alliuris

ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS.

Digital Due Diligence for Data Sovereignty

Ulrich Herfurth, attorney at law in Hanover and Brussels

May 2025

With increasing digitalisation, companies are shifting key value-added processes to external digital infrastructures, platforms and service providers. This development is leading to new forms of technical, economic and legal dependencies, which must be analysed separately as part of digital due diligence. Digital dependencies affect not only day-to-day operations but also the company's strategic capacity to act following an acquisition.

Strategic significance of digital dependencies

In the context of a transaction, it is therefore necessary to assess the extent to which the target company is dependent on individual technology providers, platforms or proprietary systems. Monostructures, a lack of alternatives or high switching costs can significantly restrict flexibility and represent a significant value and integration risk.

Cloud usage and outsourcing structures

A key focus of this area of review is the use of cloud services and outsourced IT services. It is necessary to analyse which systems and data are operated in the cloud, which cloud models (IaaS, PaaS, SaaS) are used, and which contractual provisions govern their use.

As part of digital due diligence, it is particularly important to check whether clear contractual provisions exist regarding availability, data security, liability and exit scenarios. Missing or inadequate provisions can make switching providers effectively impossible or associated with significant risks. Equally relevant is the question of whether the acquirer can integrate the existing cloud structures into their own IT landscape or whether fundamental adjustments are required.

Outsourcing structures affect not only technical operations but often also development services, support functions or security-related activities. Dependence on individual service providers must therefore be critically assessed, particularly where know-how, access rights or key processes have been fully outsourced.

Relationships with third countries and international data flows

Digital dependencies are often linked to third countries, for example where cloud providers, data centres or service providers are based outside the European Union. As part of digital due diligence, it must be assessed whether personal or business-critical data is processed in third countries and which legal mechanisms are used for this purpose.

In addition to data protection issues, geopolitical and regulatory risks also play a role here. Changes to the legal framework, export controls or government access rights can compromise the availability and confidentiality of data. These risks must be assessed not only from a legal perspective but also from a strategic one.

Vendor lock-in and technological path dependencies

A frequently underestimated aspect of digital dependencies is so-called vendor lock-in. Proprietary technologies, specific interfaces or non-standardised data formats can mean that switching providers involves disproportionate effort. As part of digital due diligence, it is therefore necessary to analyse whether the systems in use are based on open standards and whether realistic migration scenarios exist.

Such path dependencies have a direct impact on the company's future viability. They can slow down innovation processes, increase costs and limit strategic flexibility. It is therefore of particular interest to the acquirer whether these dependencies are deliberately managed or have simply arisen historically.

AI systems and data-driven applications

The use of artificial intelligence and data-driven applications is becoming increasingly important in many business models. As part of digital due diligence, it must be examined whether and to what extent AI systems are used, what functions they perform and on what data they are based.
Particular attention should be paid to issues of data quality, the traceability of decisions, and dependence on external models or platforms. AI systems whose functioning is not sufficiently documented or explainable can give rise to significant legal and operational risks. Furthermore, it must be analysed whether appropriate governance structures exist to ensure the responsible use of AI.

Data strategies and the commercial use of data

Data represents a key intangible asset for many companies. Digital due diligence should therefore also focus on the strategic use of data. It must be examined whether the target company has a clear data strategy, how data is collected, analysed and monetised, and what legal and technical framework conditions apply.

Missing or inconsistent data strategies can result in existing data potential not being utilised or new business models being built on an uncertain foundation. It is therefore in the acquirer's interest to ascertain whether data is understood as a strategic resource and managed accordingly.

Data rights

The legal ownership of data is becoming increasingly important in the context of digital due diligence. It must be clarified which data belongs to the target company, where it is stored, and what access and usage rights exist. This applies both to the company's own data on third-party systems, such as those of cloud providers, and to third-party data to which the company has access.

Unclear data rights can not only give rise to regulatory risks but also significantly reduce the economic value of data-driven business models. The review of the legal framework must therefore also incorporate data protection and contract law aspects.

Data Use Agreements

Data Use Agreements (DUAs) are a key tool for ensuring the long-term availability and responsible handling of data within the company. They establish clear and binding frameworks for the use of data across departmental and project boundaries, as well as in collaboration with external partners. In doing so, they make an important contribution to legal certainty, organisational clarity and the long-term usability of data sets.

