plan EU



WHITEPAPER · OKTOBER 2026

Digitale afhankelijkheid is een bedrijfsrisico

Waarom elke Europese organisatie moet weten waar haar software, data en betalingen staan, en een exitplan nodig heeft voor de diensten die ze niet kan missen.

SAMENVATTING

In het kort

Europese organisaties draaien voor e-mail, documenten, boekhouding, betalingen en hosting in grote mate op diensten van niet-Europese aanbieders. Dat werkt meestal uitstekend, tot het moment dat een beslissing buiten Europa ertoe leidt dat een dienst wordt beperkt, afgesloten of juridisch onhoudbaar wordt.

KERNPUNTEN

- **Het risico is niet technisch maar juridisch en politiek.** Wetgeving, sancties en exportregels van het land van de aanbieder kunnen bepalen of uw dienst blijft werken.
- **De meeste afhankelijkheden zijn onzichtbaar.** Ze zitten bij uw dienstverleners en hun onderaannemers, niet alleen in uw eigen IT.
- **Regelgeving vraagt er al om.** DORA verplicht financiële instellingen tot exitstrategieën; NIS2 en de AVG vragen inzicht in de keten; de Data Act maakt overstappen tussen clouddiensten eenvoudiger.
- **Overstappen is niet altijd nodig, voorbereid zijn wel.** Een exitplan per kritieke dienst maakt het verschil tussen een lastige week en wekenlang stilstand.

Deze whitepaper beschrijft waar die afhankelijkheden zitten, welke mechanismen ze tot een risico maken, wat de regelgeving vraagt en hoe u in vijf stappen van inzicht naar een uitvoerbaar exitplan komt.

Voor wie? Bestuurders, directeuren en compliance- en IT-verantwoordelijken van Europese organisaties in alle sectoren, met extra aandacht voor financiële instellingen die onder DORA vallen.

1 De stille afhankelijkheid

Vraag een willekeurige organisatie welke software ze gebruikt, en het antwoord is snel gegeven: een kantoorpakket, een boekhoudprogramma, een CRM-systeem, een betaalprovider. Vraag vervolgens waar die diensten draaien, onder welk recht de aanbieder valt en wat er gebeurt als de dienst morgen niet meer beschikbaar is, en het wordt stil.

Dat is begrijpelijk. Clouddiensten zijn juist populair omdat u er niet over na hoeft te denken. Maar daardoor is in korte tijd een situatie ontstaan waarin de dagelijkse bedrijfsvoering van veel Europese organisaties afhangt van een klein aantal aanbieders buiten Europa, zonder dat iemand daar bewust voor heeft gekozen.

> **Het probleem is niet dat u niet-Europese diensten gebruikt. Het probleem is dat u niet weet wat u moet doen als ze wegvallen.**

Een voorbeeld dat bleef hangen

In 2025 werd breed bericht dat de hoofdaanklager van het Internationaal Strafhof in Den Haag, na Amerikaanse sancties tegen het hof, geen toegang meer had tot zijn e-mail bij een Amerikaanse aanbieder. Over de precieze toedracht bestaan verschillende lezingen. Maar het principe werd voor veel organisaties ineens concreet: een besluit van een buitenlandse overheid kan via een leverancier direct doorwerken in een Europese organisatie, ook als die organisatie zelf niets verkeerd heeft gedaan.

Hetzelfde kan gebeuren door minder dramatische oorzaken: een prijsverhoging die een dienst onbetaalbaar maakt, een product dat wordt stopgezet, een account dat door een geautomatiseerde controle wordt geblokkeerd, of een aanbieder die wordt overgenomen.

2 Drie mechanismen achter het risico

Afhankelijkheid van een niet-Europese aanbieder wordt een risico via drie routes. Ze staan los van de kwaliteit of goede bedoelingen van de leverancier.

01

Rechtsmacht

Een aanbieder valt onder het recht van het land waar hij gevestigd is. De Amerikaanse CLOUD Act (2018) maakt het bijvoorbeeld mogelijk dat Amerikaanse autoriteiten gegevens opvragen bij Amerikaanse aanbieders, ook als die gegevens in Europa zijn opgeslagen. Dat kan botsen met de AVG.

02

Sancties en exportregels

Overheden kunnen bedrijven verplichten diensten aan bepaalde personen, organisaties of landen te stoppen. De leverancier heeft dan geen keus. Voor u kan dat betekenen dat een dienst wegvalt, of dat een klant of tegenpartij niet meer bereikbaar is.

03

Technische controle

Bij clouddiensten en verbonden apparaten houdt de aanbieder de technische sleutels. Updates, licentiecontroles of het uitschakelen van functies kunnen op afstand gebeuren, met of zonder kwade opzet.

