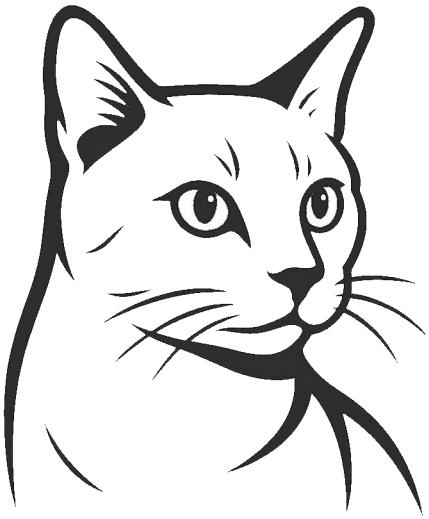
POSITION PAPER



Gevolgen van de Solvinity-overname voor Logius-dienstverlening

27 januari 2026

Stichting Librekat
www.librekat.nl

POSITION PAPER

Gevolgen van de Solvinity-overname voor Logius-dienstverlening

Dit is document beschrijft de overname van Solvinity door Kyndryl en de betekenis voor dienstverlening van Logius. De focus is gericht op DigiD, maar ook wordt stilgestaan bij de berichtenbox, omdat hier veel communicatie tussen burger en overheid in wordt gefaciliteerd.

Deze position paper beschrijft hoe de voorgenomen overname van Solvinity door Kyndryl de strategische positie van vitale Nederlandse digitale overheidsvoorzieningen wezenlijk verandert, ondanks het feit dat de operationele dienstverlening op korte termijn intact blijft. Sinds 2020 levert Solvinity het infrastructuur- en hardwareplatform onder regie van Logius voor kernvoorzieningen zoals DigiD, MijnOverheid (inclusief de Berichtenbox) en Digipoort. De verantwoordelijkheid voor beleid, architectuur en dienstverlening ligt volledig bij de overheid, maar de technische continuïteit is afhankelijk van een private infrastructuurleverancier.

Door de overname verschuift het eigendom en de uiteindelijke zeggenschap over deze leverancier naar een niet-EU-partij, wat volgens het Europese Cloud Sovereignty Framework leidt tot een ***daling van het soevereiniteitsniveau*** *van circa SEAL-3 (digitale weerbaarheid onder EU-controle) richting SEAL-1 (Formele juridische soevereiniteit)!*

De paper plaatst deze verschuiving expliciet in een veranderd geopolitiek klimaat, waarin Amerikaanse wetgeving, sanctieregimes en politieke druk aantoonbaar kunnen doorwerken in digitale dienstverlening, zelfs bij strikt contractuele afspraken en datalocatie binnen Europa. Vanuit klassieke informatiebeveiligingsprincipes (beschikbaarheid, integriteit en vertrouwelijkheid) identificeert de paper hoge strategische soevereiniteitsrisico's, middellange-termijn autonomierisico's en concrete uitvoeringsrisico's, en maakt zij duidelijk dat dit geen technisch maar een fundamenteel politiek vraagstuk is.

De kernboodschap is dat de overheid nu expliciet moet kiezen ***welke risico's zij bereid is te dragen bij vitale digitale voorzieningen*** *met de bijbehorende kosten, en dat uitstel of impliciete acceptatie neerkomt op een politieke beslissing zonder expliciete verantwoording.*

Logius en Solvinity

In 2020 heeft Solvinity van Logius de opdracht gekregen om het onderliggende infrastructuur- en hardwareplatform te leveren voor een aantal rijksbrede digitale voorzieningen. Het gaat daarbij om datacentercapaciteit, servers, opslag, netwerk- en beveiligingsvoorzieningen. Solvinity levert deze infrastructuur. De zeggenschap over en verantwoordelijkheid voor de publieke digitale diensten ligt bij Logius.

Logius bepaalt de architectuur, beveiligingseisen, governance en het gebruik van de systemen, en is als uitvoeringsorganisatie verantwoordelijk voor de werking van onder meer DigiD. DigiD zelf, de applicatie, gegevensverwerking en beleidsmatige aansturing, is en blijft volledig in handen van de Nederlandse overheid. DigiD vormt de sleutel tot alle dienstverlening van de overheid en gerelateerde diensten, zoals toegang tot informatie in de zorg.

In 2025 is aangekondigd dat Solvinity wordt overgenomen door Kyndryl. Kyndryl is een grote Amerikaanse IT-dienstverlener die wereldwijd infrastructuur beheert voor overheden en grote bedrijven, en in 2021 is afgesplitst van IBM. Het bedrijf levert geen consumentenproducten, maar richt zich op het technisch draaiend houden van vitale IT-systemen. Door de overname verandert de dagelijkse technische dienstverlening niet automatisch, maar komt het eigendom en de uiteindelijke zeggenschap over de infrastructuurleverancier in Amerikaanse handen. Er ontstaat een nieuwe bestuurlijke en strategische context rondom een platform dat wordt ingezet voor essentiële publieke voorzieningen.

Naast DigiD maken ook andere kernvoorzieningen van Logius gebruik van deze infrastructuur, waaronder MijnOverheid (waaronder de Berichtenbox voor overheid-burgercommunicatie), Digipoort (het berichtenverkeer tussen overheid en bedrijven), Machtigen en voorzieningen binnen het OIN-stelsel voor organisatie-identificatie. Voor PKIoverheid geldt dat het afsprakenstelsel PKIoverheid beheert, regie voert en toezicht houdt op de certificaatdienstverleners binnen het stelsel." Op het Solvinity-platform draait geen losse applicatie, maar een samenhangend geheel van digitale overheidsdiensten, waarvoor de overheid beleidsmatig verantwoordelijk is, terwijl de technische continuïteit afhankelijk is van een private infrastructuurleverancier.

Europees kader om soevereiniteit inzichtelijk te maken

Het Cloud Sovereignty Framework van de Europese Commissie is een beoordelingsraamwerk dat is ontwikkeld om inzichtelijk en vergelijkbaar te maken in hoeverre digitale met name cloud- en platformdiensten daadwerkelijk onder Europese zeggenschap, wetgeving en controle vallen. Het raamwerk is nadrukkelijk bedoeld voor situaties waarin eigendom, zeggenschap en jurisdictie uit elkaar kunnen lopen, zoals bij overnames door niet-EU-partijen.

Binnen dit kader introduceren de SEAL-niveaus (Sovereignty Effective Assurance Levels) een oplopende schaal (SEAL-0 t/m SEAL-4) waarmee wordt aangegeven hoe sterk de Europese digitale soevereiniteit is geborgd: van geen betekenisvolle soevereiniteit (SEAL-0) tot volledige digitale soevereiniteit onder uitsluitend EU-recht en EU-controle (SEAL-4). In het kader van een overname bieden de SEAL-niveaus een concreet instrument om te beoordelen of een organisatie na de overname nog kan voldoen aan Europese eisen rond rechtsmacht, datatoegang, continuïteit en strategische autonomie, los van formele contracten of goede bedoelingen. Het raamwerk helpt bestuurders en overheden om het gesprek te voeren over feitelijke controle in plaats van louter juridische structuren.

SEAL-niveau	Betekenis
SEAL-0 (Geen digitale soevereiniteit)	De dienst of technologie staat volledig onder niet-EU-zeggenschap en niet-EU-jurisdictie. Europese wetgeving biedt in de praktijk geen effectieve bescherming of afdwingbaarheid.
SEAL-1 (Formele juridische soevereiniteit)	EU-wetgeving is formeel van toepassing, maar kan in de praktijk worden ondermijnd door niet-EU-eigendom, buitenlandse wetgeving of extraterritoriale bevoegdheden
SEAL-2 (Datasoevereiniteit)	Gegevens vallen onder EU-recht en kunnen technisch worden beschermd, maar er bestaan nog significante afhankelijkheden van niet-EU-partijen (bijvoorbeeld beheer, updates of sleutelmaterialen).
SEAL-3 (Digitale weerbaarheid)	EU-wetgeving is effectief afdwingbaar en de dienst is grotendeels onder EU-controle ingericht, met beperkte en beheersbare niet-EU-afhankelijkheden.
SEAL-4 (Volledige digitale soevereiniteit)	Volledige Europese controle: eigendom, bestuur, technologie, data en operationeel beheer vallen uitsluitend onder EU-recht en EU-jurisdictie, zonder kritieke niet-EU-afhankelijkheden.

