

From Data Protection to Value Creation in Finance: Data Valuation, Accounting, Mergers & Acquisitions and Governance

Practical applications in Data Driven Organisations

Joint study by the CNPD Luxembourg “Dispositifs de confiance”, the CNIL “Analyse Economique” and the ICO “Economic Analysis” departments.

Autumn 2026



Published in October 2026.

This report is the result of a joint study by the CNPD Luxembourg “Dispositifs de confiance”, the CNIL “Analyse économique” and the ICO “Economic Analysis” departments.

Authors: **Elena-Cristina GERTH** (Chef de service “Dispositifs de confiance”, CNPD Luxembourg), **Angeliki LASHAND** (Head of Economic Analysis, ICO), **Aymeric PONTVIANNE** (Chef de mission “Analyse Economique”, CNIL)

Contributors: Edouard Bassard (Service “Dispositifs de confiance », CNPD Luxembourg), Oscar COMBE (Analyse économique, CNIL), Ben MAHON (Economic Analysis, ICO)

Editorial support: Angelica FERNANDEZ (Service “Guidance”, CNPD Luxembourg), Ryan DUCHÊNE (Service “Communication Digitale”, CNPD Luxembourg)

Acknowledgments: We would like to acknowledge the support of Alain Herrmann (Commissaire CNPD Luxembourg), Tom Reynolds (Director of Economic Analysis, ICO), and Vincent Villette (Secrétaire général, CNIL).

We would also like to express our gratitude to the individuals who participated in this study through surveys and interviews, including participants of the Data Protection Laboratory (DaProLab), hosted by the CNPD in Luxembourg, at its session on 6 July 2026.

Disclaimer: This document represents the findings of the study conducted by the CNPD, CNIL and ICO on the interaction between data protection compliance and value creation in data driven organisations, it aims at encouraging discussion with market participants, academics and other regulators on this topic. The emerging and encouraged best practices reported shall have no legal effect.

Table of Contents	3
Executive summary	4
1 Introduction and Objectives	8
1.1 Context and Rationale of the Study	8
1.2 Objectives and Key Questions of the Study	9
2 Analytical Framework	11
2.1 Overall Methodological Approach and Interviews	11
2.2 Literature review	12
2.3 Quantitative surveys	19
3 Study Findings and Key Practices	21
3.1 Strategic aspects of data protection for organisations	21
3.2 Accounting treatment and financial exposure linked to data topics	31
3.3 Transactional and valuation impacts of data protection compliance	47
4 Emerging Good Practices	61
5 Conclusion	65
6 References	67
Annexes	70
A Statistical findings	70
B Practical example: Business combination involving a customer database (IFRS 3, IAS 38 and IAS 36)	94
C Stakeholders consulted	99

Executive summary

Data is a fundamental driver of economic activity, innovation and organisational performance. As organisations increasingly rely on data to support decision-making, develop new products and services, manage risks and enable emerging technologies such as artificial intelligence, the question extends from how data should be protected and governed, to how its value can be recognised, measured and leveraged. It is therefore, timely to reflect on data as a source of value creation in an operational way.

Against this backdrop, the Commission Nationale pour la Protection des Données (CNPD) in Luxembourg, the Commission Nationale de l'Informatique et des Libertés (CNIL) in France, and the Information Commission's Office (ICO) in the UK, conducted a joint study to examine the relationship between data protection compliance, data governance and value creation. While the study mostly drew on evidence from stakeholders active in financial markets, its findings are relevant to organisations facing similar challenges in the management and use of data in the digital economy as a whole.

The study was designed around three

complementary areas.

First, it examined whether data protection compliance and broader data governance practices are perceived solely as regulatory requirements, or as strategic capabilities that contribute to trust, organisational resilience, competitiveness and long-term performance.

Second, it explored the accounting consequences of the general recognition of data as an “economic asset”, reviewing existing valuation methodologies, the conditions under which data-related assets may be recognised under current applicable accounting standards, and the extent to which existing financial reporting frameworks are capable of reflecting value creation in a data-driven economy.

Third, it analysed the role of data protection compliance and data-related questions in investment decisions, mergers and acquisitions and related due diligence processes, where data quality and data protection compliance increasingly influence risk assessments and transaction outcomes.

To answer these questions, the study

combined a review of academic, professional and regulatory literature, stakeholder interviews, and a quantitative survey with companies. It explored how organisations, issuers, investors, financial sector associations, auditing firms, rating agencies, legal firms and consulting companies assess data protection compliance impacts and more generally data-related opportunities and risks, and how these considerations influence organisational decision-making and financial reporting.

The findings highlight the well-documented convergence between data protection, cybersecurity and AI governance, reflecting the need for integrated approaches to managing data-related risks and opportunities.

Moreover, the study showcased, as its main result, the relevance of an integrated approach of data-related questions for organisations when it comes to value creation. First recognising and assessing the upsides of compliance, the role of data in organisations and future cash flow generation and then taking into account and further inquiring about data risks likely to reduce these benefits, with a view to mitigating them. This two-step approach allows the complex reality of managing

transparency to be translated into operational performance for organisations.

More specifically, **a major focus of the study was the economic value of data which was explored by reviewing the growing body of literature dedicated to the valuation of data and by analysing existing valuation methodologies that could be applied to estimating the value of compliance with personal data, including cost-based, income-based and market-based methods.** The findings demonstrate the existing gap between valuation methodologies for data and those that are suitable for valuation of personal data as an asset and the partial recognition of the importance of personal data in environmental, strategic and governance frameworks. These methodological and reporting limitations have led to a growing interest among organisations that operate with personal data, academics, practitioners and policymakers to understand existing methods for measuring and valuing data, assessing its contribution to organisational value, and examining the financial and accounting implications of its recognition as an asset.

Furthermore, the study also examined the conditions under which data may be recognised as an asset under existing accounting frameworks. **Particular attention was given to the treatment of internally generated data and to the accounting criteria required for asset recognition.** The study identified the recurring observation within the literature and among stakeholders that although data is frequently described as one of organisations' most valuable resources, only part of its value appears in financial statements. This has led to growing discussion regarding whether existing accounting standards, developed in a different economic context, could more adequately capture value creation in data-driven business models.

In addition, **the study investigated the role of data-related topics, including compliance and governance, in transactions and investment processes.** The findings show that data-related considerations and data protection compliance are becoming increasingly important in mergers and acquisitions, due diligence exercises, investment assessments and corporate risk evaluations. Data protection compliance, data quality, accessibility and security are increasingly viewed as factors that can influence transaction outcomes, organisational resilience and long-term value. In this context, a proper economic valuation of data assets, compliance and governance appears key to understanding and showcasing

value creation and reduces uncertainty and risks.

Finally, the report identifies emerging trends and shares a number of good practices observed across organisations and market participants. These practices are intended to support how to manage compliant data assets, improve preparedness for transactional and due diligence processes, and enable organisations to derive strategic value from data, leveraging compliance with data protection requirements.

Overall, the study highlights that the value of compliance with data protection extends beyond its operational use. Effective data protection can support organisational resilience and trust, while also influencing how organisations are assessed in transactions and investment decisions and in consumer confidence and trust perceptions. It is time to recognise the overarching economic importance of data into operational methodologies regarding its valuation, accounting treatment and representation in financial reporting.

With these findings and emerging good practices in mind, the report aims to help organisations better protect, assess and derive value from data assets throughout their lifecycle and to improve transparency in standardised information. This will in turn reassure consumers that their data protection rights are respected.



1 Introduction and Objectives

1.1 Context and Rationale of the Study

Data protection regulators have duties to ensure that data protection legislation is upheld. They also have to give consideration to markets functioning well, allowing participants to operate within fair and competitive environments, while protecting people's personal data rights.¹ In delivering these duties, they aim to reduce uncertainty for regulated organisations and enhance trust for people in the use of their personal data. They inform their thinking by developing knowledge of the markets they regulate, engaging with stakeholders and developing awareness of the benefits and risks that arise from current and evolving uses of personal data. They use these insights to identify and respond to short term market issues and ensure longer term stability and resilience that supports economic growth, competition and innovation.

As a major contributor to economic value creation, the financial sector is also among the most data-intensive sectors of the economy. Data-driven activities, including use of personal data, are a core part of business models in financial markets. It follows that compliance with data protection and data governance are important components of organisational operations. Similarly, organisations in financial markets are familiar with the importance of incorporating trust, transparency and effective risk management in their corporate governance. Therefore, this thinking can be extended to explore whether organisations view data protection only as regulatory requirement, or if they also identify it as a potential driver of organisational value.

In this context, the Commission Nationale pour la Protection des Données (CNPD), the Commission Nationale de l'Informatique et des Libertés (CNIL), and the Information Commission's Office (ICO) have collaborated to better understand how data protection compliance

¹ 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. General Data Protection Regulation 2016, Article 4 and the United Kingdom General Data Protection Regulation 2016, Article 4

is perceived within financial sector organisations. The initiative involved exploratory research with stakeholders and organisations in financial markets to identify whether compliance and robust data governance practices are regarded as strategic assets that contribute to organisational resilience, competitiveness, and value creation.

For the purpose of this study reference to "data" comprises of all data that organisations would hold within the usual conduct of their operations, including personal data. There is specific reference to "personal data", where the discussion concerns practices, legislation or treatment that solely apply to personal data.

1.2 Objectives and Key Questions of the Study

Regulators have long established experience in the benefits of cross regulatory collaboration. This is a cross regulatory topic of interest and by collaborating, CNPD, CNIL and ICO have combined resources to gather diverse and informed views from financial markets participants in Luxembourg, France and the United Kingdom. Working together provides for a broader understanding of the research questions in different markets and thus, an enhanced view of the benefits that regulation can provide for organisations.

1.2.1 Objectives of the study

The objective of this study is to generate insights that support regulators in better understanding the

economic and strategic implications of data protection compliance and data governance frameworks in financial markets. **The study aims to explore how personal data-related governance frameworks influence organisational performance, risk assessment, investment and transaction decisions, and corporate valuations, while also examining the extent to which data and personal data can be recognised, measured, and reported as an asset in financial statements under existing accounting frameworks.**

While the study considers the perspective of financial markets and financial market participants, the learnings extend beyond the financial services sector and can be used to inform regulatory thinking across a range of sectors. They can also be used to identify further areas where further research would be beneficial. The findings and best practices could be considered within country specific regulatory context to support the compliant use of data to create strategic and operational value, facilitate use of AI in a data protection compliant manner and mitigate cyber security risks.

The findings are shared in this report to facilitate collective knowledge generation amongst stakeholders, market participants, academia and regulators. To this end this study also includes emerging trends, valuation approaches and best practices identified with a view to facilitate knowledge sharing across market participants.

1.2.2 Key questions

The study aimed to examine three topics, each broken down into several questions that guided the approach taken during interviews, survey and literature review.

A. Perceptions and strategic value of data protection compliance

- How is data protection compliance perceived within the financing ecosystem?
- To what extent do investors, lenders, rating agencies, auditors and transaction advisors assess data governance, data quality and compliance when evaluating corporate resilience and long-term performance?
- How are data-related considerations incorporated into organisational decision-making?
- Which practices enable organisations to incorporate compliance with data protection in cybersecurity and AI strategies?

B. The treatment of compliance with data protection as an asset in accounting frameworks

- Do strong personal data governance frameworks and privacy practices generate measurable economic benefits for organisations?
- What methods exist for recognising, measuring, and valuing data, including personal data, as a corporate asset, and under which accounting conditions can data-related assets be reflected in financial reporting?

C. The value of compliance with data protection in financial transactions

- How do data protection, cybersecurity, and compliance-related factors affect corporate valuations, risk assessment, and financial performance?
- How are data governance and compliance considerations integrated into financial markets transactions and processes, such as mergers and acquisitions (M&A), due diligence processes, and investment decisions?



2 Analytical Framework

2.1 Overall Methodological Approach and Interviews

The study focuses on the role of data protection compliance, data governance frameworks, and data-related assets within organisations operating in Luxembourg, France and the United Kingdom, with particular attention to publicly listed companies and organisations that are active participants in capital markets.

To provide a comprehensive understanding of how data-related considerations are assessed in practice, the study also includes organisations that influence or support investment, valuation, and reporting processes, such as audit firms, accounting professionals, valuation specialists, credit rating agencies, consultancies and transaction advisors.

In addition, the study takes into account the regulatory and reporting environment in which these organisations operate. It therefore, incorporates the perspectives of relevant regulatory authorities and standard-setting bodies to examine how data protection compliance, data governance frameworks including cybersecurity considerations, and the recognition

and measurement of data-related assets are reflected in corporate reporting, valuation frameworks, and financial market practices.

This report relies on both primary and secondary research for the study, involving qualitative and quantitative evidence gathering.

A literature review was conducted as a first step, to identify the approaches available, if any, to quantify the value of data and personal data. The literature review focused on robust and reliable sources that are either peer reviewed, published by public sector institutions that follow public research and analysis principles, such as reports from regulators, or are published by reputable organisations, alongside the methodology and assumptions. The findings of the literature review were used to inform development of the interviews conducted. Existing Environmental, Social and Governance (ESG) frameworks were reviewed to identify whether these included specific references to personal data. Existing accounting standards frameworks were also reviewed to identify if these include rules covering the quantification and valuation of personal data as an asset in company accounts.

Semi-structured interviews were conducted from March to May 2026 with professionals and experts from organisations in financial markets. Twelve interviews were completed with organisations including consultancies with expertise in law, application of data protection legislation and mergers and acquisitions, as well as auditors, financial sector associations, investor associations, stock exchanges, rating agencies and market authorities. The interviews were conducted either in hybrid format, in person and online, or online.

Interview responses were summed up thematically, following the themes used in the questionnaires. Insights then emerged from analysis of the responses in the areas of quantification of the value of data, other indicators of the value of personal data, views about the role of compliance with data protection in organisational governance, cyber security, treatment of data in accounting practices, the value of data in mergers and acquisitions, the value of compliance with data protection in corporate ratings and the role of compliance with data protection in AI.

Furthermore, the project was first presented at the Venice Privacy Symposium Conference in April 2026, to gather feedback from the Conference participants. After the qualitative phase, online surveys were also conducted with data protection officers (DPOs) in France and in Luxemburg in May 2026 to gather quantitative evidence.

The preliminary findings of the study were shared at the CNPD Data Protection Laboratory (DaProLab) in July 2026, in order to invite evaluation

of the findings from expert audiences and to gather further insights. All the organisations contacted for the interviews were invited to the event. This report presents the findings of our study, having collected, analysed and considered responses, evidence and data from the interviews, the engagement and the surveys we conducted respectively.

2.2 Literature review

The literature review findings focus on data valuation, accounting treatment of data, and cybersecurity. The objective was to assess the state of the art of knowledge regarding the recognition of personal data and data-related governance practices in corporate reporting and valuation processes. In particular, the literature review examined whether existing accounting frameworks adequately capture the value of data assets, how data protection and governance considerations affect valuation and investment decisions, and whether compliance-related factors translate into measurable financial outcomes for companies. It is important to note that our literature review often identified evidence for valuing or accounting for the value of ‘data’, which does not differentiate between data and personal data. Where the literature refers to data, we also refer to data in the literature review and where the literature or our conclusions refer to personal data, we make explicit reference to personal data.

2.3.1 Data valuation

Data has several unique characteristics that make it challenging to value as an asset. Firstly, data has an important use value component. The value of

data for one firm is very different to the value for another. Valuations of the same dataset can therefore be different in magnitude for different organisations (Veldkamp, 2023). Moreover, data is generally considered non rivalrous, meaning that it can be used repeatedly, even by different organisations, without losing its value. Nevertheless, some data loses value over time, as it goes out of date. In addition, data is generally non-excludable meaning that once it is made available, it is difficult to prevent others from accessing or using it. However, this characteristic does not always hold, particularly when data is used as an input for a product or service and access can be restricted through legal, technical, or contractual mechanisms. In some markets, an organisation that holds data can prevent other organisations from using it. Most data is a by-product of other business activities more often than an asset procured entirely in its own right (Veldkamp, 2023). Organisations may collect large amounts of data through other transactions, for example through data on online purchases and they may also collect data through offering free services such as online search engines or social media services.

This feeds into another key characteristic, increasing returns and economies of scale. Increasing business activity generates more data, which in turn can drive more activity, in a virtuous circle. This means that data can create large economies of scale and barriers to entry (OECD, 2022). Finally, data often has low specificity. It can be used for a large variety of purposes and re-used for purposes other than those specifically intended (OECD, 2022). One key caveat that is largely absent from the literature is the distinction between

personal and non-personal data.

The characteristics discussed largely hold for personal data, however, there are instances where personal data can be excludable. In these cases, even though an organisation cannot prevent another organisation from using it, organisations that hold large volumes of personal data and benefit from the existence of network effects, may act as barriers to entry or to growth for other organisations that hold the same personal data. This tends to be market and purpose specific, where there are a few incumbents or where there is little product or service differentiation. Similarly, although organisations can use personal data for a variety of purposes, these have to be consistent with the data subject’s rights in respect of their personal data, guaranteed by data protection law.

Data drives value for organisations in several ways. Veldkamp (2023) argues that data benefits organisations through four channels, improving business processes, reducing risk, growing market power and innovating. **However, unlike most other assets the primary benefit of data is that it allows organisations to make better, more informed decisions and reduces uncertainty. This means that pricing tools usually used in finance for valuing risk are central to valuing data. Similar to Veldkamp, Farboodi, et al. (2025) find that most value of financial data comes from risk reduction.**

Data is a key pre-requisite for AI deployment and training of AI models (Babina, et al., 2024). This is a key driver for future valuations of data. Deloitte (2025) argue that **targeted datasets are vital for AI usage in business. They also argue that valuing data can help**



frame the importance of investments in data for boards. Valuing data could help channel investment towards key areas necessary for future growth, and with boards targeting AI rollout this increasingly could be data collection, storage, processing, and compliance.

Tambe et.al (2020) quantify the benefits of increasing data investment. Rather than focusing purely on data, they utilize digital capital, which incorporates data, but also other intangible assets, such as skills within organisations required to process and use data. They find that since 2010 digital capital grew at roughly double the rate of physical IT capital. They also find that digital capital accumulation is a significant predictor of firm productivity over the next three-year period. Like Veldkamp, Xiao et al (2025) argues that data creates value by reducing

risk, allowing firms to better understand consumer demand, improving performance, and reducing information asymmetry. They argue that data assets significantly enhance the quality of firms' investment. The effect is greater for larger firms which are better able to invest in analysing and utilising data.

There are five broad valuation methods widely agreed throughout the literature (Deloitte, 2025), (Veldkamp, 2023), (OECD, 2022), (Sargent & Denniston, 2023). The income method estimates expected revenue from data assets. This can be done either with present value or expected future value over a certain time-period. Deloitte (2025) propose **three sub methods. Firstly, the multi-period excess earnings method which directly estimates cash flows attributable to data and subtracts earnings proportional to**

those from other assets involved. The method directly forecasts the cash flows attributed to data, then deduct charges mobilised to support data operations, or compliance capital expenditure, and discount the net flows to present value. This method is adapted when the contribution of a data set to business profitability can be clearly identified.

Secondly, the relief-from-royalty method values data by estimating the royalties the company avoids paying because it owns the data. This is useful when data clearly involves avoiding costs if it was acquired elsewhere and is particularly useful where comparable licensing agreements exist for equivalent data sources. The with-and-without (differential cash flow) method compares forecast revenue without using a data asset to those with the asset. It compares the company's projected

performance with using the data and its performance without it. The present value of this difference can be considered as the value of data. This method can be used when the upside generated by data is a cost avoidance.

The cost method estimates the value of a data asset by estimating the cost of replicating or replacing the data asset. Rather than directly measuring that value of the data it measures the cost of replacing the dataset with an equivalent one of similar quality. Where an equivalent dataset is available for purchase, or can be easily be constructed, the cost method can be easily calculated. There are two slight variations of this method. Firstly, the historical cost method uses past costs incurred in gathering the dataset to estimate replacement costs. This doesn't take into account technological advancements which

could reduce cost, or indeed the passage of time which could make gathering some historical data impossible. The reproduction cost method measures the direct and indirect costs of creating a dataset, or an estimate for what a third-party provider would quote to build an equivalent dataset. While the cost method can be simple to calculate, where the dataset is a unique, proprietary dataset the cost method may not be possible to calculate.

The final method is the market method. This looks at prices paid for broadly comparable assets. Adjustments are often made in practice for some differences between datasets. As the data broker market is rather opaque, the prices of transactions are not always public, and many deals don't disclose the key features of the datasets necessary for the comparisons. The lack of dataset transactions, and information about those that do occur mean this valuation method is rarely used in practice (Deloitte, 2025). Deloitte largely recommend the method as a robustness check in combination with either the income or cost approach. In contrast, PwC recommends this method as the best approach when transactions are observable (PwC UK, 2020).

General best practice is to value data using two separate methods and attempt to get agreement between the estimates. The same broad valuation approaches have been also applied at a national level to help quantify data's economic contribution (OECD, 2022).

2.3.2 Accounting treatment

The treatment of data as an asset

in accounting is part of the broader reflection about the difference between what creates corporate value and what is captured in financial statements. The literature mainly reveals a gap in that regard.

A line of research argues that the relevance of value demonstrated in accounting statements has declined, as intangible assets have grown. Lev and Sougiannis (1996) show that capitalising R&D produces more value-relevant figures, Lev and Zarowin (1999) document the decline of financial-statement usefulness and Lev and Gu (2016) report a falling correlation between market and book values as intangible expenditure increases. This is contested by Li & McClure (2023), who find that incorporating items related to intangible assets and alternative performance does not lead to a decline in combined value relevance, but rather a more complex relationship.

Data is an intangible asset with distinctive properties. The ICAEW's 2025 report discusses the complexity of the mechanisms through which data creates value, the complexity of legal ownership and control, and the difficulty in reliable measurement.

These correspond to the IFRS recognition criteria: identifiability, control, and reliable measurement. Under the IFRS framework, an entity controls a resource only if it can direct its use and obtain benefits, yet, data-related laws, and privacy protections tend to reduce the firm's control. Estimating the value of data assets is complicated. The OECD (2022) describes the three valuation methods discussed previously, income, cost and market and concludes that none is superior. The purpose of this report is to provide advice as to good practices and contribute to overcome

such limitations.

As set out by the ICAEW, the literature on this matter is divided into two approaches. The enhanced-disclosure position holds that recognition is difficult given measurement and ownership challenges and favours richer note and narrative disclosure (Skinner, 2008) (Wyatt, 2008). The enhanced-recognition idea proposes amending IAS 38 to admit more internally generated intangible assets, because non-recognition itself may erode relevance (Lev, 2018) (Aboody & Lev, 1998). The IASB's ongoing review of IAS 38 is central to this. This asymmetry also manifests in goodwill; EFRAG's (2021) discussion paper notes that an acquired intangible asset can be recognised or included in goodwill, but the same asset developed

internally is expensed, leading to distortion in comparisons between acquisitive and organic growth². Consistent with this, Kepler et.al (2026) find that **consumer data is among the most important intangible assets recognised in acquisition purchase-price allocations, and as such, personal data currently appears in balance sheets almost exclusively through M&A. In short, the literature makes a case for a better recognition of data as an asset, including from a transparency and accuracy point of view.**

Gao et.al (2025) explore companies' inclusion of data in financial reporting, after the enactment of a new accounting rule addressing the recognition and disclosure of data resources. They combine two

² Goodwill is “an asset representing the future economic benefits arising from other assets acquired in a business combination that are not individually identified and separately recognised” (IFRS 3, Appendix A)





surveys of listed firms with 2024 archival data and find a wide gap between perceived value and practice, with only about 2% of firms recognised data assets in 2024. This was due to a reduction in the initial optimism, after compliance costs and litigation concerns led companies to wait before including data assets in financial reporting. Conversely, studies have explored the benefits of compliance. **A set of recent studies also examines the consequences of valuing data as an asset.** Guo et.al. (2026) assess how data assets affect firm value across five technology sectors, using accounting (ROA, ROE) and market (Tobin's Q, market-to-book) measures. **They find that data increased value provided by data assets varies widely between industries.** Wang and Hou (2025) show that **increased estimation of corporate data as an asset significantly reduces market pricing**

errors, thereby enhancing overall capital pricing efficiency.

2.3.3 Cybersecurity

There is a significant strand of literature examining the impact of cybersecurity breaches on company valuations. **While cybersecurity incidents are not the sole indicator of compliance with data protection, they can help illustrate the impact of non-compliance with data protection on company valuations.** Compliance can be difficult for markets to measure and assess but cybersecurity incidents provide an indicator of possible inadequate data protection practices, and have reputational effects that may impact investor and consumer decisions.

Day & Booker (2024) argue that the main mechanism for cybersecurity

breaches to have an effect on valuations is through company reputation. They find significant reductions in stock prices in the short run after a breach. This is echoed by Martins et.al (2025) who also find a short-term negative impact from cybersecurity breaches across 53 firms. **They also find high returns for cybersecurity firms when breaches occur, indicating that cyberattacks can cause an increase in spending on protective measures. Potential exposure to a cybersecurity breach and the remediation costs that follow could impact organisations' perception of the importance of protective measures and compliance with data protection.**

Both papers however have small samples sizes. Muktadir-Al-Mukit & Ali (2025) use a much larger sample size of 776 firms and find a similar negative effect on stock prices. **Firms with higher societal expectations of security and privacy, such as financial firms, experienced a larger impact from a breach. This is consistent with reputation being the main mechanism through which a breach impacts company valuations.** They also found that the source and credibility of news about a breach had a significant impact. Where a breach was reported in a 'credible' source, namely the Financial Times or CNN, the breach had a larger impact. A significant limitation is selection bias that is observed when credible sources are more likely to report large and consequential breaches. However, this could point to the importance of credible information about compliance in valuation decisions.

Cybersecurity breaches may provide insights into the short-term effects of data protection failures on valuations. There is also a strand

of literature examining valuations. However, the specific impact of data protection compliance, and more specifically compliance with personal data rules has not been extensively explored in the literature.

2.3 Quantitative surveys

Online quantitative surveys were undertaken in May 2026 with DPOs from France and Luxembourg, based on a questionnaire (25 questions) covering business models, governance, internal metrics, accounting treatment, M&A, cybersecurity and AI. The survey was not conducted in the UK due to time constraints.

In France, the survey covered DPOs of companies (private sector) with more than €5million turnover. It received 204 responses from companies of various sectors and sizes, representing not only the financial sector, but also a wide range of financial instrument emitters including SMEs, allowing coverage of a variety of situations with a good statistical relevance.

The DPOs were invited to complete the questionnaire with the help of the financial department of their company, to gather relevant knowledge on accounting and valuation practices. The findings are provided in Annex 7. The effects studied are statistically significant, reflecting the statistical quality of the database generated. Apart from the relevance of the topics, the idea of the survey was to build bridges between the legal and IT focus of the DPOs and the financial teams. This attempt proved to be successful within the context of conducting the survey in France, based on the feedback provided.

In Luxembourg, the survey sample consisted of company DPOs selected from the CNPD official register, prioritising companies with the largest employee populations. **The results of the statistical analysis conducted on the practices documented by the surveys can be found in Annex 7. They are based on descriptive statistics, correlation analyses and logistic regressions, where relevant.**

For both surveys in France and Luxembourg, the findings are presented in an aggregated format



and responses from individual companies were neither published nor shared between authorities participating to the project.

The CNIL, CNPD and ICO would like to thank the participating DPOs and their organisations for the time they dedicated to this study and for the quality of their insights and contributions on this emerging topic.

3. Study Findings and Key Practices

This section presents the principal findings of the study and the key practices identified through interviews with financial market participants and other relevant stakeholders, complemented by quantitative survey evidence and qualitative analysis.

The analysis is structured around three interrelated themes emerging from the qualitative and quantitative evidence. First, it examines the perception of compliance with data protection as a strategic asset in organisations, including the differentiated impact of data protection across financial market participants, its increasing strategic relevance, and the role of data governance as a prerequisite for AI deployment. Second, it explores the accounting implications of data and data protection-related matters, particularly their representation in financial reporting, the treatment of data assets, and the recognition, measurement, and impairment of databases under existing accounting standards.³ Third, it analyses the transactional and valuation implications of data protection compliance, including its influence on customer data value,

credit assessments, M&A transactions, data due diligence, and data asset valuation.

Collectively, these findings demonstrate that data protection has evolved beyond a compliance requirement to become a strategic, financial, and investment consideration in the data-driven economy.

3.1 Strategic aspects of data protection for organisations

3.1.1 Differentiated Perception of Data Protection Across Financial Market Participants

The findings indicate that the significance of data protection is not uniform across financial market actors. Rather, its perceived value, associated risks, and strategic relevance vary according to stakeholders' functions, regulatory responsibilities, and decision-making objectives. Across the interviews, participants consistently highlighted that data protection has evolved beyond a compliance requirement

³ The core principle in International Accounting Standard 36 (IAS 36) is that an asset must not be carried in the financial statements at more than the highest amount to be recovered through its use or sale. If the carrying amount exceeds the recoverable amount, the asset is described as impaired. IAS 36 Impairment of Assets

and is increasingly integrated into broader considerations relating to governance, risk management, operational resilience, and value creation.

For investors and financial institutions, data protection maturity is generally viewed as an indicator of governance quality in data-intensive environments. Interview participants associated robust data governance frameworks, including for data protection, with greater operational reliability, improved risk management, and enhanced organisational resilience. Conversely, weak data governance frameworks may be perceived as sources of downside risk, particularly in organisations that process significant volumes of personal data. **In this context, privacy-by-design principles are increasingly expected to be embedded within operational and decision-making processes, reflecting the growing importance of data governance in investment and risk assessments.**

Auditors, consultants, and legal advisors indicated that assessments typically examine the existence of personal data inventories, and the lawfulness of processing activities. Deficiencies identified during these reviews may affect transaction timelines, increase remediation costs, or influence valuations. **These findings suggest that data protection considerations are becoming increasingly embedded within financial, legal, and transactional assessments.**

For rating agencies, data protection is primarily considered within broader assessments of cybersecurity, operational resilience, and enterprise risk management. **Participants explained that analyses frequently**

incorporate indicators such as data breaches, ransomware incidents, and other cyber-related events. In this context, the maturity of data governance frameworks is considered relevant, where it may influence an organisation's operational performance, resilience, or long-term financial profile.

Interview participants noted that experience from past data breaches and cyber incidents has prompted many organisations to strengthen their data governance and risk management frameworks. In a number of cases, such events have led to increased management and board-level oversight of data-related risks, reflecting a growing recognition of the potential financial, operational, and reputational consequences of data protection failures. **However, this recognition remains uneven across financial market organisations, with cyber incidents often acting as a catalyst for elevating data protection and data governance issues to board-level attention.**

Overall, the findings demonstrate that financial market participants assess data protection through different but interconnected lenses. Investors tend to emphasise governance quality and risk management, auditors focus on compliance and transaction readiness, and rating agencies evaluate the implications for operational resilience and creditworthiness. **Collectively, these perspectives illustrate how data protection has become increasingly embedded within the financial sector, not only through regulatory frameworks but also through investment decisions, due diligence processes, portfolio transactions, corporate ratings, and cybersecurity**

governance. Beyond compliance, effective data governance contributes to trust, supports the use and reuse of data, and enables more informed organisational decision-making.

3.1.2 Data Protection as a Financial & Strategic Factor in a DataDriven World

The value of compliance with data protection for organisations

Personal data is a core input for a range of organisations that enables them to offer their products and services. Personal data is broadly recognized as a source of value creation in data intensive sectors, such as technology, digital platforms, financial services, insurance, healthcare, and e-commerce. In the banking sector, for example, data collection enables organisations to comply with sectoral regulations, such as Anti Money Laundering (AML) regulations and is considered valuable. Moreover, one of the banking business models' core components is personal data collection and use. Even in these data intensive sectors, personal data has a notional value and is rarely recognized as a standalone asset in accounting. The estimation methods and challenges with valuing personal data as an asset were discussed extensively in the literature review section. **The interview findings supplemented our understanding and identified that the value of personal data is reflected indirectly through operational efficiency and customer insights.** Apart from the valuing personal data as an input, data quality, traceability and lawful use are becoming operational assets for business models. This is consistent with

the literature findings about personal data driving value through improving business processes, reducing risk, increasing market power and innovation (Veldkamp, 2023, Farboodi et al, 2025).

We now turn to the value of compliance with personal data protection. **Our study has identified that compliance with data protection is increasingly seen as a strategic asset that adds value to organisations in the financial sector.** This is a significant finding, because valuations of compliance with personal data protection tend to focus on the costs of compliance, as they are more immediate and easier to quantify. Therefore, Boards and decision makers have traditionally viewed compliance with data protection solely as a cost. For example, some interview participants noted the perception of compliance with data protection as a burden in the banking sector, due to the costs involved. **Our study of valuation methods has provided insights into two drawbacks that emerge from the lack of standardised valuation methods that may partially explain the perception of compliance with data protection solely as a cost.** Firstly, despite its enabling capacity, the role of compliance with data protection diminishes as a strategic factor and is less likely to be perceived as offering a competitive advantage. Secondly, the current valuation methods may underestimate data-related risks, particularly in transactions where personal data constitutes a significant asset. Valuation of the benefits is often perceived through non-monetary indicators, such as reduced regulatory and reputational risk, enhanced trust with investors, customers and partners, and improved access to markets,

procurement processes and public funding. For example, compliance with GDPR is a formal requirement for access to EU research funding, with guidance issued on processing special category data for EU funded research (EU Commission, 2018). Beyond the value that compliance with data protection creates for strategic matters, it is also important in routine operations. These routine operations include data sharing agreements, which are significant transactional documents, within the responsibility of the Board and requiring review by the DPOs. Other examples include due diligence processes, warranties and representations and investor risk assessments.

Some of the study participants suggested that while compliance with data protection may not be seen as a standalone value creating activity for organisations, beyond the requirement to comply with regulations, non-compliance with data protection represents a quantifiable financial risk that can negatively affect organisations’ valuations. In this case, the value of compliance with data protection is a risk factor, embedded within broader cybersecurity and governance assessments and forms part of measurable risk exposure, where non-compliant data does not hold market value and compliance is a prerequisite for asset recognition rather than an asset in itself.

During the study, we also identified a range of indicators that are commonly used to communicate compliance maturity and trustworthiness to consumers, business partners, markets, and investors. These indicators include cost savings achieved through the reuse of compliance controls, eligibility

for restricted procurement procedures, lower cyber insurance premiums, increased trust and conversion rates and efficiency in responding to data subject requests. Data protection certifications are recognised across sectors and further regarded as value enabling mechanisms providing independent third-party evidence of compliance, enhancing credibility through objective assessment, benefiting from regulatory recognition and increasing visibility in public procurement processes.

Data Protection Compliance as a Component of Organisational Governance

The study findings indicate that organisations that integrate data protection into their broader governance frameworks can generate long-term value through improved data quality, greater operational efficiency, enhanced organisational resilience, and stronger stakeholder trust.

Participants indicated that operational efficiency with collecting, processing and storing personal data can allow for further use of personal data, increasing revenue generation. Additionally, we have found that data protection is a requirement across other regulatory frameworks, therefore, the effort involved in complying with data protection allows organisations to meet multiple regulatory obligations, reuse existing controls and achieve cost optimization and more coherent governance. For example, participants indicated that in EU countries, the professional secrecy and the protection of commercially sensitive information existed prior to the widespread recognition of data

protection obligations brought about by the GDPR coming into force. In the financial sector, organisations were already subject to extensive requirements governing the handling, protection, and disclosure of confidential information. The GDPR did not replace these pre-existing obligations, rather, it developed a comprehensive framework specifically addressing the processing of personal data, accountability, transparency, and data subject rights. Consequently, information governance and data management had already been embedded in financial market operations prior to the GDPR, although the Regulation significantly expanded the scope of and formalised data protection compliance⁴.

Our study has identified that despite its enabling role and growing recognition as a strategic asset, data protection is not consistently or distinctly embedded in organisational governance processes. While compliance activities, such as the DPO function, compliance controls and documentation and IT robustness reduce risk and improve audit quality, data protection is only partially present in the governance pillar of Environmental, Social and Governance (ESG) frameworks. We have indicatively examined ESG frameworks that are broadly used in the EU and the UK, such as the Corporate Sustainability Reporting Directive (CSRD) and European Sustainability Reporting Standards (ESRS) in the EU and the Sustainability Reporting Standards (SRS) in the UK

⁴ Markets in Financial Instruments Directive, Article 76. The professional secrecy duty applies to all persons who work for competent authorities or entities to whom tasks are delegated, as well as auditors and experts instructed by the competent authorities.





that are voluntary for any entity that chooses to use them (EU Commission, 2022) (Department for Business and Trade, 2024). The ESG frameworks examined tend to refer to data, they do not make specific reference to personal data. The ESRS include provisions that require organisations to disclose how their undertakings impact on consumers’ privacy and data protection rights.

We have identified that the value of compliance with data protection is perceived differently across different actors or types of organisations. DPOs are more likely to see the merits of compliance, beyond the legislative and regulatory obligations. Boards tend to perceive the value through reputational aspects that may emerge from cybersecurity incidents, data breaches and complaints that arise from subject access requests. Similarly to DPOs, marketing departments

within organisations may recognise the value of compliance with data protection, responding to the emerging importance of data protection for consumers and investors. While these distinct perceptions are common, the banking sector may provide an exception as risk management frameworks are highly mature, and boards increasingly view data protection as a business benefit. One of the reasons that may give rise to the disparity between perceptions of Boards, DPOs and other operational units within an organisation, is the lack of standardised indicators to assess data protection maturity. The study has found that some organisations may integrate data protection in their corporate strategies that are monitored through Key Performance Indicators (KPIs), combining compliance and business performance and are overseen at top

management level.

Participants have also suggested that data governance frameworks should be outcome-oriented, ensuring that governance mechanisms, policies, and controls are designed to support the achievement of clearly defined business, compliance, and innovation objectives. This may bridge the gap between the challenges rising with personal data valuations and the need to demonstrate the value in accounts outputs. It would also provide a tangible way of linking compliance with data protection to organisational objectives that are regularly assessed and valued.

Our study has also identified that transparency may signal an organisation’s maturity in processing personal data in a compliant manner, and may therefore, act as a competitive advantage

for organisations. There is some transparency in demonstrating maturity with data protection compliance, however, this is not sufficient, as companies tend to describe compliance processes as operational information that is not shared with investors and markets and the language used to demonstrate compliance with data protection is high level and does not provide sufficient transparency for consumers. **This finding links to an emerging need for distinct strategic indicators, such as KPIs, or inclusion of such indicators in ESG reporting, to reflect data protection maturity internally for boards and DPOs, as well as externally, for markets, investors, auditors and consumers.**

The EU and the UK have recognized the importance of cyber security in financial markets and have designated banking and financial

markets infrastructure as critical entities in the EU Critical Entities Resilience Directive and the financial sector as a Critical National Infrastructure (CNI) sector in the UK (EU 2022/2557, 2022) (National Protective Security Authority, 2026). Following the designation of financial markets and the banking sector as critical infrastructure, organisations that operate in these sectors would expect increased scrutiny regarding their cyber security preparedness. Our research has indicated that although some companies disclose certain cyber security and data protection risks, there is no standardised metric enabling markets and investors to clearly assess the quality of data governance. Respondents have also indicated that data protection is considered as part of cybersecurity policy for most organisations in the financial sector, motivated by the prevalence of reputational impacts in

case of cyber breaches.

Personal data governance is approached through a risk management perspective. The most significant perceived impact of data protection breaches is the loss of trust and reputational damage, rather than the direct effect of data breaches on company valuations, share prices, or ratings. Despite the limited prominence in ESG standards, weak personal data governance may emerge in internal audit findings and give rise to public concerns or disclosures at shareholders’ meetings. **Therefore, data governance has become a material audit and reporting factor that can mitigate disclosure and reputational risks.**

Our study has indicated that data protection compliance impacts company valuations mainly in the event of incidents, such as major data



breaches or regulatory sanctions. This impact is generally negative, and event driven and has short term effects on company valuations or share prices. The financial impact of data breaches tends to be short term, is sector specific and may be more significant for larger, highly visible companies, mainly driven by the reputational impact of the breach. Conversely, the impact of data breaches on company ratings depends on the type of the breach, while most data protection breaches do not tend to impact short term changes in company ratings, serious data protection failures that would affect long term financial resilience, may weaken the company’s credit profile, lead to a negative outlook revision and affect company valuation through a downgraded rating. Additionally, prolonged data breaches that may lead to business or service disruption are more likely to affect companies’ financial resilience that may in turn impact valuations, stock prices and ratings. Data breaches also have an impact on people and consumers’ perceptions both about sharing their data with organisations, as well as using products and services from organisations with weak data governance practices. As a result, this may impact on organisations’ ability to collect and use personal data, in order to provide or enhance their services.

Effective governance frameworks, supported by robust data protection, cybersecurity, and risk management controls, can strengthen organisational resilience and cybersecurity maturity. Improved oversight, accountability, and data management practices help organisations better identify, assess, and mitigate risks. Organisations with mature governance and compliance

frameworks, including strong data protection practices, are often better positioned to recover from incidents, thereby limiting reputational damage and reducing potential impacts on valuations, stock prices, and credit ratings.

3.1.3 Data Governance as a prerequisite for AI deployment

During the interviews, organisations consistently identified AI as a major opportunity and a key component of their long-term strategy and growth ambitions. Participants highlighted several emerging use cases already being deployed, including the use of AI to extract and process information from forms and other business documents. **Organisations also emphasised that effective data management, data quality, and data protection practices are essential prerequisites for the successful deployment of AI.** These capabilities help ensure that personal data is processed on an appropriate legal basis, that data remains accurate and usable, and that relevant information is retained and accessible for legitimate business purposes.

Organisations argued that strong data management and governance capabilities can create a competitive advantage by enabling the effective use of AI and transforming compliance from a regulatory obligation into a strategic asset. Without reliable, well-managed, and appropriately governed data, organisations may struggle to realise the full value of AI technologies.

The interview participants identified that European organisations remain reliant on non-European digital infrastructures and technology

providers, due to the supply chain structure of the AI developer market. This may constrain their ability to fully realise the value of personal data as a strategic asset for innovation and AI development.

For particular organisations, such as financial institutions and regulators, trust in safety is a key differentiator. **As organisations scale the deployment of AI solutions, participants emphasised that strong data protection compliance, transparency, and effective governance frameworks are essential to maintaining and strengthening customer trust, particularly when personal data is used in AI-related processes.** As highlighted above in section 3.1.2, a key finding is a mismatch between Boards and DPOs’ perceptions of the role of compliance with data protection. AI deployment could provide a potential avenue for DPOs to make a clear business case for good governance, beyond minimum legal requirements, by demonstrating the benefits for organisations’ growth and strategic priorities.

Responsible governance frameworks are becoming increasingly important given the adoption of agentic AI within organisations, artificial intelligence systems that go beyond merely responding to queries and can perform tasks autonomously. Participants from functions that support financial services indicated that they are closely monitoring the evolution of these systems because they appear to amplify cybersecurity risks, particularly because the use of automated agentic systems without human oversight multiplies vulnerabilities such as prompt injection and data poisoning.

The quantitative survey, conducted

with data controllers in France, reveals rapid adoption of AI tools among the companies surveyed, with over two-thirds (69%) already using enterprise-licensed AI tools to boost productivity, signaling that AI has become part of daily professional life. A study in the UK has also identified that use of AI tools in processing personal data has increased from 6% in 2024, to 8% in 2025 and 14% in 2026 (ICO, 2026).

The survey conducted with French organisations has also found that AI adoption is accompanied by varying levels of awareness and understanding, with 18% deliberately blocking public generative AI tools due to confidentiality and intellectual property concerns. A quarter of respondents (26%) are already connecting AI to their internal databases, while 11.6% are deploying chatbots or assistants for either internal or customer-facing use. At the forefront of innovation, 5% are commercializing their own revenue-generating AI models. While organisations vary significantly in their understanding and maturity regarding AI governance, risk management, and compliance requirements, many have reported implementing specific data safeguards, such as using tools “based on existing AI with data anonymization and filtering”, deploying a “customized, secure version of Copilot built to specific requirements” or using restricted-access legal AI systems. Organisations are also formalizing rules through measures such as AI charters, “sections governing AI usage”, pilot programs limited to a select group of employees prior to large-scale rollout, and the blocking of tools deemed problematic.

The survey conducted with French organisations has also found (see

in the statistical report) that AI adoption is correlated with financial factors, such as company size (in terms of revenue) and less with data dependency, suggesting that the capacity to fund and invest time in AI projects has been determined by other factors. A direct link has also been established between the adoption of advanced AI applications (such as AI connected to internal databases, customer-facing chatbots, or commercialized AI models) and the incorporation of data-related risks into financial assessments (e.g., credit ratings, M&A valuations, or cost of capital). These results indicate that some companies that invest in AI also start to consider the associated data-related risks.

3.2 Accounting treatment and financial exposure linked to data topics

3.2.1 Stakeholder’s perspectives on data and data protection compliance in financial statements

The interviews conducted with financial auditors and regulators provide valuable insights into how data questions are progressively integrated into financial risk assessment, while remaining anchored within the traditional objectives of the audit function.

A first key observation concerns the level of organisational preparedness. Several respondents noted that many organisations are not yet fully equipped to assess and discuss the financial implications of data protection. Internal alignment remains limited, as departments such as legal, compliance, IT and finance

often approach the issue from distinct perspectives. As a result, the translation of data risks into financial metrics remains fragmented and underdeveloped.

From an audit perspective, data protection is not assessed as a standalone compliance objective, but rather through its potential impact on financial reporting. Auditors emphasised that their primary responsibility was to identify and assess risks of material misstatement in the financial statements. In this context, data protection considerations arise through two main channels. First, they are linked to data quality, which underpins the reliability of accounting information. Second, they fall within the scope of ‘Non-Compliance with Laws and Regulations’ (NOCLAR), where breaches of data protection rules may lead to financial consequences such as fines, operational disruption or impairment of assets. This approach is consistent with ISA 250 (Consideration of Laws and Regulations in an Audit of Financial Statements), which requires auditors to obtain sufficient appropriate audit evidence regarding compliance with laws and regulations that have a direct or indirect effect on the financial statements, and to evaluate whether instances of non-compliance could result in material misstatements (IAASB, 2016).

A key challenge, identified across interviews, lies in the difficulty of translating qualitative compliance features into quantifiable financial risks. Data protection approaches are often designed from a legal perspective and do not directly provide inputs for financial valuation or risk measurement. In practice, auditors and financial practitioners rely on scenario-based analyses,

assessing the potential financial impact of regulatory breaches, including sanctions, business interruption, reputational damage or reduced usability of data.

Beyond these direct impacts, respondents highlighted that data protection risks can also influence financial valuation parameters, in particular the Weighted Average Cost of Capital (WACC)⁵. Increased uncertainty regarding the legality and sustainability of data use may lead investors and valuation professionals to require higher returns, thereby increasing the cost of financing a company's capital. This mechanism represents a crucial transmission channel between data protection risk and financial valuations, as it amplifies the effect of reduced cash flow expectations.

This dual effect is particularly significant in data-driven business models, where value is inherently linked to the use of data. When these data assets are affected by compliance issues, their economic value may be significantly impaired. In some cases, it was explicitly argued that an asset which cannot be legally used should not be considered to possess market value. This issue is particularly relevant for personal data assets: personal data collected, processed, or retained in breach of applicable data protection legislation, may become unusable for commercial purposes. In such circumstances, the legal limitations attached to the asset directly affect its ability to generate future economic benefits and,

consequently, its economic value.

From an accounting perspective, the dynamics between the value of compliance with data protection and value reporting are reflected in several accounting provisions. **To understand the effects of these dynamics, this report focused primarily on their implications for relevant International Financial Reporting Standards (IFRS), including IAS 38 (Intangible Assets), IAS 36 (Impairment of Assets), and IFRS 3 (Business Combinations).**

The standards reviewed emerged from the qualitative interviews conducted with auditors, consultants, and supervisory authorities, which highlighted the importance of accounting issues related to customer lists and customer databases, particularly in business combinations (e.g.: acquisition or merger) and valuation exercises⁶. In particular, a deterioration in expected future benefits may lead to impairment of goodwill and intangible assets under IAS 36 (Impairment of Assets). Regulatory risks may also give rise to provisions under IAS 37 where obligations are probable and measurable. In acquisition contexts, data-related value is often embedded in goodwill through purchase price allocations, and any subsequent deterioration in expected synergies, particularly those linked to data exploitation, may trigger impairment losses. In addition, changes in the discount rate, reflecting increased risk, directly affect value in use calculations.

⁵ WACC (Weighted Average Cost of Capital) is the average cost of a company's debt and equity financing, weighted by their proportions in the capital structure, and is commonly used as a discount rate in corporate valuation and IAS 36 impairment testing.

⁶ A business combination is "a transaction or other event in which an acquirer obtains control of one or more businesses" (IFRS 3, Appendix A).

From a governance and assurance perspective, respondents indicated that auditors consider the broader control environment, including internal controls, IT systems and organisational structures. **Elements such as the presence of a DPO, internal audit activities related to data protection legal frameworks, and the existence of certifications, codes of conduct or other recognized compliance frameworks may provide additional comfort, as they demonstrate that structured compliance mechanisms are in place.** However, these elements remain only one input among others and do not eliminate audit procedures, as their relevance ultimately depends on the extent to which they mitigate risks of material misstatement.

From an accounting standards perspective, respondents did not identify a fundamental gap in the existing framework. The current IFRS standards, particularly IAS 36, IAS 37, IAS 38 and IFRS 3, were considered sufficiently broad to capture data protection and data risks.

However, the application of these standards requires a high degree of professional judgement, especially given the evolving nature of data-related risks. This suggests that the main challenge lies not in the absence of rules, but in their interpretation and consistent application in practice.

3.2.2 Data Assets and Data Protection in Financial Reporting

This section examines the accounting implications of data topics by analysing how compliance obligations are reflected under key accounting standards and processes. Using practical examples, it illustrates

their impact on financial statements and accounting treatments. Accordingly, the analysis focuses on IAS 38 (Intangible Assets), IFRS 3 (Business Combinations), and IAS 36 (Impairment of Assets), as these standards provide the framework for recognizing, measuring, valuing, and testing data-related assets for impairment.

A key objective is also to identify the circumstances under which databases can be recognized as assets and how data protection requirements may influence their valuation and accounting treatment. The comparison with local Generally Accepted Accounting Principles (GAAP), like French GAAP (PCG) in France, Luxembourg GAAP in Luxembourg, and UK GAAP in the United Kingdom further highlights differences in the treatment of similar economic realities across jurisdictions.

IAS 37 (Provisions, Contingent Liabilities and Contingent Assets) is not examined in detail, as the report focuses on the recognition, valuation, and impairment of data-related assets rather than on the accounting treatment of obligations, such as fines or litigation risks.

The Growing Recognition of Data as an Economic Asset

Recent academic and professional literature increasingly highlights the strategic and economic importance of data, raising questions about whether existing accounting frameworks adequately capture its value. **As data has become a core driver of business performance, several authors and institutions have argued that it should be viewed and managed more explicitly as an asset.**

The Deloitte report (2025) emphasised that data has become a critical resource for many organisations and presented examples of companies that recognize data-related assets in their financial reporting, where such assets are considered fundamental to the business model. The report argues that, in many cases, data generates significant economic benefits through operational efficiencies, improved decision-making, innovation, and the creation of new revenue streams. **Consequently, the report suggests that data should be assessed using valuation approaches commonly applied to other intangible assets, namely the income approach, the cost approach, and the market approach, as discussed in the literature review.** These methods seek to estimate the economic value of data based on its expected future benefits, the costs incurred to create or replace it, or comparable market transactions.

In addition to highlighting the value of data, the authors introduce the concept of “data debt.” This concept reflects the idea that while effectively managed data assets can create substantial value and support business growth, bad data governance can impose significant costs on organisations. Such costs may arise from data quality issues, cybersecurity incidents, data breaches, regulatory sanctions, or failures to comply with data protection and privacy requirements. Therefore, data should not only be considered a potential source of value creation but also a source of risk that requires appropriate management and governance mechanisms.

Similarly, the Institute of Chartered Accountants in England and Wales examines the growing role of data within modern business models

and questions whether existing accounting standards adequately reflect its economic significance (ICAEW, 2025). The report highlights the increasing disconnection between the value generated by data-driven activities and the limited recognition of internally generated data assets within financial statements. As businesses increasingly rely on data to create competitive advantages, customer insights, innovation capabilities, and operational efficiencies, the report suggests that current accounting frameworks may not fully capture the resources that contribute to corporate value creation.

Academic research has also sought to address the challenges associated with measuring and recognizing data (Blycha, et al., 2026). The authors propose a structured valuation framework designed to assess enterprise data in accordance with existing accounting standards. The paper argues that the failure to easily and reliably value data causes mispricing and allocative distortions. The framework considers situations in which data have qualified either as an intangible asset under IAS 38 or, in certain business contexts, as inventory under IAS 2. This approach contributes to the ongoing debate regarding the appropriate accounting treatment of data and provides a potential methodology for bridging the gap between economic value and financial reporting requirements.

Taken together, these developments illustrate a growing consensus that data represents a significant business resource, whose economic importance extends beyond its traditional treatment in financial statements. **While accounting standards such as IAS 38 continue**

to impose strict recognition criteria, recent professional and academic contributions suggest that data increasingly exhibits characteristics associated with valuable intangible assets and may require more sophisticated valuation and reporting approaches in the future.

3.2.3 Quantitative findings

Survey results conducted with French organisations indicate that the recognition of databases in financial statements remains limited and inconsistent. Most respondents, among those having an opinion on the subject matter, reported that their databases are not reflected in the financial statements at all (38%). Where databases are recognised, the prevailing approach is cost-based, primarily through the capitalization of IT development and database

creation costs as intangible assets, for almost a third of the respondents (28%). Only a small proportion of respondents (5%) reported that databases are reflected through goodwill arising from acquisition transactions. These findings suggest that current accounting practices tend to focus on the costs incurred to create databases, rather than on the underlying economic value generated by data assets.

In line with previous findings, the survey results suggest that even acquired data is still only rarely treated as a standalone asset. More than half of respondents (53%,) indicated that no specific valuation is performed for acquired data. Nevertheless, some accounting recognition practices are emerging: 18% of respondents reported recognizing acquired data as a separate intangible asset on



balance sheets, while 14% indicated that its value is captured indirectly through goodwill without being separately identified. The remaining responses reveal a significant degree of uncertainty regarding the accounting treatment of acquired data, highlighting that the recognition of data as an asset remains an evolving practice and an area where awareness and accounting methodologies could be further developed.

3.2.4 Recognition, measurement and impairment of databases under IAS 38, IFRS 3 and IAS 36

Building on the above considerations, this section focuses on the analysis of IAS 38 (Intangible Assets), IFRS 3 (Business Combinations) and IAS 36 (Impairment of Assets), as these standards provide the most relevant framework for examining the recognition, measurement and subsequent valuation of customer databases.

In addition, a comparative perspective is integrated throughout the analysis, with reference to French GAAP (PCG), Luxembourg GAAP, and UK GAAP (FRS 102), in order to highlight differences in the treatment of customer-related intangible assets across accounting frameworks.

Finally, the analysis is supported by a practical example in Annex XX, illustrating how customer databases are recognised, measured and potentially impaired in a transaction

7 IAS 38, paragraph 21

8 IAS 38, paragraph 12 and 13

9 IAS 38, paragraphs 10 and 18–23, which distinguish between acquired and internally generated intangible assets, with the latter subject to significant recognition restrictions, particularly in relation to internally generated goodwill and similar items.

context, thereby linking theoretical principles to real-world valuation and accounting practices.

Recognition of databases under IAS 38

IAS 38, adopted in 2001 and published in 2004, governs the recognition, measurement and depreciation of intangible assets. Under this standard, an intangible asset is recognised only if it is probable that the expected future economic benefits attributable to the asset will flow to the entity and if its cost can be measured reliably⁷. In practice, these criteria are generally satisfied for separately acquired intangible assets, as the purchase price reflects market participants’ expectations regarding future economic benefits.

In addition to these recognition criteria, IAS 38 requires that the asset must be identifiable and controlled by the entity⁸. An intangible asset is identifiable when it is either separable or arises from contractual or legal rights. This is particularly relevant for customer databases, which are typically considered separable as they can be for example, transferred, licensed or otherwise exchanged, as long as they comply with data protection regulations. Control implies that the entity could obtain the future economic benefits flowing from the asset, depending on the appropriate data protection lawful basis.

IAS 38 also clearly distinguishes between acquired intangible assets and internally generated ones⁹.



Internally generated goodwill cannot always be recognized as an asset because the control and separability criteria are not easily demonstrated. Moreover, IAS 38 explicitly carves out “customer lists” from being recognised as intangible assets (§632), yet not all datasets are composed of customer databases.

Recognition of internal databases as intangible assets under IAS 38

Although internally generated databases are not generally recognized as intangible assets, certain circumstances may allow them to meet the recognition criteria established by IAS 38 Intangible Assets. **Three situations are particularly relevant:**

- **presence of IT development costs related to the creation of databases;**
- **databases or datasets that are protected by intellectual property rights or other legal rights**
- **Specialized (structured) internal databases.**

In such particular cases, databases developed for internal use may satisfy recognition criteria and therefore qualify as intangible assets.

i. Presence of IT development costs related to the creation of databases

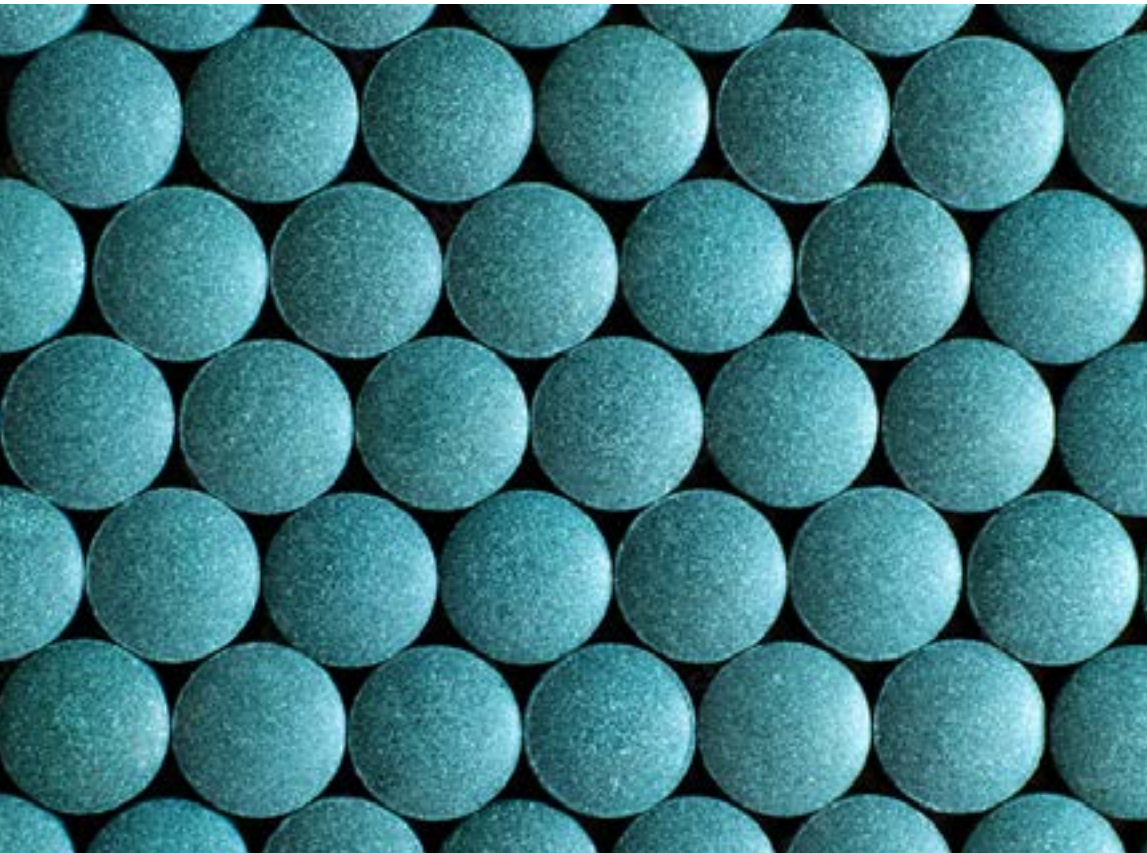
A key aspect of IAS 38 is the distinction between the research phase and

the development phase of an internally generated intangible asset. Expenditures incurred during the research phase must be recognized as an expense when incurred because future economic benefits cannot yet be demonstrated. **By contrast, development expenditures may be capitalized when the entity can demonstrate technical feasibility, intention to complete and use the asset, ability to generate future economic benefits, availability of adequate resources to complete the project, and the ability to measure attributable costs reliably. These requirements are set out in IAS 38 and constitute the basis for the capitalisation of internally developed databases.**

For database development projects, capitalisable expenditures generally include costs that are directly attributable to creating and

preparing the asset for its intended use. Such costs may include salaries of software developers and database engineers, external consultancy fees related to system design and development, testing activities, and other directly attributable implementation expenditures. In accordance with IAS 38, the asset is initially measured at cost, comprising only those expenditures that can be directly linked to the creation of the database.

Conversely, certain costs cannot be included in the carrying amount of the database and must be recognized as expenses when incurred. Examples include training costs for users, general administrative overheads, maintenance activities, and expenditures incurred during preliminary investigations or feasibility studies. **IAS 38 specifically excludes such expenditures from**



capitalisation because they do not directly contribute to the creation of a separately identifiable intangible asset capable of generating future economic benefits.

Therefore, under IFRS, the accounting treatment of database creation costs depends on whether the expenditures meet the recognition criteria for internally generated intangible assets under IAS 38. **Where the development criteria are met, eligible costs are capitalised and subsequently depreciated over the asset’s useful life. Otherwise, the expenditures are recognised immediately in profit or loss. This approach ensures that only those IT investments expected to generate future economic benefits are recognized as assets in the statement of financial position.**

ii. Intellectual property rights attached to databases

The existence of intellectual property rights associated with a database may facilitate compliance with the IAS 38 requirements relating to identifiability and control. Legal rights such as copyrights, database rights, licenses or exclusive rights of use can demonstrate that a database is an identifiable resource separate from the entity. These rights provide evidence that the database can be distinguished from other assets and may therefore satisfy the identifiability criteria. **For example, the French Code de la propriété intellectuelle includes a provision creating a sui generis IP right on a database, when a “substantial investment” has been devoted to it¹⁰. Other databases can fall within the scope of copyright law under the EU directive 96/9/EC on legal protection of databases.**

10 Article L. 341-1 du code de la propriété intellectuelle

Furthermore, legal protection strengthens the entity’s ability to control the future economic benefits arising from the database. By restricting access by third parties and granting exclusive rights to use, exploit, license or commercialise the underlying information, such rights enable the entity to derive economic benefits from the database while preventing others from doing so.

Consequently, databases protected by intellectual property rights may qualify as intangible assets under IAS 38 when the legal rights establish both identifiability and control. However, the existence of legal protection alone is not sufficient. The entity must also demonstrate that the database is expected to generate future economic benefits and that its cost can be measured reliably, in accordance with the general recognition criteria of IAS 38.

iii. Specialised internal databases and datasets

In addition to legally protected databases, certain specialised internally developed databases or datasets may satisfy the recognition criteria of IAS 38. This may be the case where significant development efforts have been undertaken to collect, enrich, structure, clean, validate or organise data, thereby creating a resource that generates economic value for the entity.

Examples include proprietary datasets used for training artificial intelligence models, curated healthcare research databases, geospatial databases, technical or scientific data repositories, and other specialised datasets developed for

commercial exploitation or strategic business purposes. Databases that are subject to exclusive licenses or that provide the entity with unique competitive advantages are particularly relevant in this context.

Where such databases are identifiable, under the control of the entity, capable of generating probable future economic benefits, and where the related development costs can be measured reliably, they may qualify for recognition as intangible assets under IAS 38. Each case must nevertheless be assessed individually, considering the specific characteristics of the database and the evidence available to support compliance with the standard’s recognition requirements.

Internally generated customer lists are explicitly prohibited from recognition, as they cannot be distinguished from the overall value of the business and therefore fail the identifiability and reliable measurement criteria¹¹. Therefore, many data-related, indirect expenditures, such as costs incurred to improve data governance, enhance data quality, or ensure compliance with data protection regulations, are expensed as incurred because they do not meet the recognition criteria¹².

While IAS 38 defines the general

11 IAS 38, paragraph 63.

12 IAS 38, paragraphs 21 and 68–69, which establish that expenditures that do not meet the recognition criteria for intangible assets, particularly internally generated costs, must be recognised as expenses when incurred.

13 IFRS 3, paragraphs 10 and B31–B34, which require the acquirer to recognise identifiable intangible assets separately from goodwill if they meet the definition of an intangible asset and can be measured reliably.

14 Conceptual Framework for Financial Reporting, paragraphs 4.3–4.4, defining assets and liabilities, and IFRS 3, paragraph 10, which requires the recognition of identifiable assets and liabilities that meet these definitions in a business combination

15 IFRS 3, paragraphs 10 and B31–B32

framework for recognizing customer databases, additional requirements apply when such assets are acquired in the context of a business combination¹³.

Recognition and initial measurement in Business Combinations under IFRS 3

When a customer database is acquired as part of a business combination, IFRS 3 Business Combinations applies. IFRS 3 is based on the acquisition method of accounting, which requires the identification and measurement of the assets acquired and of the liabilities assumed at their fair value at the acquisition date. To be recognized, these items must meet the definitions of assets and liabilities set out in the Conceptual Framework for Financial Reporting and must form an integral part of the business combination transaction¹⁴.

In this context, IFRS 3 extends the application of IAS 38 by requiring that all identifiable intangible assets be recognized separately from goodwill, even if they were not previously recognized by the acquiree¹⁵. As previously mentioned, in line with IAS 38, identifiability is established when an asset is separable or arises from contractual or legal rights. **As a result, even customer lists, user datasets**



and customer-related intangible assets may be frequently recognized at the acquisition date at their fair value, including when they have been developed internally.

This approach may lead to the recognition of assets that were not previously recorded in the financial statements of the acquiree, which is particularly significant in data-driven environments. A customer database, acquired in such a transaction, may therefore qualify as an intangible asset if it is expected to generate future economic benefits. Its useful life is determined based on the period over which these benefits are expected¹⁶.

Measurement of goodwill under IFRS 3

16 IAS 38 defines useful life as the period over which an asset is expected to be available for use by an entity, or the number of production or similar units expected to be obtained from the asset by the entity.

Under IFRS 3, goodwill represents the excess of the value attributed to an acquired business, including any non-controlling interests and previously held interests, over the net fair value of the identifiable assets acquired and liabilities assumed. It reflects future economic benefits arising from assets that cannot be individually identified and separately recognized.

In a data-related context, goodwill may incorporate the value associated with synergies arising from the combined use of data, improved analytical capabilities, or the development of new data-driven services, subject to compliance with the applicable regulatory frameworks.

IFRS 3 also provides a measurement period following the acquisition

date, during which provisional amounts initially recognized may be adjusted¹⁷. This allows the acquirer to refine the valuation of assets and liabilities, including customer databases. Adjustments are limited to information relating to facts and circumstances that existed at the acquisition date and are recognized retrospectively, which may result in corresponding adjustments to goodwill.

Data protection, ownership and amortisation of data assets

As stated above, under IAS 38, the recognition as intangible assets is not the general rule for internally generated customer databases, as it is difficult to demonstrate all the recognition criteria. Acquired customer databases, either separately or through a business combination, may satisfy the recognition criteria.

