plan EU



WHITE PAPER · OCTOBER 2026

Digital dependency is a business risk

Why every European organisation needs to know where its software, data and payments are, and needs an exit plan for the services it cannot do without.

An initiative of Luce Holding B.V.

SUMMARY

In brief

For email, documents, accounting, payments and hosting, European organisations rely heavily on services from non-European providers. That usually works very well, until a decision made outside Europe causes a service to be restricted, cut off or legally untenable.

KEY POINTS

- **The risk is legal and political, not technical.** The laws, sanctions and export rules of the provider's home country can determine whether your service keeps working.
- **Most dependencies are invisible.** They sit with your service providers and their subcontractors, not just in your own IT.
- **Regulation already requires it.** DORA obliges financial institutions to have exit strategies; NIS2 and the GDPR require insight into the supply chain; the Data Act makes switching between cloud services easier.
- **Switching is not always necessary, being prepared is.** An exit plan for each critical service makes the difference between a difficult week and weeks of standstill.

This white paper describes where these dependencies lie, which mechanisms turn them into a risk, what regulation requires and how to get from insight to a workable exit plan in five steps.

Who is it for? Board members, directors and compliance and IT officers of European organisations in every sector, with particular attention to financial institutions that fall under DORA.

1 The silent dependency

Ask any organisation which software it uses and the answer comes quickly: an office suite, an accounting package, a CRM system, a payment provider. Then ask where those services run, which law the provider is subject to and what happens if the service is no longer available tomorrow, and the room goes quiet.

That is understandable. Cloud services are popular precisely because you do not have to think about them. But as a result, within a short time a situation has arisen in which the day-to-day operations of many European organisations depend on a small number of providers outside Europe, without anyone having consciously chosen this.

> **The problem is not that you use non-European services. The problem is that you do not know what to do if they disappear.**

An example that stuck

In 2025 it was widely reported that the chief prosecutor of the International Criminal Court in The Hague, after US sanctions against the court, no longer had access to his email at a US provider. Accounts of exactly what happened differ. But for many organisations the principle suddenly became concrete: a decision by a foreign government can, through a supplier, directly affect a European organisation, even if that organisation itself has done nothing wrong.

The same can happen for less dramatic reasons: a price increase that makes a service unaffordable, a product that is discontinued, an account blocked by an automated check, or a provider that is taken over.

2 Three mechanisms behind the risk

Dependence on a non-European provider becomes a risk through three routes. They are unrelated to the quality or good intentions of the supplier.

01

Jurisdiction

A provider is subject to the law of the country where it is established. The US CLOUD Act (2018), for example, allows US authorities to request data from US providers, even if that data is stored in Europe. That can conflict with the GDPR.

02

Sanctions and export rules

Governments can require companies to stop providing services to certain people, organisations or countries. The supplier then has no choice. For you, that can mean a service disappears, or a client or counterparty can no longer be reached.

03

Technical control

With cloud services and connected devices, the provider holds the technical keys. Updates, licence checks or switching off features can happen remotely, with or without bad intent.

Not only the United States

The debate often focuses on US tech companies, because they serve most of the market. But the same applies to providers from other countries. A clear example is connected vehicles, charging points, inverters and other equipment with software that can be updated or switched off remotely. In January 2025 the United States adopted rules barring Chinese and Russian software from connected vehicles from model year 2027, for exactly that reason. For European companies with vehicle fleets, logistics or energy installations, this is a direct question: who can operate your equipment remotely?

Why now?

These risks have always existed, but three developments make them more urgent: geopolitical relations have become less predictable, more and more business processes run exclusively in the cloud, and European regulation now expects organisations to demonstrably manage these risks.

3 The hidden chain

The biggest dependencies are often not in your own IT, but with your service providers. Your accounting firm, payroll provider, IT manager or auditor also uses software and hosting, and you do not see those choices.

Example: the financial chain

A fund manager often outsources fund administration to a specialist administrator, works with a depositary or trustee and an external compliance firm. Each of these parties runs on its own systems: an administration package, a document platform, an email environment, a hosting provider. The manager remains ultimately responsible, but often has no view of which parts are outside Europe.

LINK	TYPICAL QUESTION THAT REMAINS UNANSWERED
Your own organisation	Which services do we use, and which are business-critical?
Direct service provider	Which software and which hosting does their service to us run on?
Subcontractors (sub-processors)	Where is the data stored and which law applies to these parties?
Contract	What has been agreed on termination, data transfer and exit?

The answer to these questions usually does exist, in data processing agreements, lists of sub-processors and contract terms, but it is fragmented and takes a lot of time to collect. That is exactly where things go wrong in practice.

Tip. Ask your most important service providers for their current list of sub-processors, including country of establishment and data location. Under the GDPR, a processor may not engage a sub-processor without your authorisation and must inform you of changes in advance.

4 What regulation requires

European rules do not oblige anyone to use only European suppliers. They do require organisations to know their dependencies, manage risks and be able to switch when necessary.

REGULATION	FOR WHOM	WHAT IS RELEVANT
DORA Regulation (EU) 2022/2554, applicable since 17 January 2025	Banks, insurers, investment firms, authorised fund managers and other financial entities (only registered sub-threshold AIFMs are excluded)	Register of all ICT service contracts; risk assessment before contracting; mandatory exit strategies for ICT services supporting critical or important functions; attention to concentration risk.
NIS2 Directive (EU) 2022/2555	Essential and important entities in sectors including energy, transport, healthcare, digital infrastructure and public administration	Duty of care for supply chain security, including assessment of suppliers and service providers.
GDPR Regulation (EU) 2016/679	Any organisation processing personal data	Transfers to countries outside the EEA only with appropriate safeguards; since the Schrems II judgment (2020) it must be assessed case by case whether the law of the receiving country undermines those safeguards.
Data Act Regulation (EU) 2023/2854, applicable since 12 September 2025	Customers and providers of cloud services	Right to switch to another provider; switching charges are being phased out and disappear from January 2027. That makes an exit plan more workable in practice.

Please note. This table is a simplified overview and not legal advice. Exactly which obligations apply to your organisation depends on your sector, size and licences. For each regulation you can check on the legislation pages whether it applies to you.

5 From insight to exit plan

Plan EU uses a fixed approach in five steps. You can go through the first steps yourself with the scan; for the in-depth work and the exit plan, we guide you.

1

Domain

Based on your domain name we map publicly visible services, such as email and hosting providers.

2

Sector

Your sector determines which regulation and which typical dependencies are relevant.

3

Questions per area

Short multiple-choice questions per area: office software, accounting, payments, hosting, communication, service providers.

4

Report

For each answer, a rating on the Plan EU risk scale, with an explanation and European alternatives.

5

Exit plan and advice

A step-by-step plan for every non-European service. Where needed we review contracts, collect suppliers' answers and guide the switch.

The risk scale

● Sovereign	◐ Manageable	○ Vulnerable	■ Critical
European provider, data and management within the EU.	Non-European, but not business-critical or easy to replace.	Non-European and important to your operations.	Non-European, business-critical and hard to replace.

The scan stores no data that is not needed for the report. We assess situations, not suppliers: the report describes factually where a service is based and what that means for you. More on this in our methodology.

6 What a good exit plan contains

An exit plan is not a moving plan. It is preparation that ensures you can switch when needed, planned or under pressure. For every service rated vulnerable or critical, record at least the following:

- **Function and owner.** Which business process depends on the service and who is responsible?
- **Data.** Which data is stored there, in which format can you export it, and how often do you do so?
- **Alternative.** At least one European alternative, with a rough estimate of cost and lead time.
- **Contract.** Notice period, agreements on data transfer, exit assistance and your rights under the Data Act.
- **Emergency scenario.** What do you do in the first 48 hours if the service suddenly disappears?
- **Dependencies.** Which other systems or integrations stop as well?
- **Review date.** When is the plan reviewed and rehearsed?

For dozens of widely used services, such a plan is ready in our exit plans.

Five things you can do this month

1. List the ten services without which your organisation would grind to a halt within a day.
2. For each service, note the provider's country of establishment and where the data is stored.
3. Ask your most important service providers for their list of sub-processors.
4. Test whether you can actually export your most important data in a usable format.
5. Run the scan on plan-eu.eu for a first overview.

Sources

- Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA), in particular Article 28.
- Directive (EU) 2022/2555 (NIS2), in particular Article 21 on supply chain security.
- Regulation (EU) 2016/679 (GDPR), Chapter V; CJEU 16 July 2020, C-311/18 (Schrems II).
- Regulation (EU) 2023/2854 (Data Act), Chapter VI on switching between data processing services.
- Clarifying Lawful Overseas Use of Data Act (CLOUD Act), United States, 2018.

plan EU

PLAN-EU.EU

About Plan EU

Plan EU helps European organisations map their digital dependencies and draw up a workable exit plan. With an online scan, a clear report and tailored advice, from a DORA second opinion to guidance when switching to a European alternative.

plan-eu.eu

info@plan-eu.eu

Plan EU is an initiative of Luce Holding B.V. This white paper has been compiled with care on the basis of public information as of October 2026 and is intended as general information. No rights can be derived from it and it does not constitute legal, tax or investment advice. Plan EU is not an institution of the European Union.