In overnames zie je vaak organisaties een SEAL-niveau omlaag gaan, ook als contracten formeel intact blijven. Voor kritieke overheidstaken wordt doorgaans SEAL-3 of SEAL-4 als ondergrens gezien. De infrastructuur voor DigiD zou met de overname bewegen van SEAL-3 (digitale weerbaarheid onder EU-controle) richting SEAL-1 (Formele juridische soevereiniteit) door de overname van de infrastructuurleverancier door een niet-EU-partij. Dit is een majeure impact.

Veranderd klimaat

De voorgenomen overname van Solvinity vindt plaats in een realiteit die het afgelopen jaar fundamenteel is gewijzigd sinds het aantreden van de nieuwe Amerikaanse regering. Waar IT-aanbestedingen voorheen vaak door de IT-afdeling sec werden beoordeeld op technische kwaliteit en prijs, is steeds vaker een (politiek-)bestuurlijke afweging nodig wat betreft het effect van het product op de strategische autonomie van de organisatie. Drie recente ontwikkelingen illustreren dat de vanzelfsprekendheid waarmee wij Amerikaanse dienstverleners vertrouwden, onder druk staat.

1. Het precedent van 'Shutter Control' (Maxar).

De casus rondom satellietbedrijf Maxar maakt duidelijk dat commerciële leveringscontracten ondergeschikt zijn aan geopolitieke belangen. Ondanks privaatrechtelijke afspraken bleek de Amerikaanse overheid via Shutter Control in staat de levering van data aan bondgenoten te beperken of te sturen. Zoals dat is gebeurd na een conflictueus gesprek tussen de Amerikaanse regering en de president van Oekraïne voor het leveren van satelliet beelden. Dit schept een precedent voor andere sectoren: het eigendom van de infrastructuur bepaalt uiteindelijk wie de 'schakelaar' bedient, niet de betalende klant.

2. Erosie van het juridisch vangnet (Privacy Shield).

De juridische basis voor data-uitwisseling is instabiel. Het vertrouwen in trans-Atlantische afspraken is geschaad door de onzekerheid rondom de opvolgers van het Privacy Shield. Het politieke klimaat in de VS, waarbij toezichthoudende organen (zoals de ombuds-functie voor privacy) door executieve besluiten zoals van de regering-Trump buitenspel kunnen worden gezet, toont de kwetsbaarheid aan. Garanties voor de bescherming van data van niet-Amerikanen blijken in de praktijk afhankelijk van de politieke waan van de dag in Washington. Momenteel loopt er een juridische strijd in Europa over de geldigheid van dit vangnet.

3. Escalatie rondom Europese regelgeving (De casus X).

De verhoudingen tussen Amerikaanse tech-bedrijven en de Europese wetgever zijn verhard. Na de invoering van de Digital Services Act (DSA) en de bijbehorende boetes en waarschuwingen aan het adres van platform X, is zichtbaar geworden dat Amerikaanse partijen bereid zijn de confrontatie te zoeken. Er wordt openlijk gedreigd met het terugtrekken van diensten of het negeren van Europese sancties, gesteund door politieke druk vanuit de VS. Dit illustreert een nieuw risico: Amerikaanse eigenaren van vitale infrastructuur kunnen hun positie gebruiken als hefboom in bredere handelsconflicten tussen de VS en de EU. Nederlandse overheidsdata kunnen hierdoor onbedoeld onderdeel worden van een politiek machtsspel.

In de zaak rond het ***Internationaal Strafhof*** *werd zichtbaar hoe geopolitieke spanningen zich concreet vertalen naar digitale afhankelijkheden. Toen de Verenigde Staten sancties instelden tegen functionarissen van het Strafhof, werkte dat niet alleen door in diplomatieke en financiële sfeer, maar raakte het ook operationele digitale dienstverlening, zoals e-mail en andere essentiële IT-voorzieningen. Leveranciers met een Amerikaanse juridische binding* ***bleken daardoor gevoelig voor politieke besluitvorming buiten Europa,*** *ongeacht contractuele afspraken of de locatie van data. Digitale diensten zijn onderdeel van geopolitieke machtsuitoefening, en dat afhankelijkheid van niet-Europese jurisdicties kan leiden tot feitelijke verstoringen van de continuïteit en autonomie van zelfs internationale rechtsstatelijke instellingen.*Bij deze voorbeelden moeten we bedenken dat het internationale recht op dit moment onder druk staat door een overgang naar een nieuwe, pluriforme wereldorde; een wereld waarin de oude machtsstructuren verbrokkelen en grootmachten (VS, China, Rusland) sturen op basis van Realpolitik.

Informatiebeveiligingsvraagstuk

Het thema raakt de kern van informatiebeveiliging en moet worden bezien vanuit de klassieke beveiligingsdoelen beschikbaarheid, integriteit en vertrouwelijkheid (BIV). Deze drie uitgangspunten vormen al sinds de jaren zeventig het fundament van informatiebeveiliging, aanvankelijk in militaire en overheidscontexten en later in civiele en commerciële informatiesystemen. In de decennia daarna zijn zij expliciet vastgelegd in internationale normen, auditkaders en overheidsbeleid, en sindsdien leidend bij het beoordelen van risico's rond automatisering, uitbesteding en ketenafhankelijkheden. De toepassing van BIV op digitale overheidsvoorzieningen zoals DigiD en andere Logius-diensten is daarmee geen nieuwe benadering, maar de voortzetting van een decennialang beproefd beveiligingsprincipe in een context van toenemende digitalisering en complexiteit.

De risico's binnen dit thema manifesteren zich steeds langs deze drie beveiligingsdoelen. Beschikbaarheid komt in het geding wanneer de continuïteit van de onderliggende infrastructuur niet langer volledig door de overheid kan worden afgedwongen, bijvoorbeeld bij verstoringen, leveranciersafhankelijkheid of strategische besluitvorming buiten de publieke invloedssfeer. Integriteit raakt aan de mate waarin de overheid aantoonbaar kan borgen dat systemen, configuraties en gegevens niet ongewenst worden gewijzigd, en dat toezicht, auditing en wijzigingsbeheer effectief blijven binnen een uitbesteed technisch domein. Vertrouwelijkheid betreft het risico dat persoonsgegevens en authenticatiegegevens, al dan niet indirect, blootstaan aan onbevoegde toegang of juridische aanspraken buiten het Nederlandse en Europese rechtskader. Deze risico's zijn geen theoretische constructies, maar klassieke informatiebeveiligingsvraagstukken die zich in een moderne, uitbestede digitale infrastructuur opnieuw en versterkt voordoen.

De risico's

De ontwikkelingen dwingen tot een herijking van de risicoanalyse rondom Solvinity en Logius. De vraag is niet langer alleen of de dienstverlening nu voldoet, maar of de Nederlandse staat voldoende grip houdt in een scenario waarin Amerikaanse wetgeving of politieke druk botst met Nederlandse belangen en regelgeving.

Strategische soevereiniteitsrisico's (hoog)

Risico	Uitleg	BIV
Verlies van uiteindelijke zeggenschap	Infrastructuur voor kernvoorzieningen valt onder een buitenlandse moedermaatschappij	B / I / V
Beperkte beleidsvrijheid	Strategische keuzes worden beïnvloed door externe commerciële belangen	B / I
Juridische extraterritorialiteit	Buitenlandse wetgeving kan indirect invloed uitoefenen op infrastructuur en bedrijfsvoering	V
Onomkeerbare afhankelijkheid	Technische en contractuele complexiteit maakt herinbesteding praktisch zeer moeilijk	B
Structurele onderhandelingszwakte	Overheid heeft op termijn minder keuzeruimte bij contractverlenging	B / I
Afhankelijkheid	Beperkte herstelbaarheid bij gedwongen infrastructuurmigratie: bij het wegvallen van de bestaande omgeving kunnen digitale vertrouwensmechanismen niet direct worden overgezet, waardoor de overheid onvoldoende autonoom is om vitale diensten snel te herstellen.	B / I

B = Beschikbaarheid, I = Integriteit en V = Vertrouwelijkheid

Autonomierisico's op middellange termijn

Risico	Uitleg	BIV
Governance op afstand	Besluitvorming ligt buiten directe democratische controle	I
Verlies van systeemkennis	Kritieke kennis verschuift naar leverancier	B / I
Beperkte strategische wendbaarheid	Beleidswijzigingen vereisen instemming of medewerking externe partij. Zeker bij geopolitieke conflicten kan dit gaan opspelen	B
Toegang tot informatie of dienstverlening voor een vreemde mogendheid	Op basis van wetgeving wordt toegang tot systemen of informatie geëist. Omdat het platform door Solvinity wordt beheerd is toegang op basis van een bevel mogelijk. Dat betreft niet alleen DigID, maar ook de berichtenbox. Probleem daarbij is dat deze toegang niet of zeer moeilijk detecteerbaar is. Er is al langer bekend dat ook verzamelde versleutelde gegevens langer worden bewaard onder het motto 'collect now, decrypt later'.	V

B = Beschikbaarheid, I = Integriteit en V = Vertrouwelijkheid

Praktische uitvoeringsrisico's (onderliggend)

Risico	Uitleg	BIV
Escalatie buiten nationale sfeer	Incidentafhandeling vereist afstemming over landsgrenzen als het incident belangrijk genoeg is of van geopolitieke aard is	B
Publiek vertrouwen onder druk	Uitlegbaarheid richting burgers wordt lastiger	V
Fragmentatie van verantwoordelijkheden	Onduidelijkheid over wie feitelijk kan ingrijpen	I
Migratie naar andere oplossing is tijdrovend	Bij onvoldoende voorbereiding kan migratie van de oplossing extra tijd in beslag nemen. Denk daarbij bijvoorbeeld aan het uitgeven van beveiligingscertificaten aan alle gebruikers, het uitvoeren van audits om de veiligheid te borgen, het inrichten van een goed functionerende beheersorganisatie.	B

B = Beschikbaarheid, I = Integriteit en V = Vertrouwelijkheid

De beleidsopties

Bij strategische risico's rond DigiD, de Berichtenbox en andere Logius-diensten zijn er in beleids- en risicomanagement vier klassieke handelingsopties. Voor de overheid verschillen deze opties sterk in realiteitsgehalte en politieke betekenis.

De discussie gaat niet over de vraag óf er risico's zijn, maar welke risico's de overheid bereid is structureel te dragen, en welke zij actief wil vermijden of beheersen. Dat is een politieke keuze, geen technische.

1. Vermijden – het risico structureel wegnemen

Dit is de meest ingrijpende optie en raakt aan fundamentele keuzes over de inrichting van de digitale overheid.

Mogelijke stappen:

- Overname verbieden.
- Versnelde overstap naar de opvolger van DigiD (eIDAS). Momenteel is er bijvoorbeeld al een implementatie gemaakt door het Belgische bedrijf 'itsme', die ook in Nederland kan werken.
- Herinbesteden van de infrastructuur naar een volledig publieke of staatsgecontroleerde omgeving. Dat maakt een stap naar SEAL niveau 4 mogelijk.
- Splitsen van vitale kernvoorzieningen van commerciële infrastructuur
- Wettelijk vastleggen dat bepaalde digitale voorzieningen uitsluitend onder nationale zeggenschap mogen vallen
- Opbouwen van een overheidsbrede infrastructuurvoorziening voor vitale diensten

Politieke betekenis:

- Maximale (digitale) soevereiniteit
- Hoge kosten en lange doorlooptijd
- Dwingt expliciete keuzes over wat "kritieke infrastructuur" is

2. Mitigeren – het risico beheersbaar maken

Kern: de afhankelijkheid accepteren, maar scherp begrenzen.

Mogelijke stappen:

- Aanscherpen van contractuele eisen op exit, uitwijk en herstelbaarheid
- Verplichten van technische en organisatorische scheiding (ringfencing) voor vitale diensten
- Versterken van audit- en toezichtbevoegdheden van de overheid
- Opbouwen van parallelle voorzieningen of fallback-scenario's
- Eisen stellen aan kennisborging binnen de overheid
- Opstellen van een integraal digitaal sourcing beleid voor wat wel of niet mag worden uitbesteed en onder welke voorwaarden. Hierbij kan voor dienstverlening aansluiting worden gezocht bij het Europees beleid dat al is uitgewerkt.

Politieke betekenis:

- Minder ingrijpend, sneller uitvoerbaar
- Verlies van vertrouwelijkheid: het afschermen van (gevoelige) data voor een vreemde mogendheid kan niet technisch gegarandeerd worden en is afhankelijk van afspraken en wetgeving buiten de Nederlandse of Europese jurisdictie.
- Lost structurele afhankelijkheid niet volledig op, maar vermindert het
- Vereist permanente bestuurlijke aandacht

3. Overdragen – het risico bij een andere partij leggen

Kern: het risico contractueel of juridisch doorschuiven.

Relevante constatering voor de overheid: Voor soevereiniteits- en autonomierisico's is dit geen serieuze optie.

Waarom niet:
- De overheid blijft politiek en maatschappelijk verantwoordelijk
- Continuïteit van voorzieningen als DigiD en de Berichtenbox is niet "verzekerbaar"
- Reputatie- en vertrouwensschade zijn niet overdraagbaar

Politieke betekenis:
- Belangrijk om expliciet uit te sluiten
- Voorkomt schijnzekerheid ("het staat in het contract")

4. Accepteren – het risico bewust dragen

Kern: erkennen dat het risico bestaat en besluiten het te aanvaarden.

Dit vereist expliciete politieke verantwoordelijkheid.

Mogelijke stappen:
- Formeel vastleggen welk soevereiniteitsverlies acceptabel wordt geacht
- Transparant maken welke afhankelijkheden bestaan
- Periodieke herbeoordeling van het risico (bijvoorbeeld bij geopolitieke veranderingen)
- Heldere communicatie richting burgers en parlement

Politieke betekenis:
- Laagste kosten op korte termijn
- Hoog afbreukrisico bij incidenten
- Vereist expliciete verantwoording: dit risico is bewust genomen

De opties zijn samengevat:

Optie	Effect op soevereiniteit	Politieke gewicht
Vermijden	Maximale controle	Hoog
Mitigeren	Beperkte afhankelijkheid	Gemiddeld
Overdragen	Niet realistisch	Niet mogelijk
Accepteren	Structurele afhankelijkheid	Politiek risicovol

Openstaande vraagstukken

Hieronder staat een samenhangende set van kernvraagstukken waarop duidelijkheid nodig is om een inhoudelijk, politiek zuiver debat te kunnen voeren. Ze zijn bewust geformuleerd als open vraagstukken (geen stellingnames), zodat Kamerleden ze kunnen gebruiken voor vragen, positionering en moties. Ze zijn geclusterd naar soevereiniteit, governance, continuïteit en politieke verantwoordelijkheid.

Soevereiniteit en autonomie (fundamenteel)

1. Welke digitale overheidsvoorzieningen kwalificeren we als vitaal, in die zin dat structurele afhankelijkheid van Amerikaanse zeggenschap onwenselijk wordt geacht?
2. Welke mate van verlies aan autonomie is acceptabel bij kernvoorzieningen zoals DigiD en de Berichtenbox?
3. Is de huidige inrichting het resultaat van een expliciete politieke keuze, of het gevolg van geleidelijke uitbesteding zonder integraal besluitmoment?
4. Waar ligt de ondergrens van digitale soevereiniteit: wanneer is een afhankelijkheid niet langer aanvaardbaar, ook als de dienstverlening technisch goed functioneert?

Eigendom, zeggenschap en verantwoordelijkheid

5. Hoe verhouden eigendom van infrastructuur, zeggenschap over de leverancier en verantwoordelijkheid voor publieke diensten zich tot elkaar in crisissituaties?
6. Heeft de overheid in de praktijk voldoende doorzettingsmacht om bij conflicterende belangen haar publieke verantwoordelijkheid waar te maken?
7. Is de huidige governance ingericht op dagelijkse stabiliteit, of ook op strategische stress-scenario's (geopolitiek, juridische conflicten, escalaties)?

Continuïteit en herstelbaarheid

8. In hoeverre kan de overheid zelfstandig en tijdig herstellen of uitwijken wanneer de bestaande infrastructuuromgeving niet meer beschikbaar is?
9. Welke structurele herstelbeperkingen bestaan er die niet contractueel of technisch snel oplosbaar zijn?
10. Zijn deze beperkingen expliciet meegewogen in eerdere besluitvorming over uitbesteding van kernvoorzieningen?
11. Wat is de maatschappelijk aanvaardbare maximale uitvalduur van voorzieningen als DigiD en de Berichtenbox in een crisissituatie?

Juridische en geopolitieke context

12. Welke juridische en geopolitieke ontwikkelingen kunnen de handelingsvrijheid van de Nederlandse overheid in de toekomst beperken?
13. Hoe wordt omgegaan met situaties waarin juridische kaders conflicteren met beleidsdoelen of publieke belangen?
14. Is er een scenario-analyse gemaakt voor veranderende geopolitieke omstandigheden, en zo ja, hoe robuust zijn de uitkomsten?

Beleidsopties en omkeerbaarheid

15. Welke van de huidige keuzes zijn omkeerbaar, en welke leiden feitelijk tot langdurige of permanente afhankelijkheden?
16. Welke beleidsopties zijn op dit moment nog realistisch binnen een termijn van 5 tot 10 jaar?
17. Welke risico's kunnen met mitigatie worden beheerst, en welke blijven structureel bestaan, ongeacht aanvullende maatregelen?
18. Waar ligt het punt waarop risicoacceptatie een expliciet politiek besluit moet zijn in plaats van een impliciet gevolg?

Democratische verantwoording en transparantie

19. Op welk moment wordt de Kamer actief betrokken bij besluiten die de digitale autonomie structureel beïnvloeden?
20. Hoe wordt aan burgers uitgelegd wie uiteindelijk de controle heeft over kernvoorzieningen van de digitale overheid?
21. Is voldoende inzichtelijk welke risico's bewust worden genomen en wie daar politiek verantwoordelijk voor is?

Colofon

Deze paper van Stichting LibreKAT is gemaakt met hulp en ondersteuning van diverse personen en organisaties: AdversIQ B.V., Anovum B.V., BIT B.V., ESET, Chris van 't Hof (DIVD), Chateau IT, Cloudaware Cybersecurity, Coderial B.V., Cynalytics B.V., DIVD, DIVD Academy, DSEC Consulting, Freedom Internet, Guido de Nobel, Innerheight Internet Diensten B.V., IP Zorg, Jesse Six Dijkstra, Jeroen Baten, Koopman Digital Forensics & Consulting (KDFC), Mathison B.V., Mischa Rick van Geelen, Van Buuren IT Security B.V., The Good Cloud B.V, Pieter Muller, ProcoliX, Vereniging Open Domein, OID Foundation, CEDO, Hans de Raad, OpenNovations B.V., Sebastiaan van 't Erve, Stichting Petities.nl, Mr. Victor de Pous, Unicorn Holding B.V., Weissheid, Oosenbrug Advies, Vigilis Consultancy, Tektok en De Winter Information Solutions.

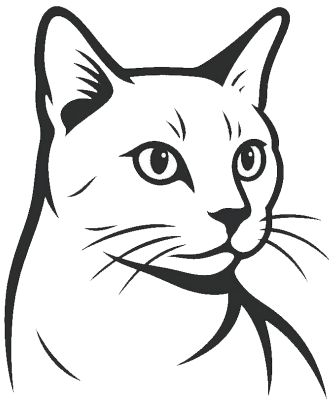
Over Stichting LibreKAT

Stichting Librekat zet zich in voor een veiligere digitale samenleving. De stichting richt zich daarbij op open, controleerbare en verifieerbare informatiebeveiliging. Dit doen we door kennisdeling, community-vorming en het ondersteunen van open source-oplossingen binnen cybersecurity. Zo bieden wij OpenKAT voor het in kaart brengen van kwetsbaarheden, de Methodiek voor Informatiebeveiligingsonderzoek met auditwaarde (MIAUW), checklists voor informatiebeveiliging en organiseren wij de Cyberonderzoeksraad om complexe problemen te onderzoeken en helder uit te leggen.

Onze doelstelling omvat onder meer:

- Het stimuleren van ontwikkeling en gebruik van open source-software en -hardware voor veilige digitale infrastructuren.
- Het bevorderen van transparantie en reproduceerbaarheid in beveiligingsprocessen.
- Het organiseren en ondersteunen van onderzoek, trainingen en activiteiten rond digitale weerbaarheid.
- Het verbinden van burgers, bedrijven, overheid en maatschappelijke organisaties om de collectieve digitale weerbaarheid te vergroten.

Het bestuur van de Stichting bestaat uit:
- Brenno de Winter, voorzitter
- Jan Klopper, secretaris
- Astrid Oosenbrug, penningmeester



www.librekat.nl