Accordingly, internally developed customer lists, internally accumulated user or client data, and more broadly data-related expenditures that cannot be separated from the ongoing activities of the entity may be recognized as expenses.

A dataset that is recognised as an asset and meets the IAS 38 criteria, may benefit from amortisation. Following initial recognition, in accordance with IAS 38, intangible assets with finite useful lives are depreciated systematically over their estimated useful lives¹⁸. Useful lives must be determined based on the period over which business benefits are expected from the data set.

On this topic, it is often argued that

17 IFRS 3 paragraphs 45-49
18 IAS 38, paragraphs 88-89 and 97

the useful life of a dataset is relatively short, due to a quick obsolescence of data. According to available evidence, the retention period of personal data in Europe ranges from 3 months to 20 years, with an average retention period of 6 years (Iron Mountain & De Braw Blackstone Westbroek, 2013). **For datasets that include personal data, protection principles of purpose limitation, data minimisation and storage limitation apply to identify the period for the lawful use of the dataset. Therefore, the period identified can be a proxy to define amortisation duration, from an accounting point of view. This helps understand why data sets can be considered as amortisable assets. It is also often argued that the ownership criterion is hard to meet, because of the presence of data protection rights, especially consent requirements, constraining databases' economic ownership for e- companies. Data protection legislation provides for the use of personal data, including in commercial environments, and provides a framework that balances the lawful use of personal data, while protecting consumers' data protection rights. Although consent is relied upon frequently, companies may rely on other lawful basis for commercial use of data. For example, companies may gather data on the basis of contractual necessity and may be able to use it under the legitimate interest's lawful basis. The right to erasure is also cited as a restricting factor, this provides consumers with the right to have their personal data deleted for a range of reasons. There are provisions for companies to keep hold of personal data if they are legally obliged to have it in order to comply with**

financial or other regulations under GDPR or UK GDPR.¹⁹ Conversely, some data protection provisions, such as the data accuracy principle or provisions for third parties to access lawfully collected data, generate data exclusivity for the data holder and reinforce the IAS 38 asset identifiability and control criteria. It becomes evident that when compliance with data protection is embedded in operations, it may create synergies in applying accounting criteria for the recognition of data as an intangible asset.

Subsequent measurement and impairment under IAS 36

Once recognized, these assets, without prejudice to their possible amortisation, are subject to impairment testing under IAS 36 Impairment of Assets, which ensures that assets are not carried at amounts exceeding their recoverable amount.²⁰

The recoverable amount is defined as the higher of an asset's fair value, less costs of disposal and its value in use, corresponding to the present value of the future cash flows expected to be derived from the asset. At each reporting date, a company must assess whether there are indications that an asset may be impaired. In addition, goodwill and intangible assets with indefinite useful lives or not yet available for use must be tested for impairment on an annual basis.

IAS 36 distinguishes between external and internal indicators of impairment. In a data-driven context, external indicators may include adverse changes in the

19 Your right to get your data deleted | ICO
20 IAS 36, paragraphs 6, 9 and 10
21 IAS 36, paragraphs 12, 59 and 66

regulatory environment, such as stricter data protection requirements. Internal indicators may include underperformance of a customer database or significant changes in its use.

When an asset does not generate independent cash inflows, impairment testing is performed at the level of a cash-generating unit, defined as the smallest identifiable group of assets generating largely independent cash inflows. This situation is common in data-driven environments, where customer databases derive value from their integration with other assets.

If the carrying amount of an asset or cash-generating unit exceeds its recoverable amount, an impairment loss is recognized. This is particularly relevant for goodwill, which often incorporates expected synergies, including those related to the use of data. A deterioration in these expected benefits may therefore result in impairment²¹.

Comparison with FR GAAP, LU GAAP and UK GAAP

The accounting treatment of customer databases under IFRS presents both conceptual similarities and important differences when compared with French GAAP (PCG), Luxembourg GAAP and UK GAAP (FRS 102).

Across the different accounting frameworks, intangible assets are generally recognised on the basis of similar underlying principles, requiring identifiability and the expectation of future economic benefits. While IFRS explicitly refers to control over the

resource, FRS 102 requires that future economic benefits attributable to the asset are expected to flow to the entity and that its cost or value can be measured reliably. These approaches reflect a common conceptual foundation regarding the nature of intangible assets.

However, all three local GAAP frameworks adopt a more conservative approach to the recognition of internally generated customer databases. Under local norms, such assets are generally not recognised, as the costs cannot be reliably measured and cannot be distinguished from internally generated goodwill. As a result, expenditures relating to internally developed customer lists are typically expensed.

More significant differences arise in the context of business combinations. IFRS 3 requires systematic identification and separate recognition of all identifiable intangible assets, including customer databases, even when previously unrecognized. By contrast, under FR GAAP and LU GAAP, the allocation of purchase price is less detailed, and customer-related assets are more frequently included within goodwill. **UK GAAP adopts an intermediate approach, generally requiring the recognition of identifiable intangible assets, but with less emphasis on detailed valuation than IFRS.**

Differences are also observed in subsequent measurement. **Under**

22 See French GAAP (Plan Comptable Général, articles 214-3 and 214-4) and UK GAAP (FRS 102, section 18.19–18.23), which require goodwill to be depreciated over its useful life. Luxembourg GAAP follows a similar prudential approach

23 Under UK GAAP (FRS 102, Sections 18 and 19), identifiable intangible assets are recognised separately from goodwill in a business combination if they meet the definition and recognition criteria. They are measured at fair value at the acquisition date, but the

IFRS, goodwill is not depreciated and is subject to annual impairment testing, whereas under FR GAAP, LU GAAP and UK GAAP, goodwill is typically depreciated over the asset’s finite useful life. This reflects a more prudential approach in local GAAP frameworks, where systematic depreciation reduces reliance on forward-looking valuation assumptions²².

Overall, while the conceptual basis is broadly aligned, IFRS adopts a more principle-based and economically focused approach, particularly in business combinations and impairment testing, whereas FR GAAP and LU GAAP remain more conservative, and UK GAAP occupies an intermediate position.

The main difference between IFRS and local GAAP frameworks lies in the allocation of intangible value.

IFRS requires a systematic separation of identifiable intangible assets from goodwill, whereas French and Luxembourg GAAP allow a larger portion of intangible value, including customer-related elements, to remain within goodwill.

UK GAAP applies a similar separation principle, where it should be demonstrated that assets accrue future benefits and costs incurred are identifiable, in order to be recognised as intangible assets, while during business combinations, goodwill is recognised as an asset²³.

Loan portfolios and the accounting treatment of embedded customer data

The accounting treatment of loan portfolios provides a complementary perspective on the recognition of customer-related intangible value, particularly when considering the role of borrower data. While loan portfolios are consistently recognized as financial assets across accounting frameworks, the treatment of the underlying customer data embedded within those portfolios reveals significant conceptual limitations.

Under all frameworks, loan portfolios are recognized as financial instruments. **However, the data associated with borrowers, such as repayment behaviour, credit history or segmentation information, does not give rise to separate recognition as an intangible asset.** This is primarily due to the difficulty of meeting the criteria of identifiability and control. Such data is rarely separable from the contractual relationship represented by the loan itself and is often subject to legal and regulatory constraints, notably in relation to personal data protection.

Under IFRS, the acquisition of a loan portfolio in a business combination may lead to the identification of certain related intangible assets, such as servicing rights or contractual arrangements, provided they meet the criteria of separability or arise

from enforceable rights. In this case, these elements are recognized separately from goodwill, in line with the disaggregation approach of IFRS 3. By contrast, the broader value linked to borrower data, including insights derived from behavioural data or customer relationships, is not recognised as a distinct asset and remains either embedded within the financial asset or included in goodwill.

This differs in emphasis, rather than in principle, under French and Luxembourg GAAP. While the recognition of the loan portfolio itself remains unchanged, there is no requirement to systematically identify and separate data-related intangible elements in a business combination. **As a result, a larger portion of the underlying economic value, including that associated with customer data, remains included in goodwill or implicitly captured in the valuation of the financial instrument.**

UK GAAP follows a similar conceptual approach to IFRS in requiring the identification of intangible assets when they are separable or contractual. However, in practice, fewer elements are recognised separately, which leads, similarly to French and Luxembourg GAAP frameworks, to a greater concentration of value within goodwill.

Overall, while loan portfolios are consistently recognized across

standard does not require the same level of detailed identification and valuation as IFRS 3, which may result in fewer separately recognised intangible assets

Table 1 - Recognition and Allocation of Customer Databases under IFRS and Local GAAP

Category	Examples	Generates Data?	Recognized)	Not Recognized	IFRS Standard
Technology-based	Software, platforms, development costs	Yes	Acquired or internally developed software (development phase only)	Research phase, internally generated raw data	IAS 38
Customer-related	Customer lists, relationships	Very high	Acquired customer lists (e.g., in M&A)	Internally generated customer lists	IAS 38 / IFRS 3
Marketing-related	Brands, trademarks	Yes	Acquired brands/trademarks	Internally generated brands	IAS 38
Intellectual Property	Patents, copyrights, IP rights attached to data bases	Yes	Legal IP rights (patents, copyrights & databases) IP rights attached to data bases	Non-protected know-how	IAS 38
Contract-based	Licenses, franchises, agreements	Yes	Contractual rights (licenses, agreements)	Non-separable contracts	IAS 38
Know-how	Processes, trade secrets	Yes	If identifiable and legally protected	Diffuse/internal know-how	IAS 38
Data (standalone asset)	Internal datasets, raw data	Core	Acquired externally Specialized data sets	Internally generated raw data	IAS 38
Goodwill & embedded data	Goodwill (incl. data value)	Indirect	Recognized in business combinations	Internally generated goodwill	IFRS 3 / IAS 38

accounting frameworks, the economic value derived from borrower data remains only partially reflected in financial statements. As in the case of customer databases, the key distinction lies not in the existence of the asset, but in the extent to which its underlying components are separately identified or absorbed within goodwill.

3.3 Transactional and valuation impacts of data protection compliance

Accounting practices play an important role in how organisations assess and recognise the value of data-related assets. However, the value of data and the benefits derived from compliance are not limited to accounting considerations alone.

In many cases, valuation occurs outside of an accounting context, especially in transactions, where the subject matter is the economic value of a company, as opposed to its book value. Typically, in over-the-counter transactions, like in a merger and acquisition (M&A) context, with the view to an Initial Public Offering (IPO) or during funding operations, the book value appears to be limitative and to be complemented with other components, to take full account of the value creation provided by a company. During over-the-counter operations, where a market price has not yet been established, transparency and robust data governance frameworks will typically be rewarded, while weak data policies are often penalised, by investors.

In such contexts, the value of data and regulatory compliance come fully

into play, as they can have a strong influence on deal pricing. This is especially true in the digital economy or for technology actors, however, with the overall digitalisation of the economy, data practices end up affecting a large range of retail or business to business (B2B) industries. According to a study by EY, in 2024, intangible assets (recognised or not) and goodwill represented 79% of the CAC 40 market capitalisation (EY, 2025). Part of this value is based on data assets. In the UK, in 2023, £244.7 billion was invested by all firms in intangible assets, £85.3 billion more than invested in tangible assets (ONS, 2025). Investment in intangible assets has been higher than in tangible assets since 1998, with the gap consistently growing (ibid). Similarly, in Luxembourg investment in intangible assets in 2019 resulted in 15% of gross value added (GVA) compared to investment in tangible assets that resulted in 11% (Conseil national de la productivité, 2023). It is expected that over the counter transactions are likely to increasingly recognise the value of data from an accounting point of view, as discussed in the previous subsection, and reflect the altering financial reality that incorporates the value of data.

In this perspective, the review approach applied in this report is twofold. The integration of data aspects in financial valuations cannot only be based on data risks (the risk of value losses when data is not managed well or when compliance is not done properly) but should also cover upsides (the value creation stemming from data assets themselves or the benefits of good governance and compliance). Those are two faces of the same coin: only when the value of data is clearly assessed, can the risks be quantified, and the other

way around, a good knowledge of data assets allows the mapping of risks in a meaningful manner. For this reason, any assessment of the value of data and the economic impact of compliance should consider both potential benefits and potential risks. This balance was endorsed by the practitioners who participated in the Daprolab workshop and is also recognised in Deloitte 2025 Tech Value survey that finds that data valuations and “data debt” are inherently interconnected in investment decisions (Deloitte, 2025).²⁴

3.3.1 Takeaways from open references and interviews

The idea that the value of data is often underestimated or weakly taken into account by existing frameworks, as opposed to their business value, is not new and is even cross-cutting in the economic literature. In the last couple of years, the OECD has developed a framework on how to integrate the value of data as an asset in national accounting frameworks (OECD, 2022). This approach treats data, from a macroeconomic point of view, as an investment. According to the OECD, the ‘data capital’ represents, from 5% to 9% of GDP in Europe (OECD, 2022, p. 29). As for the accounting treatment of data, this work concludes clearly that “the value of data and intangible assets in firm-level data is underestimated” (Ibid. p17). As discussed in the literature review section, the economic literature has tried to bridge this gap. Various approaches coexist, as the topic is still in its infancy, and reports

24 Data debt is caused by factors such as life cycle costs, quality problems, compliance and data security risks and data decay that weaken the value of data.
25 That took place in July 2026 at the CNPD Luxembourg
26 According to the interviews made with the stakeholders.

have advised governments to develop data valuation methods (Frontier Economics, 2021). Researchers have published a data valuation model under the Discounted Cash Flow (DCF) approach (Cheong, et al., 2023). Others have focused their efforts, again in a published article, on an example of listed tech firms, using market-based metrics (Xiaochuan, et al., 2026). In terms of valuation service availability, the interviews conducted have indicated the emergence of various consultancies that are now specialising in the economic valuation of data assets for financial purposes.

Published research also shows that more disclosure of policies and risks from IPO issuing companies, leads to a reduction of information asymmetries, which in turn leads investors to impose lower deal prices (Ding, 2016). This is understandable from a microeconomic point of view, where market transactions can lead to suboptimal outcomes in the absence of sufficient information amongst parties, making markets operate inefficiently.

With this in mind, it becomes clear why and how compliance and data governance are key to safeguarding the value of such assets. Interviews conducted in the context of this study have made clear, as one of the participants underlined, that “compliance protects value by ensuring that data can legally and sustainably generate future cash flows”²⁶. M&A practitioners reported that, “in M&A transactions, data lawfulness and governance directly influence[d] valuation, deal structure, and the ability to close a transaction”.

Others made clear that “strong data protection practices preserve deal value and reduce transaction risk” when it comes to financial operations.

3.3.2 Data compliance and risks in credit ratings

A prominent example of this is the impact of data breaches on company ratings. For a long time, data protection and cybersecurity were treated as technical or legal concerns. But a string of incidents (e.g. the Yahoo case in 2013) that visibly affected corporate balance sheets has changed how rating agencies look at these issues, and they now include cyber risk, data protection practices, and related governance and risk management arrangements into their assessment of an organisation’s risk profile. Rating agencies assess an organisation’s credit capacity, the ability to service its debt. Their reading of “data” risk therefore, runs through the lens of debt repayment, rather than share valuation. Data protection is not treated as a category in its own right, it is folded into cybersecurity, the “cyber posture”, its exposure and governance.

Whereas a data breach’s impact on the share price is often volatile and short-lived, a rating agency is likely to have a more structural effect through the bond market. Over the long run, neither ratings nor share prices are durably affected. The documented effect of data breaches is mainly short-term, given the “non-continuity” of the event.

Rating agencies can act at two levels: revising the outlook (a negative outlook signals a higher probability of a future downgrade) or lowering the rating itself (a downgrade). The

financial mechanism for valuing data breaches or cyber incidents that affect ratings, runs as follows: A weaker rating raises the issuer’s perceived default risk, so investors demand a higher credit spread (the premium paid over the risk-free rate) on new issuances. Mechanically, a higher spread means a higher coupon, and therefore a higher cost of long-term financing. The cost of a downgrade is not linear and varies with market conditions and it is typically modest within investment grade, but it rises sharply near the BBB-/BB+ boundary. For high-yield issuers the effect is generally larger as cyber losses compound the fragility of entities. The added value by this process stems from its access to non-public, company-specific information, including data obtained directly from management, enabling a more informed assessment of an entity’s risk profile and resilience.

Ratings can affect two areas. The first is whether Earnings Before Interest, Taxes, Depreciation and Amortisation (EBITDA) can cover charges, driven mainly by future cash flows and balance-sheet analysis. The second is the information implied about a business’s risk profile, including competitive advantage and market position. In practice, rating agencies take negative rating action, when an attack significantly disrupts core operations and inflicts longer-term financial damage. Our interviews indicated that the impact on solvency is assessed through questions about disruption in the company’s vital activities, effective management of containing the damage, impact on credit metrics, absorbed losses and the company’s track record on earlier incidents. The assessment is fundamentally a downside-only analysis. An incident seems to penalise

the issuer, although improving one’s data practices seems to generate no upside for ratings.

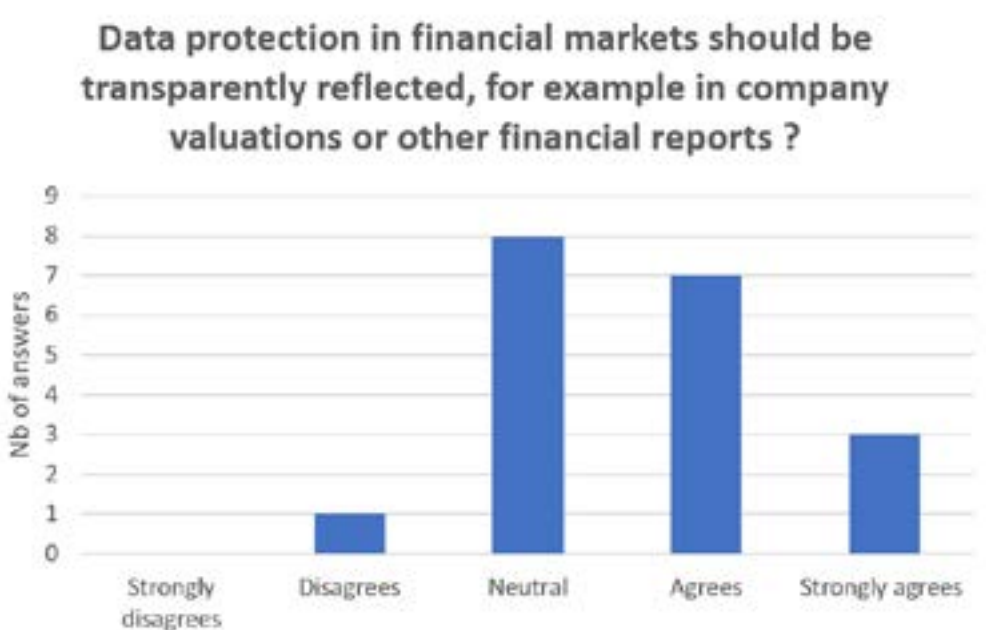
While the merits of such practices are to reflect data exposure and risks, one can understand the limit of this approach, based on market practices (see section 3.2), which do not always quantify data compliance or good governance efforts. Conversely, there is scope for data protection compliance aspects to be considered positively for company ratings, through assessment of ESG strategies. These, however, do not seem to be mature enough yet, to include compliance with data protection consistently, as it was discussed in the organisational governance section of the report.

As already discussed in section 3.2, equity markets do not generally quantify compliance with regulations, as companies are expected to comply with regulations. This leads to penalising factors when public information is disclosed showing that this is not the case, for example, non-

compliance reported by a regulator or demonstrated by a data breach. Yet, this does not sufficiently demonstrate the materiality of data protection questions for the financial ecosystem. For a company, the number of complaints received, or the severity of the cyberbreaches faced reflects the quality of its “data stewardship” and its cyber-protection policy. The lower this quality, the more likely and costly the risks affecting the company reputation, and the better this quality, the higher the trust of clients, business partners and rating agencies. Transparency in data protection practices allows markets to assess companies’ activities in their entirety and, not only penalise them for data risk exposure, but also reward them for compliant data practices.

3.3.3 Survey findings

The quantitative evidence gathered during this study supports the inclusion of data protection information in M&A valuations. The survey was conducted by CNIL, with French DPOs. Amongst 204



Graph 1: survey of French companies that participated in an M&A operation in the last 5 years, May 2026

respondents, 37% had carried out a M&A operation in the last five years.

When asked if “data protection should be transparently reflected, for example in company valuations or other financial reports”, from a scale from 1 to 5, 50% of companies with M&A operations in the last 5 years agreed or strongly agreed with

this view (see Graph 1 below), over 40% were neutral and less than 5% disagreed.

The evidence suggests that M&A operations, in particular, act as an enabler for sharing the financial value of data. This is not surprising, as such transactions are based on the economic valuation of companies



Graph 2: survey of French companies that participated in an M&A operation in the last 5 years, May 2026.

and not merely on the book or stock market value. The evidence indicates that data compliance is one of the indicators used in M&A transactions, albeit in most cases in a high-level manner. Yet, in some cases, probably reflecting the sectorial exposure to data for such operations, the due diligence processes take the value of databases or compliance into

account (see Graph 2), and even include a roadmap for compliance in 14% of cases.

Having said that, the financial valuation of data risks is not yet general practice, and while M&A operations act as accelerator, the valuation of data risks does not currently appear in companies’

Table 2: Answers to the question: "To your knowledge, how are data-related risks primarily factored into your company's financial valuation, whether internally or via external players?", French DPO respondents, May 2026²⁷

	Respondents that did not participate in M&A	Respondents that participated in M&A
In a past acquisition	4,5%	13,5%
In credit rating	3%	6%
On the balance sheet or in the DCF method	3%	6%
Total	10,5%	25,5%

decision-making systematically. **Companies that conducted M&A operations in the past 5 years are more likely to include data related risk in credit ratings or in their balance sheets (see Table 2).** Nonetheless, there remains significant potential for including the value of compliance with data protection in financial transactions. The ambition of this report is to showcase, and hopefully help develop, good practices on this front.

3.3.4 Transactional (M&A) aspects and due diligence considerations

Transactions (during IPO, M&A or financing proceedings) help overcome the data due diligence disclosure dilemma underlined above.