A key advantage of Data Use Agreements lies in ensuring compliance and reducing risks. Clearly defined

responsibilities and usage rules ensure that legal requirements, such as those relating to data protection or the protection of trade secrets, are met. At the same time, such agreements prevent data from being used in an uncontrolled manner, misused, or, out of caution, no longer shared at all. In this way, DUAs help to ensure that data remains available, discoverable and correctly interpretable in the long term.
Furthermore, data usage agreements foster trust and collaboration within the company as well as with external stakeholders. When it is transparently regulated who is permitted to use data and under what conditions, the coordination effort is reduced, and data exchange becomes more efficient. This facilitates the multiple use of data – for example, for analysis, reporting or the use of AI – and thus increases the economic value of the existing data.

In terms of content, data usage agreements should specify the purpose and scope of data use, i.e. clearly define what the data may be used for. Equally important are provisions regarding access and usage rights, responsibility for data quality, timeliness and documentation, as well as appropriate security and protection measures. In addition, the data lifecycle, including retention, archiving and deletion periods, the conditions for disclosure to third parties, and liability and penalty provisions should be laid down. Finally, the handling of the data following the termination of the agreement must also be clarified.
Overall, data usage agreements thus form a central pillar of sustainable data governance. They combine legal safeguards with operational clarity and create the conditions for using data within the organisation in a sustainable, responsible and value-adding manner.

Cloud and platform strategies in a competitive context

Beyond a purely contractual perspective, it is necessary to analyse the role that cloud and platform solutions play in the competitive environment. Cloud architectures can offer significant economies of scale, but at the same time lead to the standardisation of IT structures. As part of digital due diligence, it must therefore be assessed whether the target company gains competitive advantages through its cloud strategy or whether it positions itself as technologically interchangeable.

AI governance and strategic responsibility

The use of AI systems requires a dedicated governance structure that goes beyond traditional IT governance. It is necessary to assess whether clear responsibilities exist for the development, deployment and monitoring of AI, and whether ethical, legal and economic risks are systematically addressed. A lack of governance structures can result in AI applications achieving short-term efficiency gains but creating significant liability and reputational risks in the long term.

Broader strategic perspective and long-term controllability

The analysis of digital dependencies is closely linked to the question of the company's long-term controllability. Of particular strategic relevance is whether the target company is capable of making technological decisions independently or whether it is effectively controlled by external providers. These dependencies affect not only costs but also the pace of innovation and marketability.

Data strategy as a value-creation and control instrument

Finally, the data strategy should be viewed as the unifying element across all digital due diligence areas. A consistent data strategy defines which data is strategically relevant, how it is protected, used and shared, and what investments are required for this. As part of digital due diligence, it must be assessed whether such a strategy exists or whether data is merely used opportunistically. This assessment is of central importance for the company's long-term value development.

Risk assessment and transaction relevance

The analysis of digital dependencies, cloud and outsourcing structures, as well as AI and data strategies, provides key insights for the overall assessment of a transaction. High levels of dependency, a lack of exit options or unclear governance structures can trigger significant investment requirements following the acquisition.

These risks must be taken into account when determining the purchase price, structuring the transaction and planning post-merger integration. Digital due diligence thus helps not only to identify existing risks but also to realistically assess the target company's long-term strategic positioning.

+ + +

The Alliuris Group

The Alliuris Group consists of 20 law firms and 400 business lawyers within Europe, Asia and America.

Contact	Ulrich Herfurth Alliuris Communication
Web	www.alliuris.law
Mail	info@alliuris.org
Fon	+49-511-307 56-20
Fax	+49-511-307 56-21

IMPRINT

EDITORS: ALLIURIS A.S.B.L. ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS | BRUSSELS

MANAGEMENT: Luisenstr. 5, D-30159 Hannover
Fon +49-511-307 56-20, Fax +49-511-307 56-21

BRUSSELS · PARIS · LONDON · UTRECHT · KNOKKE · LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HELSINKI · HANOVER · VIENNA · SOFIA · WARSAW · POZNAŃ · ATHENS · ISTANBUL · DUBAI ·MOSCOW · GUANGZHOU · BEIJING · SHANGHAI · NEW DELHI · MUMBAI · NEW YORK · SAO PAULO ·BUENOS AIRES · LIMA · SANTIAGO DE CHILE MEXICO CITY

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt