EUROPEAN COMPANY LAWYERS ASSOCIATION

A PAN-EUROPEAN STUDY

DATA-DRIVEN BUSINESS MODELS

The role of legal teams in delivering success

In partnership with:

Osborne Clarke

EUROPEAN COMPANY
LAWYERS ASSOCIATION

DATA-DRIVEN BUSINESS MODELS

The role of legal teams in delivering success

In partnership with:

Osborne Clarke

TABLE OF CONTENTS

IMPRINT

Project Cooperation:
European Company Lawyers Association (ECLA) & Osborne Clarke

Project Management:
Tobias Heining (Osborne Clarke), Marten Männis (ECLA), Julie Marshall (Osborne Clarke), Ellie Moodie (Osborne Clarke), Marcus M. Schmitt (ECLA)

Publisher:
ECLA Association Services SPRL

Managing Directors:
Dr. Michael Henning, Sönke Reimers, Marcus M. Schmitt

Authors:
Paul Anning, Henrik Bergström, Claire Bouchenard, John Buyers, Valentin de le Court, Benjamin Docquir, Grégoire Dumas, Konstantin Ewald, Jeremy Godley, Dr Johannes Graf Ballestrem, Victoria Gwynedd-Jones, Dr Sebastian Hack, Catherine Hammon, Tim Harris, Jonathan Hazlett, Felix Hilgert, Vikram Jeet Singh, Nick Johnson, Dipika Keen, Katherine Kirrage, Karima Lachgar, Nina Lazic, Elisabeth Macher, Gianluigi Marino, Samuel Matínez, Jonathan Mills, Dr Flemming Moos, Gemma Nash, Xavier Pican, Tamara Quinn, Will Robertson, Dr Tobias Rothkegel, Dr Jens Schefzig, Paul Schmitz, Adrian Schneider, Thomas Stables, Maia Steffan, Olgierd Świerzewski, Mark Taylor, Seirian Thomas, Robyn Trigg, Steven Verschuur, Dr Sabine Von Oelffen, Dr Daniel Walter, Joanne Zaaijer, Laurene Zaggia, Guohua Zhang

Advisory Council:
Mark Cockerill, Sally-Anne Hinfey PhD, Nick Johnson, Elisabeth Macher, Jonathan Marsh, Dr. Jens Schefzig, Timo Spitzer

Year of release 2022
Art Direction: Uwe Laube
Chart design: Thomas Hirt

These materials are written and provided for general information purposes only. They are not intended and should not be used as a substitute for taking legal advice. Specific legal advice should be taken before acting on any of the topics covered.

References to the law in Part 2 of this report are up to date as at 1 March 2022, unless stated otherwise.

Acknowledgments:
The European Company Lawyers Association (ECLA) sincerely thanks all participants in the study, the advisory council as well as ECLA's national member associations for their support in making this study possible.

ECLA also thanks Osborne Clarke for the great cooperation, continuous support, and highly valuable input during the entire project.

Jonathan Marsh
President
European Company Lawyers Association (ECLA)
Further information

Marcus M. Schmitt ✉
General Manager
European Company Lawyers Association (ECLA)
Further information

DEAR READER

Over the last decade, data collection and related activities have entered mainstream discussions. This has been led by the technological advancements and efficiency gains that both businesses and consumers have enjoyed, combined with the regulatory responses by governments and institutions on national and supranational levels. Data collection and utilisation has become a widespread discussion topic in all public spheres, whether it concerns democratic elections, the monetisation of consumer activities online or public health. It has become the driving force for innovation for businesses, providing new avenues previously not feasible.

Companies are realising the inherent value that systematic data collection and utilisation can bring to their organisations, and are establishing a variety of processes necessary for the improvement of their product and service lines. This has created a new approach for businesses: data-driven business models. Though the field is still in its infancy in some sectors, it is already at the core of the worldwide digital economy. Consumers and businesses alike are exposed to a diverse set of data-driven business models. The rate at which companies have started to introduce them has also accelerated in recent years, partly due to the established business benefits and partly due to the increased technical capabilities.

This has brought new legal challenges that corporate legal departments and external law firms must address for businesses. The increased regulatory scrutiny that the European Union and other jurisdictions have established highlights the importance for businesses of getting their data collection processes right from the outset. A company can only be as successful as its weakest component and if that concerns the legal advice the company operates under, it is destined to fail before it has begun.

For this purpose, Osborne Clarke and the European Company Lawyers Association (ECLA) have partnered on an international thought leadership study that explores data strategies across Europe and the related legal implications to offer an in-depth guide on how to successfully overcome these legal challenges. This guide will be available for all in-house counsel across Europe and includes potential solutions, success stories and an international benchmark for in-house counsel to determine their positioning among peers.

Nick Johnson ✉
Partner
United Kingdom
Further information

Elisabeth Macher ✉
Counsel
Germany
Further information

Dr Jens Schefzig ✉
Partner
Germany
Further information

DEAR READER

Data is the fuel of digital transformation. Be it AI, Digital Twins, Open Finance, Smart Data, Internet of Things, Industry 4.0, Web 3.0 or the Metaverse; all digital mega-trends depend on data. Across all industry sectors, companies need to find new ways to use data compliantly and sustainably in order to succeed. In a competitive global market, those who fail to adapt may find their historic business models are simply not sustainable.

A complex new regulatory framework for data is emerging. The EU had already set the gold standard for data protection with the General Data Protection Regulation, but this report barely mentions the GDPR. Data regulation goes far beyond privacy law, encompassing areas as diverse as intellectual property, criminal law, labour law, tax law, sector-specific regulation, cybersecurity and competition law. New data-focused EU laws like the Data Act, the Digital Markets Act and the Artificial Intelligence Act are now also set to come on-stream in the next few years, and against this backdrop it can be difficult to find simple legal solutions.

Legal departments have to rise to this challenge and provide actionable advice to their internal clients. However, the legal questions are often new – or at least new to the business – and the project can be fast-moving. And with data-driven business models often operating across national borders, there can be the additional challenge of reconciling advice from different jurisdictions – plus of course the need to factor in emerging regulation, to try and future-proof the business model. Some legal departments are well prepared for these challenges; others may need to move quickly to acquire the necessary skillsets, processes and relationships.

However, the challenges also create opportunity. Legal teams are uniquely well-placed to take a strong leadership role in the design, delivery and ongoing implementation of successful data-driven business models. We at Osborne Clarke have had the privilege of working alongside some outstanding in-house teams in helping develop ethical, sustainable and practical legal frameworks for using data, in defending those against challenges, and in using regulatory and legal action to drive business advantage. We are therefore excited to present this study as it provides both empirical data to assist in legal teams' strategy and budget discussions, and also legal analysis and insights to help navigate the regulatory risks and opportunities of the new data economy.

INTRODUCTION

As the European Data Strategy emphasises, data is seen by policymakers in Europe as a raw material that should be available to all.

INTRODUCTION

"... data should be available to all – whether public or private, big or small, start-up or giant. This will help society to get the most out of innovation and competition and ensure that everyone benefits from a digital dividend. This digital Europe should reflect the best of Europe – open, fair, diverse, democratic, and confident".

The European Data Strategy, 2021

As data and digital technology transform businesses, an opportunity is emerging for in-house legal teams to embed themselves at the heart of their organisations as enablers of innovation and change.

Regulation for data-driven business models is on the cusp of a major expansion. The European Union is seeking to set the global gold standard in this field, while also opening up access to data to fuel innovation and actively shape the resulting expansion of the European data ecosystem. As is so often the case with EU law, it will not only apply to EU businesses, but to any entity doing business in the EU, or with EU customers. Notwithstanding Brexit, the shifts in the EU digital landscape will have an impact on many UK businesses – and indeed, on many global businesses. Data-driven business models will need to be adapted or designed with this new legal environment in mind. The increasing complexity and scope of data and digital regulation means that legal teams will need new skills and a 'hands-on' mentality.

This study is separated into two Parts – Part 1 deals with the empirical results of a survey of in-house legal teams across key sectors in Europe, including the UK and other non-EU countries, conducted by ECLA. The aim of the study was to gain a comprehensive understanding of how companies in Europe generally approach data-driven business models and related data usage activities, and to highlight any sectoral insights that significantly diverge from the general outlook. Part 2 outlines the relevant legal issues essential for companies to understand in order to navigate successfully through the complexities that data-driven business models bring.

Data-fuelled opportunity

Our survey confirms that all sectors surveyed are embracing data-driven business models and using them in a wide variety of ways. 87,4% of responding companies offer, or plan to offer data-driven products and services. That includes a variety of services offered by these companies, including purely data-driven services, which are offered by 79% of companies that offer data-driven products and services, and hybrid service bundles, which are offered by 70% of these companies.

34,7% of those offering or planning to offer hybrid service bundles see data as enabling them to offer new products/services. This is an important finding, highlighting that there is a mixture of outcomes following the adoption of data-driven business models. Sometimes existing products and services can be enhanced or delivered in new ways. Other times, completely new offerings and even markets emerge from data-driven innovation.

In Part 2 of this report, we consider various examples of data-driven business models, from adding connectivity to existing products to make them 'smart' to innovations in the financial services markets from open banking and open finance more generally. We also review two applications of digital twins (an advanced form of Internet of Things technology), including industrial software systems and the transformation from selling an asset to providing that asset 'as a Service' and their application in the built environment, as part of the technology for smart buildings and cities. These examples bear strong witness to the value that can be generated by harnessing the power in data.

More access to more data

Our survey found that data is collected by respondents from both internal and external sources. Unsurprisingly, customer data is the most common external source, collected by 82,2% of respondents with data-driven products and services. However 33,1% of respondents cited access to data as an obstacle to implementing these offerings. In Part 2 we review the legal issues around the development of a dataset, including its creation (whether by acquisition or organically) and the pooling of different datasets.

> ... data is seen by policymakers in Europe as a raw material that should be available to all.

As the European Data Strategy emphasises, data is seen by policymakers in Europe as a raw material that should be available to all. Apart from personal data, it has generally been down to corporate policy and contractual arrangements as to whether data is shared or not. The indication from the survey results is that businesses tend to use that freedom to restrict data sharing. The survey found stronger support for a closed, proprietary approach to data than an open, collaborative one in all sectors except for the Technology, Media, and Communications sector, where there was stronger positive support for an open approach (32,1%) than a proprietary one (22,6%), and the Financial Services and Retail & Consumer Goods sectors, where sup-

Definition: **data-driven business model**

Data-driven Business Models combine two central trends of the digital age:

- the growing importance of data; and
- the increasing focus on the business model as the central design level.

The data-driven business model concept lays out the benefits for users of data-based services and introduces methods for managing (promoting, pricing, sale, and delivery) of such products (Bange and Derwisch, 2016). There are generally three main types of data-driven business models:

- data users;
- data suppliers; and
- data facilitators.

Data users focus on the actual use of available data resources, either on internal value creation (e.g. the use of data or data analysis results for the continuous improvement of processes) and/or on external value creation (e.g. data-driven development of new or existing innovative products).

The focus of data suppliers and data facilitators is on supporting data users by supplying them with relevant data or data products (suppliers) or by offering supporting data services and data infrastructure solutions (facilitators). It should be noted that the three data-driven business model types introduced often overlap. (Strahringer and Wiener, 2021). This report considers both data-driven products and services that are supplied to customers and data-driven business models where data is used for internal business purposes.

port was balanced between the two, at 21,4% and 15,4% for the two industries, respectively. Moreover, the survey indicated that data access does not create a significant challenge with only 13% responding that they had been involved in disputes regarding data rights or data access. In Part 2, we review the difficulties that can arise around securing access to data. Absent specific contractual rights, the legal bases on which to claim an entitlement to access to data held by a third party are, at present, mainly drawn from competition law or sector-specific regulation. The proposed new rights under the EU's Data Act will significantly alter this landscape.

New legislation at EU level proposes to shake up access to data, including creating extensive new rights to access data for the entity whose use of a product or service has generated data held by the provider of that product or service. The portability of data from one platform to another will be boosted. Further new EU legislation proposes new regulatory frameworks for the data ecosystem, including for "data intermediaries" that supply and facilitate the availability of data. Of course, the interface with existing rights, particularly trade secrets and privacy, will need to be carefully crafted – data is not always protected by intellectual property rights but where it is, those existing rights need to be integrated into the approach of the new regulatory proposals (an issue that is explored in Part 2). The EU is, moreover, overhauling existing digital regulation that was created for a much earlier phase of the internet, as well as creating an entirely new framework for ensuring effective competition in certain digital markets. It is also developing "European Data Spaces" to boost the availability of data in particular sectors, the first of which being healthcare data.

Part 2 considers the objectives and provisions across all of this legislative change, covering the likely impact on data-driven business models of the Data Act, the Data Governance Act, the Digital Markets Act and the Digital Services Act

Sector specifics: **Energy and Utilities**

The Energy & Utilities (E&U) sector is undergoing seismic change driven by conflict, climate change, and the decarbonisation imperative. The replacement of fossil-fuel technology with renewable generation assets is introducing complexity into the fundamentals of this sector – the balancing of energy supply with demand. In this context, the finding that 23,8% of E&U respondents have no plans to introduce data-driven products and services was surprising, as was the result that only 11,1% of E&U respondents that offer purely data-driven services aim to use data to improve decision-making capabilities. Moreover, respondents did not expect their business's use of artificial intelligence to increase. The proportion of businesses taking a proprietary approach to data was the highest of any sector at 46,7%, with only 10% taking an open collaborative approach. The coming changes to EU data regulation, which are creating extensive data access rights, may necessitate a shift in expectations.

A further surprising result was the lower level of concern about legal and regulatory obstacles to data-driven business models relative to the responses from other sectors. This is a heavily regulated sector and there is a widespread view that regulation in Europe has not kept pace with digitalisation-powered change, and is not well suited to current practices. Generally speaking, the responses for this sector indicated a lack of familiarity with the legal issues around data-driven business models, and weak responses around data strategy and governance. This is reinforced by the fact that 36,4% of E&U respondents consider that there is a lack of internal experience and skillsets required for implementing data-driven business models in the sector.

The results overall can be interpreted as reflecting – in line with many sectors that are undergoing extensive transformation – the range of engagement with digital technology in this traditional sector with many long-standing incumbents facing deep changes to their industry.

(all of which, at the time of writing, are at different points in the EU's legislative process and not yet law). Part 2 also considers the data aspects of the proposed new regulation for artificial intelligence (AI). Many of these initiatives have parallels in the UK, although they are typically moving at a different pace and with different areas of emphasis.

Data is a policy focus in many other jurisdictions, which businesses with international sales into those countries will also need to monitor. In Part 2 we consider developments in India, which is moving towards a framework modelled on the General Data Protection Regulation (GDPR); China, where the final three-pillar framework encompasses data protection and cybersecurity; and the USA, where data privacy is fragmented but fast-evolving, and already more protective of consumers than its reputation.

...a more open data ecosystem will facilitate innovation...

The policymakers' intention, particularly in European jurisdictions, is that a more open data ecosystem will facilitate innovation, ensure competitive, contestable markets, boost the development of AI, and power increased productivity. There is no doubt that once these new regulatory frameworks for data and data-driven markets are in place, businesses will no longer have the same unfettered freedom to decide whether and how to commercialise or share their data. But enhanced obligations and restrictions are not the only consequence of the new regime – it will also create extensive new legal rights and open up new data-driven opportunities.

Sector specifics: **Financial Services**

Unsurprisingly, given the nature of the industry, 60,4% of respondents from the Financial Services (FS) sector already offer data-driven products/services, and a further 30,2% plan to introduce them. That said, the focus for most respondents who offer hybrid service bundles is on improving existing offerings (69,7%), with a much smaller number focused on innovating with new products or services (24,2%). However, this low figure should certainly not be read as reflecting a lack of disruptive innovation in this sector as a whole, in the context of the growth of open banking and open finance initiatives (most advanced in the UK) and the thriving field of fintech.

There are a number of indicators in the survey results that businesses in the financial services sector generally have a more advanced understanding of data-driven business models than many other sectors, with positive responses above the cross-sector averages in areas including board-level expertise on data-driven business models (39,3%), data strategy (42,9%), consideration of the ethical and reputational angles of the use of data (53,6%), and the expected increased use of artificial intelligence (50%).

However, the picture regarding legal and regulatory frameworks in this heavily regulated sector is more complex. Legal/regulatory obstacles dominated responses, having been identified by 76,7% of FS respondents as a challenge to implementing data-driven business models. Just 3,5% of responding companies consider the current legal/regulatory framework in Europe to be well-structured; only 7,4% consider it to be clearly understandable; and only 3,7% consider it to be supportive of data-driven business models – the lowest proportions for these statements across the surveyed industries.

The juxtaposition of results that suggest both a confident and mature understanding of data-driven business models but also significant dissatisfaction with the legal and regulatory framework may reflect the extent of the disruption in this sector. This disruption comes in the form of initiatives based on novel legal frameworks, such as open banking, and new technologies, such as blockchain and cryptocurrency, that are not yet subject to bespoke regulation. In the latter situation, businesses must carefully consider whether and how existing financial regulation frameworks apply to these new, fundamentally different decentralised and distributed technologies – something that can be difficult and contentious.

Legal and regulatory challenges

A core objective of the survey was to understand the position of corporate legal departments amid this widespread, data-fuelled activity in their businesses. The picture painted by the survey reflects the disruptive impact of transformation strategies and the extent of adaptation that is needed to adopt what can be fundamentally different business models compared with what went before.