In such cases, emitters of financial instruments, such as shares, report the data and compliance aspects to a selected range of possible transactors, conducting the so-called “due diligence” process, leading the emitter or target to unveil company specific information to an acquirer or investor, or their advisers. It is undeniable that such processes are of paramount importance in today’s digital economy, if not in the economy as a whole, and especially in the most innovative sectors. According to PWC data, the combined capitalisation of the world’s top 100 companies amounted to \$51.8 trillion in early 2026, while the M&A transactions reached \$4.5 trillion in 2025 (an increase of 50% to 2024) (PWC, 2026). Against this background, venture capital

companies had \$3.5 trillion assets under management worldwide, according to the World Economic Forum, often covering companies exposed to significant data risks (World Economic Forum, 2026). **M&A activity is higher with data-intensive firms (Schoch, 2020), reflecting the phenomenon called “data driven mergers”, where big players purchase companies themselves instead of purchasing their datasets, to avoid legal data privacy constraints. This is more prominent with the rise of generative AI, where the training of datasets has become a strategic component of economic innovation and provides a structure that makes it more likely to meet the accounting criteria to be recognised as specialised data bases, cf. section 3.2.**

In the M&A process, the lawfulness of databases clearly impacts their usability and future returns. According to the case law of French courts, a non-compliant data file cannot be sold legally, it has no economic value and the clause foreseeing its selling is unlawful²⁷. In the same way, the number and quality of datasets influence the future revenue of the M&A target and therefore, influence the deal price. Lastly, on the risks side, weak data management practices and data governance result in more administrative requests and increased costs for companies. The same reasoning goes for asset deals (where only intangible assets with a data component are traded) and share deals (where shares of a data company are traded, e.g. in venture investment).

Can information asymmetries relating to data aspects be reduced during the preparation of an M&A deal, by integrating information in the due

diligence process?

The following graph illustrates the due diligence process in M&A operations. The whole process can last from 6 to 18 months. It can be adapted to funding and IPO operations. It starts with a public information memorandum to which one or several possible acquirers can respond and agree on contractually binding non-disclosure agreements (NDAs). The due diligence phase is conducted with each of these possible acquirers on the basis of a “data room” containing the relevant information, exchange of written questionnaires and meetings with the target company’s management. When the target company selects one of the possible acquirers, the negotiation becomes exclusive and the acquirer deepens the due diligence efforts to extract more information. The signing of the deal stabilises the conditions, but the contract is binding only at closing stage. Lastly, operations are further refined post-deal, for example through a transitional services agreement (TSA).

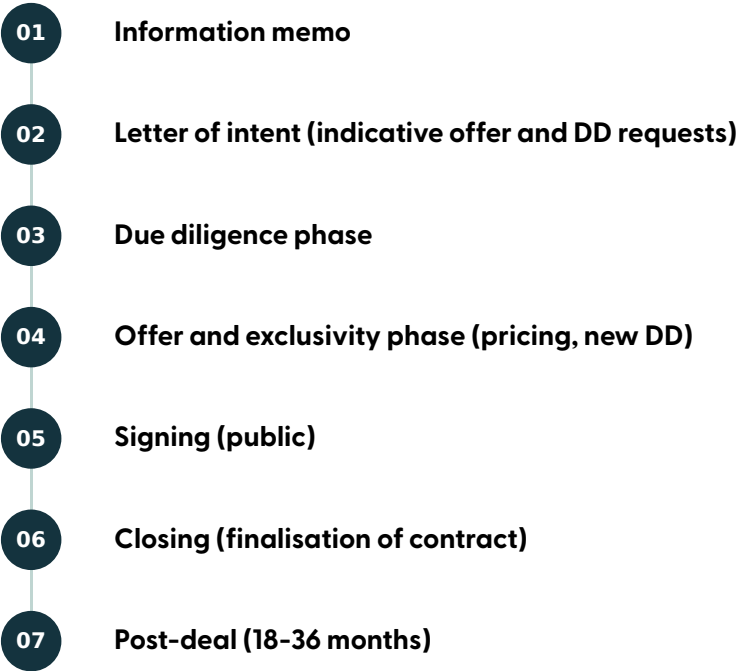


Fig. 1: the phases of the M&A process,

27 Cour de cassation, chambre commerciale, 25 juin 2013.

adapted from Ceddaha, 2025

Data aspects (both upsides and risks) are currently covered or can be covered, or they can even develop to a fully-fledged Data Due Diligence (DDD), depending on the company, its business model and its risks, mainly in the intermediary phase (due diligence and exclusivity phase). Data aspects can also be covered post-deal with the help of a data compliance roadmap (see below), for example when operational aspects of data management are implemented. But practitioners may insist on considering data questions as early as possible, so that they can inform the search choices of the target and acquirers alike. Upsides can be described by the target at the information memorandum stage, and the letter of intent can underline the interest of focusing on data risks during the due diligence phase itself.

As regards the due diligence process itself (phases in grey in Fig.1), it has become more complex and diversified with time, especially with parties with less knowledge of the M&A process. It covers IT and ESG aspects and regulatory compliance (legal aspects). **Data protection is at the intersection of those issues,**

and there is no obvious advantage in allocating it to any of these components over another. In data protection considerations, neither the legal nor the technical aspects should be underestimated. Earlier in the report, we have identified indicators, such as ESG reporting, data protection compliance KPIs for the Board and quantification of the value of data protection in financial statements, that could be used to demonstrate a company's data protection compliance, as part of the due diligence. A comprehensive option would also be to create a specific DDD, with a strong valuation component and with expert financial advice. This approach would enable the effective integration of legal and technical considerations into financial valuation, capturing both the benefits of sound data management and data protection compliance, and the risks arising from inadequate controls, weak oversight, or data-related incidents.

Most of the time the due diligence is based on a first-level coverage of the general legal or IT audit (cf. Graph 1). This option mainly results in a general declaration of compliance from the target company, non-auditable by construction and unlikely to lead to



Fig. 2: Proposal of a simplified audit matrix for a Data Due Diligence with financial materiality

a proper identification of risks and business upsides. This kind of “tick-the-box” approach is a suboptimal practice both for the acquiring and the target companies, because it does not mitigate for the existing information asymmetries.

The evidence collected during this study, together with the literature review, indicates that the due diligence process would benefit from a more granular approach, grounded in an audit matrix identified in Fig. 2.

First Step of the DDD

A description of how data and data compliance affect the company's business models and value creation and its products or services and an assessment on the data held by the company, their volume, quality and level of structuration.

A list of risks related to data the company holds, their likelihood, severity and time horizon, starting with the sensitivity of data, and possible mitigation techniques, with an assessment of the role of different stakeholders (for example, clients, business partners, regulators, attackers);

A simplified assessment of a company's compliance with data-related regulatory requirements, together with an evaluation of the maturity of its governance frameworks, controls and data management practices, as well as the presence of certifications and recognised assurance mechanisms that may contribute to value creation. These may include data protection certifications, adherence to codes of conduct, or certification under standards such as ISO/IEC 27001.

Moreover, where appropriate, prospective acquirers could be provided with a vendor due diligence (VDD) report, outlining the value generated by the organisation's data assets and related business capabilities. The report could also present the organisation's governance framework, compliance arrangements and data management processes, helping to evidence the value of previous investments in risk management, data protection and operational controls. The acquirer would subsequently complete its own assessment of residual risks and material compliance issues.

Second Step of the DDD

Once this step has been completed, the transactors would assess the information on data revealed by the due diligence process and its impact on the M&A deal price and conditions.

If the due diligence process reveals a need for urgent changes in compliance or urgent derisking measures, the changes can be integrated in suspensive clauses (covenants), between the signing and closing stages. This approach may not be the most effective for major changes as the time period between signing and closing is likely to last a few weeks or months. A more fruitful incentive for the target may be to negotiate earnouts (a supplement in the price, paid if certain conditions are met), at closing stage or even after closing. This can be used, for example, to fund the capital expenditure (capex) required by new compliance or derisking efforts, without affecting the price of the deal negatively.

More centrally, the objective of an appropriate DDD should be to reduce

the likelihood of triggering the liability or net asset guarantee, and therefore, its cost, when such guarantee is foreseeable. **The acquisition contract indeed assumes the company’s compliance with regulations: it is in the interest of the target company to document this compliance, as the risk will remain with the company for some time.** This is all the more true in the case of a share deal, where the risk is borne by the company. The liability guarantee can also be triggered if an unidentified risk occurs. External actors, like warranty insurers, can price such risks, which can increase the deal price if properly identified and mitigated, through guarantee cost reduction.

Third Step: Data and Compliance Roadmap

Finally, the most important good practice detected by our interviews (and consistent with the quantitative survey) is the definition of a Data and Compliance Roadmap for the post-deal phase.

Strong governance, data management and compliance can indeed be not only a tool for value creation during the merger, but can help upgrade the governance, IT systems and data practices of the target and acquirer alike. The resulting benefits for the target in that regard can sometimes be greater than the acquirer’s, allowing for unexpected upsides for the acquirer in the post deal phase. Apart from this alignment on best practices, a merger or a new shareholder investment can prompt review of a company’s

28 Financial multiples, or price-to-book ratios, are tools to assess a company’s financial valuation based on the ratio between the company’s market value and an accounting metric like earnings, EBITDA or sales, as compared to similar companies in the same industry.

operational processes that would directly benefit from improvements in data protection compliance.

A multi-year Data and Compliance Roadmap, also reduces the cost of the liability guarantee, or even makes it obsolete by optimising the data profile of the target. The new capex, if required by the roadmap, can be funded by a series of earnouts conditional to the realisation of the roadmap, these may in turn be funded by corresponding reductions in the acquirer’s operational costs.

As a result, the risks would be recognised and mitigated, and the deal price would be more reflective of the company’s comprehensive value and would not be affected by information asymmetries. The deal price would likely be higher, all other things being equal, and/or would justify higher multiples²⁸, when it comes to the quantification of value creation. Additionally, M&A negotiations may be more predictable, more balanced, and in the end more likely to succeed.

3.3.5 Financial valuation aspects

We have examined the benefits of integrating valuation of data assets and data risks in credit ratings and M&A transactions. In this section we discuss other aspects of financial transactions that may benefit from such consideration of data assets and data risks.

In a digitalised economy, where intangible assets are not well reflected by the frameworks and

metrics in force, considering the value of data helps explain the presence of important multiples in financial valuations, for example (typically, between 5 and 25 depending on the sector²⁹). Integrating data assets and data compliance into financial valuations increases corporate capital pricing efficiency. This approach was underlined through the insights gathered through the study interviews and supported by published empirical research (Wang and Hou, 2025). For companies that hold large volumes of data, it helps explain and justify value creation in a deal, even when the value of data is reflected only partially in stock prices and book value.

Data intensive sectors that may be more concentrated, benefit from higher economies of scale, and can maintain more important profits in the long run. This leads to higher multiples than in traditional sectors, less exposed to data. The available evidence indicates that multiples for software, digital advertising, AI, fintech and health sectors are quite high, whereas they are low for trade, food, energy or manufacturing.

Moreover, the assessment of the economic value of data, also helps reconsider the compliance costs, which are often otherwise treated as operational expenses. Compliance expenses have the features of an investment and may therefore, be treated as such, they can take the

29 See for example the sectoral data published by the well-known financial valuation specialist Aswath Damodaran from NYU Stern. https://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/vebitda.html

form of R&D expenses or capex, they are mobilised for the purpose of the business cycle, and they generate future value, as discussed in the accounting treatment of data section.

During the Daprolab workshop, it emerged that the more granular the due diligence based on the data sets a company holds, their purposes, content and life cycle, the better the link to business profitability, and the greater the impact on value creation. The same goes for data risks, which should be specifically identified, with the help of the company’s data protection impact assessment (DPIA) for example.

Data risks can affect company value on various horizons. They can affect business profitability in the short run, if a company is affected by a data breach or if its reputation is affected by non-compliant data processing or by an enforcement case by a data protection authority, these incidents may have short term impacts that may be reversible in the longer term. They also have a long-term component, for example, data breaches may produce spillovers, such as public awareness of data risks leading to tighter regulations or public mistrust for tech and AI companies growing over time. These types of data risks can alter both market conditions and public trust.

With regards to financing availability,

there is evidence that data intensive sectors (and more generally, sectors with more intangible assets) face a financing gap, because of the challenges with valuing intangible assets and lack of indicators about compliance with data protection to inform financing decisions (OECD, 2021). They are less able to collateralise their assets and the

Table 3: the impact of data on the economic value and financing conditions of a company

Impact on business profitability	Impact on financing conditions
Data-based business models generate high and more stable profitability upsides, reflected in higher future cash-flows (short term).	The effect of data exposure on the cost of own funds is ambiguous: A higher profitability reduces the costs of own funds, all things being equal. Data risks tend to increase the risk premium in the cost of own funds, especially if the company is young (the uncertainty is higher).
Good data management and governance help secure performance and reduce data risks (short term).	
The effect is magnified when the company is mature and benefits from an established market position.	
Data risks, if not mitigated, affect future profitability (short term) as well as long-term growth potential of the company.	The net effect depends on the development stage and market position of the company.
Data-based business models generate high and more stable profitability upsides, reflected in higher future cash-flows (short term).	
Good data management and governance help secure performance and reduce data risks (short term).	
The effect is magnified when the company is mature and benefits from an established market position.	
Data risks, if not mitigated, affect future profitability (short term) as well as long-term growth potential of the company.	

asymmetry of information concerning the financial value of their assets is greater (lacking transparency on their data upsides and risks). Therefore, they tend to rely more on own funds financing. This is particularly the case in the tech sector.

The impact of including data upsides and risks in the financial valuation of a company, also depending on its age and market position, can be summarised as follows:

This table also helps understand why better integration of data upsides and risks in accounting frameworks and more transparency from emitters regarding their data policies, as proposed by the present report, would have a positive effect on innovation financing.

3.3.6 Integration of data questions in the Discounted Cashflow method

We have used the Discounted Cash Flow (DCF) method indicatively in order to demonstrate that it is possible to integrate better data aspects in financial valuations. It may not always be possible to apply this method, and organisations should assess the feasibility of applying this, or similar methods, in their valuation processes. The DCF model, as a financial valuation method based on the future cash flows generated by a company, is time-discounted by the cost of capital, and it is relevant because it integrates the effects on profitability and the penalising effects of risks alike.

The approach presented below is a high-level overview. Application would need to be specified by type of company, nature of risks and integration of tax and capex aspects. We would welcome further discussion with M&A actors on the use and application of the approach.

The economic value of a company is calculated (as opposed to the book value of its assets) based on the revenues generated by the company at a given time horizon (typically, the horizon of the business plan). This economic value is mirrored by the value of own funds and the value of debt (as opposed to their book values on the liability side):

$VE = VOF + VD$

Where VE is the economic value of a company, VOF is the value of the company’s own funds and VD is the value of the company’s debt.

The weighted average cost of capital (WACC) plays an important role in the calculation. It depends also on the financing structure and is defined as:

$$WACC = \frac{V_{OF}}{V_{OF} + V_D} K_{OF} + \frac{V_D}{V_{OF} + V_D} K_D$$

where $\frac{V_{OF}}{V_{OF} + V_D}$ reflects a firm-specific risk premium (see table 2) and $\frac{V_D}{V_{OF} + V_D}$ a credit spread (always higher for data-intensive companies). The effect of taxes here is neglected.

Data risks are therefore more likely to affect the WACC, if the company is young and its market more competitive. It is therefore reasonable to integrate short term data risks in the choice of a higher WACC for these companies.

The economic value is the sum of the value of future cash flows (FCFi), time discounted by the WACC, and of a final value (FV) that depends on assumptions on long-term profitability and a long-term growth rate for the company. This final value is an important part of the economic value estimation and is sometimes hard to justify. It is therefore, reasonable to integrate long-term data risks in the calculation on the final value to reflect the effects of data risks on long term profitability and long-term growth rate, this inclusion reduces the final value.

$$VE = \sum_{i=1}^n \frac{FCFi}{(1 + WACC)^i} + \frac{FV}{(1 + WACC)^n}$$

On the basis of a given horizon of the business plan n and a given financing structure, the positive effects of data intensity on profitability, increased by a top-up factor if data stewardship and governance is carried out correctly. For example, if a privacy certification is present, that could be integrated into the future cash flows FCF.

The detection of non-compliance or poor data management and governance practices in the company would reduce this upside.

The final value (FV) would be affected by long-term data risks, such as societal and cyber risks, which are general and non-diversifiable. This also helps make the FV more realistic.

In this approach, the WACC would not be systematically penalised. But it would increase with identified data risks, especially for younger companies and those acting in more competitive markets. It could also be affected by other company-specific data considerations, such as the necessity of compliance or cybersecurity investments.

Sensitivity analyses may complement the economic value estimation to test

the impact of the occurrence of a given data risk. Such analyses would assess the short-term, risk specific impact on the company, without penalising the economic value in the central estimation. Conducting sensitivity testing, alongside the economic value estimation can be used as an internal risk management tool, supporting decision making on compliance investments. **The economic value and sensitivity testing can be shared and inform discussions with insurers and rating agencies. In relevant cases, where the business model is highly dependent on data, it can also be used as a stress-testing tool.**

The discussion in this section shows that financial valuation of data assets and data risks is key for value creation in the digital economy, it reduces information asymmetries in transactions and enhances funding possibilities.



4 ● Emerging Good Practices

This report discusses the study findings from engagement with financial sector organisations through semi-structured interviews and workshops, the analysis of ESG and accounting frameworks and the findings of quantitative surveys conducted in Luxembourg and France. This section distils the findings about the value of compliance with data protection in the financial sector and summarises emerging good practices in three themes, accounting, financial valuation and governance, cyber risk and AI.

Accounting good practices

1 As organisations increasingly rely on internally generated databases, including these with personal data, the potential recognition of such databases as assets merits consideration on a case-by-case basis. This is particularly relevant where databases are well structured and appropriately governed, as non-compliant databases may give rise to legal, operational, and valuation risks that can limit their use and economic value. **Mapping of databases provides organisations with an understanding of the personal data they hold and**

gives them the opportunity to assess and improve the quality of these datasets, applying data protection principles, such as data accuracy and data minimisation, where applicable. Reviewing current valuation practices and accounting frameworks also allows organisations to reconsider their datasets' status against IAS 38 criteria and valuation as intangible assets.

2 Organisations would benefit from integrating data protection frameworks in their accounting practices. **Integrating data protection compliance considerations (legal basis, retention periods, data accuracy, etc.) into accounting practices can provide a guide for action.** Using data protection principles in accounting practices and involving DPOs in the accounting process facilitates improved communication and creates a common understanding about recognising and valuing datasets as strategic assets. Such an approach may support more robust decision-making by ensuring that datasets considered in valuations, transactions, or strategic initiatives meet the legal, quality, and governance requirements necessary to create and sustain business value.



3 Parties in M&A transactions, auditors and rating agencies increasingly consider data-related risks when assessing the value of personal data assets. **The valuation of personal data-related assets should be reviewed regularly and, where appropriate, supported by impairment assessments.** Such reviews can help organisations maintain an up-to-date understanding of their datasets, identify legal, operational, or cybersecurity risks affecting their value, and ensure that datasets used in business operations and AI applications remain reliable, compliant, and fit for purpose.

4 The study findings and analysis of the international accounting standards have indicated that **updating IAS 38 would facilitate valuation of datasets containing personal data as an intangible asset.** The IAS 38 dates back to 2001 and has been updated several times to reflect evolving conditions, therefore, further revision would ensure that it accounts for the data-driven economy, where data is an intangible asset. Engagement between regulators and standard setters would help

assess feasibility and would inform a proportionate and appropriate approach.

Financial valuation good practices

5 Organisations are starting to develop a more **integrated approach to assessing the value of data, by considering both benefits and costs associated with data collection, use and storage and data protection compliance, alongside the risks arising from low data quality, non-compliance or cybersecurity incidents.** Incorporating data-related considerations into valuation processes can provide a more comprehensive view of the factors that influence the economic value of datasets. Such an approach may support more informed decision making, assist organisations to identify and mitigate data-related and cyber security risks, and provide a more balanced view of the impacts of data protection compliance in strategic and financial assessments. While not all of these impacts may directly be reflected in balance sheets, they may contribute to value creation over the longer term. Being able to assess risks, such as data

quality, and benefits, such as trust, that are difficult to quantify, may provide organisations with useful indicators in their engagement with investors, consumers and regulators.

6 Organisations **include and document their personal data compliance assessment, as part of their due diligence for financial transactions.** In M&A and investment transactions this documentation helps identify and assess data protection compliance issues, strengthening transparency and confidence in the decision-making process. This enables purchasing parties, investors and other stakeholders involved in financial transactions to access relevant information on data protection compliance and data-related risks throughout the due diligence process.

7 Valuation methods and accounting frameworks often rely on estimates of future revenues and cash flows, complemented by sensitivity analysis. **Data protection compliance and data-related risks can be integrated into DCF valuations by assessing their potential impact on future cash flows and value creation.**

Similarly, income-based and relief-from-royalty valuation methods reflect expected future benefits. In this context, IAS 36 defines value in use as present value of estimated future cashflows.

8 Market participants that participate in or support M&A transactions recognise that **demonstrating data protection compliance as part of a financial transaction may require a structured roadmap to address identified compliance gaps and data-related risks.** In M&A operations companies may need time to address compliance gaps (e.g.: upgrade IT systems and strengthen personal data management practices). Such a roadmap can create the conditions for value creation, including post-deal, while helping to reduce the cost of liability guarantees.

Governance, cyber and AI good practices

9 Organisations are increasingly adopting a strategic view of compliance with data protection as a business asset. Organisations

that hold large volumes of personal data and have a clear data strategy, including for personal data, are best positioned to mitigate strategic, operational and cybersecurity risks and activate the benefits of compliance. **Ensuring senior decision makers and the Board have a written data and compliance strategy and building KPIs to reflect the value of personal data and compliance are important components in developing a strategic view.**

10 Organisations are starting to recognise the importance of integrating data protection in organisational and AI governance. **When internally generated data is critical to AI development and deployment, integrating data protection into both organisational and AI governance frameworks improves efficiency, reduces risks and ensures consistency. Organisations have found it beneficial to develop AI and ethics functions in DPO teams to support broader AI deployment and governance.**

11 Organisations integrate data protection rules in cyber resilience strategies. This is the most well-established practice in considering data as part of organisational strategies. As part of their strategies, organisations model the financial and reputational consequences of data breaches and cyber incidents to improve preparedness, guide cybersecurity investments, and

reduce potential impacts on company performance and market perception. **This includes quantifying data protection risks and conducting cyber stress tests, simulating major data breaches and privacy incidents, to assess impacts. Integrating data protection metrics into cyber risk reporting also provides a comprehensive view of cybersecurity and data protection risks to the Board.**

12 Organisations can leverage the benefits of data protection certifications. **Compliance indicators, such as data protection certifications and approved codes of conduct, help demonstrate compliance and transform it into a competitive advantage.** In the context of data asset ownership, valuation, and accounting, data protection certifications can provide assurance that processing activities comply with applicable data protection requirements. This strengthens confidence in the legality, integrity, and ongoing usability of data assets, including those underpinning AI systems and AI-enabled services. In the context of mergers, acquisitions, and investment transactions, data protection certifications also facilitate due diligence by demonstrating independent evidence of compliance and helping stakeholders assess privacy-related risks, liabilities, and the sustainability of data-driven and AI-related assets.

5. Conclusion

This report has examined the multifaceted uses and value that compliance with data protection creates for organisations in financial markets.

While compliance with data protection requirements, from data mapping and data protection impact assessments to the implementation of technical and organisational safeguards, can represent a significant operational and financial undertaking, particularly for smaller organisations, the analysis presented in this report suggests that these costs should be viewed as an investment. Indeed, they must be weighed against the tangible benefits that robust data protection practices deliver, including enhanced customer trust, reduced exposure to reputational and legal risk, greater operational resilience, increased value for datasets and a stronger foundation for sustainable digital innovation.

A central thread running through this report is the growing recognition of data as a strategic asset. Financial organisations increasingly rely on the collection, processing, and analysis of personal data to develop new products, refine risk models, and personalise services. This shift requires a parallel evolution in how

organisations perceive compliance, not merely as a defensive, regulatory obligation, but as an opportunity to build governance structures that unlock the value of data responsibly. Organisations that embed data protection principles, such as data minimisation, purpose limitation, and privacy by design, into their broader data strategy, are better positioned to capture this value, while maintaining the trust of their investors, customers and regulators alike.

The report is the result of enhanced cooperation among CNPD, CNIL and the ICO, and has served to develop a sense of common understanding of data protection compliance in financial organisations across these three markets. Strengthening these channels of cooperation remains essential to developing knowledge about application of data protection rules across markets.

Closely tied to this is the recognition that data protection is a cornerstone of trust and stability for financial organisations and the broader financial ecosystem. As financial services become increasingly data-driven and interconnected, spanning banks, insurers, fintech providers, and third-party service providers, the protection of personal data underpins

the security and integrity of the entire system. Weaknesses in data governance or protection practices at any point in this ecosystem can have ripple effects, undermining consumer confidence and exposing organisations to systemic risk. Ensuring strong, consistent data protection practices is therefore not only a matter of individual compliance, but a shared responsibility that supports the resilience of the financial sector as a whole.

Finally, this report was built on the evidence gathered through



surveys and open dialogue with stakeholders. Such engagement provides invaluable insight into the practical challenges organisations face in achieving compliance, while also surfacing emerging risks and good practices that might otherwise go unnoticed. **Learning from these exchanges enables both regulators and regulated entities to refine their approaches over time, ensuring that regulatory frameworks remain proportionate, workable, responsive to a rapidly evolving data landscape, and support organisations to innovate and grow.**

6. References

Aboody, D. & Lev, B., 1998. The value relevance of intangibles: The case of software capitalization.. Journal of Accounting Research, Volume 36, pp. 161-191.

Babina, T., Anastassia, F., He, A. & Hodson, J., 2024. Artificial intelligence, firm growth, and product innovation. Journal of Financial Economics, Volume 151.

Blycha, N. A. et al., 2026. Pricing the Unpriced Asset: A Standards-Based Method for Valuing Enterprise Data under IAS 38 and IAS 2, s.l.: s.n.

Ceddaha, F., 2025. Fusions-Acquisitions. Paris: s.n.

Cheong, H., Kim, B. & Vaquero, I. U., 2023. A Data Valuation Model to Estimate the Investment Value of Platform Companies: Based on Discounted Cash Flow. Journal of Risk and Finanical Management , 16(6).

Conseil national de la productivité, 2023. Rapport Annual 2022-2023. [En ligne] Available at: <https://odc.gouvernement.lu/dam-assets/domaines/cnp/cnp-rapport-2022-2023.pdf>

Day, K. & Booker, Q., 2024. Market Reactions to Cybersecurity Incidents: A Case Study Approach. Issues in Information Systems, pp. 260-276.

Day, K. & Booker, Q., 2024. Market Reactions to Cybersecurity Incidents: A Case Study Approach. Issues in Information Systems, Volume 25.

Deloitte, 2025. Valuing data assets can be key to unlocking board-level support for data modernization and transformation, s.l.: s.n.

Department for Business and Trade, 2024. UK Sustainability Reporting Standards. [En ligne] Available at: <https://www.gov.uk/guidance/uk-sustainability-reporting-standards>

Ding, R., 2016. Disclosure of Downside Risk and Investors' Use of Qualitative Information: Evidence from the IPO Prospectus's Risk Factor Section. International Review of Finance, 16(1).

EFRAG, 2021. Better Information on Intangibles – Which is the Best Way to Go?, s.l.: s.n.

EU 2022/2557, 2022. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council

- Directive 2008/114/EC (Text with EEA relevance). s.l.:s.n.
- EU Commission, 2018. Ethics and data protection. [En ligne]
Available at: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf
- EU Commission, 2022. Directive (EU) 2022/2464. [En ligne]
Available at: <https://eur-lex.europa.eu/eli/dir/2022/2464/oj/eng>
- Farboodi, M., Singal, D., Veldkamp, L. & Venkateswaren, V., 2025. Valuing Financial Data. The Review of Financial Studies, 38(3), pp. 938-980.
- Frontier Economics, 2021. The value of data assets: A report fro the department of culture, media and sport. [En ligne]
Available at: https://assets.publishing.service.gov.uk/media/6399f93d8fa8f50de138f220/Frontier_Economics_-_value_of_data_assets_-_Dec_2021.pdf
- Gao, X., Liu, J. & Lu, H., 2025. Accounting for Data Assets (Working Paper)
- Guo, X., Li, P. & Wang, F., 2026. How do data assets enhance firm value in the digital economy: Evidence from listed tech firms. Financial Research Letters.
- IAASB, 2016. ISA 250 (Revised), Consideration of Laws and Regulations in an Audit of Financial Statements. [En ligne]
Available at: <https://www.iaasb.org/publications/isa-250-revised-consideration-laws-and-regulations-audit-financial-statements-13>
- ICAEW, 2025. A new emergening type of intangible. [En ligne]
Available at: <https://www.icaew.com/-/media/corporate/files/policy-and-research/research-and-academics/data---a-new-emerging-type-of-intangibles.ashx>
- ICO, 2026. Data Controller Study. [En ligne]
Available at: <https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/data-controller-study/>
- Iron Mountain & De Braw Blackstone Westbroek, 2013. European Document Retention Guide, s.l.: s.n.
- Kepler, J., McClure, C. & Stewart, C., 2026. Competition Enforcement and Accounting for Intangible Capital. The Journal of Finance.
- Lev, B., 2018. The deteriorating usefulness of financial report information and how to reverse it.. Accounting and Business Research, 48(5), pp. 465-493.
- Lev, B. & Gu, F., 2016. The End of Accounting and the Path Forward for Investors and Managers. s.l.:Wiley.
- Lev, B. & Sougiannis, T., 1996. The capitalization, amortization, and value-relevance of R&D. Journal of Accounting and Economics, 21(1), pp. 107-138.
- Lev, B. & Zarowin, P., 1999. The Boundaries of Financial Reporting and How to Extend Them. Journal of Accounting Research, 37(2), pp. 353-385.
- Li, K. & McClure, C., 2023. Evolution in Value Relevance of Accounting Information. The Accounting Review, 98(1), pp. 1-28.
- Martins, A. M., Moutinho, N. & Cró, S., 2025. Stock market effects of major cyber-attacks: evidence for breached

- and cybersecurity listed firms. Journal of Banking Regulation, pp. 868-877.
- Martins, A. M., Moutinho, N. & Cro, S., 2025. Stock market effects of major cyber-attacks: evidence for breached and cybersecurity listed firms. Journal of Banking Regulation, 26(868-877).
- Muktadir-Al-Mukit, D. & Ali, H., 2025. The Dynamics of Stock Market Responses Following the Cyber-Attacks News: Evidence from Event Study. Information Systems Frontiers.
- Muktadir-Al-Mukit, D. & Ali, H., 2025. The Dynamics of Stock Market Responses Following the Cyber-Attacks News: Evidence from Event Study. Information Systems Frontiers.
- National Protective Security Authority, 2026. About us: Critical National Infrastructure.
- OECD, 2022. Measuring the value of Data and Data flows, OECD Digital Economy Papers 345.
- ONS, 2025. Investment in intangible assets in the UK: 2023. [En ligne] Available at: <https://www.ons.gov.uk/economy/economicoutputandproductivity/productivitymeasures/bulletins/investmentinintangibleassets/intheuk/2023>
- PWC, 2026. Global Top 100 companies by market capitalisation : March 2026.
- Sargent, T. & Denniston, L., 2023. Valuing Data: Where Are We, and Where Do We Go Next?. Center for International Governance Innovation, Volume 280.
- Schoch, D. S., 2020. Mergers and Acquisitions in the Data Economy. [En ligne]
- Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3686247
- Skinner, D., 2008. Accounting for intangibles – a critical review of policy recommendations. Accounting and Business Research, Volume 38, pp. 191-204.
- Tambe, P., Hitt, L., Rock, D. & Brynjolfsson, E., 2020. Digital Capital and Superstar Firms. National Bureau of Economic Research Working Papers, Volume 28285.
- Veldkamp, L., 2023. Valuing Data as an Asset. Review of Finance, 27(5), p. 1545-1562.
- Wang, S. & Hou, L., 2025. Data assetization and corporate capital pricing efficiency. Financial Research Letters, Volume 86.
- World Economic Forum, 2026. The Future of Venture Capital: Unlocking Liquidity and Growth, Insight Report. [En ligne]
Available at: https://reports.weforum.org/docs/WEF_The_Future_of_Venture_Capital_2026.pdf
- Wyatt, A., 2008. What financial and non-financial information on intangibles is value-relevant? A review of the evidence. Accounting and Business Research, Volume 38, pp. 217-256.
- Xiaochuan, G., Pencheng, L. & Wang, F., 2026. How do data assets enhance firm value in the digital economy: Evidence from listed tech firms. Financial Research Letters, Volume 91.
- Xiao, S., Wu, K., Xiao, X. & Changqui, L., 2025. How do data assets affect firm investment?. International review of financial analysis, Volume 106, pp. 1-12.

A Statistical findings

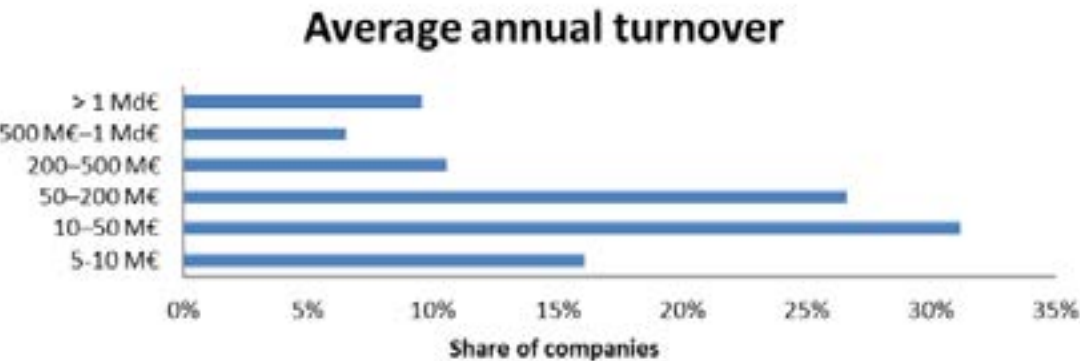
1. Methodology

The survey received 204 responses from a variety of companies. It was distributed through Framafirms to organisations equipped with a Data Protection Officer, and built from the CNIL’s DPO records, cross-referenced with a public business registry.

Several features of the data should be kept in mind when reading the results. First, most questions were multiple choice: a single company could select several answers, and could therefore, exhibit several characteristics at once. Accordingly, for a better readability of the results, the percentages are calculated based solely on the number of companies that answered the question concerned and not

based on the total number of answers to the question. Each percentage can thus be read as “X% of the companies that answered this question...”. As a consequence, the percentages for a given question may add up to more than 100%. Second, not all companies completed the entire questionnaire: the number of respondents, therefore, varies slightly from one question to another, and each result is computed only on the number of companies that actually answered the relevant question. Finally, all statistical links reported hereafter are measured through appropriate tests and should be understood as associations rather than causal relationships.

2. Company Profiles and Business Models

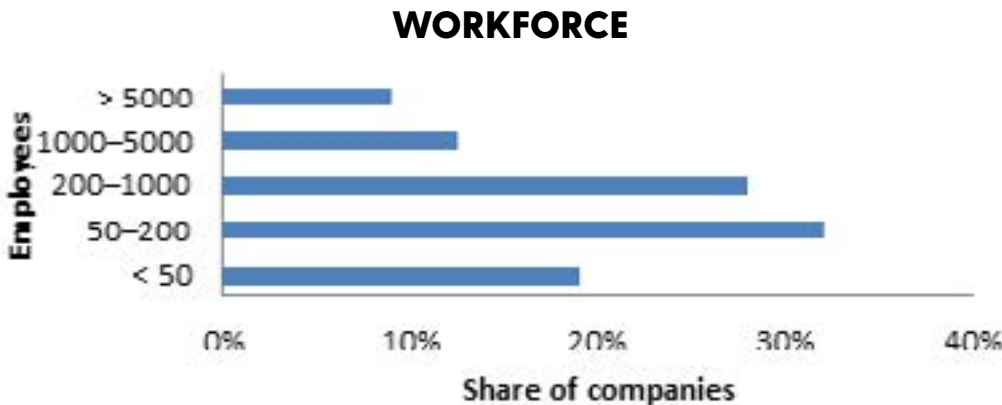


Graph 4 Average annual turnover

The response profile sketches a sample dominated by SMEs and mid-market companies. Almost half generate less than €50M in revenue (16% below €10M and 31% between €10M and €50M), while a quarter falls into the €50–200M bracket; large companies remain a minority, with only 16% exceeding €500M in revenue and less than 10% exceeding one billion euros.

The comparison between the companies contacted and the respondents reveals a selection bias related to size that is important to

bear in mind when analysing results: companies with over €200 million in revenue, which represent only 10% of the sample, constitute 27% of respondents, those with less than €50 million fall from 72% to 47%, while those with less than €10 million in revenue fall from 35% to 16% (highly significant difference). Large companies, better equipped with DPO and finance functions, were therefore more likely to respond. The sample thus overrepresents large organisations, suggesting that the results primarily reflect the practices of medium to large companies.



Graph 5 Number of employees

The workforce structure confirms this premise: a third of the respondents employ between 50 and 200 employees, and slightly more than a quarter between 200 and 1,000, while structures with over 5,000 people represent only 9% of the sample.

Geographically, Île-de-France alone concentrates more than a third of the headquarters (34.5%), ahead of Auvergne-Rhône-Alpes (12.7%), with the other regions sharing the remainder more diffusely.

On a sectorial level, the sample is comprised of companies offering

miscellaneous services (25%), manufacturing (16%), financial and insurance activities (11%), and commerce (10%), followed by transport, healthcare, and information-communication.

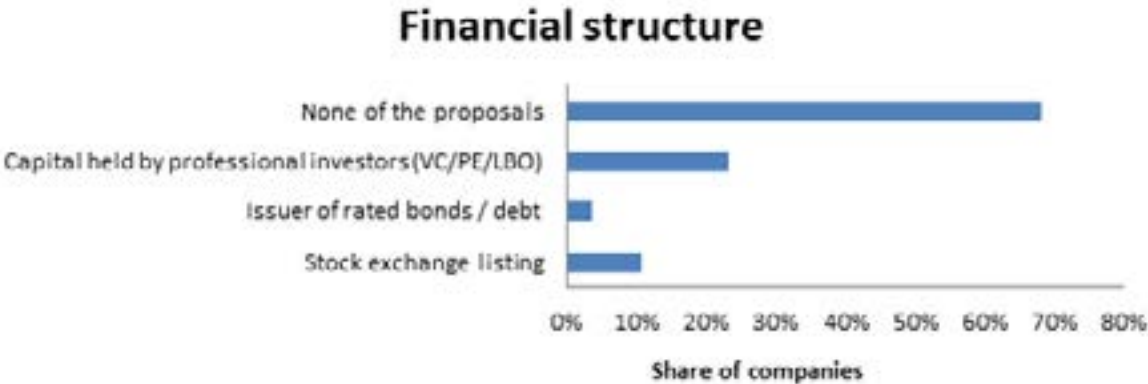
Companies were asked at what level of their structure they were responding to the questionnaire: group DPO (40.7%), “not concerned” (32.0%), at the company level (30.9%), and at the group finance department level (20.6%). A third of respondents declared themselves “not concerned”: these are, in all likelihood, independent companies,

not part of a group. For them, the question of the scope of the response is irrelevant. On the other hand, the two remaining levels belong to a group and specify the perspective of their response: most often that of the Group DPO (who responds on behalf of the entire group), sometimes that of the sole proprietorship. The dominant combination of several responses is group DPO and group finance department (31 respondents), this indicates more structured groups where the respondent simultaneously holds the role of Group DPO and operates within a group consolidation framework.

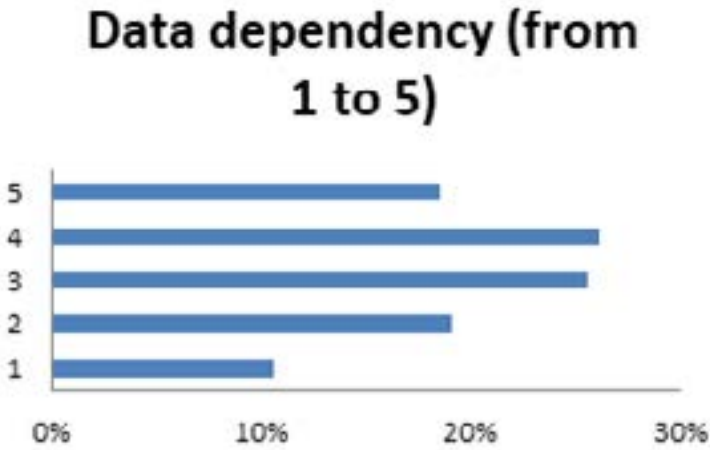
From a financial perspective, the majority of respondents have no

direct exposure to the markets: more than two-thirds (68%) are neither listed, nor debt issuers, nor owned by professional investors, while 23% have capital held by funds (Venture Capital / Private Equity / LBO) and 11% are publicly traded. These companies are also familiar with external growth operations, since 37% have already carried out an acquisition in the last five years.

Note that 43% of group companies have financial exposure (listing, debt, funds), compared to 11% of independent companies, and 53% of group companies have participated in an M&A operation, compared to 19% of independent companies.



Graph 6 Financial structure



Graph 7 Business model data dependency

When asked about their business model's dependence on data, they average 3.23 on a scale of 1 to 5, with a rather balanced distribution: about 30% declare themselves slightly dependent (levels 1-2) against 45% highly dependent (levels 4 and 5).

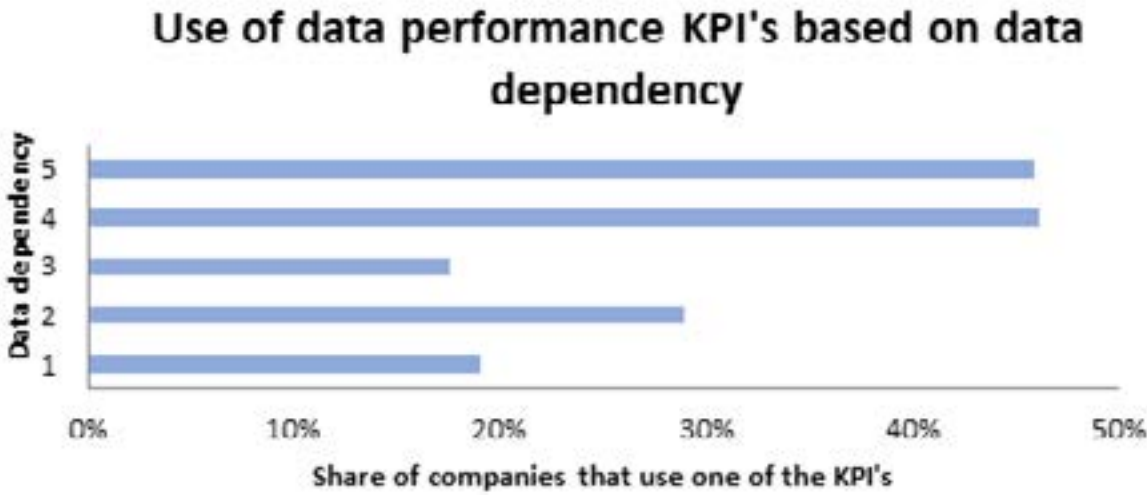
The respondents provide insights into the nature of the processed data and how compliance is perceived within the company. Nearly three out of four companies (71.5%) report processing standard B2C information. More sensitive data is not marginal, however, as 37.5% of respondents indicate handling it, while behaviour and profiling data remain in a minority (16.5%). A significant share of "other" responses (26.5%) is explained by the textual responses given by the companies indicating B2B data.

The perception of data compliance is multifaceted: mainly understood as a regulatory and legal issue, it is also for 57.5% perceived as an operational factor affecting reputation. Compliance "as an asset" or a competitive advantage is shared by slightly more than a third of companies (34.5%), which means they view data protection as a value driver.

3. Data and Financial Materiality

3.1 Data management through indicators

To the question: Have you implemented specific key performance indicators (KPIs) that link data governance and financial performance?



Graph 8 Use of data performance KPI based on data dependency

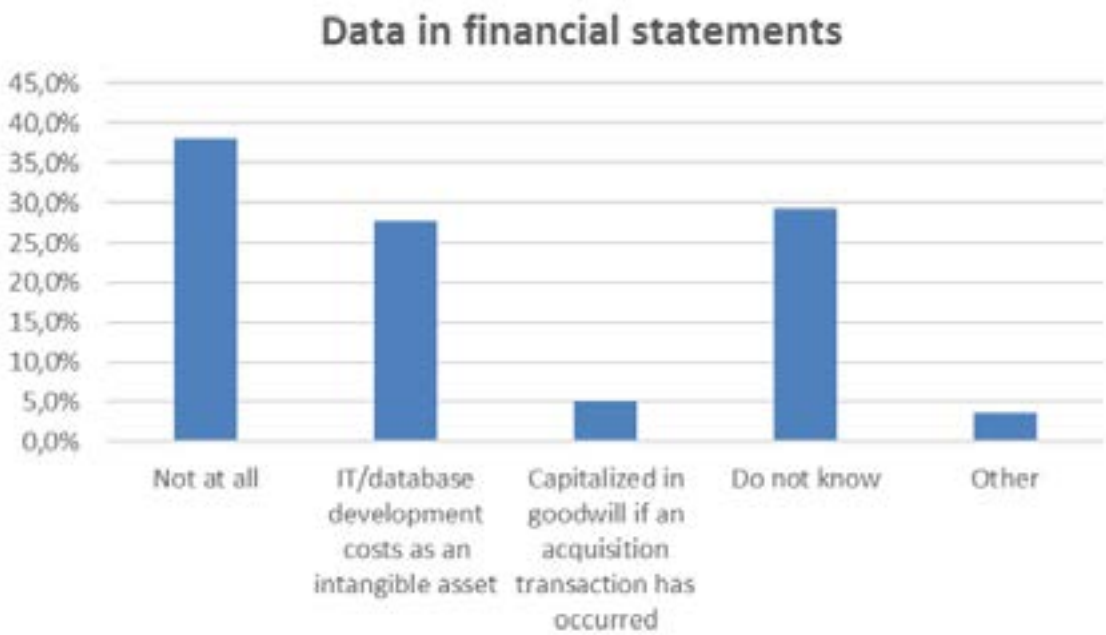
65% have responded that they have no KPIs linking data to performance. Respondents have indicated that when KPIs exist, these indicators are primarily risk-oriented (24%) and customer/sales KPIs (11%) and use of financial KPIs linked to data (6% of responses) remains rare.

