IRIS.
INTRANET



Digitale veiligheid en datasoevereiniteit

Waarom een toekomstbestendig sociaal intranet begint bij Nederlands eigenaarschap, open source en lokale hosting.

03-2026

Data in eigen land

Als CISO of IT-manager ben je verantwoordelijk voor informatiebeveiliging, privacy en datasoevereiniteit. Die verantwoordelijkheid groeit. Europese regelgeving, zoals NIS2 en de Baseline Informatiebeveiliging Overheid (BIO) stellen steeds strengere eisen aan waar en hoe gegevens worden verwerkt. Datasoevereiniteit is nu nog belangrijker.

Het sociaal intranet is de plek waar alles samenkomt. Hier delen collega's persoonlijke profielen, belangrijke beleidsstukken en HR-informatie. De centrale vraag voor jou is simpel: wie heeft er toegang tot deze data, waar staat het opgeslagen en onder welke wetgeving valt de leverancier?

"Je intranet is het kloppend hart van je organisatie. Behandel het ook zo."

Inhoudsopgave

Waarom datasoevereiniteit nu op de agenda staat	4
Het risico van de “standaardkeuze”	5
Iris Intranet: 100% datasoeverein	6
Compliance die je kunt verifiëren	7
Technische architectuur die soevereiniteit ondersteunt	9
Wat Iris Intranet jouw organisatie brengt	11
Audit-tool: Leveranciersbeoordeling datasoevereiniteit	12
Tot slot	13

Waarom datasoevereiniteit nu op de agenda staat

Datasoevereiniteit gaat over de vraag wie de feitelijke en juridische zeggenschap heeft over jouw gegevens. Het gaat over eigenaarschap van de leverancier, de locatie van dataopslag, de wetgeving die van toepassing is op die leverancier en de technische mogelijkheid om data te exporteren of te verwijderen.

Voor elke organisatie die werkt met gevoelige informatie of kritieke processen is dit een belangrijk vraagstuk. Het raakt direct aan:

1. **Wettelijke verplichtingen:** NIS2, BIO en AVG stellen eisen aan waar en hoe je persoonsgegevens en bedrijfskritische informatie verwerkt.

2. **Geopolitieke realiteit:** Wetgeving van buiten de Europese Unie (EU), zoals de Amerikaanse CLOUD Act, kan buitenlandse overheden toegang geven tot data bij leveranciers met niet-Europees eigenaarschap. Dit geldt ook als die data in de EU staat.

3. **Continuïteit en autonomie:** Afhankelijkheid van één groot buitenlands platform brengt risico's mee bij sancties, overnames of beleidswijzigingen waar je als organisatie geen invloed op hebt.

De trend is helder: steeds meer organisaties stellen datasoevereiniteit als harde eis in hun inkooptrajecten.



Het risico van de “standaardkeuze”

Veel organisaties gebruiken een sociaal intranet dat op het eerste gezicht goed functioneert. De dagelijkse gebruikerservaring is prima en de beheerders zijn tevreden. Maar wie onder de motorkap kijkt, ziet vaak een ander verhaal.

Stel jezelf eens de volgende vragen over je huidige of toekomstige intranetleverancier:

- Waar is het hoofdkantoor gevestigd en wie zijn de eigenaren of investeerders?
- Op welke technologie is het platform gebouwd, en welke afhankelijkheden brengt dat met zich mee?
- In welke datacenters draait de applicatie en onder welke wetgeving vallen deze locaties?
- Kan de leverancier aantonen dat geen enkele partij van buiten de EU juridisch toegang kan afdwingen tot jouw data?
- Een intranetplatform op basis van proprietary (Microsoft-)technologie, mondiale clouds en niet-Europese eigenaren geeft vaak niet de antwoorden die je zoekt. De juridische en technische architectuur laat het simpelweg niet toe om volledige soevereiniteit te garanderen.

“Datasoevereiniteit begint niet bij een vinkje in je inkoopformulier. Het begint bij de fundamentele keuzes van je leverancier.”



Iris Intranet: 100% datasoeverein

Bij Iris is datasoevereiniteit geen extra optie, maar de basis van alles wat we doen. Elke architectuurbeslissing, elke partnerkeuze en elk hostingmodel is doordacht vanuit één perspectief: jouw data blijft van jou, valt onder de Nederlandse wetgeving en wordt beheerd door Nederlandse partijen.

Nederlands eigenaarschap

Iris wordt ontwikkeld door triptic B.V. We zijn in 1997 opgericht in Eindhoven en daar zijn we altijd gebleven. We hebben geen buitenlandse aandeelhouders of investeerders. Onze eigenaren? Die komen uit de Achterhoek. Onze ontwikkelaars zitten in Eindhoven en de hosting vindt plaats in Rijen en Eindhoven.

Dit is een bewuste keuze die direct gevolgen heeft voor jouw risicoprofiel. Omdat we volledig van Nederlands eigendom zijn, bieden we een juridische blokkade tegen wetgeving zoals de Amerikaanse CLOUD Act. Buitenlandse overheden kunnen bij ons geen toegang afdwingen, omdat er geen juridische basis is bij niet-Europese investeerders of moederbedrijven. Hoe soeverein wil je het hebben?

Open source als fundament

Iris is gebouwd op betrouwbare open-sourcetechnologie met een Linux stack als ruggengraat. Hoewel Iris zelf een closed-source licentie kent, is het product opgebouwd uit open-source bouwblokken.

Waarom dat ertoe doet? Open-sourcetechnologie vermindert vendor lock-in, vergroot transparantie en geeft jou en je auditors de mogelijkheid om de technologische keuzes te verifiëren. Je bent niet afhankelijk van de roadmap of het licentiemodel van één groot technologieconcern.

Hosting in Nederland, onder jouw regie

Jouw data blijft binnen de Europese Economische Ruimte (EER). Bij onze standaard private-cloudhosting staat de data aantoonbaar in Nederland.

“Ontwikkeld in Eindhoven. Gehost in Rijen en Eindhoven. Eigenaren uit de Achterhoek. Zo simpel is het.”

Compliance die je kunt verifiëren

Voor een CISO zijn certificeringen de bewijslast voor risicobeheersing. Iris en het team achter Iris voldoen aan de belangrijkste kaders:

ISO 27001:2022

Triptic is gecertificeerd door Kiwa met een brede scope: ontwikkeling, implementatie en beheer van het sociaal samenwerkingsplatform Iris, inclusief ondersteunende adviesdiensten. Alle bedrijfsprocessen – van ontwerp en ontwikkeling tot beheer en beëindiging van de dienst – vallen onder het informatiebeveiligingsbeleid.

Baseline Informatiebeveiliging Overheid (BIO)

Iris voldoet aan de BIO. Dit is specifiek relevant voor gemeenten, provincies, waterschappen en andere overheidsorganisaties die wettelijk verplicht zijn om conform dit kader te werken.

Naleving van NIS2 en Dora

Wij leggen de focus op de praktijk van naleving. Iris ondersteunt jouw compliance-verplichtingen direct via:

- **Incidentmeldingsprocessen:** Onze protocollen sluiten aan op de strikte meldtermijnen en rapportage-eisen van de NIS2.
- **Proactief risicobeheer:** Wij voeren continu risico-analyses uit op onze infrastructuur en software, zodat jij aantoonbaar “in control” bent.
- **Strikte ketenverantwoordelijkheid:** Wij borgen de veiligheid in de gehele toeleveringsketen (Supply Chain Security), een harde eis binnen NIS2 en DORA.

GIBIT-inkoopvoorwaarden: beperken van vendor lock-in

Iris past naadloos binnen de GIBIT-inkoopvoorwaarden. Onze leveringsstructuur - met heldere verwerkersovereenkomst en een exit-strategie met volledige data-export – sluit aan op wat GIBIT vraagt van IT-leveranciers.

Ketenverantwoordelijkheid: Beheersing van het ‘Supply Chain Risk’

Een informatiebeveiligingsbeleid is slechts zo sterk als de zwakste schakel. Daarom maken wij ketenverantwoordelijkheid expliciet onderdeel van onze risicobeheersing. Wij eisen van al onze leveranciers dat zij aantoonbaar ISO 27001-gecertificeerd zijn en gevestigd zijn in Nederland met Nederlandse of Europese eigenaren.

Partner	Rol	Locatie & certificering
triptic B.V.	Ontwikkeling & leverancier	Eindhoven – ISO 27001
a&m impact	HR- en administratie	Doetinchem – ISO 27001/NEN7510
Nieuwenborg SolIT	Systeembeheer & hosting	Eindhoven – ISO 27001
Previder	Primair datacenter	Rijen – ISO 27001
EcoRacks	Secundair datacenter (backup)	Eindhoven – ISO 27001
Northwave	Security partner (pentests)	Nederland – breed gecertificeerd
Stack Secure	Awareness & phishing tests	Nederland – ISO 27001

Technische architectuur die soevereiniteit ondersteunt

Een belofte van datasoevereiniteit is pas geloofwaardig als de technische architectuur die belofte waarmaakt. Dit zijn de technische kenmerken die Iris onderscheiden:

Losse tenants: jouw data is echt van jou

Iris werkt anders dan multi-tentant SaaS-platformen. Elke opdrachtgever heeft een volledig eigen omgeving met een eigen codebase, database-instantie, bestandsopslag en zoekindex. Dit is een cruciale risico-beperkende maatregel: je elimineert hiermee het risico op data-spill (lekken van data tussen klanten) volledig.

Encryptie en transport

- **Transport:** Alle verbindingen via TLS 1.3, met een 100% score via de internet.nl-test.
- **Data in rest:** We versleutelen backups met AES-256 (GCM-modus). Dit gebeurt inclusief client-side encryptie voordat data de back-upserver bereikt.
- **Wachtwoorden:** Deze slaan we op met ARGON2-hashing en met per-user random salt.

Iris is standaard ‘password less’ geconfigureerd via SSO. In het kader van bedrijfscontinuïteit bieden wij een eigen user management als authenticatie-fallback. Mocht de toegang tot een mondiale cloudservice (zoals Microsoft Entra ID) wegvallen, dan blijft je intranet bereikbaar voor cruciale communicatie.

Monitoring en proactief beheer

Wij monitoren alle Iris-platformen 24/7. Onze monitoringsystemen draaien op eigen serverinstanties in de datacenters in Eindhoven en Rijen. Dit is een bewuste maatregel om te garanderen dat foutlogging en applicatietelemetrie binnen de Nederlandse jurisdictie blijven. Eventuele persoonsgegevens die in foutmeldingen terechtkomen, schonen we proactief op voordat ze worden opgeslagen. Zo borgen we dat monitoring nooit leidt tot ongewenste data-expositie.

Release- en patchbeleid

Iris hanteert een strak releasebeleid met wekelijkse micro-releases, minimaal vier minor releases per jaar en maximaal één major release per jaar. We rollen beveiligingspatches via geautomatiseerde Gitlab-pipelines naar alle platforms uit. Je kunt updates niet weigeren. Dat klinkt streng, maar het is in jouw belang: het voorkomt verouderde software en ongepatche kwetsbaarheden.

Document management

De kern van Iris is een meertalig Enterprise Content Management Systeem met een eigen Document Management Systeem. Dit systeem fungeert als backup voor de opslag van jullie essentiële documenten (bijv. beleids- en procedurele documenten). Hiermee bouw je de afhankelijkheid van mondiale cloud services af of verminder je deze. De makers van Iris houden Europese DMS alternatieven, zoals NextCloud of de Proton Suite, goed in de gaten. Zodra de technische mogelijkheden en de vraag groeien, ontwikkelen wij integraties om deze informatie in Iris te visualiseren.

Privacy en security ‘by design’

Het ontwerp- en ontwikkelproces van Iris volgt het privacy- en security-by-design-principe. Ontwikkeling vindt “contentloos” plaats: we werken nooit met productiedata van opdrachtgevers. Daarnaast kent Iris een geavanceerde anonimiseerflow die vertrokken medewerkers stapsgewijs anonimiseert, conform AVG-vereisten.

Wat Iris Intranet jouw organisatie brengt

Datasoevereiniteit en informatiebeveiliging zijn essentieel, maar uiteindelijk moet een intranet ook gewoon prettig werken. Iris combineert beide.

Eenvoud die werkt

Iris brengt nieuws, informatie en dagelijkse tools – zoals Microsoft 365, Google Workspace, Topdesk, AFAS en Zenya – samen op één centrale plek. Medewerkers vinden informatie, delen kennis en werken samen vanuit één omgeving, zonder na te hoeven denken over de techniek erachter. Meer dan 250.000 medewerkers met Iris zonder dat de applicatie een helpfunctie heeft. Zo simpel is het!

Relevante informatie, geen ruis

Iris koppelt gebruikers automatisch aan groepen en zogenaamde taxonomieën op basis van velden uit het HR-systeem of je digitale werkpleksoftware (zoals EntraID, Google Workspace, HelloID) en kanaliseert content naar de juiste interne doelgroepen. Zo bereikt relevante informatie de juiste medewerkers, zonder dat iedereen overspoeld raakt.

Bewezen in de praktijk

Meer dan 1750 opdrachtgevers en meer dan 250.000 eindgebruikers werken dagelijks met Iris. Van gemeenten en waterschappen tot zorginstellingen en nutsbedrijven. We richten het platform in als een standaardproduct: je profiteert direct van de nieuwste functionaliteit en hebt altijd volledige ondersteuning.

Snelle implementatie

Waar vergelijkbare trajecten soms maanden duren, staat een Iris-implementatie binnen tien minuten. Geen maandenlange migratieprojecten, maar direct aan de slag. Zo simpel is het.

Audit-tool: Leveranciersbeoordeling datasoevereiniteit

Gebruik onderstaande tool als instrument voor je interne audit, bij je volgende inkooptraject of voor de periodieke beoordeling van je huidige leverancier. Deze criteria helpen je om technische beloftes feitelijk te toetsen aan de risicokaders van jouw organisatie. Tip van Iris: stel dezelfde vragen aan je huidige intranetleverancier. De antwoorden vertellen je meer dan welke brochure dan ook.

Toetsvraag	Iris Intranet
Is de leverancier volledig in Nederlandse handen, zonder niet-EU investeerders?	Ja
Staat de data gegarandeerd binnen de EER, bij voorkeur in Nederland?	Ja
Draait het platform op open-sourcetechnologie?	Ja
Heeft elke opdrachtgever een volledig eigen omgeving (geen multi-tenant)?	Ja
Is de leverancier ISO 27001 gecertificeerd?	Ja
Voldoet het platform aan BIO, NIS2 en DORA?	Ja
Past het platform binnen GIBIT-inkoopvoorwaarden?	Ja
Zijn alle ketenpartners ISO 27001 gecertificeerd en in de EU gevestigd en hebben ze een Nederlandse of Europese eigenaar?	Ja
Is er een heldere exit-strategie met volledige data-export?	Ja
Wordt er gewerkt met ‘privacy by design’ en ‘security by design’ in het ontwikkelproces?	Ja

Tot slot

Datasoevereiniteit is geen luxe. Het is een verantwoordelijkheid die hoort bij het beheer van gevoelige gegevens en essentiële diensten. Het begint bij bewuste keuzes: voor een leverancier met Nederlands eigenaarschap, voor hosting op Nederlandse bodem en voor een architectuur die transparantie en onafhankelijkheid mogelijk maakt.

Iris bewijst dat je die keuze kunt maken zonder concessies te doen aan gebruiksvriendelijkheid of functionaliteit. Een sociaal intranet dat verbindt en informeert, gebouwd op een fundament waar je als CISO en ICT-manager met een gerust hart op kunt bouwen.

Verbinden en informeren. Zo simpel is het.

Meer weten?
Neem contact op met het team van Iris voor een vrijblijvend gesprek over hoe wij passen binnen jouw risicomanagement en IT-strategie.

Iris Intranet – triptic B.V.

Piuslaan 70A, 5614 CM Eindhoven
040-2463050 | info@irisintranet.com | www. irisintranet.com

Iris is 100% van Nederlandse bodem: ontwikkeld in Eindhoven, met data die veilig binnen onze grenzen blijft.

INFORMEREN
EN VERBINDEN

zo simpel is het.

iris.

Piuslaan 70A, 5614 CM Eindhoven
040 266 0333
irisintranet.com