Niet alleen de Verenigde Staten

Het debat gaat vaak over Amerikaanse techbedrijven, omdat die het grootste deel van de markt bedienen. Maar hetzelfde speelt bij aanbieders uit andere landen. Een duidelijk voorbeeld zijn verbonden voertuigen, laadpalen, omvormers en andere apparatuur met software die op afstand kan worden bijgewerkt of uitgeschakeld. In de Verenigde Staten zijn in januari 2025 regels vastgesteld die software uit China en Rusland vanaf modeljaar 2027 uit verbonden voertuigen weren, juist om die reden. Voor Europese bedrijven met wagenparken, logistiek of energie-installaties is dit een directe vraag: wie kan uw apparatuur op afstand bedienen?

Waarom nu?

Deze risico's bestonden altijd, maar drie ontwikkelingen maken ze urgenter: de geopolitieke verhoudingen zijn minder voorspelbaar geworden, steeds meer bedrijfsprocessen draaien uitsluitend in de cloud, en Europese regelgeving verwacht inmiddels dat organisaties deze risico's aantoonbaar beheersen.

3 De verborgen keten

De grootste afhankelijkheden zitten vaak niet in uw eigen IT, maar bij uw dienstverleners. Uw administratiekantoor, salarisverwerker, IT-beheerder of accountant gebruikt zelf ook software en hosting, en die keuzes ziet u niet.

Voorbeeld: de financiële keten

Een fondsbeheerder besteedt de fondsadministratie vaak uit aan een gespecialiseerde administrateur, werkt met een bewaarder of trustee en een externe compliancepartij. Elk van die partijen draait op eigen systemen: een administratiepakket, een documentplatform, een e-mailomgeving, een hostingpartij. De beheerder blijft eindverantwoordelijk, maar heeft vaak geen zicht op welke onderdelen buiten Europa staan.

SCHAKEL	TYPISCHE VRAAG DIE ONBEANTWOORD BLIJFT
Eigen organisatie	Welke diensten gebruiken we, en welke zijn bedrijfskritisch?
Directe dienstverlener	Op welke software en welke hosting draait hun dienst aan ons?
Onderaannemers (subverwerkers)	Waar staan de gegevens en onder welk recht vallen deze partijen?
Contract	Wat zijn de afspraken over beëindiging, overdracht van data en exit?

Het antwoord op die vragen bestaat meestal wel, in verwerkersovereenkomsten, lijsten met subverwerkers en contractbepalingen, maar het is versnipperd en kost veel tijd om te verzamelen. Precies daar gaat het in de praktijk mis.

Tip. Vraag uw belangrijkste dienstverleners om hun actuele lijst met subverwerkers, inclusief vestigingsland en locatie van de gegevens. Onder de AVG mag een verwerker geen subverwerker inschakelen zonder uw toestemming, en moet hij u vooraf informeren over wijzigingen.

4 Wat de regelgeving vraagt

Europese regels verplichten niemand om uitsluitend Europese leveranciers te gebruiken. Ze vragen wel dat organisaties hun afhankelijkheden kennen, risico's beheersen en kunnen overstappen als dat nodig is.

REGELING	VOOR WIE	WAT RELEVANT IS
DORA Verordening (EU) 2022/2554, van toepassing sinds 17 januari 2025	Banken, verzekeraars, beleggingsondernemingen, fondsbeheerders met een AIFMD-vergunning en andere financiële entiteiten (alleen geregistreerde 'lichte' fondsbeheerders vallen erbuiten)	Register van alle ICT-dienstverleningsovereenkomsten; risicobeoordeling vóór contractering; verplichte exitstrategieën voor ICT-diensten die kritieke of belangrijke functies ondersteunen; aandacht voor concentratierisico.
NIS2 Richtlijn (EU) 2022/2555	Essentiële en belangrijke entiteiten in onder meer energie, transport, zorg, digitale infrastructuur en overheid	Zorgplicht voor beveiliging van de toeleveringsketen, inclusief beoordeling van leveranciers en dienstverleners.
AVG Verordening (EU) 2016/679	Iedere organisatie die persoonsgegevens verwerkt	Doorgifte naar landen buiten de EER alleen met passende waarborgen; sinds het Schrems II-arrest (2020) moet per geval worden beoordeeld of het recht van het ontvangende land die waarborgen ondermijnt.
Data Act Verordening (EU) 2023/2854, van toepassing sinds 12 september 2025	Afnemers en aanbieders van clouddiensten	Recht om over te stappen naar een andere aanbieder; overstapkosten worden afgebouwd en verdwijnen vanaf januari 2027. Dat maakt een exitplan praktisch beter uitvoerbaar.

Let op. Deze tabel is een vereenvoudigd overzicht en geen juridisch advies. Welke verplichtingen precies op uw organisatie van toepassing zijn, hangt af van uw sector, omvang en vergunningen. Per regeling kunt u op de wetgevingspagina's toetsen of u eronder valt.

5 Van inzicht naar exitplan

Plan EU werkt met een vaste aanpak in vijf stappen. De eerste stappen kunt u zelf doorlopen met de scan; voor de verdieping en het exitplan begeleiden wij u.

1

Domein

Op basis van uw domeinnaam brengen we publiek zichtbare diensten in kaart, zoals e-mail- en hostingaanbieders.

2

Sector

Uw sector bepaalt welke regelgeving en welke typische afhankelijkheden relevant zijn.

3

Vragen per onderdeel

Korte meerkeuzevragen per gebied: kantoorsoftware, boekhouding, betalingen, hosting, communicatie, dienstverleners.

4

Rapport

Per antwoord een beoordeling op de risicoschaal van Plan EU, met uitleg en Europese alternatieven.

5

Exitplan en advies

Voor elke niet-Europese dienst een stappenplan. Waar gewenst toetsen wij contracten, verzamelen we de antwoorden van leveranciers en begeleiden we de overstap.

De risicoschaal

● Soeverein	◐ Beheersbaar	○ Kwetsbaar	■ Kritiek
Europese aanbieder, data en beheer binnen de EU.	Niet-Europees, maar niet bedrijfskritisch of eenvoudig te vervangen.	Niet-Europees en belangrijk voor de bedrijfsvoering.	Niet-Europees, bedrijfskritisch en moeilijk te vervangen.

De scan bewaart geen gegevens die niet nodig zijn voor het rapport. Wij beoordelen situaties, geen leveranciers: het rapport beschrijft feitelijk waar een dienst gevestigd is en wat dat voor u betekent. Meer hierover in de methodiek.

6 Wat een goed exitplan bevat

Een exitplan is geen verhuisplan. Het is een voorbereiding die ervoor zorgt dat u kunt overstappen wanneer dat nodig is, gepland of onder druk. Voor elke dienst in de categorie kwetsbaar of kritiek legt u ten minste het volgende vast:

- **Functie en eigenaar.** Welk bedrijfsproces hangt van de dienst af en wie is verantwoordelijk?
- **Gegevens.** Welke gegevens staan er, in welk formaat kunt u ze exporteren, en hoe vaak doet u dat?
- **Alternatief.** Ten minste één Europees alternatief, met een globale inschatting van kosten en doorlooptijd.
- **Contract.** Opzegtermijn, afspraken over dataoverdracht, bijstand bij exit en de rechten onder de Data Act.
- **Noodscenario.** Wat doet u in de eerste 48 uur als de dienst onverwacht wegvalt?
- **Afhankelijkheden.** Welke andere systemen of koppelingen stoppen mee?
- **Toetsmoment.** Wanneer wordt het plan herzien en geoefend?

Voor tientallen veelgebruikte diensten staat zo'n plan al klaar bij de exitplannen.

Vijf dingen die u deze maand kunt doen

1. Maak een lijst van de tien diensten zonder welke uw organisatie binnen een dag stilvalt.
2. Noteer per dienst het land van vestiging van de aanbieder en de locatie van de gegevens.
3. Vraag bij uw belangrijkste dienstverleners hun lijst met subverwerkers op.
4. Test of u uw belangrijkste gegevens daadwerkelijk kunt exporteren in een bruikbaar formaat.
5. Doorloop de scan op plan-eu.eu voor een eerste overzicht.

Bronnen

- Verordening (EU) 2022/2554 betreffende digitale operationele weerbaarheid voor de financiële sector (DORA), m.n. artikel 28.
- Richtlijn (EU) 2022/2555 (NIS2), m.n. artikel 21 over beveiliging van de toeleveringsketen.
- Verordening (EU) 2016/679 (AVG), hoofdstuk V; HvJ EU 16 juli 2020, C-311/18 (Schrems II).
- Verordening (EU) 2023/2854 (Data Act), hoofdstuk VI over overstappen tussen gegevensverwerkingsdiensten.
- Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Verenigde Staten, 2018.

plan EU

PLAN-EU.EU

Over Plan EU

Plan EU helpt Europese organisaties hun digitale afhankelijkheden in kaart te brengen en een uitvoerbaar exitplan op te stellen. Met een online scan, een helder rapport en advies op maat, van DORA second opinion tot begeleiding bij de overstap naar een Europees alternatief.

plan-eu.eu

info@plan-eu.eu

Plan EU is een initiatief van Luce Holding B.V. Deze whitepaper is met zorg samengesteld op basis van openbare informatie per oktober 2026 en is bedoeld als algemene informatie. Er kunnen geen rechten aan worden ontleend en zij vormt geen juridisch, fiscaal of beleggingsadvies. Plan EU is geen instelling van de Europese Unie.