vallen. Economische zeggenschap betreft eigendom, financiering en afhankelijkheid van aandeelhouders of investeerders. Organisatorische zeggenschap betreft de vraag waar besluitvorming over beheer, beveiliging, continuïteit en incidentrespons plaatsvindt. Technische zeggenschap betreft de vraag wie toegang heeft tot systemen, data, sleutels, beheeromgevingen en updateprocessen.

Een aanbestedende dienst die digitale soevereiniteit wil borgen, zal daarom niet kunnen volstaan met een verklaring dat de dienst “Europees” is. Nodig is inzicht in de volledige controleketen. Wie is de contractspartij? Wie zijn de groepsmaatschappijen? Wie zijn de uiteindelijke belanghebbenden? Wie levert hosting, support, monitoring, identity management, encryptie, software-updates en netwerkdiensten? Welke onderdelen zijn essentieel voor continuïteit? Welke partijen kunnen feitelijk toegang krijgen tot data of beheerlagen? En welke partijen kunnen door een derde staat worden verplicht tot medewerking?

Deze vragen zijn aanbestedingsrechtelijk te vertalen naar transparantie-eisen, geschiktheidseisen, selectiecriteria, technische specificaties, gunningscriteria en contractuele uitvoeringsvoorwaarden. Daarbij moet telkens worden bewaakt dat de eis verband houdt met de opdracht en niet verder gaat dan nodig. Voor een laag-risicodienst kan een uitgebreide eigendomsanalyse disproportioneel zijn. Voor kritieke infrastructuur of gevoelige gegevensverwerking kan diezelfde analyse juist noodzakelijk zijn.

In het bijzonder kunnen eisen worden gesteld aan de wijze waarop leveranciers omgaan met wet- en regelgeving, toegang tot data en de mogelijkheid voor overheden om controle uit te oefenen op systemen. In een digitale context waarin gegevens en infrastructuur grensoverschrijdend zijn, is het relevant om rekening te houden met de invloed van buitenlandse rechtsordes op de beschikbaarheid en vertrouwelijkheid van data. Door te sturen op transparantie, controleerbaarheid, dataportabiliteit, open standaarden en beperking van afhankelijkheden van buitenlandse rechtsregimes, kunnen aanbestedende diensten

voorwaarden creëren die beter aansluiten bij Europese waarden en juridische kaders. In de praktijk zullen dergelijke eisen vaak beter kunnen worden ingevuld door leveranciers die binnen de Europese rechtsorde opereren, zonder dat dit expliciet als selectiecriterium wordt gehanteerd.

Het voorgaande kan worden vertaald naar concrete eisen in aanbestedingen. Door het stellen van objectieve en toetsbare voorwaarden kan binnen het bestaande juridische kader worden gestuurd op oplossingen die bijdragen aan digitale autonomie. Op grond van de AVG-verplichtingen van de aanbestedende dienst als verwerkingsverantwoordelijke kan bijvoorbeeld een eis worden gesteld zoals:

“De inschrijver en alle subverwerkers zijn niet onderworpen aan wetgeving van derde landen die de overheid van dat land het recht geeft ongecontroleerd toegang te vorderen tot persoonsgegevens die worden verwerkt in het kader van deze opdracht, tenzij de inschrijver aantoont dat een dergelijke vordering effectief kan worden geblokkeerd door EU-rechtsmiddelen.”

Deze eis is functioneel: hij sluit niet uit op grond van nationaliteit of eigendom, maar op grond van de juridische situatie van de verwerker. In de praktijk kunnen de meeste Amerikaanse aanbieders, voor zover zij onder de CLOUD Act vallen, niet aan deze eis voldoen, terwijl Europese aanbieders dat doorgaans wel kunnen. De rechtvaardiging voor deze eis is de AVG-verplichting van de aanbestedende dienst zelf. Dit maakt de eis proportioneel en koppelbaar aan het voorwerp van de opdracht.

Hieronder volgen nog enkele andere voorbeeldformuleringen:

“De inschrijver maakt inzichtelijk in hoeverre hij onderworpen is aan buitenlandse wetgeving die toegang tot data kan verplichten, en op welke wijze wordt gewaarborgd dat dergelijke toegang wordt voorkomen of gemitigeerd, waaronder alternatieve toeleveranciers, escrow-afspraken, data-portabiliteitsgaranties en exit-procedures”.

“De inschrijver waarborgt dat alle data worden opgeslagen, verwerkt en getransporteerd binnen de Europese Economische Ruimte, en dat deze data uitsluitend onderworpen zijn aan Europees en nationaal recht. Replicatie, back-up of failover naar locaties buiten deze jurisdictie is verboden en technisch uitgesloten.”

“De inschrijver treft passende technische en organisatorische maatregelen om te voorkomen dat data toegankelijk zijn voor autoriteiten op grond van buitenlandse rechtsregimes.”

“De inschrijver verschaft een analyse van de leveringsketen van de dienst, met identificatie van alle afhankelijkheden van buiten-EU-entiteiten (licentiehouders, subverwerkers, infrastructuurleveranciers, cloudplatforms, sleutelbeheer), vergezeld van een beoordeling van het risico dat buitenlandse overheidsmaatregelen de continuïteit raken.”

“De inschrijver verschaft een verklaring over de juridische structuur van de entiteit die de dienst feitelijk levert, waaruit blijkt in welke mate deze entiteit operationeel en juridisch zelfstandig beslissingen kan nemen ongeacht instructies van een buiten de EU gevestigde moederorganisatie.”

“De inschrijver toont aan dat de continuïteit van de dienstverlening gedurende de gehele looptijd van de overeenkomst niet afhankelijk is van toestemming, licenties, technische middelen of bedrijfsbesluiten van een buiten de Europese Unie gevestigde moederorganisatie of een derde partij die onderworpen is aan exportcontrole-wetgeving, sanctieregelgeving of andere overheidsbevelen van landen buiten de Europese Unie, die de dienstverlening aan de aanbestedende dienst kunnen beïnvloeden, opschorten of beëindigen zonder dat daartegen een effectieve rechtsmiddel open staat bij een EU-rechter.”

“De aanbestedende dienst behoudt zich het recht voor om inschrijvingen uit te sluiten indien onvoldoende waarborgen bestaan ten aanzien van controle, toezicht en naleving van toepasselijke EU wet- en regelgeving.”

Op die manier kan het aanbestedingsrecht juist een instrument voor digitale soevereiniteit zijn. Het dwingt de aanbestedende dienst om politieke en bestuurlijke zorgen te vertalen naar objectieve eisen. Dat maakt de aanbesteding juridisch robuuster en inhoudelijk preciezer. Niet de herkomst van een leverancier is daarbij beslissend, maar de mate waarin een andere statelijke actor invloed kan uitoefenen op de continuïteit van de bedrijfsvoering of op de vertrouwelijkheid van persoonsgegevens.

5.3 Change of control bepalingen

Een change of control-bepaling is een essentieel instrument om soevereiniteitsrisico's gedurende de looptijd van een ICT-contract te beheersen. Bij gunning beoordeelt de opdrachtgever de leverancier op basis van de toen bekende eigendomsstructuur, zeggenschapsverhoudingen, onderaannemers en risicobeheersing. Die uitgangssituatie kan echter veranderen. Een leverancier kan worden overgenomen, een moedermaatschappij kan wijzigen, zeggenschap kan verschuiven naar een investeerder uit een derde land, of een strategisch onderdeel kan worden ondergebracht bij een andere groepsmaatschappij.