Concerns about dealing with the legal and regulatory landscape for data-driven business models are widespread. The most commonly cited obstacle to implementing data-driven business models was legal and regulatory challenges at 67,3% of respondents. Even before the coming reforms to data and digital regulation, 68,1% of participating lawyers consider the European legal/regulatory framework to be too complex and 63,4% find it confusing. This lack of clarity matters because the legal and regulatory context for data-driven business models is fundamental to their viability. Only 11,4% of respondents considered that their business is well prepared for the legal challenges of data-driven business models, and only 25,7% reported board-level expertise around such models.

The next-most cited obstacle to implementing data-driven business models was cybersecurity (38,2% of respondents). This issue typically increases in scope and significance with digitalisation and greater use of data flows, and as

Sector specifics: **Life Sciences & Healthcare**

Results for the Life Sciences and Healthcare (LSH) sector indicate a more advanced state of the market as regards data-driven business models. 57,7% of LSH companies responded that they already offer data-driven products/services, and 24,5% plan to offer them soon. Innovation is clearly a focus, with 51,9% of responding companies that offer hybrid service bundles using or planning to use data to provide novel products or services – the highest proportion among the surveyed industries. Unsurprisingly for a sector focused on medicine and human health, 91,3% of companies that currently offer or plan to offer data-driven products/services use customer-provided datasets. Purchased databases are much more widely used in this sector than others, with 60,9% of companies reporting this as an external source – almost double the general cross-sector result. Similarly, the score of 56,7% for respondents who have been involved in the strategic acquisition of data is the highest result in any sector.

Nevertheless, lack of access to external data was cited as an obstacle to the development of data-driven business models by 51,5% of LSH respondents. For EU companies, this may ease not only due to the cross-sector proposals to enhance access to data, but also due to the EU's initiative to open up access to health data through the ground-breaking proposals for a European Health Data Space.

The results for this sector are also notable for the contrast between the strong results around innovation and activity, and concern about obstacles. Generally speaking, more LSH respondents seem to struggle with more obstacles than other sectors, including legal and regulatory challenges (75,8%), lack of internal experience and skills (57,6%), access to external data (51,5%), and cybersecurity risks (48,5%). LSH is the only sector where sector-specific challenges were a significant concern (45,5%). The reasons for these results are unclear, but may reflect the fact that LSH is a regulated sector, and that much of the data used concerns the health of individuals, which receives additional protection under the GDPR as "special category" data.

Consistent with those findings, only 10% of LSH respondents felt their company was well prepared for the challenges of data-driven business models.

supply chains take on a digital dimension. There are legal obligations and responsibilities in relation to systems and data security that need to be understood and managed, so this is not just an issue for the IT department. Cyber-related concerns are a focus in Part 2 where we offer an illustrative example of how to respond to a ransomware attack (preparedness and careful management are key).

> ...businesses need to be developing an understanding of the new laws...

Given the extent of change to data and digital regulation that is on the horizon, businesses need to be developing an understanding of the new laws that are likely to impact on them, and the associated timeframes (taking note, moreover, of the impact of developments outside Europe). As well as monitoring for compliance risks, legal teams can take a pro-active lead by highlighting the new rights and protections that will be created, ensuring that there is awareness in the business of when those new rights are in play, and exercising them where necessary to protect their business's interests.

Sector specifics: **Real Estate & Infrastructure**

Most of the companies surveyed in the Real Estate and Infrastructure sector (REI) already offer data-driven products and services (70,4%) and 14,8% are planning to introduce such products and services. The results are surprising[1], placing the REI sector, perceived as traditional, second to the Technology, Media and Communications sector. It is, however, reflective of the nascent digitalisation we are seeing at all levels, from data-driven construction techniques to Internet of Things-based digital tools for building and asset management, to apps and digital interfaces for tenants, occupiers, and the casual users of the built environment. We are also seeing interest in the further development and deployment of tech and data to support and improve the trading of real estate assets – AI, tokenisation and blockchain are all under consideration – as well as solutions to improve connectivity, sustainability, accessibility, and social impact across the built environment. It is encouraging to see this level of tech and data sophistication across the sector.

In terms of the challenges that in-house legal teams experience when implementing data-driven business models, the results were far more balanced than in other sectors where legal and regulatory constraints tend to dominate. While this is still the primary concern of REI respondents at 55%, there was a spread of only 15 percentage points between the scores for the first and fifth-ranked obstacles, compared with a spread of 35 percentage points for the cross-sector results. This reduced focus on legal and regulatory obstacles for REI respondents may reflect the fact that this is not a regulated sector and that a significant proportion of the data collected and used in this sector is anonymised, non-personal data.

But change is coming. The 29,4% of REI respondents who consider the regulatory framework for data-driven business models to be stable may need to reconsider. In particular, the data access rights in the EU's proposed Data Act could have a significant impact on this sector. Given the disruption that is likely in relation to opening up access to data, a more strategic approach to the use of data may be needed by REI businesses. Results from this sector around data strategy and data governance were among the weakest: a stronger top-down approach may be called for going forward, monitoring how regulation will impact on the sector's current understanding of the value of data and how to protect it.

1 There was a smaller number of responses from REI businesses compared with other sectors (see Methodology and acknowledgements), which may have impacted on these results.

Data strategy and governance

As data becomes an increasingly valuable asset for a business and starts to underpin significant proportions of its activity, decision-making, products and services, a data strategy becomes all the more important.

However, only around 36% of respondents answered positively that they have a data strategy. Only 47% think about the ethical and reputational angles of their use of data, and only 40,2% use contract templates that include provisions dealing with data that go beyond data protection compliance. The survey results paint a picture that, although many of the component parts of a corporate data strategy and data governance policies may be in place, they are often not developed as a coherent whole. Tellingly, only 16,1% of respondents considered that the legal team had implemented the business's data strategy (of those that had one). The absence of a strategic approach is reinforced by the statistic that only 25,7% of respondents have board-level expertise around data-driven business models.

Corporate data strategy and data governance are areas where a legal department can undoubtedly add significant value to an organisation by bringing together the various relevant stakeholders to develop these policies to sit

Sector specifics: **Retail & Consumer Goods**

The Retail and Consumer Goods (R&C) sector's results show only 48,7% of R&C respondents already offer data-driven products/services (one of two surveyed industries that does not reach the 50% threshold).

For external data sources, customer-provided datasets are the most popular option, at 81,6%. This is not a surprising result, given that the consumer-facing part of this sector is rich in customer data from, for example, loyalty programmes, till receipts or online retail sales. Freely available public datasets are used by 42,1% of R&C respondents, and the sector makes above-average use of data from social media and other applications via APIs, at 31,6%. The latter may reflect the extensive use of social media for brand marketing in this sector.

60,4% of R&C companies report legal and regulatory obstacles as a point of concern. Many of the other most-cited concerns are internal facing, including poor integration of data-driven business models into internal company structures and processes (45,8%), lack of internal experience and skills (41,7%), internal data utilisation (29,2%), and lack of internal resources (27,1%). Cybersecurity risks appear to be much less of a concern in this sector than in others (27,1%), but are still on their agenda to explore, given the amount of valuable customer data that may be held by retail businesses, particularly those using online sales channels.

There are a number of further signs in this sector that the in-house legal teams are less involved in the business's data-driven business models than in others, with a higher proportion of "unsure" responses in relation to many of the survey questions from this sector compared with others. 38,5% of R&C respondents did not feel confident about their business's readiness for the legal challenges of digital transformation. Given the importance of digital interactions in this sector – not least for e-commerce and digital sales channels – the apparent unfamiliarity of many R&C legal counsel with how their companies are using data-driven business models is somewhat unexpected. This may indicate that such an understanding sits within pockets, rather than being disseminated throughout the organisation.

This is, of course, not a universal finding. Many in-house legal teams will have been closely involved in data-centric and digital initiatives for their business. But for those who are less familiar, the many changes on the horizon for digital and data regulation create an opportunity to get closer to the data-driven business models used in their companies. The new laws will create rights as well as obligations, so an awareness of where the business sits within these new frameworks will ensure that its interests can be fully protected and exercised.

across the whole business, rather than being considered an issue for the IT team. In particular, a coherent and considered approach, endorsed and adopted at board-level, can shift the culture of an organisation to ensure that all in the business understand and protect the value of data. Moreover, as we explore in Part 2, cybersecurity governance has been escalated by digitalisation from being an issue that can be left to the Chief Information Security Officer and the IT department, to being a matter for the board as a whole.

Finally, data strategy and governance can form part of Environmental, Social and Governance policies, intersecting with sustainability strategy and objectives. The potential impact of data-driven business models on a business's carbon footprint should not be overlooked and may trigger further compliance risks, or energy-saving opportunities (explored further in Part 2). Data strategy needs to be dovetailed with net-zero strategy; tech procurement processes in support of data-driven business models can be greened; and new green-focused laws on the design and provision of technology need to be monitored.

Sector specifics: **Technology, Media & Communications**

As would be expected for this data and digital technology-focused sector, a significant majority of companies in the Technology, Media & Communications (TMC) sector industry offer (87%) or plan to offer (10,9%) data-driven products or services. The share of companies not planning on doing so is negligible. The TMC sector respondents gave the strongest answers for many questions in the survey, again unsurprisingly.

In relation to the development of data-driven products/services, TMC sector responses indicate the most extensive in-house tech development skills, with 83,9% of respondents selecting this answer; and 32,1% reporting using group companies that operate at arm's length. This result is once again to be expected – although conversely 33,9% of TMC respondents report a lack of internal experience and skills as an obstacle.

Regarding the biggest obstacles when implementing data-driven business models, legal and regulatory obstacles (80,4%) and cybersecurity risks (51,8%) were the most commonly cited obstacles by TMC respondents. Notably, 33,9% of TMC respondents are concerned about uncertainties regarding the general legitimacy of the underlying business model. The focus on this issue may reflect the fact that innovative and transformative tech will often first be developed in this sector, which must grapple with the question of whether and how existing regulation relates to it.

Perhaps surprisingly for a sector that includes many of the pioneers in understanding the revenue-generating potential of data, responses around data strategy and governance were not necessarily as strong as might have been expected. Only 39,6% of respondents already have a data strategy in place (second to the FS sector). Only 47,2% think about the ethical and reputational angles of the use of data. And only 43,4% reported having board-level expertise on data-driven business models – with this latter result particularly unexpected.

Unsurprisingly, the survey results indicate strong familiarity in the TMC sector with data-driven business models, although there is also evidence of scope to strengthen data strategy and governance. The regulatory changes for this sector under the European Digital Strategy will fundamentally shift it from being unregulated, in the sense of being subject only to universal legal regimes, to being subject in some areas to policy-driven sector-specific regulation that is actively intended to shape these markets going forward. The negligible level of concern in the TMC sector about sector-specific obstacles may well change in the coming years – although, as is always the case, new obligations for some create new opportunities for others. The enduring characteristics in this sector of rapid change and constant innovation will undoubtedly persist.

Sector specifics: **Transport & Automotive**

52,2% of responding companies in the Transport & Automotive sector (T&A) already offer data-driven products and services. 40,3% plan to do so soon, the highest result for an intended launch among the surveyed industries. These results reflect the changing landscape within the sector. Vehicles are shifting to becoming connected and electric-powered, with longer term research into autonomy. Meanwhile transport services have seen extensive disruption from digitalisation with the emergence of digital platforms to support mobility, as well as the development of integrated Mobility as a Service offerings across public and private transport options.

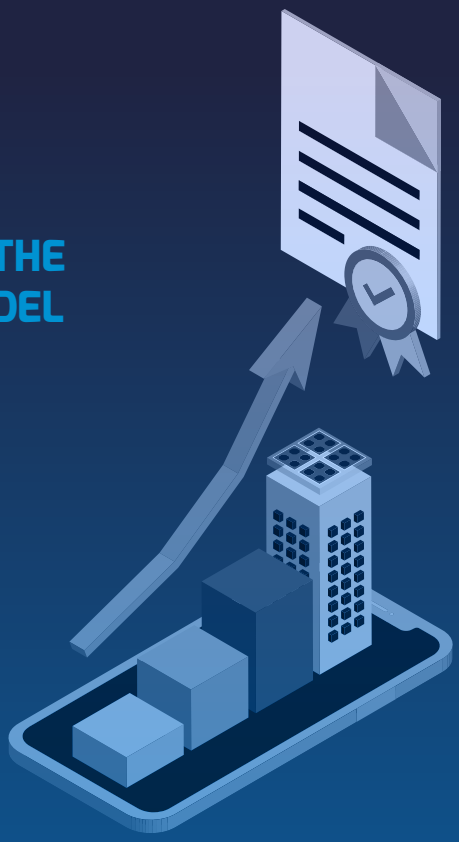
Real time data plays a significant role within the sector, with 52,4% of respondents agreeing that it is important. Again, this may reflect the growing value of real-time data flows from connected vehicles, as well as the real-time data that powers many of the innovative services in this sector, such as the location on streets of scooters, bikes or cars for public hire.

In terms of obstacles that T&A legal departments face when implementing data-driven business models, 67,4% identified legal and regulatory challenges and 46,5% selected cybersecurity risks. The latter is a high score, second only to the TMC and Life Sciences sectors. It may reflect the focus on safety in this sector – historically this has been around the safety of vehicles, but as they move to being integrated with digital software and connectivity, cybersecurity becomes a significant aspect of operating safety.

Concerning the current legal and regulatory framework for data-driven business models, although the majority of T&A respondents (as in all sectors) have difficulties with the framework, 21,2% consider it to be supportive of these new business models, and 37,5% consider it to be stable. These results may reflect the fact that there is extensive product regulation in this sector, including health and safety standards and obligations and provisions on data sharing, as well as close policy attention to liability to ensure that victims of harm from vehicles have recourse to remedies. Moreover, lawmakers in many countries have started to consider the impact of autonomous vehicles on the liability regime. So overall, this is a sector where policymakers are actively engaged and clearly future-focused. Conversely, only 14,6% of T&A respondents consider their company to be well prepared for the legal challenges of data-driven business models, so there is clearly awareness of the impending legal and regulatory consequences of data-driven transformation in this sector.

RECOMMENDATIONS

HOW THE LEGAL DEPARTMENT CAN DRIVE THE SUCCESS OF A DATA-DRIVEN BUSINESS MODEL



The increasing breadth and scope of digital and data regulation (and the trend towards ever-higher fines and stronger enforcement powers) means that the legal context for data-driven business models cannot be an afterthought.

RECOMMENDATIONS

How the legal department can drive the success of a data-driven business model

Lawyers for data-driven business models need a particular mindset. They need to be close to the technology, but also aware of the shifting regulatory landscape for digital products, services, and platforms. They need to be pragmatic and ready to immerse themselves in a data-centric project, taking their place at the heart of the business team to deliver compliance by design.

In private practice, we see new future-focused specialisations developing to support clients with data-driven business models. There is already an emerging field of digital regulation lawyers – bringing together consumer law, media and content law, advertising law, cybersecurity, competition law and aspects of financial regulation. That convergence will soon be joined by new areas of EU digital regulation, encompassing new technology such as AI, but also including a vast expansion of data regulation to deliver a new framework for the European data ecosystem. The challenges are manifold and legal departments and outside counsel must evolve quickly to ensure that they have the skillsets and resources to overcome them.

Although our survey has identified varying levels of familiarity, readiness and confidence across different sectors for the challenge of data-driven business models, it is also clear that there are opportunities for in-house counsel amid all the disruption.

How can a business's legal team proactively contribute to delivering successful data-driven business models? We propose the following areas of focus:

1. Shaping data strategy and governance

As understanding of the potential value of data grows, it also becomes important to ensure that this value is not allowed to leach out of the business. There is scope across all sectors for a more consistent and strategic approach to data. The legal department can be at the heart of such projects, bringing together relevant stakeholders to ensure that a data strategy has not only been developed, but is applied consistently across the business and embedded in commercial relationships.

Data strategy can be thought of as the practical basis on which the business approaches data. It might include negotiating positions around data in commercial deals and consideration of how business decisions will impact on the business's ability to exploit data. It might map out the business's approach as to whether data should be open and available, or closed and proprietary. It might state the business's risk appetite around data. Supply chain issues might be considered, including how cybersecurity in the supply chain should be managed, and any negotiating red lines in this respect.

Data governance covers a higher order of issues concerning the overall direction and priorities of the business, and the intersection of data-related policies with other ones. It might include ensuring sufficient and appropriate board-level expertise to

oversee the business's data strategy and data-centric projects. Responsibility for taking particular categories of decisions about data might be mapped out. The business's approach to data ethics and issues such as transparency of data-driven algorithms might be included, potentially with procedures to ensure they are considered for relevant projects. Integration of the data strategy with corporate values and with Environmental, Social and Governance (ESG) policies might also be needed.

Board-endorsed, top-down data strategy and governance policies can help to drive the development of data consciousness through an organisation, so that thinking about the use of data, the protection of its value, and creativity around its applications become embedded across the business.

2. Rethinking the role of the legal team

Legal teams may need to rethink their role, structure, and skills to be at the heart of data-driven business models. While traditionally a legal department might aim simply to manage legal risk, it will now regularly need to be at the heart of the teams that are designing data-driven business models. The legal challenges connected with regulatory compliance can be complex and fundamental: they must be taken into account from the very start.

As a result, the legal team will need to be as agile as the rest of the business. As part of the development team, the legal team should be involved even before there is a fully formed vision of exactly what the final product will be. Through close collaboration and an iterative process of improvement, compliant data-driven business models will be shaped.

A 'compliance by design' approach for new products and services requires not only a 'hands-on' mentality from the legal team, but also understanding from the business that legal compliance and risk management can be challenging. Increased budget may be needed to ensure that the legal team includes the necessary skillsets and capacity to support data-driven initiatives in a proactive way, embedded within business teams. Some legal teams are even being given a greater litigation budget to empower them to explore possibilities and be more creative and innovative.

3. A strategic framing for compliance

The increasing breadth and scope of digital and data regulation (and the trend towards ever-higher fines and stronger enforcement powers) means that the legal context for data-driven business models cannot be an afterthought. It will be increasingly the case for businesses selling into the EU that regulatory compliance must be one of the core drivers for their business model.

Many businesses take this burden and turn it into a virtue. In the TMC sector, for example, some businesses are known for their 'privacy first' approach and make it part of how they differentiate themselves from their competitors. We have seen in the Financial Services sector how some banks treat open banking as a compliance issue, while others leverage the data-sharing rights to create new offerings to win their competitors' customers.

Moreover, taking a positive approach to compliance can help to feed a compliance culture within an organisation – staff can see that it makes a positive contribution to the business and drives revenues, and is much more than a box-ticking exercise.

4. Leveraging new opportunities

Finally, the new legislative frameworks around data and data-driven business models not only create new obligations and burdens, but also new opportunities and legal rights. Some rights will be expressly stated in the text of the new legislation (perhaps a right to complain to a regulator about alleged infringements by a third party), while others may be inferred from general litigation principles or constitutional rights.

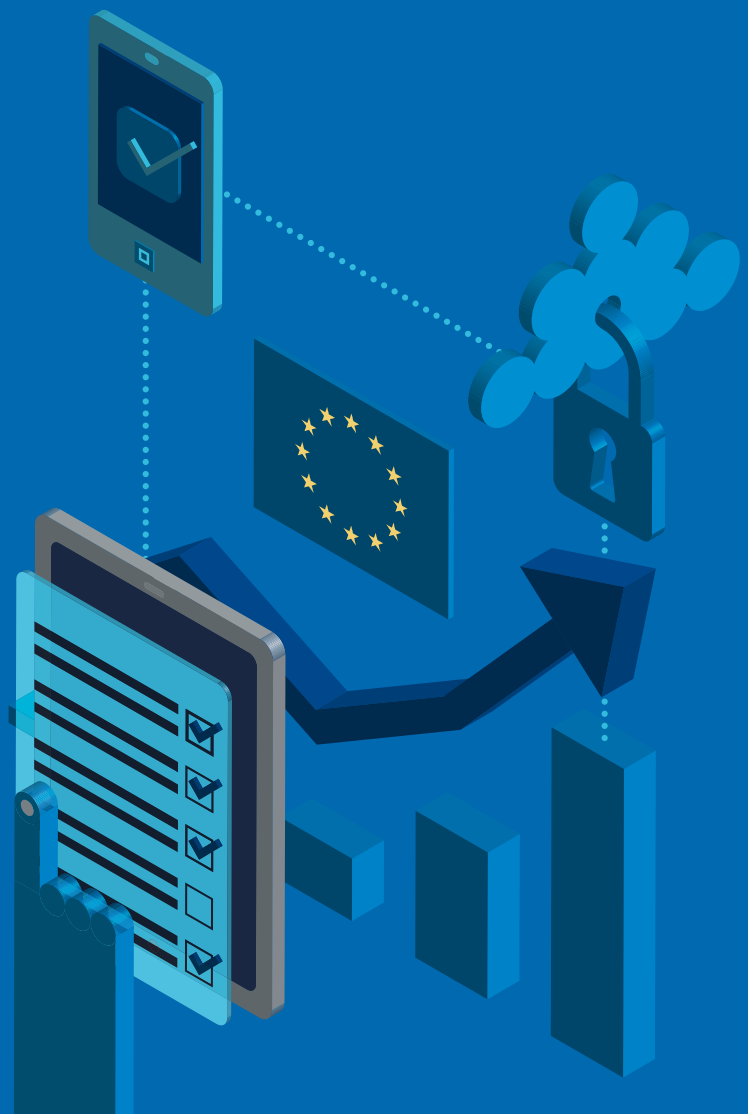
Either way, the legal team can naturally take the lead within an organisation to map out the new rights that are created by the new legislation, and start to build understanding of when they might be engaged. In-house counsel will then be on the front foot in terms of protecting the interests of the business. The positive consequences of being active exercisers of these rights could potentially include greater access to data, compensation if the business suffers harm from another's infringement, and fairer competition.

These steps will ensure that the legal team is embedded within the structures for innovation for their organisation and can play an integral part not only in managing risk and ensuring compliance, but also in securing access to the raw materials for data-driven business models, delivering their success and protecting the business's interests.

1

HOW ARE BUSINESSES ACROSS EUROPE USING DATA-DRIVEN BUSINESS MODELS?

ECLA'S PAN-EUROPEAN SURVEY



CROSS-SECTOR SUMMARY

As data becomes an increasingly valuable asset for a business, and starts to underpin significant proportions of its activity, decision-making, products and services, a data strategy becomes all the more important.

CROSS-SECTOR RESULTS

Some parts of the modern economy were born digital, some are transforming, and some have new subsectors developing around tech and data-driven opportunities.

The survey provides some incredibly valuable insights into how corporate legal departments in European companies view the growing transformative opportunities and disruptive challenges that data and data-driven business models can bring. Overall, the analysis paints a picture of all sectors being well underway in introducing data to their core business, and that most companies recognise the benefits that it brings. However, there is inevitable unevenness both between and within sectors. Some parts of the modern economy were born digital, some are transforming, and some have new subsectors developing around tech and data-driven opportunities. Different sectors experience different challenges in implementing their data-driven business models. As always, market context is key and the survey results confirm the need for a sectoral approach in establishing an effective path to the desired result.

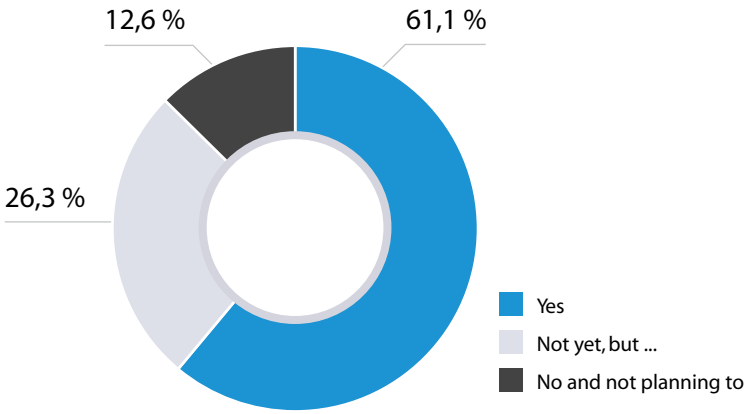
The value of data-driven business models

Some 61,1% of responding companies across Europe already offer data-driven products/services in some form.

Some 61,1% of responding companies across Europe already offer data-driven products/services in some form. 26,3% have plans to introduce this model to their businesses soon. Of these businesses combined, only 31% consider their data-related activity to be auxilliary. These results confirm that businesses already see the benefit in data-driven business models, and in harnessing the inherent value of data.

A powerful objective of digital transformation can be to enable new ways to achieve existing activities or tasks. This may involve creating hybrid products and services where data-driven services are added to existing products and services, which 60,4% of respondents using or planning hybrid service bundles were intending to do – for example, adding connectivity and data flows to existing physical products. Data can also be used to power solutions that improve activities or processes (which 76,5% of respondents using purely data-driven services offer or plan to offer), or to enable data-driven decision making (which 32,9% of respondents that offer purely data-driven services currently offer or plan to offer). Digital twins are a powerful example of the transformation that sophisticated data-driven business models can deliver, whether in relation to optimising processes or supplying assets, or for management of and operations in the built environment, even whole cities.

Does your company offer data-driven products/services?*



* Multiple choice question, results indexed to 100 %

Shifting to a data-driven business model can entail significant changes to supply chains, requiring the transforming company to enter new business relationships and to put digital infrastructure in place at a sufficient scale to support the new products and services. Those new relationships can include collaborations around both development of the new products and services, and their distribution. The majority of respondents (67,5%) undertake some development in-house, but there is also extensive interaction with third parties, whether for joint commercial development (42,5%), outsourcing to a third party (28,3%), outsourcing to an arm's length group company (24,5%) or with universities and public research institutions (18,9%).

34,7% of respondents see hybrid data bundles as enabling them to offer new products/services.

34,7% of respondents see hybrid data bundles as enabling them to offer new products/services. This is a significant finding. Digital transformation can open up entirely new opportunities and new revenue streams, potentially facilitating the emergence of wholly new markets. The creation of new products and services in the financial services markets that have been enabled by 'open banking' data flows is a strong recent example.

Accessing data

33,1% of respondents cited access to external data as one of the five main obstacles to their use of data-driven business models.

The survey confirms that datasets are being drawn from a wide variety of sources. 70,3% of respondents generate and collect data from their own operations for pre-defined purposes. 63,7% also repurpose existing data and put it to a use other than that for which it was originally collected. As regards data from external sources, data collected from customers is, unsurprisingly the most widespread option used by 82,2% of companies. Other commonly used options for procuring data include purchased datasets (32,2%), data that flows from contractual or legal obligations (32,2%) or freely available public data (36%). Data from web-scraping or

from social media or API data flows is also used as a source, albeit to a lesser extent, by 16,4% and 19,2% of respondents respectively. Nevertheless, 33,1% of respondents cited access to external data as one of the five main obstacles to their use of data-driven business models. Real time data is important for most businesses with 55.7% confirming that it plays a relevant role for their business.

Opening more data to be available to more businesses is a particular focus of policymakers, because of the recognition that data is a key factor for production. This is particularly the case for machine learning and deep learning forms of artificial intelligence, which are typically developed and honed using huge quantities of data. Access to more data could power new applications of artificial intelligence, enabling greater efficiency and new insights. 39,9% of respondents expect to increase their use of AI in business development, highlighting the need for data to power that expansion.

We can expect the use of externally sourced data to increase in coming years and for it to become easier to access a wider range of data sources. It is notable that, when asked whether their businesses tended to take an open or closed approach to data, 23,6% of respondents' businesses take an open approach to data, aiming to create value through collaboration. Slightly more at 26.6% responded that they preferred to take a proprietary approach to data to preserve value for the business. The latter group will need to understand how the new data regime in the EU will reduce their ability to keep such data proprietary.

Currently, data access rights are often governed by contractual provisions, and (apart from personal data) it is often up to the business collecting the data to decide whether to open it up for access. Intellectual property rights may often also be relevant, and the interface between proposed new rights of access to data with existing intellectual property rights including trade secrets will be important. It does not appear from the survey results that a great deal of legal challenge happens around data access at present – only 13,3% of responding businesses have been involved in a dispute on data rights or data access rights.

> We can expect the volume of data-related litigation to increase as these new rights are increasingly understood and exercised.

It is worth highlighting that the new swathe of data regulation will create new rights as well as compliance obligations. Some of these new rights may be a legal basis for submitting a complaint to a regulator; others will be rights expressly created by the new legislation, or which flow by inference from it and that are directly enforceable through the courts. We can expect the volume of data-related litigation to increase as these new rights are increasingly understood and exercised. This is an important point to bear in mind for in-house legal teams – there are examples in other fields where the pro-active use of rights to damages for harm caused to the business by the regulatory infringements of other businesses has generated significant flows of compensation.

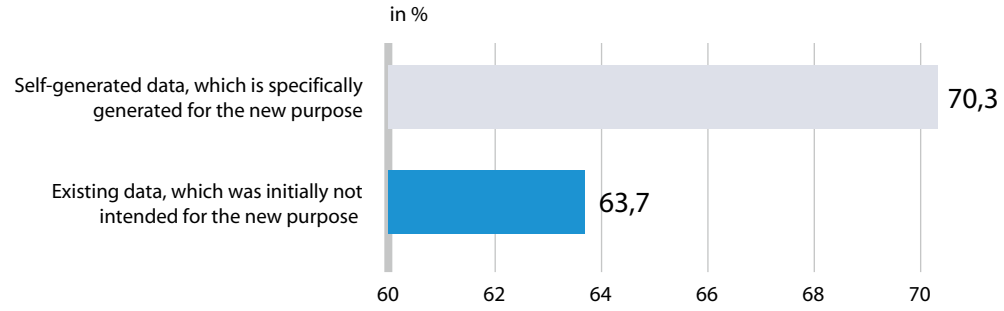
The challenge of regulation

A core objective of the survey was to understand the position of corporate legal departments amid this widespread, data-fuelled activity in their businesses. The picture painted by the survey reflects the disruptive impact of transformation strategies.

The survey results bear witness to the variety of challenges that lawyers face when implementing data-driven business models. But legal and regulatory challenges were the most commonly cited obstacles to implementing

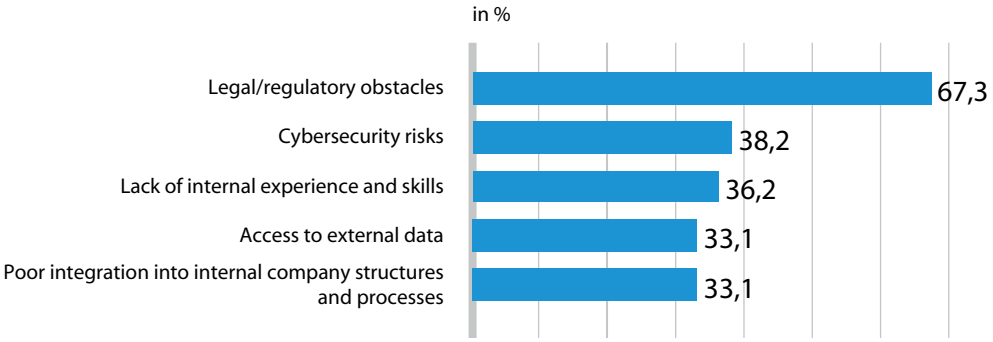
Where does your company obtain (or will obtain) the data from?

Internal data sources



In your experience, what are the biggest obstacles to implementing data-driven business models?

Up to 5 options can be chosen



data-driven business models by some margin, being experienced by 67,3% of respondents. The next-most cited obstacles were cybersecurity (38,2%), lack of internal experience and skills (36,2%), access to external data (as discussed above – 33,1%) and poor integration into internal company structures and processes (32,3%).

Cybersecurity is certainly a consideration that increases in scope and significance with digitalisation and greater use of data flows, and as supply chains take on a digital dimension. This is not only an operational issue for the IT team to manage. It also has a regulatory angle. There are legal obligations and responsibilities in relation to systems and data security, and these compliance risks need to be understood and managed.

68,1% of participating lawyers consider the European legal/ regulatory framework to be too complex and 63,4% find it confusing.

Concerns about dealing with the legal and regulatory landscape for data-driven business models are widespread. 68,1% of participating lawyers consider the European legal/regulatory

framework to be too complex, and 63,4% find it confusing. Only 11,4% of respondents answered that they considered their company to be well prepared for the legal challenges of data-driven business models.

The perception of confusing complexity is a worrying finding. The data regulation landscape in the EU is about to see a vast expansion. Data regulation will no longer be largely synonymous with privacy. There will be a swathe of new legislation both reforming existing digital regulation and enacting new frameworks specifically designed to open and shape the data ecosystem, as well as regulating data-powered artificial intelligence. The fact that 22,6% of respondents think that the regulatory framework for data-driven business models is stable suggests that there is not yet universal awareness of the huge changes on the horizon. Businesses need to be developing an understanding of the new laws that are likely to impact on them, and in what timeframe (taking note, moreover, of the impact of developments outside Europe). And as highlighted, some of the change will be the creation of new rights, as well as obligations, so legal teams will need to be in the lead with regards to identifying when those new rights are in play, and exercising them where necessary to protect their businesses' interests.

Data strategy and governance

As data becomes an increasingly valuable asset for a business, and starts to underpin significant proportions of its activity, decision-making, products and services, a data strategy becomes all the more important. However, notwithstanding the strong responses in relation to the extent of data-driven products and services and their importance to the surveyed businesses, with 61,1% of respondents offering data-driven products or services, only around 36,1% of respondents answered strongly that they have a data strategy. Only 47% think about the ethical and reputational angles of their use of data, and only 40,2% use contract templates that include provisions dealing with data that go beyond data protection compliance.

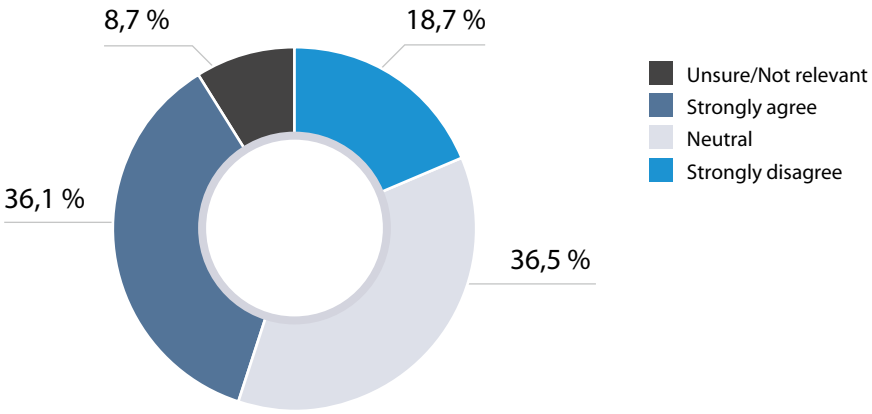
> ...a corporate data strategy and data governance policies may be in place, but do not appear to be developed as a coherent whole.

The survey responses paint a picture that, not only is there a proportion of businesses that have adopted data-driven business models without an overarching data strategy, but in several others many of the component parts of a corporate data strategy and data governance policies may be in place, but do not appear to be developed as a coherent whole. Tellingly, despite many businesses having data provisions in their template contracts, only 16.1% of respondents considered that the legal team had implemented the business's data strategy (if it had one). Moreover, the absence of a strategic approach is suggested by the statistic that only 25.7% of companies answered that they have board-level expertise around data-driven business models.

Corporate data strategy and data governance are not areas that are necessarily driven by the legal department, but there is undoubtedly significant value that in-house counsel can add. Moreover, the legal team is often well placed to broaden these policies out to sit across the whole business, rather than being considered an issue for the IT team. A coherent and considered approach, endorsed and adopted at board-level, can shift the culture of an organisation to ensure that all in the business understand and protect the value of data. For some businesses, the data provisions in a draft contract will be the first to be ceded in negotiations; for others, a data-savvy lawyer will sit at the table in every deal. As understanding of how to leverage the value in data increases, this difference in attitude can potentially start to impact on revenue streams and lost opportunities. The company's

Which of the following statements apply to your company?

Your company has a data strategy



IP strategy may need to be expanded to ensure that any intellectual property in data or databases is effectively protected. Data strategy may also intersect with a business's sustainability strategy and objectives – the impact of the technology used to deliver on a business's carbon footprint should not be overlooked and may trigger further compliance risks.

Having looked at the results through a cross-sector lens, it should be emphasised that the picture is, of course, not uniform across the various commercial sectors. Indeed, some of the particularities of different areas of commerce and industry are highlighted when the results of the survey are split by sector (as we explore in Chapter 1.4 below).

METHODOLOGY AND ACKNOWLEDGEMENTS

The survey should be seen as a definitive pan-European insight into the data-related activities of companies, as in-house counsel from over 20 countries took part in the survey.

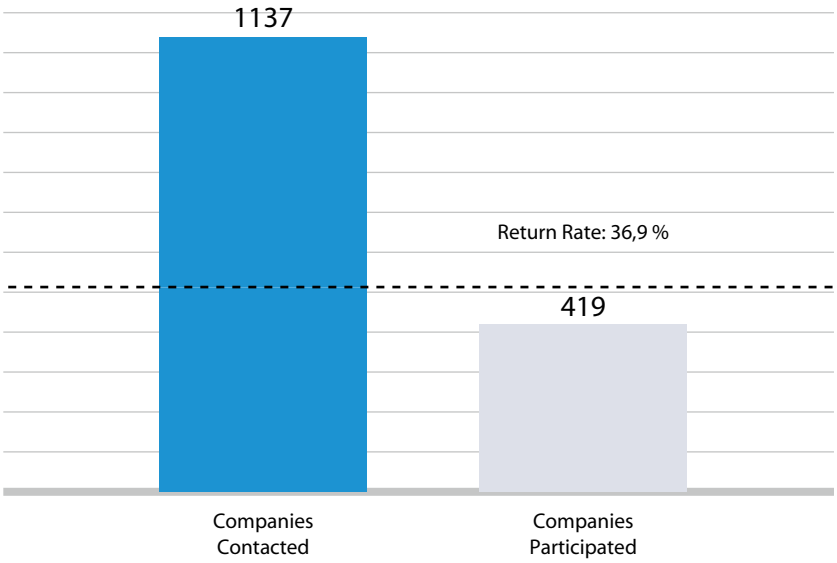
METHODOLOGY AND ACKNOWLEDGEMENTS

From December 2021 to March 2022, ECLA distributed a comprehensive study through its member associations to company lawyers across Europe. A total of 419 companies participated in this study. The survey should be seen as a definitive pan-European insight into the data-related activities of companies, as in-house counsel from over 20 countries took part in the survey.

At 18,1%, the largest proportion of participants come from Germany. The United Kingdom, at 13%, and Italy, at 12,3%, are the second and third most represented countries, respectively. 8,7% of participants hail from France, with another 7% from Belgium. Spain, at 6,3%, and the Netherlands, at 5,6%, are the remaining two jurisdictions in which at least 5% of participants took part in the survey.

Participants were classified into predefined industry sectors, which are shown throughout Part 1. This provides for an in-depth comparative insight in data-related discussions, and gives a comprehensive picture of how different industries across Europe have approached the increasing challenges that data management and utilisation brings to their organisations. A further "Other" sector was established for

Return Rate / Participation Rate



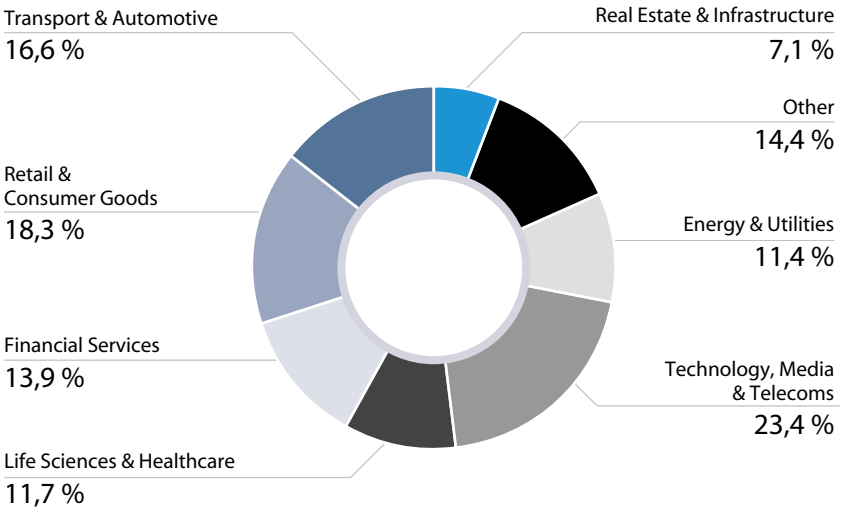
participating companies that did not fit in the predefined industries. The feedback of respondents that did not choose any of the predefined industries is included in the general results of the study.

Given that data utilisation requires considerable investments to be made by businesses, the expectation was for the participating companies to have sizeable revenue streams. 18,3% of participants work for companies that have a yearly revenue below €10 million, a further 18,9% of companies have revenues ranging from €10 million to €200 million. In addition, 19,4% of participating companies have revenue streams between €1 billion to €10 billion, with revenues for the final 18,9% exceeding €10 billion.

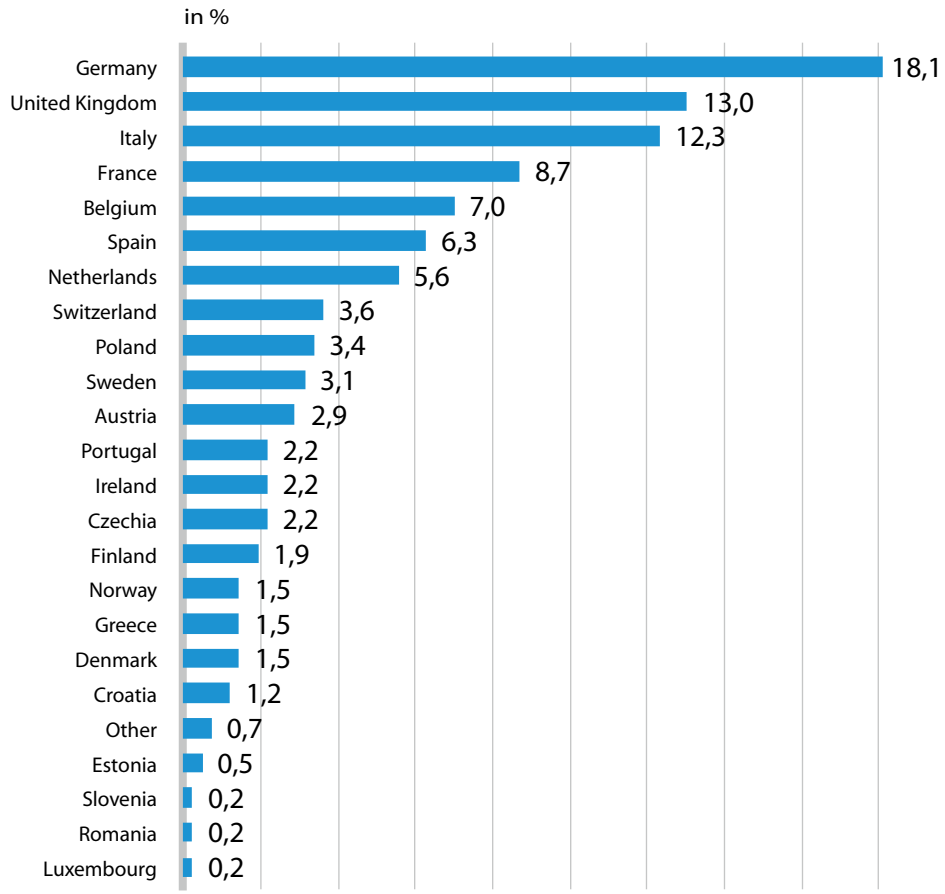
We would like to thank all survey respondents, as well as the following commentators, for their time and insights:

Mark Cockerill, VP, Legal – EMEA & Head of Global Privacy, ServiceNow and VP, ECLA
Sally-Anne Hinfey PhD, Vice President and Deputy GC, Legal (Global Privacy), Momentive
Nick Johnson, Partner, Osborne Clarke, United Kingdom
Elisabeth Macher, Counsel, Osborne Clarke, Germany
Jonathan Marsh, International General Counsel, TotalEnergies Marketing & Services and President, ECLA
Dr Jens Schefzig, Partner, Osborne Clarke, Germany
Timo Spitzer, Head of Legal Corporate & Investment Banking GER, AT, CH & Nordics, Banco Santander

Demographics*

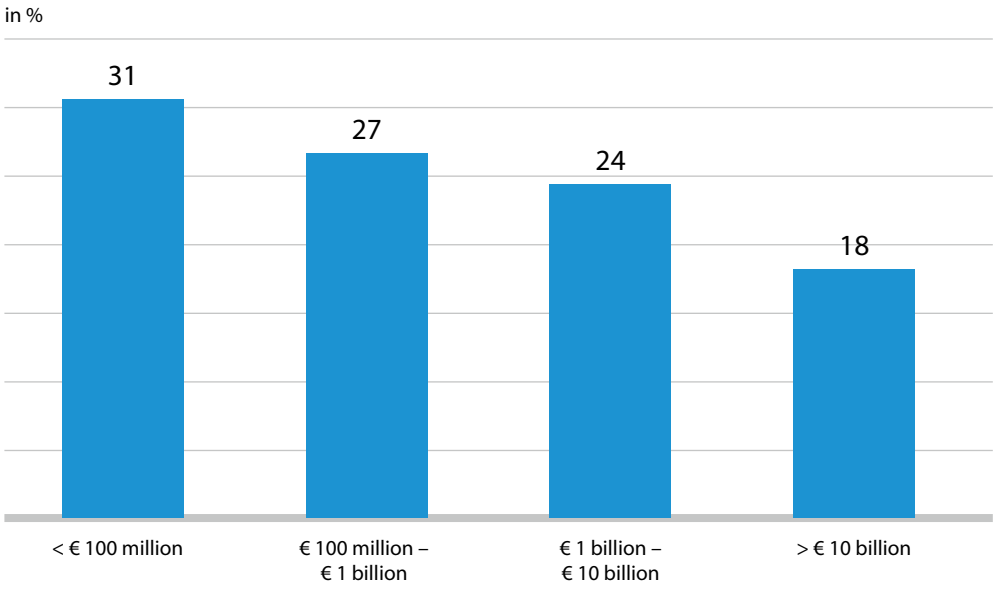


Total number of participants: 419



* Multiple choice question

Demographics – revenue category of participating companies*



* In EUR per year
* Excluding Banking, Insurance and Financial Services

1.1
DATA-DRIVEN PRIORITIES

That two-thirds of responding companies are already offering data-driven products and services should be seen as a significant result for the evolution of data-related products/ services.

The first step in gaining an in-depth understanding of the data-related activities of companies in Europe is to see whether companies offer data-driven products or services. There is a valuable distinction drawn between companies that have already started to offer such products and services, and companies that are currently on their way to doing so. For the purposes of this study, companies that have not and are not planning on implementing any data-driven activities within their organisation did not participate in the study in its entirety, as they would be unable to answer any further detailed questions. Such participants were directed to the survey questions covered in Chapter 1.3.

A. Are companies offering data-driven products/services?

Respondents could either answer the statement "Does your company offer data-driven products/services?" with "Yes", "No and we do not plan to do so", "Not yet, but we do have products/services in planning stage", "Not yet, but we do have products/services in piloting stage", "Not yet, but we do have products/services in the implementing phase", or "Not yet, but we do have products/services in introductory phase". The "Not yet, but…" answers have been consolidated in the results to give more clarity to the overall status of companies, as the end-goal of companies choosing this option is to express a positive answer for future intentions. If participants answered "No and we do not plan to do so", the participants would then be directed to the questions on the specifics of their data-driven activities.

61% of respondents from across Europe offer data-driven products and services

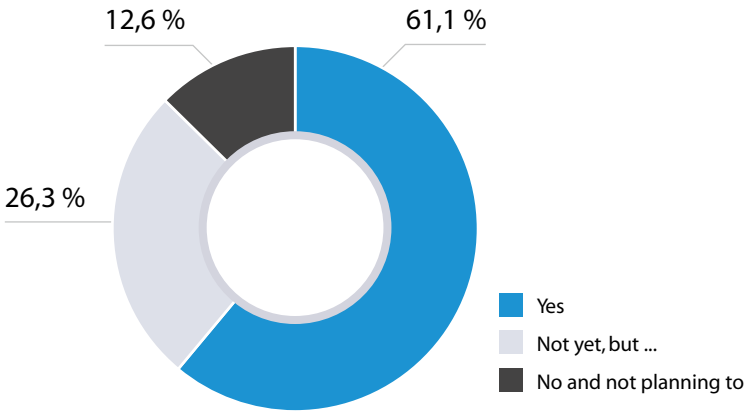
A total of 61,1% of respondents answered "Yes", indicating that their companies already offer data-driven products and services. A further 26,3% of respondents work for organisations that are at the very least in the planning stages to introduce data-driven activities in the future, even if they do not currently offer any such products or services. Just 12,6% of participating companies are not currently planning on introducing any data-driven products or services.

The options given to participants were multiple choice for the companies choosing "Not yet, but…" to further specify their activities, indicating whether the data-driven products/services they are undertaking are already in the piloting or implementing stage, or still in the planning stage. Companies that chose either "Yes" or "No and we do not plan to do so" did not opt for other choices given. For companies that are currently in the process of introducing data-driven products/services, these activities are still in their infancy, with 12,9% of the total respondents specifying their companies to be within the planning stages of their journey.

13% of responding companies have no plans to introduce data-driven products and services

That two-thirds of responding companies are already offering data-driven products and services should be seen as a significant result

Does your company offer data-driven products/services?*



* Multiple choice question, results indexed to 100 %

Figure 1.1.1

Does your company offer data-driven products/services?

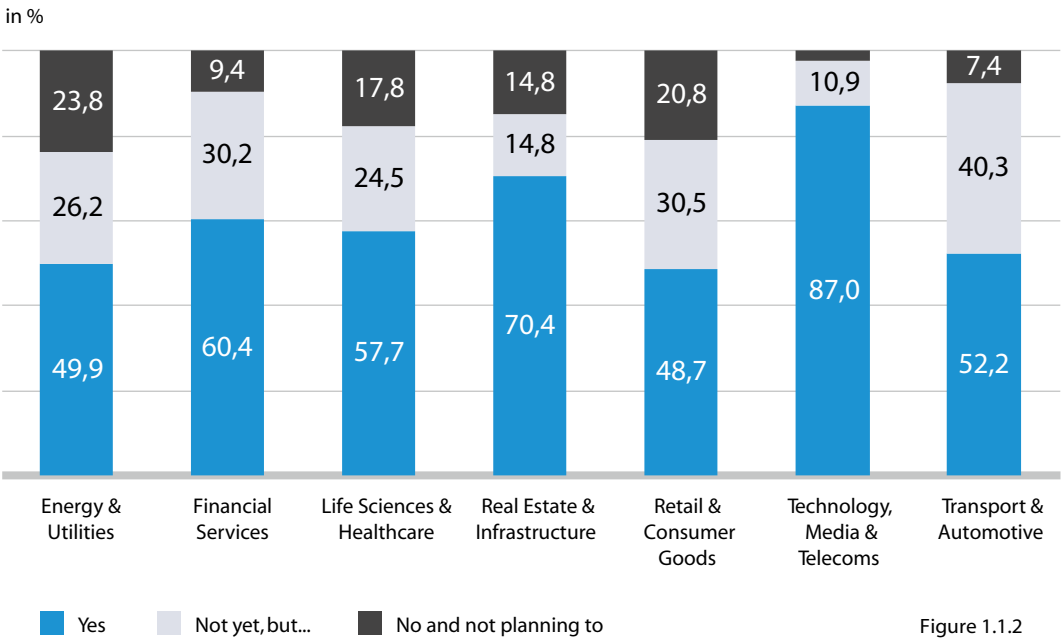


Figure 1.1.2

for the evolution of data-related products and services. That only 12,6% of responding companies indicated no short- or mid-term plans to implement data-driven activities demonstrates the importance that powering products and services through data collection and analysis is felt to have. European companies surveyed have by and large acknowledged the value that data-driven results bring to product or service improvement or expansion.

There are notable differences between the different surveyed industries. These differences can be seen through the proportion of companies that are already offering data-driven products/services and, more importantly, the proportion of companies that are not planning on implementing such activities soon. Though there are industries where most companies are already offering data-driven products/services, several surveyed sectors are currently in the development phase, with the results reflecting more closely the general results.

87% of Technology, Media & Telecoms businesses surveyed offer data-driven products/services

The Technology, Media & Telecoms industry sees the largest share of businesses already offering data driven products/services, standing at 87%. A further 10,9% of respondents are working for companies that are planning on establishing such elements soon. Only a negligible share of companies surveyed within the industry do not currently have any plans to introduce data-driven products or services. The sector can be seen as a trailblazer among the surveyed industries, with close to 9 out of 10 companies surveyed already offering data-driven products and services. This is emphasised by the fact that just 2,1% of companies surveyed within the industry are not planning on introducing any data-driven components, or at least they do not have any plans in the short- or mid-term.

The only other industry where an above-average proportion of companies already offers data-driven products or services concerns the Real Estate & Infrastructure sector, where 70,4% of responding companies already offer data-driven products/services. A further 14,8% of participants indicate that they currently are in the process of having such elements within their organisations soon, and another 14,8% had no plans to do so. The above-average proportion of respondents answering "Yes" and the second-lowest proportion answering "Not yet, but…" is surprising for an industry not often thought as pioneers in technical advancement.[1] Nevertheless, the sector continues its digitalisation journey with technology already deployed across construction, development, and management processes.

The Financial Services sector resembles the general results, with 60,4% of responding companies already offering data-driven products/services. A further 30,2% are currently at least planning on introducing such products/services to their organisations. The 9,4% of responding companies that are not planning on introducing any data-driven offerings is the third-lowest share out of the surveyed industries. The other sector that resembles the general results concerns the Life Sciences & Healthcare sector, where 57,7% of responding companies are already offering data-driven products/services. 17,8% of participants indicate however that the introduction of such products/services is on their horizon, the third-largest proportion amongst the surveyed industries.

The proportion of companies in the Financial Services sector that currently offer such products/services is surprising, as the expectation would be to see a higher share of businesses already having established data-driven components. The industry has historically been one of

1 There was a smaller number of responses from REI businesses compared to other sectors (see Methodology and acknowledgements), which may have impacted on these results.

the pioneering sectors in introducing innovation to their organisations, given that financial and operational gains are the primary goals for companies within the sector. Regardless, the low proportion of companies that are not planning on introducing any data-driven products/services indicates that the industry does understand the intrinsic value that data brings.

Only two of the surveyed sectors saw under half of respondents answering in the affirmative – Retail & Consumer Goods, at 48,7%, and Energy & Utilities, at 49,9%. These two sectors also had the largest proportion of respondents responding negatively to this question, with 20,8% of the former and 23,8% of the latter indicating no plans to offer any data-driven products or services any time soon. However, the proportion of companies that are in the planning stages is still considerable, with 30,5% of responding companies in the Retail & Consumer Goods industry planning on introducing data-driven products/services soon, and a further 26,2% of responding companies in the Energy & Utilities sector being currently in the planning stages. The proportions shown for both sectors are notable, especially when contrasting them to the other surveyed sectors or even the general results.

52% of Transport & Automotive businesses surveyed offer data-driven products/services, a further 40% are in the planning stages

The results also highlight which industries are currently most involved in the planning and introduction of new data-driven products and services. In the Transport & Automotive sector, though a relatively low percentage of responding companies (52,2%) are currently offering data-driven products/services compared with other industries, a further 40,3% of responding companies are currently at least in the planning stages with their activities. This is the largest proportion of respondents indicating their willingness to introduce such business models into their businesses.

Similarly, the 7,4% of respondents indicating no current plans to introduce data-driven products and services is the second-lowest proportion across the surveyed sectors. The considerable proportion of companies in the sector that are planning to offer data-driven business models highlights the increased possibilities that data collection and usage has provided.

That such a large proportion of the T&A industry is underway in introducing new data-driven solutions shows how the sector is currently

Osborne Clarke view

Elisabeth Macher ✉
Counsel, Germany
Further information

"We see huge shifts in this industry that will fully pan out in the coming years. Be it new business models around connected cars, Mobility as a Service and autonomous driving or the novel possibilities coming with modern repairs and predictive maintenance, each market player will need to reposition and strategise to stay competitive. Access to data is key for competition and innovation in the market, and the future will belong to those companies that manage to secure that access."

transforming its business model, as new possibilities for businesses have become possible. Companies in the sector see new opportunities, as data collection has enabled them to improve existing products and services, whether it concerns consumer mobility or logistics services, and to innovate further. It is also introducing new types of services within the sector, such as Mobility as a Service, which has already transformed consumer thinking. The conventional taxicab system is all but forgotten among younger generations, and other transportation methods, such as electric scooters, have dominated public debate in recent years. In logistics, the necessity to decrease the inefficiencies in last-mile delivery have only increased during the COVID-19 pandemic, as more consumers have pivoted to online purchases. In addition, the sector is focused, beyond efficiency gains, on providing increased transparency to the supply chain through data and ultimately, to automate the entire supply chain.

This opening question provides a starting point to the discussion of data-driven products/services and gives a broad overview of the general European landscape and the sectoral specificities that different industries enjoy. There is significant variation between the surveyed sectors, with industries such as Technology, Media & Telecoms showing considerable maturity compared with many other sectors. In addition, industries such as Financial Services and Transport & Automotive show significant optimism around the value of data-driven components, with under 1 in 10 companies surveyed having no near-term plans in their horizon to develop such offerings.

"While some industries are further advanced at the moment, data-driven business models will play a significant role in all industries in the very near future. Because of its borderless character, data-centric business models are also a huge challenge for lawmakers to meet the requirements of the markets – a great opportunity for our profession to create the future legal framework together with national and European legislations."

Mark Cockerill, Vice President of ECLA and VP, Legal – Corporate Securities, M&A & International Development at ServiceNow

B. Data-driven tasks for businesses

Having established whether companies are currently offering (or are planning on introducing) data-driven products/services, the next question, for those that were doing so, concerned which data-driven tasks companies are interested in offering. For this purpose, participants were asked to specify what data-driven tasks either already are or will be a part of their company's range of products/services. The goal was to gain an understanding of what the purpose of data utilisation is for companies across Europe. Responding companies were given a diverse set of choices, as part of a multiple-choice question, which included the core data-driven activities that contemporary businesses can utilise.

Of those businesses currently offering (or planning to introduce) data-driven products/services, 69% either have or are planning to have data analysis services as a part of their data-driven activities. This includes relevant data processing, such as data visualisation for the purposes of gaining tangible conclusions that a business can derive from data. In addition, 59,1% are further implementing or planning to implement data analysis results into more in-depth, data-driven development projects to gain further insights. Half of those companies offering (or planning to introduce) data-driven products/services are also concerned about data aggregation and data generation. The former entails the simplification and combining of datasets and data streams for a more coherent overview, whereas the latter concerns generating datasets through internal sources. Data generation can also involve establishing additional datapoints to collect and make accessible.

Data sourcing through external means sees a much lower proportion of respondents, with only 22% of companies offering (or planning to offer) data-driven products/services currently having established processes to continuously source data through external sources. This can indicate the rising challenges that data collection entails, which will be addressed later.

Most notably however, only 31% of responding companies offering (or planning to offer) data-driven products/services state that their data-related activities play a secondary role to their core business model. That 69% of those companies see their primary products as being data-driven is a significant proportion. This demonstrates the evolving landscape in how data collection and subsequent analysis and utilisation is playing an increasing role in the decision-making of companies across Europe and across industries.

Which data-driven tasks are (or will be) part of your company's range of products/services?

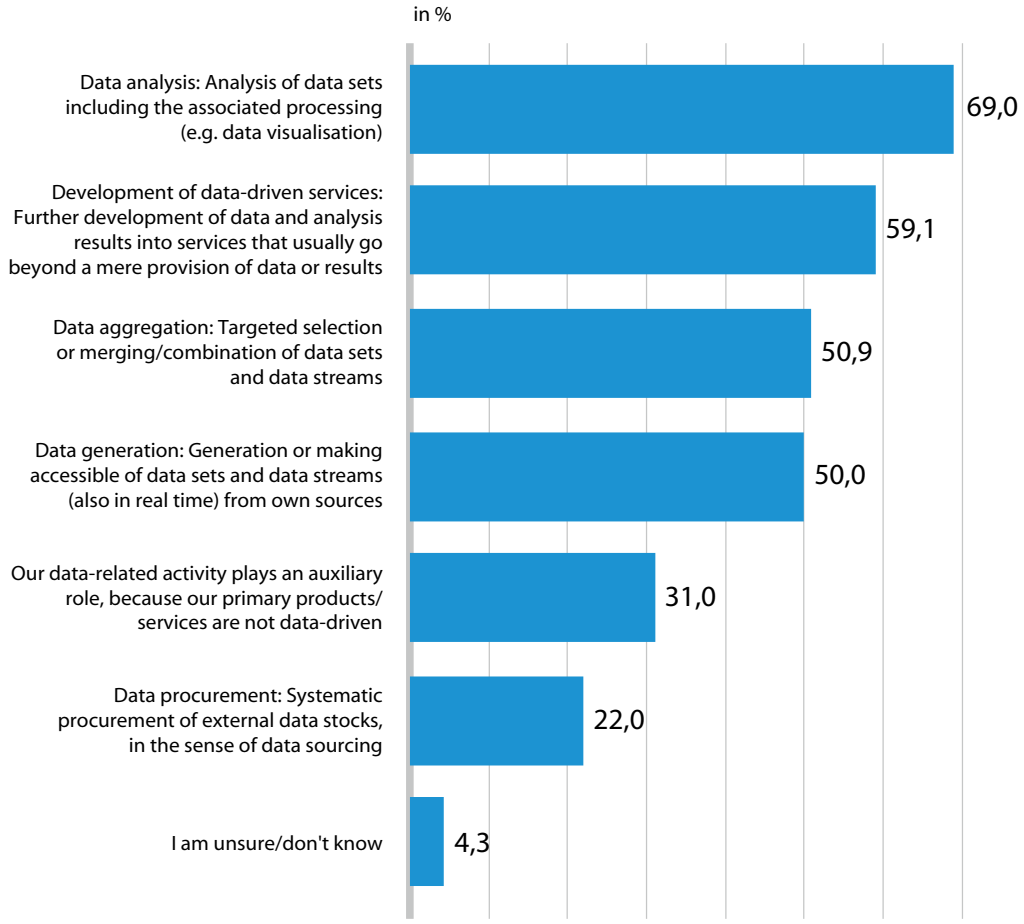


Figure 1.1.3

C. What data-driven products do businesses offer?

Another key component in understanding data-driven business models concerns the specific products/services that companies are planning to offer. Participants from companies that currently offer (or are planning to offer) data-driven products/services were asked to answer multiple-choice questions, which were divided into categories concerning the role that data plays in those services, to understand more precisely the type of services that companies are targeting. Participants were also able to choose not to answer the question or to select "I am unsure/don't know", if those options were deemed most suitable for them, or to skip the sub-question if their businesses do not offer such a data-driven service.

Of the responding companies that do offer or plan to offer data-driven products/services, 79% of participants have purely data-driven service components. In addition, 70% of respondents indicate that they have at least one form of a hybrid service bundle. 56% of responding businesses sell or plan to offer raw data and other data products as intangible goods, with a further 54% offering or planning to offer data infrastructure solutions.

Regarding purely data-driven services, respondents were given the option to highlight whether their goal is to improve core activities or processes, or to support decision-making. The former concerns the utilisation of data to increase the value of the activities/processes targeted. The latter concerns the conventional utilisation of data, to make higher-quality business decisions.

Three-quarters of businesses use (or plan to use) data to improve activities or processes

76.5% of participating companies with purely data-driven services are currently utilising or planning to offer services to improve ongoing activities or processes. That 3 out of 4 such companies see data utilisation as a method to improve processes is a considerable proportion and demonstrates the inherent value that data-driven services bring to organisations.

One-third of businesses use (or plan to use) data to support decision making

In addition, 32.9% of companies that offer (or plan to offer) purely data-driven services do so to support decision-making.

The proportion of respondents who answered "I am unsure/don't know" stands at 15,6%. Though the reasoning for choosing this option is unclear, the proportion of corporate lawyers who are unaware of the goals of purely data-driven services in their company is low.

Technology, Media & Telecoms businesses lead the way

There is not much discrepancy to be seen between the different surveyed sectors overall, as the largest divergences from the surveyed sectors to the general results amount to 10 percentage points. Companies surveyed in the Technology, Media & Telecoms industry show a more in-depth understanding of the activities of their organisation regarding purely data-driven services, as just 9,5% of respondents answered "I am unsure/don't know." The proportion of companies that offer (or plan to offer) data-driven products and services within the sector, that offer purely data-driven services to improve core activities or processes, was also the highest among the surveyed industries, standing at 85,7%. Similarly, the 41,3% of companies that offer such services to improve the quality of decision-making is the highest among the different industries.

Which data-driven products/services does your company sell or plan to offer in the future?

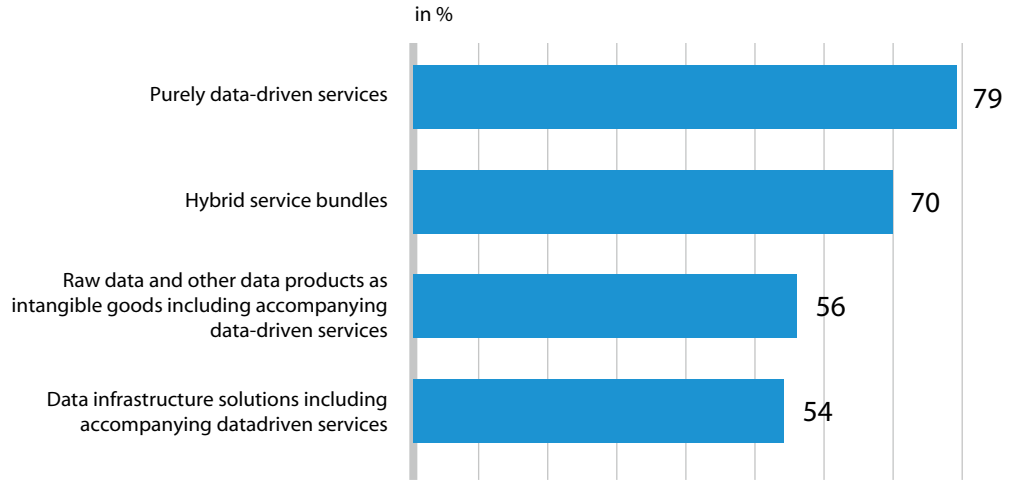


Figure 1.1.4

Which data-driven products/services does your company sell or plan to offer in the future?

Purely data-driven services

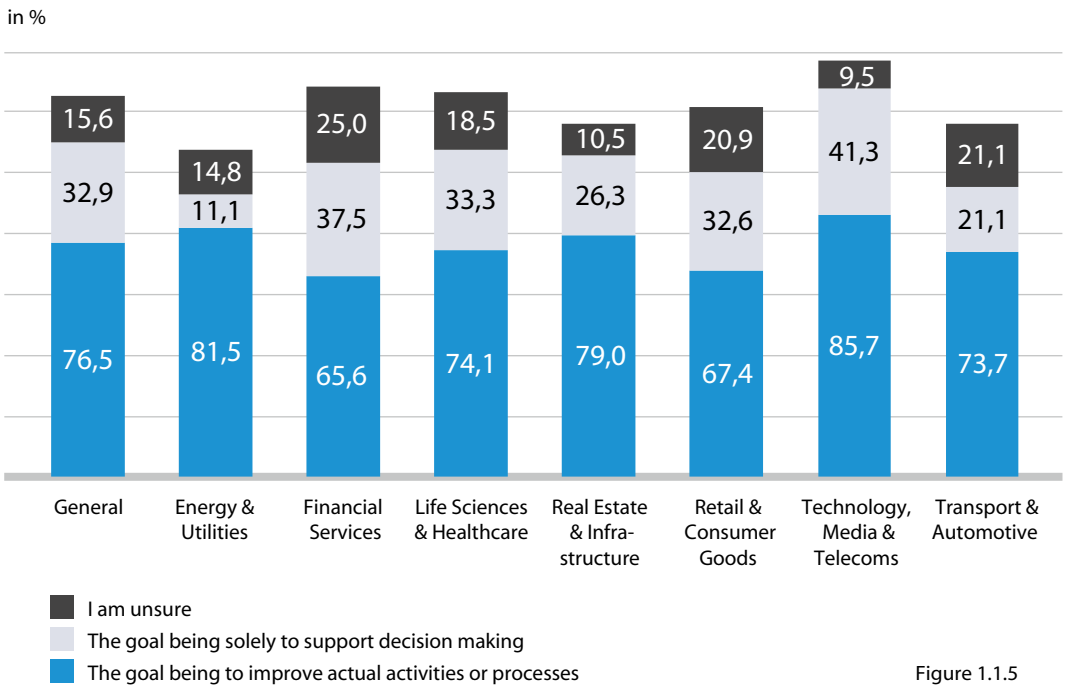


Figure 1.1.5

The only sector that diverges more considerably from the general results is the Energy & Utilities industry and more specifically, with the utilisation of data to support decision making. Just 11,1% of responding companies that offer (or plan to offer) purely data-driven services utilise them with the objective of improving the quality of business decisions an organisation can undertake.

Another data utilisation method can be classified as a hybrid service, where data plays a considerable, though not exclusive, role for the realisation of the final product/service.

Responding companies that currently offer (or plan to offer) data-driven products/services were given the option to indicate whether such hybrid bundles within their respective organisations focus on either utilising such services to supplement existing products/services or enabling them to offer new products/services altogether.

60% of responding companies use hybrid service bundles to enhance existing products and/or services

60,4% of responding companies with hybrid service bundles are using data to supplement and improve their existing products/services. That 3 out of 5 companies are either utilising or planning to use data to enhance their ongoing product/service line signifies the increasing value that companies can offer through the proper utilisation of data.

Furthermore, 34,7% of responding companies have found ways to use data to enable them to offer new products/services. The increased possibilities for novel products/services that companies can already undertake is certain to increase, as new data collection methods and analysis capabilities are being developed within organisations.

There is a considerable proportion of respondents who answered "I am unsure/don't know", standing at 24,1%.
For most of the surveyed sectors, there is little discrepancy seen regarding the utilisation of hybrid service bundles to further enhance their existing components, with all but two sectors diverging from the overall results by 9 percentage points or less. Similarly, regarding the possibilities to offer novel products/services, most sectors do not significantly differ from the general results, except for two industries.

In terms of data usage to extend existing products/services, the two most contrasting surveyed sectors are the Technology, Media & Telecoms and the Transport & Automotive sectors. For the former, close to 4 out of 5 of responding companies with hybrid service bundles are using data to improve their ongoing services and products, whereas for the latter, just 37,2% of responding companies have utilised such elements. The higher-than-average proportion of shares that the Technology, Media & Telecoms industry enjoys can be attributed to the maturity of the industry with regards to its data-driven activities, as the results throughout this survey reflect this sentiment. For the Transport & Automotive sector, the low proportion of respondents indicating data usage to enhance ongoing products/services, could be attributed to the more limited possibilities regarding the improvement that existing products/services can potentially undertake, including due to type approval requirements and limitations. As the industry is, by contemporary definitions, an established industry with over a century of activities, it should not come as a surprise that the established product/service lines offered are yet to be significantly disrupted by data utilisation, which is still in its infancy. Nevertheless, that 1 in 3 responding companies that offer hybrid service bundles are using data to enhance their existing lines should be seen as a major step forward.

Which data-driven products/services does your company sell or plan to offer in the future?

Hybrid service bundles

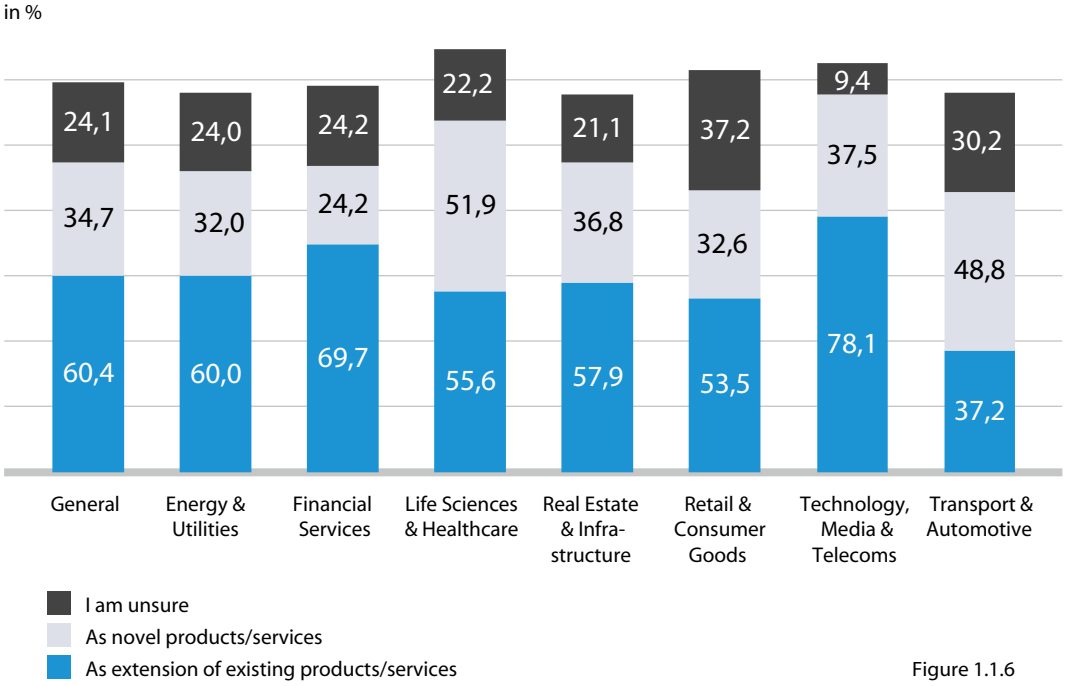


Figure 1.1.6

Half of Life Sciences & Healthcare and Transport & Automotive businesses use data to develop new hybrid service bundles

Concerning the usage of data to introduce new products and services, two sectors show significantly above-average results – Life Sciences & Healthcare, at 51,9% of those responding companies that offer hybrid service bundles, and Transport & Automotive, at 48,8%. More notably, Transport & Automotive is the only surveyed sector where the utilisation of data has enabled companies to offer novel products/services at a higher proportion than for extending existing product/service lines. This highlights the growing possibilities for novel products/services that these sectors have seen in recent years, as data collection and utilisation has enabled these industries to diverge from their previously established paths and offer a more tailored approach to the end user.

Most sectors have similar proportions of companies who are unsure about the inclusion of data either as an extension to their existing product/service line or the utilisation of data to offer new products and services altogether. The sector with the highest share of respondents answering "I am unsure/don't know" is the Retail & Consumer Goods sector, where close to 2 out of 5 legal departments do not know whether data has enabled them to either extend or offer novel products/services.

Another key aspect in understanding the data journey of European companies is to address how data as a commodity is approached and assessed.

The question aims to understand whether data in European companies is being treated beyond its value as a utility and how prominent the sale of raw data and the marketing of data products is. For this purpose, participants of companies that currently offer or plan to offer raw data and other similar data products as intangible goods were given the option to indicate whether their companies are already offering, or are planning to offer, data analysis and sale services or the development and marketing of data products.

Half of responding companies that view raw data as an intangible good offer (or plan to offer) data collection, analysis, processing, and sale of data services

Across Europe, 47,9% of respondents of businesses that offer (or plan to offer) raw data as a commodity are either offering or planning to offer data collection, analysis, and processing services and data sales. That close to one in two companies are considering data and related data products as intangible goods signifies the monetisation aspect that data collection and organisation can enable. In addition, 38% of company lawyers from such companies report that their businesses are utilising raw data to develop and market subsequent data products. The result includes the provision of supplying relevant hardware for client-side data collection, when applicable.

A total of 31% of respondents responded with "I am unsure/don't know", a larger share than under the two previous sub-questions. Since only company lawyers responded to this survey, it should be stressed that this may reflect the unfamiliarity of the legal team with relevant activities rather than the overall approach of the business.

Over two-thirds of respondents in the Real Estate & Infrastructure sector that view raw data as an intangible good plan to sell data

There are some sectoral differences when considering the two options presented. Companies that offer (or plan to offer) raw data as a commodity in the Real Estate & Infrastructure sector see a 20-percentage point increase when considering raw data collection and sale. In addition, half of the responding companies in the Life Sciences & Healthcare sector use raw data to develop and market further data products. It is also the only sector where the proportion of such companies surpasses the percentage of companies that deal with raw data collection and sale.

The share of companies that reportedly approach raw data as a commodity is higher than

Osborne Clarke view

Maria Grazia Medici ✉
Partner, Italy
Further information

"The collection and smart use of data has rapidly been prioritised to sit in the core of most Life Sciences & Healthcare service offerings - whether that is the analytics or digital clinical trials being adopted by traditional Pharma companies, the leveraging by Technology companies of health data of their users, or the ever more sophisticated exploitation of data by disruptive players."

Which data-driven products/services does your company sell or plan to offer in the future?

Raw data and other data products as intangible goods including accompanying data-driven services:

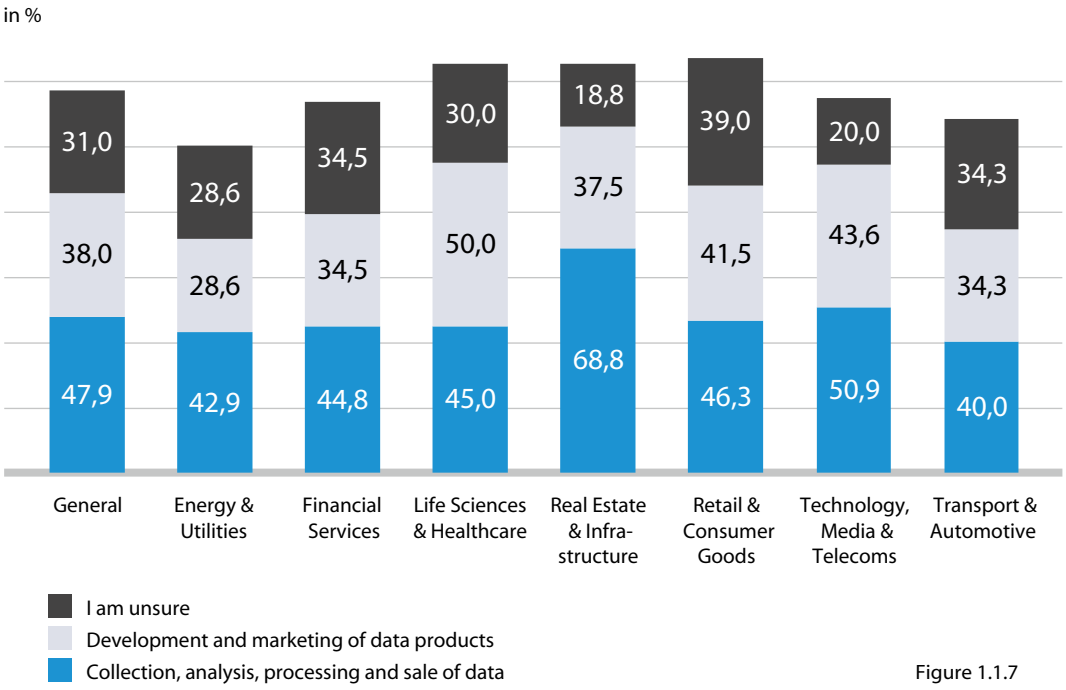


Figure 1.1.7

expected, as the experience of industry experts does not necessarily reflect the results. However, industries such as the Technology, Media & Telecoms often combine the two options within their operations, as collecting raw data and utilising it fall under the same process. In addition, the large proportion of uncertainty that company lawyers have here might indicate how legal teams in many European companies are too distanced from raw data collection and utilisation to provide an objective insight. This means that the perspective of the results for this sub-question are contingent on the industry and the interpretation of the individual.

The final aspect that was assessed concerns data infrastructure solutions, including accompanying data-driven services. This includes all relevant products and services necessary to collect, store, maintain, organise, analyse, and distribute data, both hardware and software, and any necessary human input required. Participants of companies that currently offer (or are planning to offer) data infrastructure solutions were given two options to highlight, whether the business is offering or planning to offer data-related analysis and consulting services and/or distributing data infrastructure solutions to the client/end-user. The results should reflect whether companies in Europe seek to be involved throughout the lifecycle of data utilisation, from collection to the subsequent analysis.

Which data-driven products/services does your company sell or plan to offer in the future?

Data infrastructure solutions including accompanying data-driven services

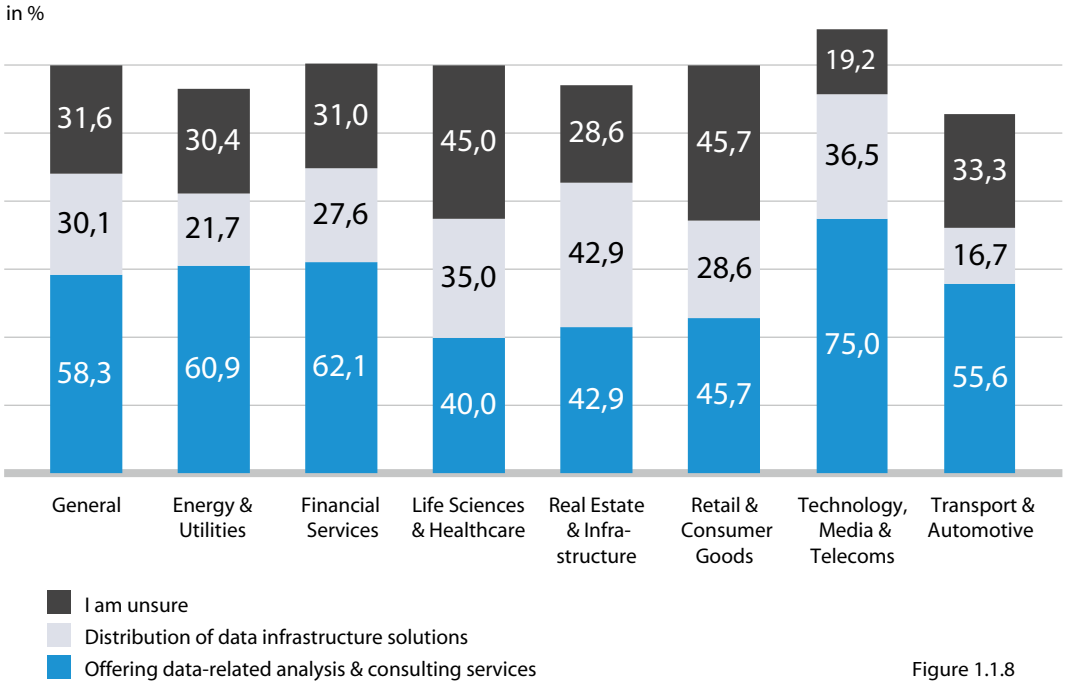


Figure 1.1.8

58% of companies offer (or plan to offer) data-related analysis and consultancy services

58,3% of responding companies that offer (or plan to offer) data infrastructure solutions are already offering or planning to offer data-related analysis and consulting services. In addition, 30,1% of companies are already offering or planning to offer infrastructure distribution services. 31,6% of participating lawyers are unsure whether their companies are either already offering or planning to offer such components.

The rapid development of data collection and utilisation possibilities, relating to the Internet of Things, edge computing and cloud computing has transformed the way an efficient data infrastructure has to be set up. Focusing on on-premise data infrastructure is seen as an outdated approach and the results strongly reflect that sentiment. That 3 in 5 companies are either already offering, or are planning to offer, data-related analysis/consulting services, and that 3 in 10 companies offer to distribute infrastructure solutions, highlights the growing necessity to unify data infrastructure for a wider applicability and usage.

Three-quarters of Technology, Media & Telecoms businesses offer (or plan to offer) data-related analysis and consultancy services

In terms of sectoral differences, there are larger discrepancies than seen under the previous sub-questions. Three out of four companies in the Technology, Media & Telecoms industry

that currently offer (or plan to offer) data infrastructure solutions already offer data-related consulting services in their business units. This is the only sector where the response of companies exceeds the general averages by at least 5 percentage points. Conversely, just 40% of companies in Life Sciences & Healthcare are considering analysis/consulting services, 18 percentage points below the general average. Furthermore, the sector sees a considerable proportion of respondents answering "I am unsure/don't know", standing at 45%. Similarly, the Retail & Consumer Goods industry sees a below-average representation of analysis/consulting services to be offered, at 45,7%. The sector is also well-represented regarding the proportion of participants answering "I am unsure/don't know", at 45,7%.

Real Estate & Infrastructure also sees a lower proportion of participants from companies indicating plans to offer data-related analysis and consulting services, at 42,9%. However, it sees an above-average representation of companies distributing or planning to distribute data infrastructure solutions, at 42,9%. The Transport & Automotive sector shows the least involvement in distributing data infrastructure solutions, at 16,7%. The low proportion for the Transport & Automotive sector indicates the lack of necessity within the industry to provide data infrastructure solutions to the end users.

Osborne Clarke view

Ian Wilkinson ✉
Partner, Real Estate & Infrastructure sector leader, UK
Further information

"The built environment has been collecting data for years. This has been the by-product of the increasing use of IoT in support of building management and the more extensive use of BIM ('Building Information Modelling', sometimes also known as 'Building Information Management') which creates data throughout the full lifecycle of a building, starting from design and construction. And, as cities get smarter, data is generated by increased connectivity between all of the components of the built environment. It's unsurprising that the industry is looking for ways to monetise that data and the intelligence that flows from it."

1.2 OBTAINING AND USING DATA

The popularity of external data sources is linked to a few key aspects, namely regulatory concerns, cost, technical complexity, and specificity of the data obtained.

One of the most insightful question concerns how companies obtain data for their data-driven purposes. Consumer data collection and utilisation has come under increased scrutiny in the past decade and the EU is about to introduce regulatory frameworks for non-personal data. So understanding how companies approach data sourcing provides valuable input into what their capabilities are and what the limiting factors might be.

A. Where do companies obtain their data from?

Participants of businesses that offer (or plan to offer) data-driven products/services were asked to indicate either where they are currently obtaining or will obtain their data from. The question is split into two parts – the first part concerning internal and the second part concerning external data sources. This enables participants to give a detailed overview of their data collection activities and highlights trends across Europe and within industries. Regarding internal data collections, participants were given the choice to indicate whether their collecting processes concern using internally generated data, done specifically for a novel purpose, or repurposing existing data.

I. Internal data sources

70% of businesses self-generate or repurpose data for new purposes

70,3% of responding companies across Europe that offer (or plan to offer) data-driven products/services are generating data specifically for novel purposes. This highlights how data is often collected with a singular purpose, as the goals that the new applications entail require datasets that the business has not previously collected. Self-generated data within this definition contains data that was previously not organised for use in a data-driven business model.

Osborne Clarke view

Marcus Vass ✉
Partner, UK
Further information

"Healthcare providers and, in particular national healthcare providers such as the NHS in the UK, hold huge unique and potentially life changing medical data sets that could enable world class clinical research. The UK government applied emergency regulations (Control of Patient Information Regulations) during the pandemic to relax restrictions on sharing medical data provided by 160 GP surgeries and 160 hospitals – and it is hoped by many that this will continue to make health services more efficient, help patients and aid research."

Where does your company obtain (or will obtain) the data from?

Internal data sources

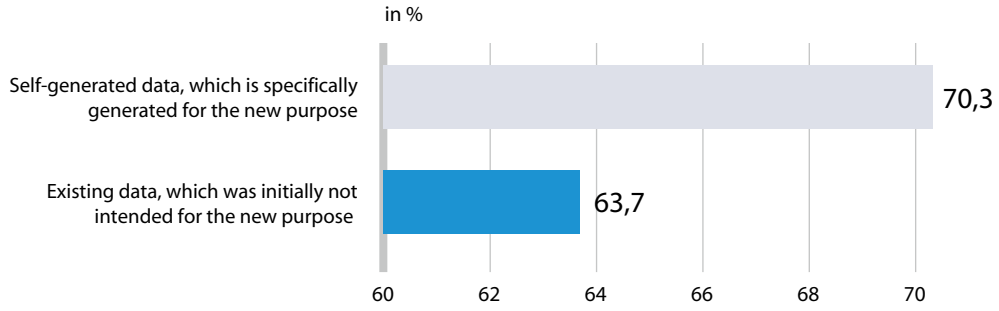


Figure 1.2.1

Where does your company obtain (or will obtain) the data from?

Internal data sources

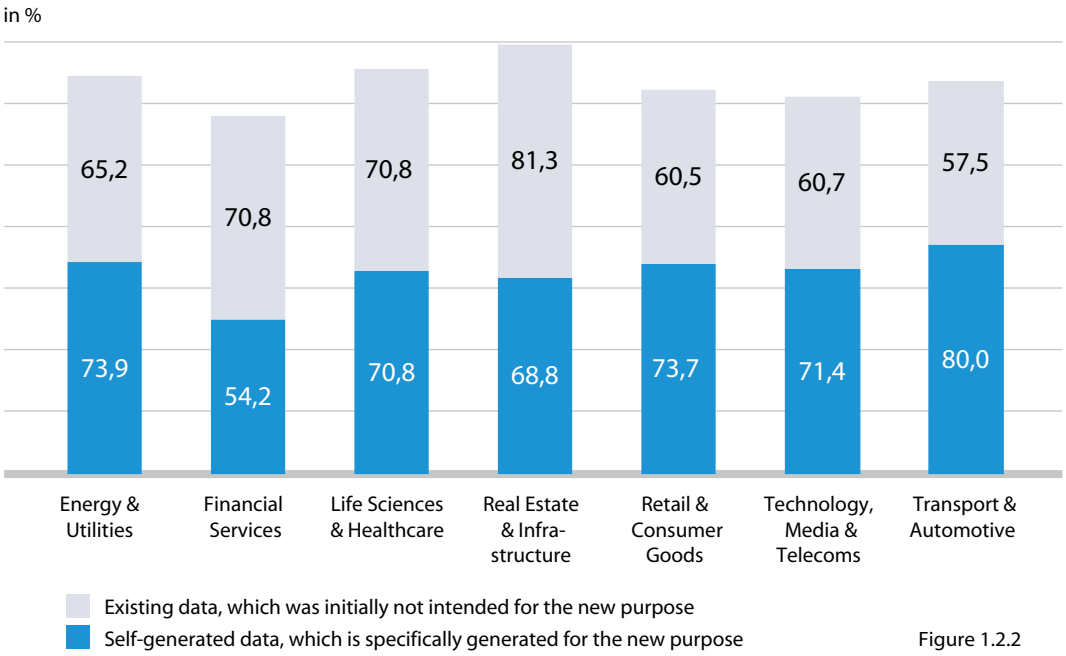


Figure 1.2.2

It also contains synthetic data generation. This is data that is artificially manufactured to mimic real world events that enables companies to by-pass regulatory limitations on usage of personal data in the last decade.

Another approach to obtaining internal data for new applications concerns the repurposing of existing data. As data collection has gained significant prominence within organisations, data collection and organisational efforts have

often already been done for prior purposes. This enables companies to save significant costs and time, as it enables them to avoid unnecessary duplication of datasets and effort. Among responding companies across Europe, 63,7% of businesses that offer (or plan to offer) data-driven products/services are repurposing existing data for new applications.

As the proportion of companies that repurpose existing data differs by just 7 percentage points from companies that self-generate new data, it is clear that many businesses are taking a flexible approach to sourcing data internally, being creative about optimising efficiency by rethinking what can be done with existing databases, but also open to investing in developing new ones where necessary.

Transport & Automotive industry leads the way in self-generating data for a new purpose

There are two industries where there is at least a 10-percentage point difference between the general and sectoral results with regard to respondents that are generating new data, with Financial Services standing at 54,2% and Transport & Automotive standing at 80%.

Real Estate & Infrastructure sector leads the way in repurposing data for a new purpose

For using existing data that was not initially intended for new purposes, most sectors do not significantly diverge from the general results. The exception concerns companies in the Real Estate & Infrastructure sector, standing at 81,3% of businesses that offer (or plan to offer) data-driven products/services, which is 17 percent higher than the general results. It is also one of three sectors where the proportion of companies that repurpose existing data is at least equal to or higher than the proportion of businesses that self-generate new data for novel purposes. The other two sectors, Financial Services and Life Sciences & Healthcare, are known for their strong regulatory environments.

II. External data sources

Besides internal data sources, companies can also obtain data through external data collection activities. Though this approach entails higher regulatory scrutiny for some businesses, there is a wider range of options that companies can undertake to obtain required datasets. For this purpose, companies that offer (or plan to offer) data-driven products/services were given options from a range of external data sources to highlight their activities to better understand the trends within the corporate environment.

Customer-provided data sets are popular with over 80% of responding businesses

By far the most popular solution for obtaining external data concerns datasets from customers, with 82,2% of businesses that offer (or plan to offer) data-driven products/services reportedly obtaining data through such sources. In addition, there are three external sources that at least a third of companies surveyed across Europe are utilising, with public data at 36%, database acquisitions at 32,2% and data acquisition through contractual agreements at 32,2%. Other freely available data sets, such as data scraping, and data obtained via APIs, are less represented.

The popularity of external data sources is linked to a few key aspects, namely regulatory concerns, cost, technical complexity, and specificity of the data obtained. Given that companies can predefine customer-provided data and tailor the parameters to their needs, coupled with ensuring that the data corresponds to legal requirements, customer interactions can be used to generate 'passive' data flows, particularly where interactions are online or digital, through data capture from tills or through reward pro-

Where does your company obtain (or will obtain) the data from?

External data sources

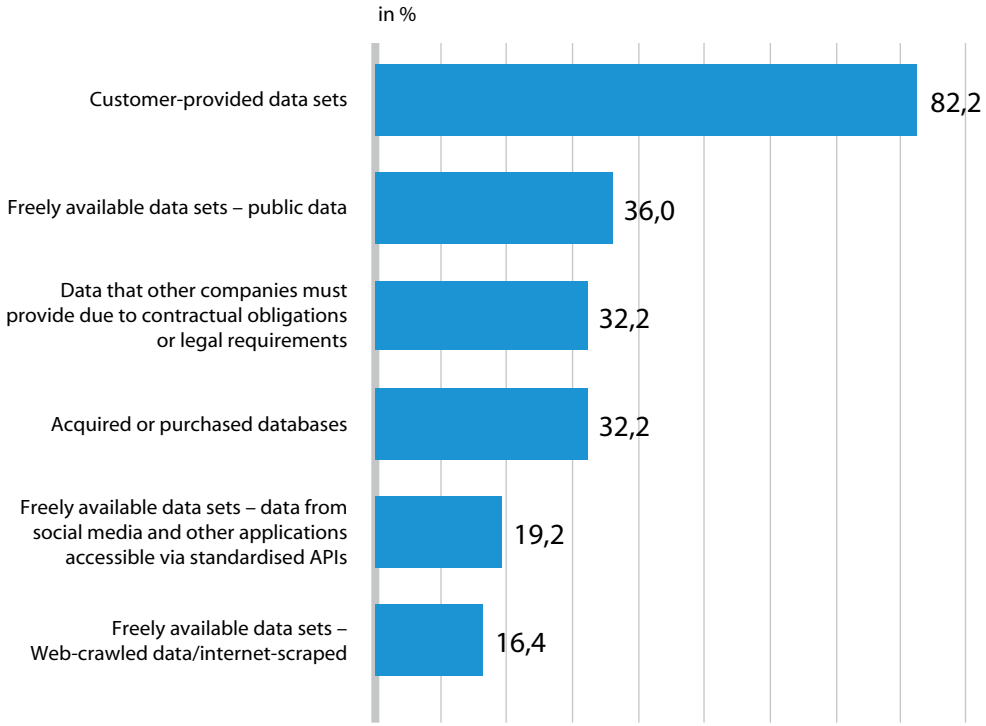


Figure 1.2.3

grammes. Other methods require a proactive engagement with a third party, which might be reflected by the lower proportion of responses. Customer-provided datasets are also the most popular external data source across the surveyed industries, ranging from 79,2% of those offering (or planning to offer) data-driven products/services in the Energy & Utilities sector to 91,4% in the Technology, Media & Telecoms sector, and 91.3% in the Life Sciences & Healthcare sector. This demonstrates how the approach is well-defined across European businesses with no significant discrepancies found.

Acquiring data through public data sources is also well-represented across industries, with at least a third of participating companies that offer (or plan to offer) data-driven products/services utilising them in all sectors besides Energy & Utilities and Life Sciences & Healthcare. This may well change with the development of European data spaces – energy and healthcare markets are a focus for these initiatives.

Financial Services businesses stand out for accessing several external data sources

Notably, the Financial Services industry uses various forms of data collection extensively, with two options – purchased databases and data obtained under contractual clauses – standing at 44% of those surveyed in the sector that offer (or plan to offer) data-driven products and services. Furthermore, 48% of companies within the sector utilise public data for their activities, the highest proportion surveyed. Data from

social media also stands at 5 percentage points above average, at 24%. The responses from this sector indicated the highest diversity of data sources amongst any of the surveyed sectors.

Similarly, the Technology, Media & Telecoms sector has been adept at obtaining data from various sources, with even the lowest result (obtaining data from social media and applications) standing at 22,4%. The sector also reports above average proportions in utilising web-scraped data for commercial purposes, at 27,6%.

61% of Life Sciences & Healthcare businesses obtain (or will acquire) data via database purchases

In terms of the purchasing of databases, only three sectors surveyed diverge less than 10 percentage points from the general results. Notably, Life Sciences and Healthcare prioritises obtaining data through database purchases, with 60,9% of companies that offer (or plan to offer) data-driven products/services utilising such methods. This amounts to nearly twice the general average.

The sector with the least amount of variance is the Energy & Utilities industry. With all options standing at below-average proportions, companies within the sector do not seem to have a clear methodology for their data collection activities.

"Data-driven business models are becoming increasingly important in the Energy & Utilities industry as well. However, the process is still in its early steps and specific data-strategies will need to be substantiated and harmonised in the future."

Jonathan Marsh, President of ECLA and International General Counsel, TotalEnergies Marketing & Services

We also looked at how companies that have opted for one data acquisition approach treated other methods.

By looking through this lens, it became clear that companies that collect external data beyond customer-provided datasets are more likely to use a larger variety of options. This may reflect the technical capability of companies, as businesses with established processes for obtaining data through social media platforms or scraping data from the web may have a more comprehensive understanding of data acquisition possibilities.

Osborne Clarke view

Thomas Devred ✉
Partner, France
Further information

"Data is not only of interest to Life Sciences companies, but also to health authorities who want to know if products and devices have demonstrably made patients' lives better, so that they can optimise national health programmes. Data is at the heart of healthcare modernisation, but is going to require us to align stakeholders and balance their commercial, ethical and legal requirements. It's an incredibly complex task, as even within EU countries, sensitivities around the secondary use of health data vary enormously."

Where does your company obtain (or will obtain) the data from?

External data sources

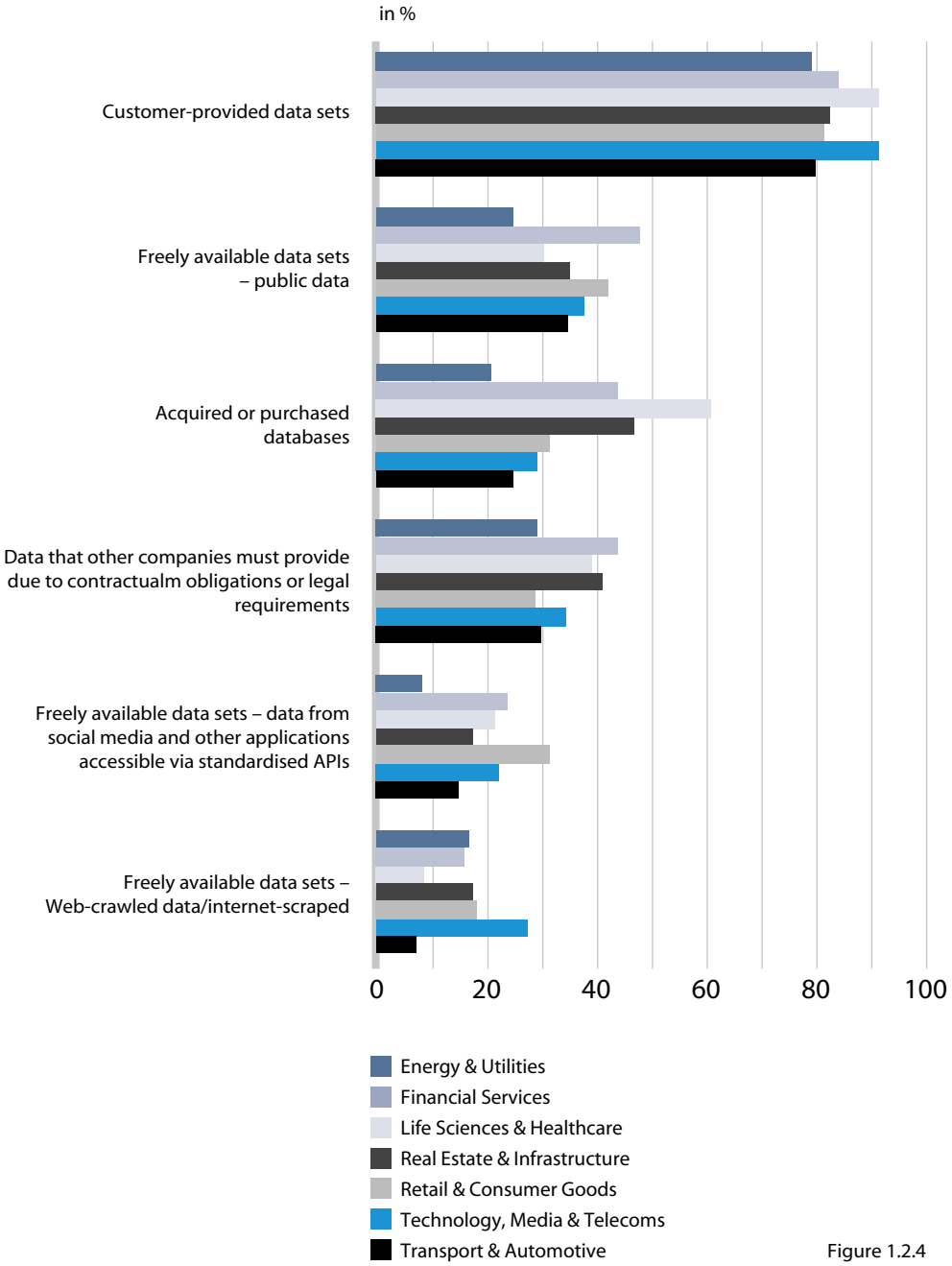


Figure 1.2.4

Where does your company obtain (or will obtain) the data from?