The link emerging between data dependency and the use of KPIs (at least one among the propositions) indicates that companies that consider their business model highly dependent on data (levels 4 and 5)

are more likely to have implemented data-performance KPIs (close to 46%), against 17% to 29% among the less dependent.

Several tests were made to validate the result (Spearman’s correlation of 0.21, p-value = 0.003, Cochran-Armitage trend test, p = 0.004). A logistic regression indicates that each additional point on the dependency scale multiplies the odds (odds ratio) of having KPIs by about 1.45. The association is statistically robust but moderate in strength.

3.2 Financial and accounting integration of data



Graph 9 Approaches of including data in financial statements

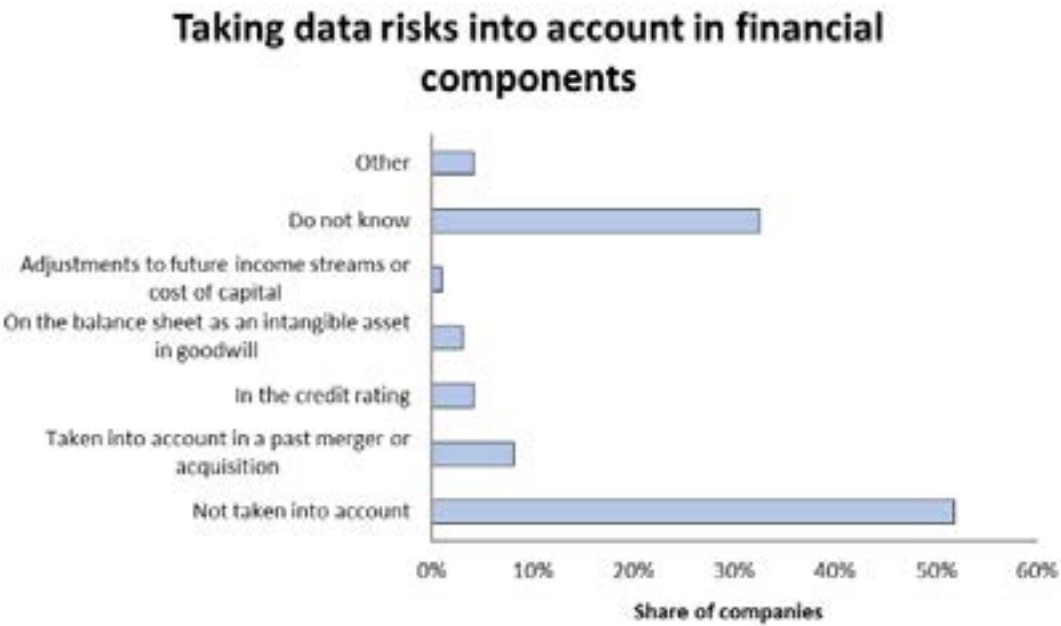
Regarding the reflection in financial statements, 38% of companies consider that their databases are “not at all” reflected, and 29% do not know, totaling 67%. 28% of respondents suggest that data is included in financial statements as the cost of IT development and database creation. Inclusion in goodwill during

an acquisition is indicated by 5% of respondents.

Link with M&A Operations: Among the 199 companies that responded to the question, those that had participated in a merger or acquisition operation (82) were more likely to have included their databases in

their financial statements, compared to the companies that had not participate in a merger or acquisition (117). Only 26% of companies that had carried out a merger or acquisition indicated that their data was “not at all” considered, compared to 47% of companies that had not participated in an acquisition (Odd Ratio = 0.39 and p-value = 0.003). This was primarily demonstrated through the capitalization of development costs

(35% versus 22% p = 0.05) and, to a lesser extent, through goodwill (9% vs 3%, 7 out of 82 versus 3 out of 117). The difference identified in goodwill is insignificant given the small number of cases. These differences partly reflect the larger size of companies that have participated in mergers and acquisitions, and the overall difference is no longer significant after accounting for size (adjusted OR = 1.8 and p = 0.07).



Graph 10 Approaches of including data related risks in financial valuations

Graph 10 shows the results to the question: To your knowledge, how are data-related risks primarily factored into your company’s financial valuation, whether internally or via external players? More than half of the respondents (52%) indicate that they do not take data related risks into account at all and nearly a third (32%) do not know. Respondents indicated that data related risks were considered during a past M&A operation (8%), in financial ratings (4%), on balance sheets as an intangible asset or goodwill (3%), or

via an adjustment of future cash flows and the cost of capital (1%).

Among the 197 responding companies, those that had participated in a merger or acquisition (82) were more likely to consider data risks into their financial valuations: 22% compared to 10% of non-participants (11 out of 115, odd ratio = 2,65 with p-value of 0.024). This effect persisted after controlling size (adjusted OR = 2.6 with a confidence interval of 1.1–6.5 and p -value of 0.035).

This question concerns only companies involved in M&A, 72 respondents answered it, that is fewer than the 82 that reported participating in an M&A operation in Question 15, this is consistent with the question, which refers to the accounting integration of acquired databases that primarily concerns buyers rather than sellers (see Annex). Among these 72 companies, more than half (38, or 53%) report no valuation at all. When a valuation does take place,

respondents indicate two methods: 14% (10 companies) fold the databases into goodwill, while 18% (13 companies) identify them as specific intangible assets on their balance sheets. This reinforces the findings from Questions 15 and 16 that goodwill is not the only vehicle to account for data value, even in an acquisition context. The others 15% (11 responses) fall under “other”, often reflecting uncertainty about the subject.

Accounting valuation of acquired databases



Graph 11 Respondents that have participated in merger or acquisition transactions in the past five years, valuation of acquired databases

We also asked companies that have participated in merger and acquisition transactions, whether the discovery of a non-compliant database could have had direct financial consequences. In almost half of the cases, respondents indicated that the discovery of non-compliant databases had no impact, in 19% it led to specific liability guarantees being set up during the transaction, in 4.5% it led to downward price revisions

and in 3% it led to cancellation of the transaction. Several verbatim responses reveal a real, albeit indirect, financial impact: remediation costs spread over time, a potential drop in profitability and risks identified post-acquisition (salesforce breach, lack of DPA with subcontractors) generated remediation costs and mobilised DPO resources.

3.3 Link between data vision and financial practices

Strategic view of compliance and practices



Graph 12 Companies’ views on data governance and integration of data governance to financial performance

We inquired about how companies perceive data governance, as an operational asset, a strategic asset, or a regulatory and legal issue. We also inquired about integration of data governance into three financial practices: use of KPIs that link data governance to financial performance, data protection included in financial reporting, and the inclusion of data risk in financial valuations. We found that companies that have a strategic vision of governance are more likely to include data governance in real practices.

Based on the (multiple-choice) question on the perception of compliance, respondents were divided into two groups: those who selected “strategic asset / competitive advantage” (strategic vision) and those who selected “operational asset” or “regulatory and legal issue” (operational vision). We then compared the adoption

of the three financial practices between the two groups: having KPIs linking data governance and performance (at least one “yes” KPI), publishing quantitative reporting on data, and taking data risk into account in valuations (rating, balance sheet, future cash flows, or past M&A). Each comparison only covers respondents who answered both the perception question and the relevant practice, and the link is measured by an odds ratio (logistic regression) complemented by a chi-square test. Companies perceiving compliance as an asset are more likely to undertake each of these practices: 49% of companies that perceive data governance as a strategic asset also use KPIs that link data governance to performance versus 25% of the organisations that view data governance as an operational asset and regulatory and legal issue, 21% include data governance quantitatively in reporting versus

8% and 24% include data risks in valuations versus 10%, with odds ratios between 2.8 and 3.1 for all of the three modalities ($p < 0.01$). The effect is not due to a simple size bias: after controlling size and business sector via the logistic regression, it remains significant across all three.

Based on Question 4 (the level at which the response was given), we compared responses provided “at the level of the group’s financial department” ($n = 40$) with all others, across the three financial-integration practices. Responses from the group finance level do not seem to be associated with greater adoption of any of the practices: data-performance KPIs from Question 12 (32.5% vs 34.9% p -value = 0.85), databases reflected in the financial statements from Question 15 (30.0% vs 30.9), and data risk factored into valuation from Question 16 (20.0% vs 13.3% with Odd ratio of 1.62 but not significant, 0.32 of p -value).

3.4 Extra-financial reporting

“To what extent do your auditors integrate data protection and compliance into their annual audit of your internal controls and financial risks?”

The level of detail published on data protection remains low for a large part of the sample. 38% of companies do not cover the subject in their extra-financial annual reports, and 22% maintain a minimal mention, a simple declaration of compliance. Communication efforts do exist, mostly qualitative (description of internal policies, role of the DPO, training actions) for 34%, while quantitative communication (volume of data subject rights requests,

amounts invested in cybersecurity, measurement of quantified risk exposure) concerns only 13% of companies.

3.5 Role of data protection in audits and controls

We also asked about companies’ audit practices regarding their data. We note that the most widespread practice amongst companies is examining basic IT elements without conducting a GDPR compliance audit (46%), followed by questioning the DPO or the legal department on ongoing regulatory fines or lawsuits (30%). We have also observed practices that include data protection in audits, such as the use of cyber/IT specialists in addition to financial auditors (21%), provision of dedicated audit document to data protection and cybersecurity (19%) and verification of databases that generate revenues to ensure that they are GDPR compliant (15%).

One particular intersection that is worth highlighting is that when data protection and cybersecurity are deemed critical and are the subject of a dedicated audit document, data risks are more frequently incorporated into various forms of valuation (Q18). Among the 189 respondents who answered both questions, 33% of companies that provided a dedicated audit document to data protection and cybersecurity, also incorporated data risks in their valuations, compared to 11% of companies that did not provide a dedicated audit document and incorporated data risks into valuations. Fisher’s test yields an odds ratio of 3.96 ($p = 0.0033$), with a 95% confidence interval of 1.52 to 10.15, a wide interval due to the small sample sizes.

We asked companies that had been involved in M&A (76 respondents), how they had audited the databases acquired during the due diligence process. Nearly two-thirds (63%) indicated that these had been included in the framework of the general legal/IT audit. 25% conducted a “Due Diligence” specifically concerning the value of the databases or compliance, and 18% carried out the “Due Diligence”, accompanied by the development of a detailed compliance roadmap. About 13% of respondents answered “Other”.

We asked how organisations integrate data protection, cybersecurity, and AI into their broader ESG (environmental, social and governance) strategies. By far, the most common response was the deletion of obsolete data that also reduces energy consumption of servers and digital carbon footprint (70%), an approach that may require little effort. Companies also apply more involved practices by applying ESG criteria to technology supplier selection (21%), reporting publicly on data protection practices (20%), setting up an ethics committee on use of sensitive data for data monetisation (13%), publishing data-

related KPIs (10%), and auditing algorithms for bias and discrimination (9%). The high share of “other” answers (21%) suggests that many firms may have developed other approaches suitable to their business models or may have no settled framework.

3.6 Normative statements for listed companies

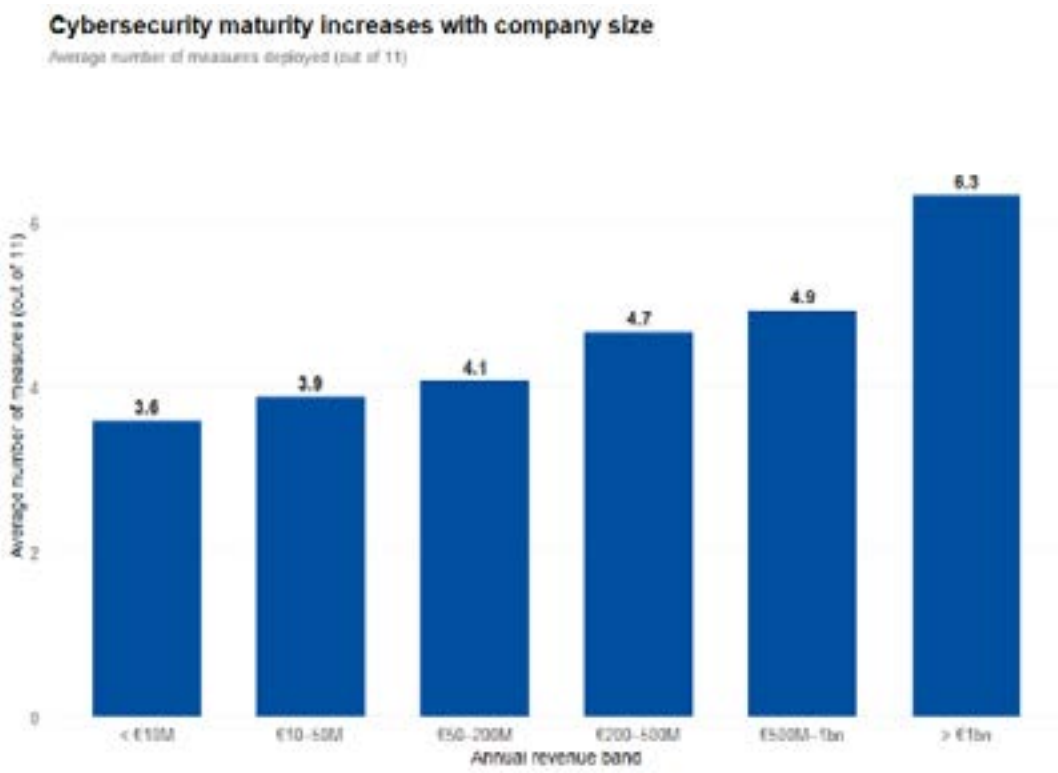
These two closing questions asked respondents to rate, on a 1–5 agreement scale, whether data protection should be reflected in a company’s market value and whether exemplary data governance should improve financing conditions. They were answered by only 19 and 18 respondents, so the results are indicative and cannot be generalised.

The agreement is moderate but clearly positive (mean 3.6/5): half of respondents agree or strongly agree that data protection ought to be reflected in market value; almost none disagree, and the rest sit on the fence. About the financing conditions, responses are noticeably more reserved (mean 3.1/5): nearly half remain neutral, and about a quarter actually disagree that exemplary governance translates into better financing terms.

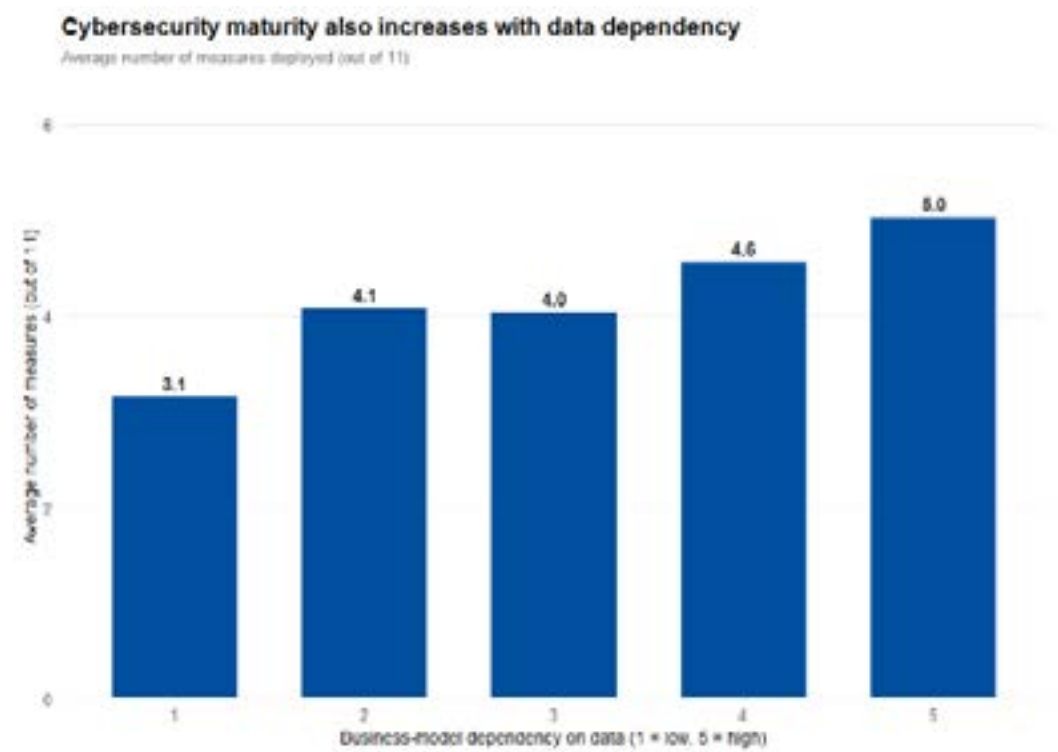
4. Cybersecurity Challenges

We have asked organisations about the actions, audit and certification

practices they have implemented in the past 5 years on data protection and cyber security. Employee training is almost universal (88.5%), closely followed by the annual update of



Graph 13 Company size and companies’ adoption of cyber security practices



Graph 14 Companies’ dependency on data and companies’ adoption of cyber security practices

internal privacy policies and employee guidelines (73%), phishing simulations (68.5%), and penetration testing on critical systems (60.5%). These four measures are adopted by a clear majority of companies, including the smallest ones, since even companies with revenue of less than €10M deploy an average of 3.6 measures out of the 11 proposed. Other practices already undertaken by companies include certifications such as ISO 27001 (27.5%), compliance audits of critical suppliers (22.5%), formal and quantified cyber reporting (21%), systematic DPIAs (37%), and GDPR certification (16%). The less used practices include automated flow mapping (11.5%) and vulnerability disclosure programs (7%).

Through cross-analysis, we measure that maturity increases significantly with size (from 3.6 measures for the smallest to 6.3 for the largest), a sign that application of these practices is likely to increase as company size, and therefore, resources, increase. The average number of deployed cybersecurity practices also increases alongside reported data dependency: from 3.1 measures (out of 11) for the least dependent companies to 5.0 for the most dependent. This link is statistically significant but of moderate strength: the Spearman correlation is 0.23 ($p = 0.001$), and a Poisson regression indicates that each additional point of dependency increases the expected number of measures by approximately 10% (IRR = 1.10; 95% CI of 1.04–1.16 with $p < 0.001$).

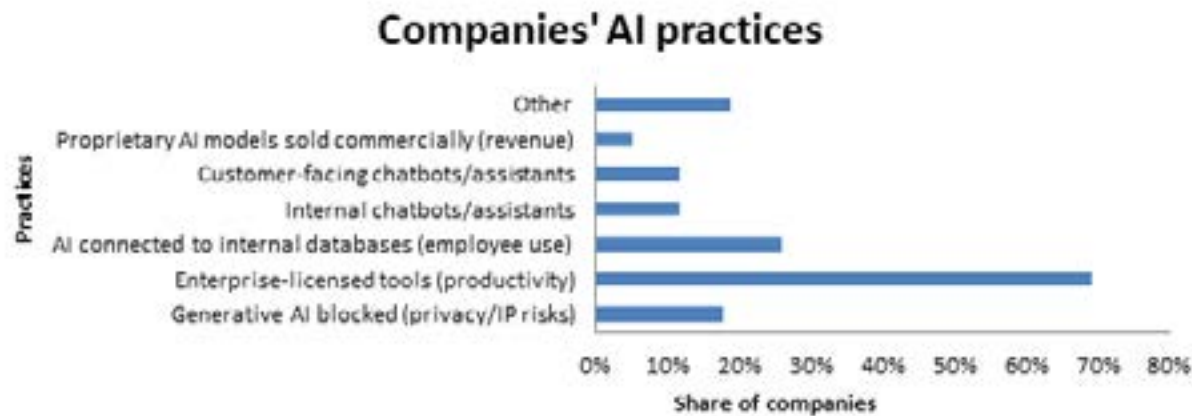
Companies are already trying to quantify the cost of a major

cyberattack: 40% rely on a rough estimate (sector averages, cyber policy), 12% calculate direct costs, and 18% go as far as integrating indirect losses, the most advanced practice. 30% perceive cyber incidents as an IT issue and do not have a process to assess the costs of a cyber incident.

According to free-text responses, several companies base their quantification on structured methods: EBIOS-RM risk analyses cross-referencing likelihood and severity, internal group models integrating direct costs, business interruptions, and potential liabilities, or estimates built “from the costs of restoring the IS, cybersecurity services, and business interruptions”. Others use the calculation of cyber insurance premiums as a risk estimation method, or its integration into the annual risk mapping reviewed at the group level. Finally, many verbatims testify to an ongoing dynamic rather than an absence: “estimate planned for the year”, “approach underway at group level: NIS2 cybersecurity action”, “system currently being built post-carve-out with the appointment of a Chief Security Officer”.

In terms of communication for listed companies (only 18 responses), the results should be read with caution. The preferred strategy consists of waiting for the technical investigation results before communicating or informing about the affected operations, rather than communicating a maximum loss figure, for example.

5. Practices around AI



Graph 15 Companies' AI practices

More than two-thirds of companies (69%) already use enterprise-licensed tools to gain productivity, AI has therefore entered daily professional life.

18% deliberately block public generative AI for confidentiality and intellectual property reasons. A quarter of respondents (26%) connect AI to their internal databases, and 11.6% deploy chatbots or assistants, whether internal or customer-facing. 5% have marketed proprietary AI models that generate revenue. The adoption of AI tools is everywhere, but the levels of integration or control in companies vary a lot.

Several companies develop their own tools “based on existing AI with data anonymization and filtering” or deploy a “customized and secure version of Copilot according to specifications” and a closed, restricted-access legal AI system. There is also formalisation of rules. There are AI charters, “chapters governing the use of AI”; pilot programs open to a few employees before widespread rollout, or the targeted blocking of

tools deemed problematic. Business use of these tools includes evaluation of claims declarations to aid expert decision-making in insurance, aid in researching and analyzing investment targets and High-Performance Computing (HPC) infrastructures made available to clients for their AI applications.

By linking the findings on AI practices with other variables, we can derive interesting insights. The number of practices adopted seems to increase with company size (in terms of revenue). Using a Poisson regression model (with a deviance/degrees-of-freedom ratio of 0.81), we find that each revenue tier (€5M–€10M, €10M–€50M, €50M–€200M, €200M–€500M, €500M–€1MD and > €1MD) is associated with an approximately 17% increase in the number of AI practices (IRR = 1.17, CI 1.08–1.27, p = 0.0001). Much like cybersecurity practices, AI adoption seems to increase as company size, and therefore, resources increase.

The number of AI practices is also positively and significantly correlated

with cybersecurity maturity (Spearman coefficient of 0.36, p < 0.001). This suggests that AI adoption goes in hand with cyber security maturity.

Companies with advanced AI applications (such as AI connected to internal databases, customer-facing chatbots, or commercialised AI models) are more likely to factor data risk into one of the financial valuations (question 16), notably 24% compared to 10% (odds ratio of 2.67, p = 0.020). In other words, the findings indicate that when AI generates value from data, companies begin to consider the associated risks in financial terms. This represents a notable link between AI usage and financial reporting.

We did not find a significant correlation between the reported value of data dependency and the number of AI practices implemented, contrary to what we found for cybersecurity measures.

6. Survey conducted with Luxembourg companies

As part of the joint study conducted by the CNPD, the CNIL and the ICO, a questionnaire was sent to selected companies based in Luxembourg to assess how data protection, cybersecurity and artificial intelligence issues are integrated into financial strategies, governance processes and, more broadly, into corporate valuation. The Luxembourg sample had a response rate of 30%.

The responding companies are predominantly large organisations. Thus, 83% report a turnover of more than 200 million euros, and two-thirds of the participants employ more than 1,000 employees. Furthermore, one-

third of the respondents are in the Finance and Insurance sectors.

Most participants report processing standard personal data (nearly 90%), whilst 50% state that they process sensitive data. By contrast, the processing of profiling or behavioural data remains more limited (around 22%). In terms of governance, the results indicate a relatively high level of maturity: 56% of organisations have implemented data performance indicators linked to financial results. 83% systematically carry out data protection impact assessments (DPIAs) and 67% have quantified cyber risk reporting in place. Conversely, only a third of companies report that they require compliance audits from their critical third-party vendors.

Despite growing maturity in data governance, the integration of data into accounting systems still appears to be in its early stages within many organisations. 28% of companies state that software and database development costs are capitalised on balance sheets as intangible assets. Conversely, nearly two-thirds of respondents either state that they do not know how data is accounted for (39%) or report that it is not subject to any identifiable accounting treatment (28%).

Regarding artificial intelligence practices, Luxembourg-based companies are already showing a significant uptake of AI tools. Nearly 78% report using AI solutions under a professional license. Furthermore, 22% connect these tools to their internal databases, 28% of the organisations surveyed have implemented chatbots for direct contact with customers, whilst 22% have chosen to block public-generative AI tools to limit risks relating to confidentiality or

intellectual property. These results suggest that artificial intelligence is gradually establishing itself as a productivity tool within organisations.

The two opinion questions in the questionnaire reveal a cautious view of the link between data protection and value creation. When asked whether data protection should be reflected in companies’ market value, the organisations surveyed expressed rather conservative views, with 89% strongly disagreeing. Similarly, the idea that exemplary data governance could lead to more favourable financing terms received moderate support (an average score of 2.7 out of 5). This perception suggests that data protection issues, for this subset of companies, are still primarily viewed through the lens of compliance and risk management, rather than as a driver of financial value creation.

Whilst the companies surveyed demonstrate a substantial level of maturity in data management and protection, the economic valuation of these assets is still in early stages. The results suggest significant potential for the development of accounting and financial practices so that data, already recognised as a governance issue, can gradually be viewed as a genuine driver of value creation.

Annex: Full Questionnaire Responses for France

Note that among the 204 forms that were submitted, 2 companies did not give any answers.

- 1. How many employees work for the company? 200 respondents
 - less than 50 employees.: 38
 - between 50 and 200 employees.: 64
 - between 200 and 1000 employees.: 56
 - between 1000 and 5000 employees.: 25
 - more than 5000 employees.: 18
- 2. What is your company’s approximate annual revenue? 200 respondents
 - less than €10M.: 32
 - between €10M and €50M.: 62
 - between €50M and €200M.: 53
 - between €200M and €500M.: 22
 - between €500M and €1bn.: 13
 - more than €1bn.: 19
- 3. In which region is your headquarters located? 197 respondents
 - Auvergne-Rhône-Alpes: 25
 - Bourgogne-Franche-Comté: 4
 - Brittany: 10
 - Centre-Val de Loire: 2
 - Corsica: 3
 - Grand Est: 11
 - Hauts-de-France: 8
 - Ile-de-France: 68

- Normandy: 7
 - Nouvelle-Aquitaine: 15
 - Occitanie: 12
 - Pays de la Loire: 15
 - Provence-Alpes-Côte d’Azur: 12
 - Martinique: 3
 - La Réunion: 2
-
- 4. If your company is part of a group, specify whether your response – 194 respondents
 - is made at the level of the group’s financial department, in order to reflect accounting consolidation and reporting issues.: 40
 - is made at the level of your company, for reasons relating to the substance of your activity or your financial structure and specify which ones.: 60
 - if you are the group DPO, check this box.: 79
 - not applicable.: 62
-
- 5. What is your company’s financial structure and level of exposure to financial markets? 198 respondents
 - stock exchange listing: shares traded on a regulated market.: 21
 - issuer of bonds or other debt securities rated by credit rating agencies.: 7
 - part of your capital is held by professional financial investors (venture capital, private equity / LBO, institutional funds).: 46
 - none of the above.: 135
-
- 6. Has your company already carried out an external growth operation in the last five years? (merger/acquisition...) 199 respondents
 - yes, as a seller: 22
 - yes, as a buyer: 73

- no: 117
-
- 7. What is your main sector of activity? 197 respondents
 - Agriculture, forestry and fishing: 3
 - Extractive industries: 1
 - Manufacturing industry: 32
 - Electricity, gas, steam and air conditioning supply: 2
 - Water supply; sewerage, waste management and remediation activities: 2
 - Construction: 4
 - Wholesale and retail trade; repair of motor vehicles and motorcycles: 20
 - Transportation and storage: 16
 - Accommodation and food service activities: 1
 - Information and communication: 14
 - Financial and insurance activities: 21
 - Real estate activities: 3
 - Professional, scientific and technical activities: 5
 - Administrative and support service activities: 15
 - Public administration: 4
 - Education: 1
 - Human health and social work activities: 2
 - Arts, entertainment and recreation: 1
 - Other service activities: 50
-
- 8. How would you evaluate your business model’s dependence on data processing? (Note: The options do not have an explicit label in the report, only a scale numbered from 1 to 5) 199 respondents
 - Option 1: 21

- Option 2: 38
 - Option 3: 51
 - Option 4: 52
 - Option 5: 37
-
- 9. How would you classify the data your organization processes? 200 respondents
 - standard B2C information (customer file, etc.): 143
 - behavior and profiling: 33
 - sensitive data: 75
 - other (detail your answer below): 53
-
- 10. What types of artificial intelligence are currently deployed within your organization, and how do they interact with your data? 198 respondents
 - generative AI tools are blocked on our networks due to risks related to data confidentiality / intellectual property.: 35
 - you use enterprise-licensed tools to optimize your internal productivity.: 137
 - you connect AI to your internal databases, exclusively reserved for use by your employees.: 51
 - we deploy/you deploy chatbots or automated assistants that interact directly with our/your clients.: 23
 - you market proprietary AI models or AI-generated analyses, which constitutes a direct source of revenue.: 10
 - other (detail your answer below): 37
-
- 11. How are data compliance and governance primarily perceived within your executive committee/board of directors? 200 respondents
 - as a regulatory and legal issue.: 166
 - as a necessary operational factor (reputation protection):. 115
 - as a strategic asset and possible competitive advantage.: 69

- other (detail your answer below): 11
-
- 12. Have you implemented specific key performance indicators (KPIs) that link data governance and financial performance? 199 respondents
 - no.: 130
 - yes, which reflect risks (number of data breaches, etc.):. 48
 - yes, customer protection / sales oriented.: 21
 - yes, we use financial KPIs related to data (detail if possible):. 12
 - other (detail your answer below): 7
-
- 13. Among the following actions, audits or certifications, which ones have been implemented within your organization over the last 5 years regarding data protection and cybersecurity? 200 respondents
 - annual update of internal privacy policies and employee guidelines.: 146
 - employee training.: 177
 - systematic execution of data protection impact assessments (DPIA):. 74
 - phishing simulations.: 137
 - penetration testing on critical systems.: 121
 - use of automated software to continuously map and classify sensitive data flows.: 23
 - continuous vulnerability disclosure programs open to external researchers.: 14
 - formal and quantified reports on cyber and data-related risks.: 42
 - certifications audited by an external body (ISO 27001...):. 55
 - compliance audits imposed on all critical third-party suppliers.: 45
 - GDPR certification.: 32
 - other (detail your answer below):. 17
-
- 14. Has your organization estimated the potential cost of a major cyberattack or data leak? 191 respondents

- you consider cyber risk primarily as an IT problem and you do not have a process to estimate the cost of a major incident for the company.: 58
- rough estimate based on industry averages or use of your cyber insurance coverage limit as a baseline estimate.: 77
- you have calculated the direct costs of an incident (restoring the IT system, etc.): 23
- you have calculated both direct costs and indirect losses (hourly cost of downtime, lost revenue, etc.): 34
- you model these risks with artificial intelligence.: 2
- other (detail your answer below): 31
- 15. How are your databases primarily reflected in your financial statements? 199 respondents
- not at all.: 76
- IT development and database software costs as an intangible asset on the balance sheet.: 55
- as an asset in goodwill (if a purchase transaction has taken place): 10
- you do not know.: 58
- other (detail your answer below): 7
- 16. To your knowledge, how are data-related risks primarily factored into your company's financial valuation, whether internally or via external players? 196 respondents
- not factored in.: 102
- taken into account during a past M&A transaction.: 16
- factored in, to your knowledge, in your financial rating.: 8
- factored into the balance sheet as an intangible asset in goodwill.: 6
- reflected by adjustments to future revenue streams or the cost of capital you use (DCF method): 2
- you do not know.: 64
- other (specify): 8

- 17. What level of detail concerning data protection is included in your annual financial reports? (if applicable) 193 respondents
- not covered.: 74
- minimal (simple statement of legal compliance): 42
- qualitative (description of policies, presence of DPO, training programs): 65
- quantitative (number of requests, investment in cybersecurity, quantified risk exposure...): 25
- other (detail your answer below): 19
- 18. To what extent do your auditors integrate data protection and compliance into their annual audit of your internal controls and financial risks? 192 respondents
- they also examine basic IT elements, but do not audit GDPR compliance.: 88
- they question the DPO/legal team to identify ongoing regulatory fines or lawsuits.: 57
- the audit firm brings in cybersecurity and IT specialists, in addition to financial auditors, to test our data infrastructure.: 41
- they verify that the databases generating your main revenues are GDPR compliant.: 29
- data protection and cybersecurity are considered critical and are the subject of a dedicated audit document.: 37
- other (detail below): 30
- 19. How does your organization concretely integrate data protection, cybersecurity and AI into its broader ESG (environmental, social and governance) strategy? 184 respondents
- you delete obsolete customer data, which also reduces the energy consumption of your servers and your digital carbon footprint.: 128
- you publish reports on your efforts to protect the data of your customers and employees.: 36
- you conduct audits of your algorithms to prevent any discrimination, bias and inequality of access to data.: 16
- you have a dedicated ethics committee that votes on sensitive data monetization projects and AI deployments.: 24
- you apply strict ESG criteria when selecting your technology providers and data brokers.: 39
- you publish a report detailing key performance indicators (KPIs) relating to user data and your

- overall level of cybersecurity.: 18
- other (detail your answer below): 39
- 20. Regarding the due diligence process: when acquiring a target company, how was the data/database compliance audited? 76 respondents
- first-level coverage within the framework of the general legal/IT audit.: 48
- within the framework of “Due Diligence”, concerning the value of databases or compliance.: 19
- within the framework of “Due Diligence” concerning the value of databases or compliance issues, with a detailed roadmap for compliance.: 14
- other (detail your answer if possible): 10
- 21. If applicable, in your previous M&A transactions, did the discovery of non-compliant data have direct financial consequences? 67 respondents
- no / no impact.: 33
- requirements for specific liability guarantee.: 13
- downward revision of the purchase price.: 3
- cancellation of a transaction.: 2
- other (detail your answer below): 20
- 22. During accounting integration, how were the acquired customer databases valued? 72 respondents
- no valuation.: 38
- they were fully integrated into goodwill (without being isolated):. 10
- they were isolated and valued as specific intangible assets on the balance sheet.: 13
- other (detail your answer below): 11*
- 23. Data protection in financial markets should be transparently reflected, for example, in company valuations or other financial reports. 19 respondents

- Option 1: 0
- Option 2: 1
- Option 3: 8
- Option 4: 7
- Option 5: 3
- 24. Exemplary data governance enables companies to obtain more favorable financing conditions (lower cost of debt / equity, improved rating, impact on WACC or weighted average cost of capital). 18 respondents
- Option 1: 2
- Option 2: 3
- Option 3: 8
- Option 4: 2
- Option 5: 3
- 25. In the event of a major cyber incident or data leak, what is your main financial communication strategy to limit short-term stock market volatility? 17 respondents
- wait for the full results of the technical investigation before communicating with the market.: 7
- communicate immediately to confirm which essential operations/data are not affected.: 6
- communicate immediately a precise figure of maximum financial losses in order to remove market uncertainty.: 2
- other (detail the answer below): 3

B. Practical example: Business combination involving a customer database (IFRS 3, IAS 38 and IAS 36)

In the context of a business combination, the interaction between IFRS 3, IAS 38 and IAS 36 can be illustrated through the acquisition of a company, whose value is primarily derived from customer data and analytics capabilities.

We assume that a company based in the EU, Company A, acquires Company B for the purchase price of EUR 20,000,000. In accordance with IFRS 3, identifiable assets and liabilities are recognised as follows³⁰:

Customer database: EUR 3,000,000

Customer relationships: EUR 2,000,000

Technology assets: EUR 1,500,000

Liabilities assumed: (EUR 2,500,000)

This results in net identifiable assets of EUR 4,000,000 and the recognition of goodwill of EUR 16,000,000³¹, reflecting expected synergies and

future economic benefits. Under IAS 38, these intangible assets are recognized separately and depreciated over their useful life. However, their economic value depends on the legal ability to use the underlying data. In this respect, as these are EU based companies, the customer database must comply with the GDPR framework. This includes, on a non-exhaustive basis, adherence to the core GDPR principles set out in Article 5, such as lawfulness, fairness, transparency, purpose limitation, data minimization, and accuracy, as well as reliance on a valid legal basis for processing under Article 6 GDPR.

The valuation of the business is performed as described in Section 3.3.6 using a discounted cash flow (DCF)³² approach, consistent with IAS 36 (value in use methodology). The main assumptions are:

Projection period: 5 years³³

30 See Table 1. Assumptions
31 See Table 2. IFRS 3 and IAS 38 - Net identifiable assets and Goodwill calculation
32 IAS 36, paragraph 30 defines value in use as the present value of future cash flows, while paragraphs 33–57 set out the principles for estimating and discounting those cash flows.
33 The projection period of five years reflects standard valuation practice and is consistent with IAS 36, which limits detailed cash flow forecasts to periods for which reliable estimates can be made. Beyond this horizon, future performance is captured through the terminal value.

Discount rate: 14%³⁴
Perpetual growth rate: 1%³⁵
Before any regulatory issue, projected cash flows increase from EUR 3,000,000 in year 1 to EUR 4,000,000 in year 5³⁶, reflecting stable development.
However, several months after the acquisition, Company A discovers that a significant portion of the customer database was collected in violation of the GDPR. Consequently, part of the data can no longer be used for commercial purposes, leading to a reduction in expected revenues.
Following the discovery of this non-compliance, projected cash flows are revised downward, ranging from EUR 2,000,000 to EUR 2,500,000 over the five-year period. The terminal value is calculated using the Gordon-Shapiro³⁷ formula:
$$TV^{38} = (CF_5 \times (1 + g)) / (r - g)$$

resulting in a value of approximately EUR 19,423,077³⁹.
Based on these revised projections, the recoverable amount is estimated at approximately EUR 17,800,000. Given that this amount is lower than the carrying amount of EUR 20,000,000, an impairment loss of approximately EUR 2,200,000⁴⁰ is recognised, in accordance with IAS 36.
This example illustrates how IFRS 3 governs the initial recognition of assets and goodwill, IAS 38 their subsequent accounting, and IAS 36 ensures that assets are not carried above their recoverable amount when non-mitigated risks affect their ability to generate future economic benefits.

34 The discount rate of 14% is based on a simplified cost of capital estimation derived from the CAPM framework. It is composed of a risk-free rate of approximately 2.5%, reflecting government bond yields, and a market risk premium of around 6%, adjusted by a sector-specific beta of about 1.5 to capture the higher volatility of digital and data-driven business models. This leads to a base cost of equity of approximately 11.5%. An additional premium of around 2.5% is then incorporated to reflect the early stage of development of the company and its operations on a very competitive market. Together, these components justify a total discount rate of approximately 14%. The numerical assumptions are illustrative and based on standard financial modelling practices, and are intended to provide a reasonable representation of market conditions rather than precise empirical estimates.
35 The perpetual growth rate of 1% reflects a conservative long-term assumption, broadly consistent with expected inflation and mature market growth in developed economies.
36 See Table 3. Discounted cash flows before discovery of a non-compliance
37 The terminal value is estimated using the Gordon-Shapiro model (Gordon, 1962), which assumes a perpetual constant growth rate. Although IAS 36 does not prescribe a specific method for estimating terminal value, this approach is widely used in practice to approximate the present value of cash flows beyond the explicit forecast period.
38 where: TV = Terminal value, CF5 = Cash flow in year 5, g = Perpetual growth rate, r = Discount rate.
39 See Table 4. Discounted cashflows after regulatory disruption
40 See Table 5. IAS 36 Impairment Calculation

Table 1. Assumptions

Assumptions	Value in EUR
Purchase price (PP)	20,000,000
Customer database FV (CD)	3,000,000
Customer Relationships (CR)	2,000,000
Technology (T)	1,500,000
Liabilities (L)	(2,500,000)
Growth rate (GR)	1%
Discount rate (DR)	14%

Table 2. IFRS 3 and IAS 38 - Net identifiable assets and Goodwill calculation

Item	Amount in EUR
Customer database (CD)	3,000,000
Customer Relationships (CR)	2,000,000
Technology (T)	1,500,000
Liabilities (L)	(2,500,000)
Net identifiable assets (NIA)= (CD)+(CR)+(T)+(L)	4,000,000
Goodwill (G) = (PP) - (NIA)	16,000,000

Table 3. Discounted cash flows before non-compliance

Year	Cash Flow in EUR	Discount Rate (DR)	Discount Factor (DF) ⁴²	Present Value (PV1) ⁴³ in EUR
1	3,000,000	14%	87.72%	2,631,578.95
2	3,200,000	14%	76.95%	2,462,296.09
3	3,500,000	14%	67.50%	2,362,400.31
4	3,700,000	14%	59.21%	2,190,697.03
5	4,000,000	14%	51.94%	2,077,474.66
Terminal Value (TV)	31,076,923.08	14%	51.94%	16,140,380.03
Total cash flow ⁴⁴				27,864,827.06

Table 4. Discounted cashflows after non-compliance

Year	Cash Flow in EUR	Discount Rate (DR)	Discount Factor (DF)	Present Value (PV2) in EUR
1	2,000,000	14%	87.72%	1,754,385.96
2	2,200,000	14%	76.95%	1,692,828.56
3	2,300,000	14%	67.50%	1,552,434.49
4	2,400,000	14%	59.21%	1,420,992.67
5	2,500,000	14%	51.94%	1,298,421.66
Terminal Value	19,423,076.92	14%	51.94%	10,087,737.52
Recoverable amount				17,806,800.86

Table 5. IAS 36 Impairment Calculation impact on assets

Item	Amount in EUR
Carrying amount (purchase price)	20,000,000.00
Recoverable amount	17,806,800.86
Impairment loss ⁴⁵	2,193,199.14

In accordance with IAS 36, impairment losses are recognised in the financial statements by reducing the carrying amount of the asset to its recoverable amount. This requirement ensures that assets are not presented in the balance sheet at amounts exceeding the economic benefits expected to be derived from them.

When goodwill is present, IAS 36 establishes a specific allocation mechanism, whereby any impairment loss is first recognised in relation to goodwill before being allocated to other assets within the same cash-generating unit (IAS 36, §§59 and 104). This reflects the fact that goodwill represents a residual and inherently uncertain component of value, often incorporating assumptions about future synergies and unidentifiable intangible assets.

From an accounting perspective, this means that the impairment loss does not lead to the recognition of a separate asset or line item. Instead, it is directly recognised as a reduction in the carrying amount of goodwill in the balance sheet. Concurrently, the impairment loss is recognised as an expense in the income statement, thereby reducing profit and, ultimately, equity value.

As a result, the financial impact of adverse events such as the reduced ability to use customer data that has not been obtained in a data protection compliant manner is primarily reflected through a decrease in goodwill recognised in the financial statements, rather than through the creation of a new accounting item.

C. Stakeholders consulted

We thank the following list of organisations for engaging in discussions with us :

- Accountancy Europe
- Association des Banques et Banquiers, Luxembourg (ABBL)
- Luxembourg Stock Exchange
- Commission de surveillance du secteur financier (Luxembourg)
- EY Avocats Paris
- Fédération bancaire française
- Financial Conduct Authority, UK
- HACA Partners Luxembourg
- Haute autorité de l'audit (H2A), France
- S&P Global Ratings
- Seyfarth Shaw LLP

And participants to the Data Protection Laboratory (6 July 2026) :

- E&Y Avocats Paris
- Commission de surveillance sur secteur financier (Data protection office)
- Fédération bancaire française
- ACO Solutions
- DUSSMAN
- Hôpital Robert Schuman, Luxembourg
- Chatbotaurus
- BGL BNP Paribas
- Stëftung Hëllef Doheem
- HACA Partners
- Seyfarth Shaw LLP
- Luxembourg Stock Exchange