Zonder change of control-bepaling kan de opdrachtgever in zo'n situatie feitelijk worden geconfronteerd met een andere risicopositie dan de positie waarop de oorspronkelijke gunning was gebaseerd. Dat is problematisch wanneer de opdracht betrekking heeft op gevoelige gegevens, vitale processen of kritieke digitale dienstverlening. De juridische contractspartij blijft mogelijk dezelfde, maar de feitelijke invloed op continuïteit en vertrouwelijkheid kan wezenlijk zijn veranderd.

Een goede change of control-bepaling bevat daarom ten minste een meldplicht. De leverancier moet voorgenomen of gerealiseerde wijzigingen in eigendom, zeggenschap, groepsstructuur, strategische samenwerking of essentiële onderaanneming tijdig melden. Die meldplicht moet voldoende ruim zijn geformuleerd om niet alleen formele aandelenoverdracht te omvatten, maar ook allerlei andere vormen van beslissende invloed. Denk aan stemrechten, contractuele zeggenschap, fusies, splitsingen, overdracht van bedrijfsonderdelen of financieringsconstructies die feitelijke controle kunnen opleveren.

Daarnaast moet de opdrachtgever kunnen onderzoeken of de wijziging gevolgen heeft voor de beveiliging, de continuïteit, de vertrouwelijkheid, de naleving van EU-regels of mogelijke beïnvloedbaarheid door een ander land. Daarvoor moet de leverancier dus niet alleen melden dát er iets gaat veranderen, maar tevens de relevante gegevens verstrekken waarmee de opdrachtgever kan beoordelen wat de mogelijke risico's zijn.

Afhankelijk van de ernst van het risico moet er de mogelijkheid zijn om bepaalde mitigerende acties te ondernemen. Denk aan het eisen van aanvullende waarborgen, een wijziging van onderaannemers, een recht op audit, de beperking van toegang, een tijdelijke opschorting van bepaalde werkzaamheden of in het uiterste geval de beëindiging van de overeenkomst.

5.4 Steward ownership als governance instrument

Steward ownership kan worden beschouwd als een governance-instrument om de zeggenschap over een onderneming te beschermen tegen zuiver financiële verkooplogica. De kern is dat de onderneming wordt ingericht rond continuïteit, missie en zelfstandigheid, in plaats van rond maximale handelbaarheid van aandelen. Wanneer de zeggenschap duurzaam is geborgd bij personen of organen die de missie van de onderneming bewaken, wordt het moeilijker om de onderneming zonder meer te verkopen aan een partij die onder invloed staat van een ongewenste statelijke actor. Daarmee kan steward ownership bijdragen aan voorspelbaarheid, continuïteit en vertrouwen.

Toch moet dit instrument aanbestedingsrechtelijk voorzichtig worden benaderd. Een aanbestedende dienst kan niet zonder meer eisen dat een leverancier een specifieke eigendoms- of governancevorm heeft. Zo'n eis kan disproportioneel zijn wanneer het onderliggende doel ook met minder beperkende middelen kan worden bereikt. Het doel is immers niet steward ownership als zodanig, maar het beperken van ongewenste zeggenschapswijzigingen en statelijke beïnvloedbaarheid. Een harde eis aan ondernemingsvorm zal daarom alleen in uitzonderlijke gevallen verdedigbaar zijn.

Wel kan steward ownership dienen als inspiratiebron voor contractuele en organisatorische waarborgen. Een opdrachtgever kan bijvoorbeeld eisen stellen aan continuïteit van zeggenschap, governanceafspraken over onafhankelijkheid, en verplichtingen om publieke belangen te borgen bij strategische wijzigingen. Zulke bepalingen kunnen vergelijkbare effecten hebben zonder dat één specifieke ondernemingsvorm wordt voorgeschreven.

Steward ownership is daarmee vooral relevant als denkkader. Het laat zien dat digitale soevereiniteit niet alleen technisch of juridisch wordt bepaald, maar ook door de institutionele inrichting van leveranciers. Wie zeggenschap heeft over een leverancier, bepaalt mede hoe de leverancier zich gedraagt bij geopolitieke druk, commerciële overnamebiedingen, wijziging van productstrategie of conflicten tussen publieke en private belangen.

5.5 Invloed op (persoons)gegevens in de dataketen

Veel soevereiniteitsrisico's ontstaan niet bij de gecontracteerde hoofdleverancier, maar dieper in de dataketen. Cloudaanbieders, hostingpartijen, supportafdelingen, loggingdiensten, leveranciers van softwareplugins, AI-diensten, beheerders en groepsmaatschappijen kunnen allemaal als onderaannemer een rol spelen bij de verwerking van gegevens of het beheer van systemen. Het is aanbestedingsrechtelijk toegestaan om te vragen welk deel van de opdracht in onderaanneming zal worden uitgevoerd, en welke onderaannemers daarvoor zijn voorzien.

Wanneer er door het ICT-product of de ICT-dienst persoonsgegevens worden verwerkt, biedt artikel 28 AVG een belangrijk juridisch aanknopingspunt. De hoofdleverancier, ook wel de verwerker genoemd, mag niet zonder voorafgaande specifieke of algemene schriftelijke toestemming van de opdrachtgever een zogeheten subverwerker inschakelen. Een subverwerker is aanbestedingsrechtelijk te beschouwen als een onderaannemer.

Bij algemene toestemming moet de verwerker wijzigingen in subverwerkers melden, zodat de verantwoordelijke bezwaar kan maken. Bovendien moeten aan subverwerkers vergelijkbare verplichtingen worden opgelegd als aan de hoofdverwerker.

Dit geeft overheidsorganisaties de mogelijkheid om grip te houden op de verwerkingsketen. Zij kunnen eisen dat subverwerkers vooraf inzichtelijk worden gemaakt, dat wijzigingen worden gemeld, dat verwerking buiten de EU of toegang vanuit derde landen wordt beperkt, dat beveiligingsmaatregelen worden doorgelegd en dat audit- of

informatieverplichtingen ook in de keten gelden. De AVG-keten maakt daarmee zichtbaar dat gegevensbescherming niet stopt bij de contractspartij.

Artikel 32 van de Data Act verbreedt deze ketenbenadering naar niet-persoonsgegevens en verplicht de aanbieders van data processing services om passende technische, organisatorische en juridische maatregelen te nemen, waaronder contractuele maatregelen, om internationale of derde-landse overheidstoegang tot en overdracht van niet-persoonsgegevens in de Unie te voorkomen wanneer die toegang of overdracht strijdig zou zijn met Unierecht of met het nationale recht van een lidstaat. Daarmee wordt duidelijk dat bescherming tegen derde-landse statelijke toegang niet alleen een beleidsmatige wens is, maar ook een expliciete verplichting onder Europees recht.

De bepaling bevat daarnaast regels voor de omgang met rechterlijke of administratieve beslissingen van derde landen. Een besluit van een derde-landse rechter, rechterlijke instantie of administratieve autoriteit dat een aanbieder verplicht om toegang te geven tot niet-persoonsgegevens in de Unie, wordt in beginsel alleen erkend of ten uitvoer gelegd wanneer daarvoor een internationale overeenkomst bestaat. Bij ontbreken van zo'n overeenkomst is toegang of overdracht slechts onder voorwaarden mogelijk. Daarbij gaat het onder meer om proportionaliteit, specificiteit van het verzoek en de mogelijkheid van rechterlijke toetsing in het derde land. Daardoor ontstaat een meer compleet juridisch kader voor soevereiniteit in de dataketen. Persoonsgegevens worden beheerst via de AVG, niet-persoonsgegevens via de Data Act.

Voor aanbestedende diensten betekent dit dat zij niet alleen een verwerkersovereenkomst moeten sluiten, maar ook bredere ketenafspraken moeten maken. Denk aan een actueel register van subverwerkers en andere ketenpartijen, meldplichten bij wijziging van supportlocaties of beheerpartijen, beperkingen op toegang vanuit derde landen, doorlegging van geheimhoudings- en beveiligingsverplichtingen, auditrechten, logging-verplichtingen en afspraken over de behandeling van verzoeken van buitenlandse autoriteiten.

De AVG en de Data Act bieden geen volledige oplossing voor digitale soevereiniteit, maar wel een juridisch stevig fundament. Zij maken duidelijk dat grip op data niet eindigt bij de hoofdleverancier en dat verwerking, toegang en overdracht in de keten controleerbaar moeten zijn. Digitale soevereiniteit vereist vervolgens dat deze wettelijke aanknopingspunten worden aangevuld met

contractuele, technische en organisatorische maatregelen die passen bij het risicoprofiel van de opdracht.

5.6 Cloud Sovereignty Framework

Recentelijk heeft ook de Europese Commissie een eigen beoordelingskader ontwikkeld voor de aanbesteding van soevereine clouddiensten. In plaats van te volstaan met de algemene vraag of een cloud “soverein” is, wordt in het Cloud Sovereignty Framework gekeken naar afzonderlijke doelstellingen en zogeheten assurance-niveaus. Daarmee wordt soevereiniteit meetbaar.

Deze benadering voorkomt dat een soevereine cloud wordt gereduceerd tot marketingtaal, omdat een aanbestedende dienst om bewijsbare maatregelen kan vragen in plaats van algemene beloften. Ook maakt deze benadering differentiatie mogelijk. Niet alle aan de cloud uitbestede werkzaamheden vereist immers hetzelfde niveau van soevereiniteit. Voor zeer gevoelige gegevens of kritieke processen kunnen bijvoorbeeld zwaardere eisen gelden dan voor minder risicovolle toepassingen. Dat maakt het mogelijk om proportioneel in te kopen.

Het framework berust op twee samenhangende beoordelingslagen. De eerste laag bestaat uit acht Sovereignty Objectives, aangeduid als SOV-1 tot en met SOV-8. Deze acht doelstellingen bepalen welke aspecten van soevereiniteit worden beoordeeld. De tweede laag bestaat uit de Sovereignty Effectiveness Assurance Levels, aangeduid als SEAL-0 tot en met SEAL-4. Deze niveaus geven aan welk soevereiniteitsniveau een aanbieder daadwerkelijk bereikt. Daarnaast kent het framework nog een Global Sovereignty Score, waarmee aanbiedingen die het vereiste minimum SEAL-niveau halen onderling kunnen worden vergeleken.

De SOV-systematiek geeft aan dat cloudsoevereiniteit kan worden beoordeeld vanuit acht verschillende invalshoeken.

SOV-1 betreft de strategische soevereiniteit. Daarbij staat de verankering van de aanbieder in het juridische, financiële en industriële ecosysteem van de EU of EER centraal. Beoordeeld wordt of de uiteindelijke beslissingsmacht binnen EU-jurisdictie ligt, hoe groot het risico is op

overname of overdracht aan niet-soevereine eigenaren, en in hoeverre Europese stakeholders invloed kunnen uitoefenen op de technologische en functionele roadmap van de aanbieder. Ook wordt gekeken naar de mate waarin de aanbieder afhankelijk is van niet-Europese financiering, naar investeringen, werkgelegenheid en waardecreatie binnen de EU of EER, naar betrokkenheid bij Europese initiatieven en naar het vermogen om veilige operaties voort te zetten wanneer ondersteuning door een leverancier wordt ingetrokken of verstoord.

SOV-2 ziet op de juridische en jurisdictionele soevereiniteit. Deze doelstelling beoordeelt het juridische kader waarbinnen de aanbieder en de dienst functioneren. Daarbij gaat het om de vraag welk nationaal recht van toepassing is op activiteiten en contracten, de blootstelling aan niet-Europese wetgeving met extraterritoriale werking, en de aanwezigheid van juridische, contractuele of technische routes waarlangs niet-Europese autoriteiten toegang tot data of systemen kunnen afdwingen. Ook internationale regimes, zoals exportcontrolemaatregelen, kunnen relevant zijn wanneer zij het gebruik of de overdracht van een clouddienst beperken. Daarnaast betreft het framework de locatie waar intellectuele eigendomsrechten kunnen ontstaan, geregistreerd en beheerd, en de jurisdictie waaronder die rechten vervolgens worden gehouden en gehandhaafd.

SOV-3 betreft data- en AI-soevereiniteit. Deze doelstelling richt zich op de bescherming, controle en onafhankelijkheid van data en AI-diensten binnen de EU of EER. Een centraal criterium is dat de klant, en niet de aanbieder, effectieve controle heeft over cryptografische toegang tot de data. Verder wordt gekeken naar inzicht in wanneer, waar en door wie data worden benaderd, inclusief auditmogelijkheden rond het gebruik van AI-modellen. Ook moet kunnen worden vastgesteld dat data onomkeerbaar worden verwijderd wanneer dat vereist is. Daarnaast beoordeelt het framework of de opslag en verwerking strikt binnen Europese jurisdicties blijven, zonder back up naar derde landen, en in hoeverre AI-modellen en dataverwerkingsketens onder Europese controle worden ontwikkeld, getraind, gehost en beheerd.

SOV-4 gaat over operationele soevereiniteit. Deze doelstelling ziet op het praktische vermogen van Europese actoren om de technologie te beheren, te ondersteunen en door te ontwikkelen zonder afhankelijkheid van buitenlandse controle. Criteria zijn onder meer de mogelijkheid om workloads te migreren of te integreren met alternatieve, door de EU gecontroleerde oplossingen zonder vendor lock-in, de capaciteit van Europese operators om de technologie te beheren en te onderhouden zonder niet-Europese leveranciersbetrokkenheid, en de aanwezigheid van een Europese kennisbasis om de dienst duurzaam te kunnen exploiteren. Ook wordt beoordeeld of operationele ondersteuning vanuit de EU wordt geleverd en uitsluitend aan EU- of EER-recht is onderworpen, en of technische documentatie, broncode en operationele knowhow beschikbaar zijn om langdurige autonomie mogelijk te maken.

SOV-5 betreft supply chain-soevereiniteit. Deze doelstelling richt zich op de herkomst, transparantie en weerbaarheid van de technologische toeleveringsketen. Het framework kijkt naar de geografische herkomst van belangrijke fysieke componenten en naar de landen waar hardware wordt geproduceerd of geassembleerd. Ook wordt gekeken naar de jurisdictie en herkomst van embedded code, firmware en software, inclusief de plaats waar software wordt ontworpen, geprogrammeerd, verpakt, gedistribueerd en geüpdatet. Verder wordt beoordeeld in welke mate de dienst afhankelijk is van niet-Europese leveranciers, faciliteiten of proprietary technologieën, en of de volledige leveranciers- en onderleveranciersketen inzichtelijk en controleerbaar is, inclusief auditrechten.

SOV-6 ziet op technologie-soevereiniteit. Deze doelstelling beoordeelt de openheid, transparantie en onafhankelijkheid van de onderliggende technologiystack. Belangrijke criteria zijn de mogelijkheid om met andere technologieën te integreren via goed gedocumenteerde en niet-proprietary API's of protocollen, en de mate waarin de oplossing gebruikmaakt van open standaarden. Ook wordt gekeken of software beschikbaar is onder open licenties, met rechten om te auditen, aan te passen en opnieuw te verspreiden. Daarnaast vraagt het framework om inzicht in ontwerp, werking, architectuur, datastromen en afhankelijkheden van de dienst.

SOV-7 betreft security- en compliance-sovereiniteit. Daarbij staat de vraag centraal in hoeverre beveiligingsoperaties, complianceverplichtingen en weerbaarheidsmaatregelen onder Europese controle staan. Criteria zijn onder meer het behalen van bepaalde certificeringen en de naleving van Europese kaders zoals de AVG, NIS2 en DORA. Verder wordt gekeken of security operations centres en incidentresponsteams uitsluitend onder Europese jurisdictie opereren, of de overheidsorganisatie of een bepaalde Europese autoriteit rechtstreeks toezicht kan houden op logging en monitoringfuncties, en of kwetsbaarheden en beveiligingsincidenten transparant, tijdig en EU-conform worden gerapporteerd. Ook is relevant of beveiligingspatches onafhankelijk van niet-Europese leveranciers kunnen worden ontwikkeld, getest en toegepast, en of Europese entiteiten onafhankelijke beveiligings- en compliance-audits met volledige toegang kunnen uitvoeren.

SOV-8 ziet tot slot op duurzaamheid. Deze doelstelling beoordeelt de autonomie en weerbaarheid van clouddiensten op langere termijn in relatie tot energiegebruik, afhankelijkheden en schaarste aan grondstoffen. Het framework kijkt naar energie-efficiënte infrastructuur, bijvoorbeeld aan de hand van lage PUE-waarden en meetbare verbeterdoelen. Ook worden circulaire praktijken betrokken, zoals hergebruik, refurbishment en verantwoorde verwerking van hardware aan het einde van de levensduur. Verder wordt beoordeeld of de aanbieder transparant rapporteert over CO₂-uitstoot, watergebruik en andere duurzaamheidsindicatoren, en of infrastructuur en operaties worden aangedreven door hernieuwbare of koolstofarme energie.

De Global Sovereignty Score wordt berekend aan de hand van deze acht SOV-doelstellingen, die ieder een eigen gewicht krijgen. De exacte waardering van antwoorden kan door aanbestedende diensten zelf worden aangepast, maar de kern blijft dat de score systematisch wordt opgebouwd uit de acht verschillende soevereiniteitsdimensies.

Deze SOV-doelstellingen bepalen dus de inhoudelijke breedte van de beoordeling. De SEAL-systematiek bepaalt vervolgens welk effectief soevereiniteitsniveau wordt gehaald.

SEAL-0 betekent dat geen sprake is van soevereiniteit: de dienst, technologie of de processen staan exclusief onder de controle van niet-Europese derde partijen en worden volledig binnen niet-Europese jurisdicties beheerst.

SEAL-1 duidt op jurisdictionele soevereiniteit: het EU-recht is formeel van toepassing, maar de praktische afdwingbaarheid is beperkt doordat de dienst, technologie of processen nog steeds exclusief onder controle staan van niet-Europese derde partijen.

SEAL-2 wordt aangeduid als data-soevereiniteit: EU-jurisdicties zijn van toepassing, maar materiële afhankelijkheden blijven bestaan en de dienst, technologie of de processen staan indirect onder controle van niet-Europese derde partijen.

SEAL-3 staat voor technologische soevereiniteit: EU-jurisdicties zijn van toepassing en Europese actoren oefenen betekenisvolle, maar nog niet volledige invloed uit.

SEAL-4 staat voor volledige digitale soevereiniteit: technologie en processen staan volledig onder EU-controle, uitsluitend onder EU-jurisdictie en zonder kritieke niet-Europese afhankelijkheden.

De Commissie wijst erop dat SEAL-4 weliswaar relevant is als hoogste niveau, maar op dit moment beperkt toepasbaar is vanwege bestaande afhankelijkheden van specifieke toeleveringsketens, zoals chips en hardware. Dat is een belangrijk inzicht. Het framework gaat dus niet uit van de fictie dat volledige onafhankelijkheid eenvoudig kan worden ingekocht, maar biedt een methode om verschillende niveaus van soevereiniteit zichtbaar en vergelijkbaar te maken.

De beoordeling in het framework berust op vragen, antwoorden, bewijsstukken en verificatie door de aanbestedende dienst. Per soevereiniteitsdoelstelling worden specifieke doelstellingen onderscheiden, waarvoor inschrijvers antwoorden moeten geven. Die antwoorden worden gekoppeld aan scores en SEAL-niveaus. De aanbestedende dienst bepaalt vooraf welk minimum-SEAL-niveau voor de opdracht vereist is. Een aanbieding die dat minimumniveau niet haalt, voldoet niet aan de

soevereiniteitseis, ook wanneer zij op andere onderdelen goed scoort. De Global Sovereignty Score is een aanvullend instrument om aanbiedingen te vergelijken die de vereiste SEAL wel behalen. Het framework hanteert daarbij als uitgangspunt dat het totale SEAL-niveau wordt bepaald door het laagste SEAL-niveau dat op een van de relevante doelstellingen of criteria wordt bereikt. Daarmee wordt voorkomen dat een ernstige zwakte op één kritiek onderdeel wordt gecompenseerd door hoge scores op minder kritieke onderdelen.

De aanbestedende dienst beoordeelt vervolgens of de gestelde mate van soevereiniteit daadwerkelijk wordt onderbouwd door documenten, verklaringen en publiek beschikbare informatie. Het framework is daarmee niet uitsluitend een zelfverklaring van de leverancier, maar vraagt om inhoudelijke beoordeling en controle door de aanbestedende dienst. Indien een aanbestedende dienst dit framework wil gaan toepassen, dan valt het zeer aan te bevelen de Implementation Guidance door te lezen.²⁰

Voor aanbestedende diensten biedt het Cloud Sovereignty Framework een praktisch instrument om soevereiniteitsambities te vertalen naar in een aanbesteding bruikbare criteria. Zij kunnen vooraf bepalen welk SEAL-niveau voor een bepaalde opdracht minimaal vereist is, inschrijvers vragen om gestructureerde informatie en bewijsstukken, en vervolgens aanbiedingen die aan het minimumniveau voldoen vergelijken op basis van een gewogen score. Zo wordt digitale soevereiniteit een toetsbaar onderdeel van de aanbestedingsprocedure.

5.7 Aanbesteden onder defensie en veiligheidsvoorwaarden

Naast het Cloud Sovereignty Framework kan ook de ‘Aanbestedingswet op defensie- en veiligheidsgebied’ relevant zijn voor ICT-aanbestedingen waarbij digitale soevereiniteit, nationale veiligheid, vertrouwelijkheid en continuïteit een centrale rol spelen. De ADV is daarbij niet alleen van belang voor het Ministerie van Defensie of voor klassieke veiligheidsdiensten. De toepasselijkheid van die wet wordt namelijk niet uitsluitend bepaald door de rol van de aanbestedende dienst, maar vooral door de

²⁰ https://commission.europa.eu/news-and-media/news/sovereign-cloud-framework-explained-2026-06-01_en

aard van de opdracht. Daarom kunnen ook de andere departementen, de gemeentes, provincies, waterschappen en allerlei andere aanbestedende diensten onder omstandigheden met de ADV te maken krijgen.

Het meest in het oog springende verschil met de reguliere Aanbestedingswet is dat de ADV de mogelijkheid kent om ondernemers die niet binnen de Europese Unie zijn gevestigd van deelname aan een aanbestedingsprocedure uit te sluiten. Die mogelijkheid mag echter niet worden losgemaakt van het toepassingsbereik van de ADV. De ADV kan niet worden gekozen omdat een aanbestedende dienst het wenselijk vindt om Europese leveranciers te bevoordelen of niet-Europese leveranciers te weren. Eerst moet de opdracht zelf onder het defensie- of veiligheidsregime vallen. Bij ICT-aanbestedingen zal dat met name aan de orde kunnen zijn wanneer sprake is van gevoelige diensten, gevoelige leveringen of gevoelige werken. Daarvoor is niet voldoende dat een systeem bedrijfskritisch is, persoonsgegevens verwerkt of bestuurlijk belangrijk is. De opdracht moet daadwerkelijk bestemd zijn voor veiligheidsdoeleinden en verband houden met gerubriceerde gegevens, of dergelijke gegevens noodzakelijk maken of bevatten. De toepassing van de ADV vraagt daarom om een voorafgaande kwalificatie van de opdracht: welk veiligheidsdoel wordt gediend, welke informatie is gerubriceerd, welke gevolgen heeft verstoring of ongeautoriseerde toegang voor nationale veiligheid, en waarom is het reguliere aanbestedingsregime ontoereikend?

Bij ICT kan een ADV-relevante situatie zich bijvoorbeeld wel voordoen bij systemen voor crisisbeheersing, beveiligde communicatie, meldkamers, politie- of opsporingstoepassingen, grensbewaking, terrorismebestrijding, bescherming van vitale infrastructuur of digitale voorzieningen die rechtstreeks samenhangen met gerubriceerde informatie. Ook software, hardware, beheer- of beveiligingsdiensten voor vitale processen kunnen onder omstandigheden binnen het veiligheidsdomein vallen. Doorslaggevend is niet het etiket dat de aanbestedende dienst op de opdracht plakt, maar de objectieve functie van de ICT binnen het veiligheidsbelang.

Wanneer de ADV terecht kan worden toegepast, beschikt de aanbestedende dienst over verschillende instrumenten die relevant zijn voor digitale soevereiniteit. Naast de mogelijkheid om niet-EU-ondernemers uit te sluiten, kan zij strengere eisen stellen aan

betrouwbaarheid, gegevensbeveiliging, leveringszekerheid, continuïteit en onderaanneming. Ook kan zij eisen dat onderaannemers aan vergelijkbare beveiligings- en betrouwbaarheidsvoorwaarden voldoen als de hoofdleverancier. Dat is bij ICT-opdrachten van groot belang, omdat de feitelijke risico's vaak niet uitsluitend bij de contractuele hoofdleverancier liggen, maar ook bij hostingpartijen, softwareleveranciers, beheerders, supportteams, security operations centres, netwerkleveranciers en andere ketenpartijen.

Tegelijkertijd moet het onderscheid met de reguliere Aanbestedingswet niet worden overdreven. Veel maatregelen die in een soevereiniteitscontext relevant zijn, kunnen ook binnen het reguliere aanbestedingsrecht worden getroffen. Daarmee is de ADV een krachtig maar begrensd instrument. Zij kan niet worden gebruikt als algemene route om bij ICT-aanbestedingen een Europese industriepolitieke voorkeur te realiseren. Zij kan wel van betekenis zijn wanneer digitale afhankelijkheid samenvalt met defensie- of veiligheidsbelangen en wanneer de opdracht daadwerkelijk binnen het toepassingsbereik van de wet valt. In dat geval biedt de ADV een juridisch kader om continuïteit, vertrouwelijkheid, ketenbeheersing en beperking van derde-landinvloed scherper te borgen dan onder het reguliere aanbestedingsregime doorgaans mogelijk is.

5.8 Zonder digitale autonomie geen soevereiniteit

Digitale soevereiniteit gaat over de bescherming van continuïteit en vertrouwelijkheid tegen ongewenste statelijke beïnvloeding. Die bescherming kan niet worden bereikt door één enkel criterium, zoals datalocatie of Europese vestiging. Zij vereist een samenhangende beoordeling van rechtsmacht, eigendom, zeggenschap, beheer, onderaanneming, technische afhankelijkheden, contractuele waarborgen en operationele alternatieven.

Het Europese aanbestedingsrecht biedt daarvoor meer ruimte dan vaak wordt aangenomen. Het laat geen willekeurige nationaliteitsvoorkeur toe, maar wel objectieve en proportionele eisen die verband houden met veiligheid, continuïteit, gegevensbescherming en leveringszekerheid.

Toch blijft het belangrijk te realiseren dat digitale soevereiniteit niet zelfstandig kan bestaan en niet volledig bereikt kan worden zonder digitale autonomie. Soevereiniteit veronderstelt dat een organisatie handelingsvrijheid bezit. Een organisatie die niet vrij is om te kunnen samenwerken, te kunnen migreren, publieke waarden te kunnen realiseren, collectief te kunnen ontwikkelen en inkopen, en een eigen digitale koers te kunnen bepalen, kan statelijke beïnvloedbaarheid slechts beperkt tegengaan.

Bijlage 1: Voorbeeldclausules

Deze bijlage bevat voorbeeldclausules voor ICT-aanbestedingen en ICT-contracten. Deze clausules zijn niet bedoeld als standaardoplossingen die zomaar zonder context kunnen worden overgenomen, maar als praktische vertaling van de uitgangspunten uit het boek. De opsomming is bovendien niet limitatief. De voorbeelden maken vooral zichtbaar hoe abstracte begrippen als leveranciersafhankelijkheid, interoperabiliteit, dataportabiliteit, exit, open source en soevereiniteit zouden kunnen worden omgezet in concrete contractuele verplichtingen. Meer voorbeeldclausules zijn te vinden in paragraaf 5.2 van dit boek, en tevens op de website van het Forum Standaardisatie (<https://www.forumstandaardisatie.nl/beslisboom/beslisboom-open-standaarden>), de website van Opensourcowerken (www.opensourcowerken.nl), en de website van de ICO-wizard (<https://www.bio-overheid.nl/ico-wizard/>).

De clausules zijn gegroepeerd naar het type afhankelijkheid dat zij beogen te voorkomen of te beheersen. Bij iedere clause wordt met een label aangegeven waar zij doorgaans thuishoort:

Label A : Te gebruiken in de aanbestedingsdocumenten.

Label C : Te gebruiken in de contracten.

Label A/C : De verplichting moet al in de aanbesteding worden aangekondigd en na gunning contractueel worden uitgewerkt.

De hoofdregel is dat verplichtingen die na gunning afdwingbaar moeten zijn, al voldoende duidelijk in de aanbestedingsstukken moeten zijn aangekondigd. De aanbesteding bepaalt de eisen en wensen, waarna het contract vervolgens de afdwingbaarheid bepaalt.

A. Open architectuur

Deze clausules worden gebruikt wanneer de oplossing moet kunnen samenwerken met andere systemen, ketenpartners, leveranciers of toekomstige alternatieven. Zij zijn relevant bij vrijwel iedere ICT-aanbesteding waarin data, koppelingen, API's, standaarden of documentatie een rol spelen.

Open standaarden 'Pas toe of leg uit'

Label: A/C

De oplossing ondersteunt en gebruikt de voor de opdracht relevante open standaarden, waaronder in ieder geval de toepasselijke wettelijk verplichte standaarden en de relevante standaarden zoals vastgesteld op de lijst van het Forum Standaardisatie (<https://www.forumstandaardisatie.nl>), conform het verplichte "pas toe of leg uit"-beleid voor de overheid.

Voor zover relevant en van toepassing op de aard van de opdracht, worden minimaal de volgende standaarden ondersteund, dan wel hun logische opvolgers:

>> hieronder komt de lijst met standaarden vanuit de beslisboom <https://www.forumstandaardisatie.nl/beslisboom/beslisboom-open-standaarden> <<

- [Standaard 1]
- [Standaard 2]
- ...

Afwijking is slechts toegestaan indien inschrijver gemotiveerd aantoont dat toepassing technisch onmogelijk of disproportioneel is en de aanbestedende dienst deze motivering schriftelijk accepteert.

Op eerste verzoek dient inschrijver de naleving van de verplichte standaarden aan te tonen door:

- a. Voor internetgerichte diensten: een actuele rapportage van internet.nl (niet ouder dan 3 maanden voor indiening);

- b. Voor koppelvlakstandaarden: technische documentatie waaruit de implementatie blijkt (optioneel: inclusief een testrapport of conformiteitsverklaring van een onafhankelijke derde);
- c. Voor overige standaarden: een ondertekende eigen verklaring, te bevestigen door middel van een demonstratie of audit op verzoek van de aanbestedende dienst voorafgaand aan of na de gunning.

Interoperabiliteit en koppelvlakken

Label: A/C

De oplossing beschikt over goed gedocumenteerde koppelvlakken waarmee integratie met systemen van de aanbestedende dienst, ketenpartners en door de aanbestedende dienst aangewezen derden mogelijk is. Deze koppelvlakken zijn gebaseerd op open standaarden.

API-toegang en wijzigingen

Label: C

Opdrachtnemer stelt gedurende de looptijd van de overeenkomst de voor integratie, beheer, audit, rapportage en migratie noodzakelijke API's beschikbaar. Opdrachtnemer kondigt wijzigingen in API's, dataformaten, koppelvlakken of authenticatiemechanismen ten minste [x] maanden vooraf schriftelijk aan en biedt gedurende een redelijke overgangstermijn ondersteuning voor bestaande koppelingen.

Dataportabiliteit en testexport

Label: A/C

Alle door of namens opdrachtgever verwerkte data, metadata, configuratiegegevens en voor interpretatie noodzakelijke contextinformatie kunnen worden geëxporteerd in een open, gestructureerd, gangbaar en machineleesbaar formaat. Op verzoek van opdrachtgever voert opdrachtnemer ten minste eenmaal per jaar een testexport uit om de feitelijke overdraagbaarheid te verifiëren.

B. Exit, migratie en overstapbaarheid

Deze clausules worden gebruikt wanneer de opdrachtgever wil waarborgen dat hij aan het einde van de overeenkomst, of eerder bij noodzaak, daadwerkelijk kan overstappen naar een andere leverancier of een eigen

omgeving. Zij zijn vooral van belang bij cloud-, SaaS-, PaaS-, IaaS-, en hostingdienstverlening.

Exitplan bij aanvang

Label: A/C

Opdrachtnemer levert binnen [x] weken na ingangsdatum van de overeenkomst een exitplan op. Het exitplan beschrijft ten minste de te exporteren data, metadata, configuraties, documentatie, koppelingen, afhankelijkheden, overdrachtsstappen, benodigde medewerking van opdrachtnemer, verwachte doorlooptijden, risico's en kosten. Het exitplan wordt jaarlijks geactualiseerd.

Medewerkingsplicht bij migratie

Label: C

Opdrachtnemer verleent volledige, tijdige en deskundige medewerking aan migratie naar een opvolgende leverancier, een door opdrachtgever aangewezen derde of een eigen omgeving van opdrachtgever. Deze medewerking omvat ten minste ondersteuning bij data-export, overdracht van documentatie, toelichting op configuraties, overdracht van koppelvakinformatie, ondersteuning bij testmigraties en beantwoording van redelijke vragen van de opvolgende partij.

Geen overstapbelemmeringen

Label: A/C

Opdrachtnemer werpt geen technische, contractuele, commerciële of organisatorische belemmeringen op die overstap naar een andere leverancier of naar een eigen omgeving van opdrachtgever bemoeilijken. Voor cloud-, SaaS-, PaaS- en IaaS-diensten geldt dat opdrachtnemer de toepasselijke verplichtingen inzake switching en dataportabiliteit uit de Data Act naleeft.

C. Rechten op software, maatwerk en open source

Deze clausules worden gebruikt wanneer software, maatwerk, configuraties, scripts, documentatie of open source componenten onderdeel zijn van de opdracht. Zij zijn vooral relevant wanneer de opdrachtgever de oplossing later door een derde wil laten beheren, aanpassen, hergebruiken of migreren

Gebruiksrechten voor beheer en doorontwikkeling

Label: A/C

Oprachtgever verkrijgt alle gebruiksrechten die noodzakelijk zijn om de oplossing gedurende en na afloop van de overeenkomst te gebruiken, te beheren, te laten beheren, te onderhouden, te laten onderhouden, te koppelen, te migreren en te laten doorontwikkelen door een derde. Deze rechten zijn niet afhankelijk van voortzetting van dienstverlening door opdrachtnemer.

Open source componenten en SBOM

Label: A/C

Inschrijver verstrekt een overzicht van de in de oplossing gebruikte open source componenten en overige derde-partijcomponenten, inclusief licenties, versies en bekende afhankelijkheden. Opdrachtnemer houdt dit overzicht gedurende de looptijd actueel en verstrekt op verzoek een software bill of materials in een gangbaar formaat.

Open source als gunningscriterium 1

Label: A

De aanbestedende dienst geeft bij gelijke geschiktheid de voorkeur aan een oplossing die wordt geleverd onder een open source licentie. Onder open source licentie wordt verstaan een licentie die de gebruiker ten minste het recht geeft de software te gebruiken, te bestuderen, te kopiëren, te wijzigen en te verspreiden, al dan niet in gewijzigde vorm.

Van gelijke geschiktheid is sprake wanneer de aangeboden oplossing in voldoende mate geschikt is om de gevraagde werkzaamheden uit te voeren en het beoogde resultaat te bereiken. Gelijke geschiktheid vereist niet dat de oplossing identiek is aan een proprietary of closed source alternatief, noch dat zij dezelfde gebruikerservaring, leveranciersorganisatie of exacte functionaliteiten biedt.

De voorkeur voor open source software wordt in deze aanbesteding geëffectueerd door [x] punten toe te kennen aan inschrijvingen waarbij de aangeboden oplossing onder een open source licentie beschikbaar is. Deze punten worden uitsluitend toegekend indien inschrijver aantoont dat de licentie daadwerkelijk ziet op de kernfunctionaliteit van de aangeboden

oplossing en niet slechts op ondergeschikte componenten, ontwikkeltools of algemene softwarebibliotheken.

Open source als gunningscriterium 2

Label: A

Bij de beoordeling van de kwaliteit van de inschrijving kent de aanbestedende dienst waarde toe aan de mate waarin de aangeboden oplossing z aan leveranciersafhankelijkheid door toepassing van open source software. Daarbij wordt beoordeeld:

- a. welk deel van de kernfunctionaliteit onder een open source licentie beschikbaar is;
- b. of de broncode beschikbaar is voor opdrachtgever en derden;
- c. of opdrachtgever gerechtigd is de software te gebruiken, te bestuderen, te wijzigen en te laten wijzigen;
- d. of meerdere marktpartijen in staat zijn beheer, onderhoud, support of doorontwikkeling te leveren;
- e. of de gekozen licentie hergebruik door andere overheidsorganisaties mogelijk maakt;
- f. of de oplossing voorkomt dat opdrachtgever afhankelijk blijft van één leverancier voor beheer, onderhoud of doorontwikkeling.

Een hogere score wordt toegekend naarmate de open source beschikbaarstelling concreter, ruimer en relevanter is voor de kernfunctionaliteit van de oplossing.

Gebruik van open source tools

Label: A/C

Een oplossing wordt voor de toepassing van deze aanbesteding niet als open source oplossing aangemerkt enkel omdat zij gebruikmaakt van open source componenten, open source ontwikkeltools of open source bibliotheken. De open source kwalificatie ziet uitsluitend op de software of onderdelen daarvan die wezenlijk zijn voor de door opdrachtgever gevraagde kernfunctionaliteit.

Opdrachtnemer staat ervoor in dat de door hem als open source aangemerkte onderdelen daadwerkelijk beschikbaar zijn onder de opgegeven open source licentie en dat opdrachtgever deze onderdelen

overeenkomstig die licentie kan gebruiken, bestuderen, wijzigen, laten wijzigen, kopiëren, verspreiden en hergebruiken.

Open source maatwerkontwikkeling

Label: A/C

De opdrachtnemer dient het project vanaf de start volledig Open Source te ontwikkelen onder de EUPL licentie, v1.2 of later.

- De broncode, documentatie en andere relevante ontwikkelbestanden worden in een publiek toegankelijke repository beheerd.
- De repository dient up-to-date te worden gehouden met alle wijzigingen, inclusief documentatie van de gemaakte keuzes.
- Eventuele vergadernotities, roadmap en technische beslissingen worden gedeeld in een openbaar toegankelijke omgeving, tenzij er gegronde redenen zijn om bepaalde informatie niet te publiceren (bijvoorbeeld beveiligingsrisico's).
- De opdrachtnemer volgt open source best practices, waaronder versiebeheer, issue-tracking en community-interactie.

D. Privacy, veiligheid en compliance

Deze clausules worden gebruikt wanneer een digitale voorziening gevolgen kan hebben voor burgers, publieke dienstverlening, gegevensbescherming, toegankelijkheid, veiligheid of verantwoording.

Privacy by design en security by design

Label: A/C

De oplossing wordt ontworpen, ingericht en beheerd volgens de beginselen van privacy by design, privacy by default en security by design. Inschrijver beschrijft welke technische en organisatorische maatregelen worden getroffen om gegevensminimalisatie, toegangsbeperking, logging, beveiliging, controleerbaarheid en passende bewaartermijnen te waarborgen.

Toegankelijkheid en inclusiviteit

Label: A/C

De oplossing voldoet aan de toepasselijke toegankelijkheidseisen voor digitale dienstverlening. Opdrachtnemer zorgt ervoor dat de oplossing zodanig wordt ontworpen en beheerd dat burgers en gebruikers niet

zonder objectieve rechtvaardiging worden uitgesloten of ongelijk worden behandeld.

Auditability en verantwoording

Label: C

Opdrachtnemer zorgt ervoor dat de werking van de oplossing, de verwerking van gegevens, relevante beslisregels, logging en beheerhandelingen controleerbaar zijn. Opdrachtgever heeft het recht om audits te laten uitvoeren op naleving van wettelijke verplichtingen, beveiligingseisen, publieke waarden en contractuele afspraken.

E. Ketencontrole en toegang tot data

Deze clausules worden gebruikt wanneer naast de hoofdleverancier ook onderaannemers, subverwerkers, hostingpartijen, supportteams, beheerders of andere ketenpartijen betrokken zijn. Zij zijn vooral relevant bij cloud, SaaS, uitbesteed beheer en internationale technologieketens.

Opgave van ketenpartijen

Label: A/C

Inschrijver verstrekt een volledig en actueel overzicht van alle onderaannemers, subverwerkers, hostingpartijen, supportpartijen, beheerpartijen en overige kritieke ketenpartijen die betrokken zijn bij de uitvoering van de opdracht of feitelijke toegang kunnen hebben tot data, systemen, beheerlagen of logging.

Toestemming voor kritieke ketenwijzigingen

Label: C

Opdrachtnemer mag geen nieuwe kritieke onderaannemer, subverwerker, hostingpartij, supportpartij of beheerpartij inschakelen zonder voorafgaande schriftelijke toestemming van opdrachtgever. Opdrachtgever kan toestemming weigeren wanneer de wijziging leidt tot onaanvaardbare risico's voor continuïteit, vertrouwelijkheid, gegevensbescherming, digitale autonomie of digitale soevereiniteit.

Doorlegging van verplichtingen

Label: C

Opdrachtnemer legt alle verplichtingen uit deze overeenkomst die relevant zijn voor beveiliging, privacy, vertrouwelijkheid, dataportabiliteit, exit, audit, documentatie, continuïteit en soevereiniteit schriftelijk op aan zijn ketenpartijen. Opdrachtnemer blijft volledig verantwoordelijk voor de naleving van deze verplichtingen door ketenpartijen.

Verzoeken van buitenlandse autoriteiten

Label: C

Opdrachtnemer meldt ieder verzoek van een buitenlandse autoriteit om toegang tot data, systemen, metadata, logging, beheeromgevingen of andere informatie van opdrachtgever onverwijld aan opdrachtgever. Opdrachtnemer verleent geen toegang indien die toegang strijdig is met Unierecht, Nederlands recht of de overeenkomst, en treft redelijke maatregelen om onrechtmatige of disproportionele verzoeken te betwisten.

F. Digitale soevereiniteit en zeggenschap

Deze clausules worden gebruikt wanneer de opdracht gevoelig is voor statelijke beïnvloeding, derde-landwetgeving, wijziging van eigendom of zeggenschap, of afhankelijkheid van niet-Europese ketenpartijen. Zij zijn vooral relevant bij kritieke voorzieningen, gevoelige data, cloudinfrastructuur en vitale processen. Zij zijn ook bruikbaar om uitkomsten van een soevereiniteitsbeoordeling, zoals een SEAL-niveau, contractueel vast te leggen. Zie overigens ook de clausules die al als voorbeeld zijn opgenomen in paragraaf 5.2.

Eigendom, zeggenschap en groepsstructuur

Label: A/C

Inschrijver verstrekt inzicht in zijn eigendomsstructuur, uiteindelijke zeggenschap, groepsmaatschappijen, relevante moedermaatschappijen en rechtsmacht waaronder deze partijen vallen. Inschrijver vermeldt tevens of en in hoeverre hij, zijn moedermaatschappijen of kritieke ketenpartijen zijn blootgesteld aan wetgeving van derde landen die toegang tot data, systemen of dienstverlening kan beïnvloeden.

Behoud van soevereiniteitsniveau

Label: C

Indien inschrijver in de aanbesteding een bepaald soevereiniteitsniveau, SEAL-niveau of vergelijkbare kwalificatie heeft opgegeven, geldt dit niveau als contractuele minimumverplichting. Opdrachtnemer meldt iedere omstandigheid die dit niveau kan verlagen onverwijld aan opdrachtgever en treft op eerste verzoek passende herstel- of mitigerende maatregelen.

Change of control

Label: C

Opdrachtnemer meldt iedere voorgenomen of gerealiseerde wijziging in eigendom, zeggenschap, groepsstructuur, uiteindelijke belanghebbenden of beslissende invloed onverwijld aan opdrachtgever. Opdrachtgever heeft het recht om te beoordelen of deze wijziging leidt tot een onaanvaardbaar risico voor continuïteit, vertrouwelijkheid, gegevensbescherming of digitale soevereiniteit. Indien daarvan sprake is, kan opdrachtgever aanvullende waarborgen verlangen of de overeenkomst beëindigen.

G. Continuïteit, roadmap en wijzigingsbeheer

Deze clausules worden gebruikt wanneer de opdrachtgever gedurende de looptijd afhankelijk is van beschikbaarheid, ondersteuning, updates, productontwikkeling of licentievoorwaarden van de leverancier.

Continuïteitsplan

Label: A/C

Inschrijver beschrijft welke maatregelen worden getroffen om de continuïteit van de dienstverlening te waarborgen bij storingen, beveiligingsincidenten, uitval van ketenpartijen, faillissement, beëindiging van ondersteuning of andere verstoringen. Opdrachtnemer houdt gedurende de looptijd een actueel continuïteitsplan beschikbaar en test dit ten minste eenmaal per jaar.

Roadmaptransparantie

Label: C

Opdrachtnemer informeert opdrachtgever tijdig over relevante wijzigingen in de productroadmap, waaronder beëindiging van ondersteuning, uitfasering van functionaliteit, wijziging van licentiemodellen, wijziging

van technische vereisten of wijzigingen die gevolgen kunnen hebben voor interoperabiliteit, dataportabiliteit, beveiliging, publieke waarden of exit.

Wijzigingen met wezenlijke impact

Label: C

Opdrachtnemer voert geen wijziging door die wezenlijke gevolgen heeft voor functionaliteit, beveiliging, interoperabiliteit, dataportabiliteit, toegang tot data, kostenstructuur of exitmogelijkheden zonder voorafgaande schriftelijke melding aan opdrachtgever. Opdrachtgever heeft het recht om aanvullende waarborgen, een overgangstermijn of een alternatief te verlangen.

H. Financiële transparantie

Deze clausules worden gebruikt wanneer de totale kosten van de oplossing niet volledig blijken uit de initiële prijs. Zij zijn vooral relevant bij abonnementsmodellen, cloudgebruik, licenties, dataverkeer, aanvullende modules, support, integraties en exit.

Total cost of ownership

Label: A

Inschrijver verstrekt een volledig overzicht van de verwachte kosten gedurende de gehele levenscyclus van de oplossing. Dit overzicht omvat ten minste implementatiekosten, licentie- of abonnementskosten, beheerkosten, supportkosten, integratiekosten, kosten voor uitbreiding, migratiekosten, exportkosten en exitkosten.

Transparantie over prijsmodel

Label: A/C

Inschrijver beschrijft het gehanteerde prijsmodel volledig en transparant. Kosten die afhankelijk zijn van gebruiksvolume, dataverkeer, opslag, API-gebruik, support, koppelingen, extra modules, export of beëindiging worden afzonderlijk gespecificeerd. Niet-gespecificeerde kosten kunnen na gunning niet aan opdrachtgever in rekening worden gebracht.

Kostenplafond voor exit en migratie

Label: C

Voor exit- en migratieondersteuning gelden de tarieven en kostenplafonds zoals opgenomen in de prijsbijlage. Opdrachtnemer brengt geen aanvullende kosten in rekening voor activiteiten die noodzakelijk zijn om data, documentatie, configuraties of andere overeengekomen onderdelen over te dragen, tenzij opdrachtgever vooraf schriftelijk met die kosten heeft ingestemd.

Gebruik van Generatieve AI

Bij dit boek is op twee manieren gebruikgemaakt van Vlam-chat, de AI-assistent voor de Rijksoverheid, gebaseerd op Mistral Medium 3:

- Vlam-chat heeft de teksten gereviewd op flow, taalgebruik, spelling en grammatica.
- Vlam-chat is gevraagd concrete suggesties te doen voor verbetering. De overgenomen suggesties betroffen het toevoegen van een terugblik aan de inleidende paragraaf van hoofdstukken 3, 4 en 5.

Voordat Vlam-chat aan de hand van het conceptmanuscript om bovengenoemde input is gevraagd, zijn de teksten van het manuscript eerst zelf geschreven door, of gebaseerd op eerder werk van de auteur. Zo wordt voorkomen dat via dit boek informatie met de lezer wordt gedeeld waarvan de auteur zelf geen kennis heeft en waarvan het dan onduidelijk is wat de mogelijke gevolgen kunnen zijn. Door zelf eerst teksten te schrijven, en die vervolgens als volledig manuscript aan Vlam-chat beschikbaar te stellen, wordt het ook voor Vlam-chat duidelijker wat precies de bedoeling is van een specifiek stuk tekst.

De diensten van Vlam draaien op de servers van het eigen overheids-datacenter. Alle gegevens blijven daardoor binnen de beveiligde omgeving. De in het manuscript behandelde kennis is bovendien totaal niet vertrouwelijk van aard en bevat geen persoonsgegevens. Hierdoor wordt het gebruik van Generatieve AI, inclusief het uploaden van het volledige manuscript, verantwoord geacht en als potentieel waardevolle aanvulling gezien om tot een voor de lezer zo bruikbaar mogelijke tekst te komen.