Additional data points – what did 100 % of respondents who chose a specific option also choose

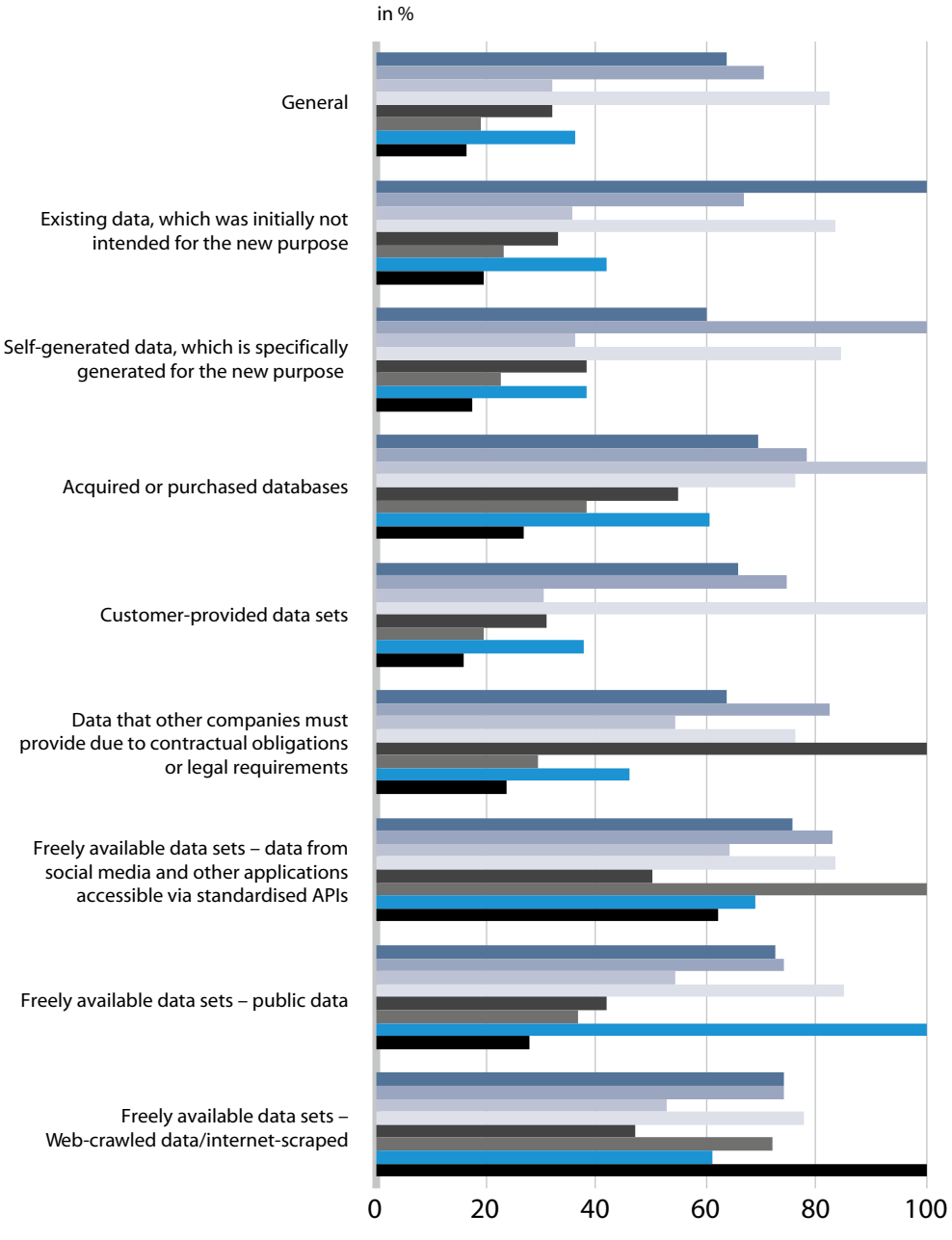


Figure 1.2.5

B. Developing & distributing data-driven products/ services

The next aspect concerns how data-driven products/services are developed and distributed within companies. For this purpose, participants of companies that offer (or plan to offer) data-driven products/services were asked to highlight their development and distribution approaches. The two aspects were separated into two sub-questions, with options given based on widely utilised approaches.

67,5% of responding companies that offer (or plan to offer) data-driven products/services develop their data-driven products/services through fully integrated internal teams. This was the only option that reached a 50% threshold within the general results. In addition, 24,5% of responding companies have opted to entrust a sister company with developing their product/service line. Commercial third parties also play a large role in the developing of data-driven products/services. 42,5% of companies have opted to collaborate on developmental projects with external businesses. A further 28,3% of businesses have decided to fully outsource their development.

How does your company (or is your company planning to) develop and distribute data-driven products/services?

Development …

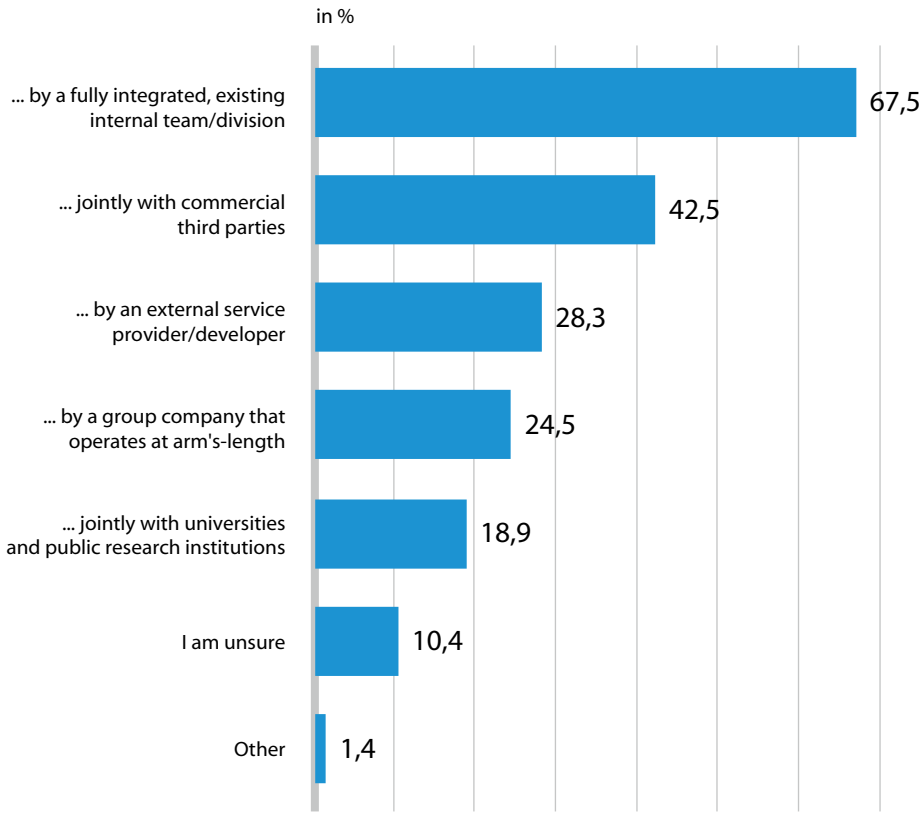


Figure 1.2.6

How does your company (or is your company planning to) develop and distribute data-driven products/services?

Development …

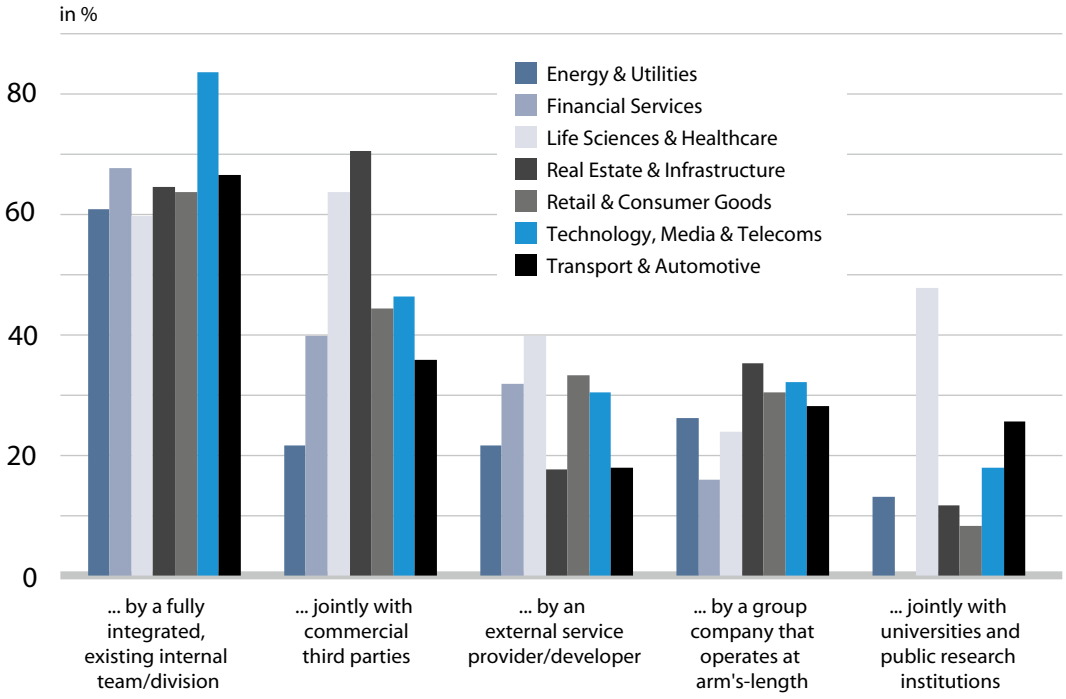


Figure 1.2.7

It should be noted that companies utilise a variety of approaches for their developmental projects, dependent on the specificities of the data-driven product/service. For example, when looking at the raw data, of the responding companies that have developed a product/service range jointly with commercial third parties, 72,5% have also had products/services developed internally by an existing internal team. Similarly, companies that have fully outsourced development for a specific project to an external provider, also have a 72,6% share of companies that have completed the developmental phase by an internal team.

Real Estate & Infrastructure and Life Sciences & Healthcare businesses are most likely to collaborate with commercial third parties

Although utilising existing internal structures for development remains a popular option throughout the surveyed sectors, in particular the Technology, Media & Telecoms sector, where 83,9% of businesses that offer (or plan to offer) data-driven products/services have chosen this option, in sectors such as Real Estate & Infrastructure and Life Sciences & Healthcare, joint collaborations with commercial third parties see a higher proportion of companies represented. In Real Estate & Infrastructure, 70,6% of participants of companies that offer (or plan to offer) data-driven products/services reportedly develop data-driven products and services together with commercial third parties, whereas 64% of companies in the Life Sciences & Healthcare industry have opted to do so. This contrasts the general results and sectors such as Energy & Utilities, where only 21,7% of companies have opted to take this route.

The Life Sciences & Healthcare sector has the largest variety overall when considering the developmental routes that a company can take. Besides joint collaborations with external providers, 40% of companies have also delegated development to third parties. Furthermore, 48% of participating companies that offer (or plan to offer) data-driven products/services have collaborated with research institutions in the development phase. This is the only industry where collaboration with universities is being done to this extent and signifies the role that public research institutions have traditionally played in innovation within the sector.

Conversely, none of the respondents from the Financial Services sector have collaborated with public research institutions in the development phase. Its distribution reflects the general results well, with some variance seen within the sector regarding the usage of sister companies.

The proportion of commercial third parties utilised for distribution purposes, as opposed to development purposes, is noticeably lower. Though 65,8% of companies that offer (or plan to offer) data-driven products/services still distribute through an integrated team, joint and outsourced distribution with external providers decreases by 12 and 15 percentage points, respectively. Similarly, only a marginal proportion of companies reported joint distribution with universities and similar public research institutions. This is unsurprising, given that companies are interested in controlling the distribution flow of their product/service line. That the development and distribution proportions remain similar for internal teams

How does your company (or is your company planning to) develop and distribute data-driven products/services?

Distribution …

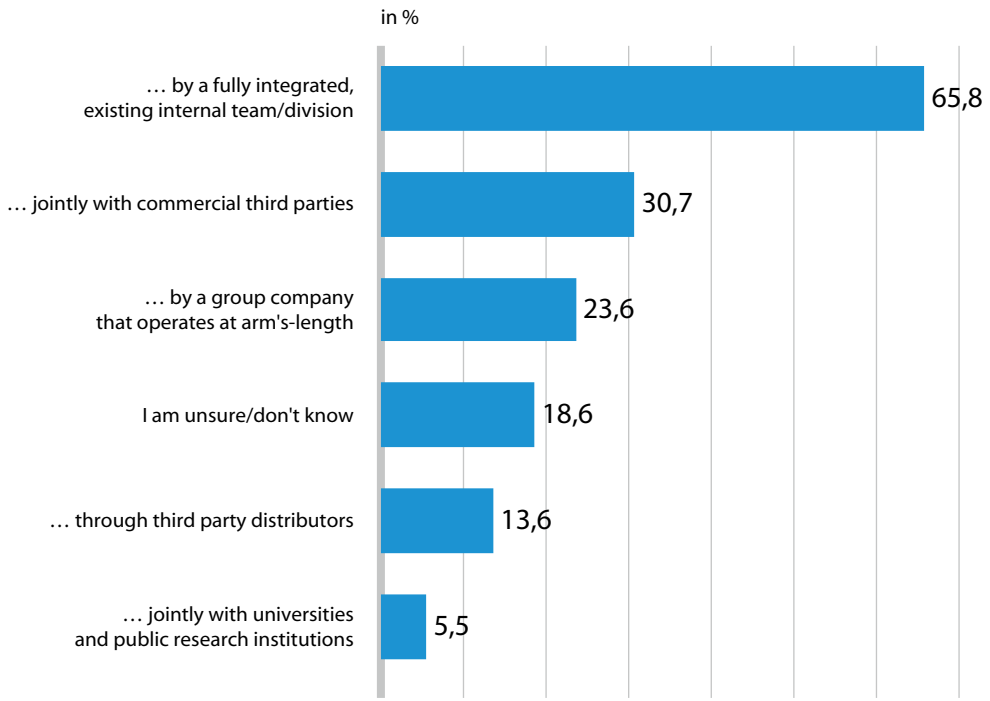


Figure 1.2.8

How does your company (or is your company planning to) develop and distribute data-driven products/services?

Distribution …

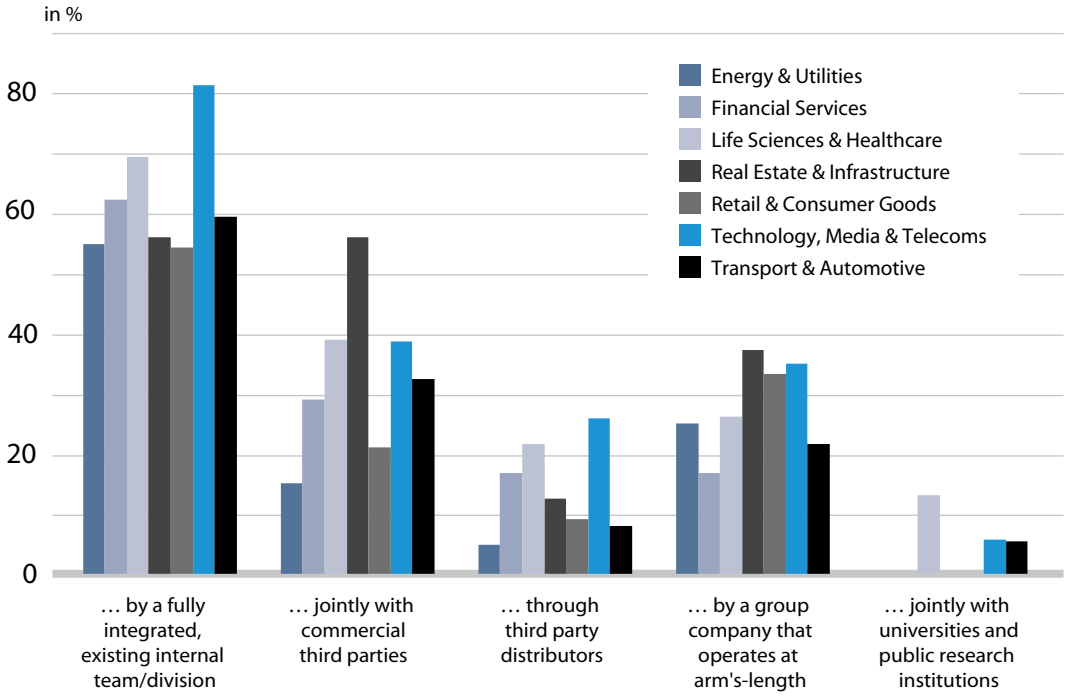


Figure 1.2.9

and group companies illustrates how the two phases are strongly linked for businesses.

Across sectors, distribution through an integrated team remains the most popular solution, which largely reflects the developmental phase. Like the strength of in-house development, 81,5% of companies that offer (or plan to offer) data-driven products/services in the Technology, Media & Telecoms sector have opted to distribute their data-driven products/services through existing internal divisions. Though joint distribution with commercial entities stands at a lower proportion compared with the development phase, it is still widely utilised in a few industries, with 56,3% of Real Estate & Infrastructure, 39,1% of Life Sciences & Healthcare, and 38,9% of Technology, Media & Telecoms companies doing so, respectively.

1.3 THE COMPANY LAWYERS' VIEW ON DATA-DRIVEN BUSINESS MODELS

67,3% of companies report legal and regulatory obstacles as one of the biggest hindrances.

The final Chapter of this empirical Part 1 deals with the challenges and obstacles with which European companies are faced when introducing and implementing data-driven business models. The opinions expressed under this Chapter are largely subjective and reflect the perspective of legal departments across Europe. The fact that so many in-house lawyers appear to find a number of difficulties in supporting data-driven business models can be interpreted as a reflection of the considerable shift in skillsets needed in the legal department as a business undergoes digitalisation. It may also reflect a historical secondary role for the legal team in digitalisation projects, and in developing new data-driven products and services. As data and digital regulation expands, there is a clear opportunity for in-house counsel to embed themselves in the heart of this project, delivering compliance by design and playing a central role in enabling the success of these projects.

A. Largest obstacles for introducing data-driven business models

All participating lawyers were asked to highlight their largest obstacles in implementing data-driven business models within their companies. Respondents were given a wide range of options to choose from, with a maximum of five choices allowed. To gain a clearer understanding, different thematic issues have been consolidated for the general results. In addition, the sectoral results highlight the five most persistent obstacles currently present within each industry.

67% of companies say legal and regulatory obstacles hinder the implementation of data-driven business models

Legal restrictions: 67,3% of companies report legal and regulatory obstacles as one of the biggest hindrances. This is also the option most represented, as it is the only option within the general results that exceeds a 40% threshold. Tax-related obstacles, however, see marginal representation, with just 5,5% of companies reporting it as one of the five biggest challenges.

Security concerns: 38,2% of companies see cybersecurity risks as a major obstacle. This is the second most represented concern within the general results. The option saw notable variance across the surveyed industries, with a 10+ percentage point swing in both directions for some sectors. This supports the notion that certain industries, which regularly deal with sensitive data, may have higher concerns than other sectors.

Business deficiencies: Various deficits regarding the organisational and substantive side of the business are represented. 36,2% of companies report that their companies lack the necessary experience and skillset required within their divisions to implement data-driven products/services. A further 25,6% of companies identified their internal resources to be lacking for proper implementation. In addi-

In your experience, what are the biggest obstacles to implementing data-driven business models?

Up to 5 options can be chosen

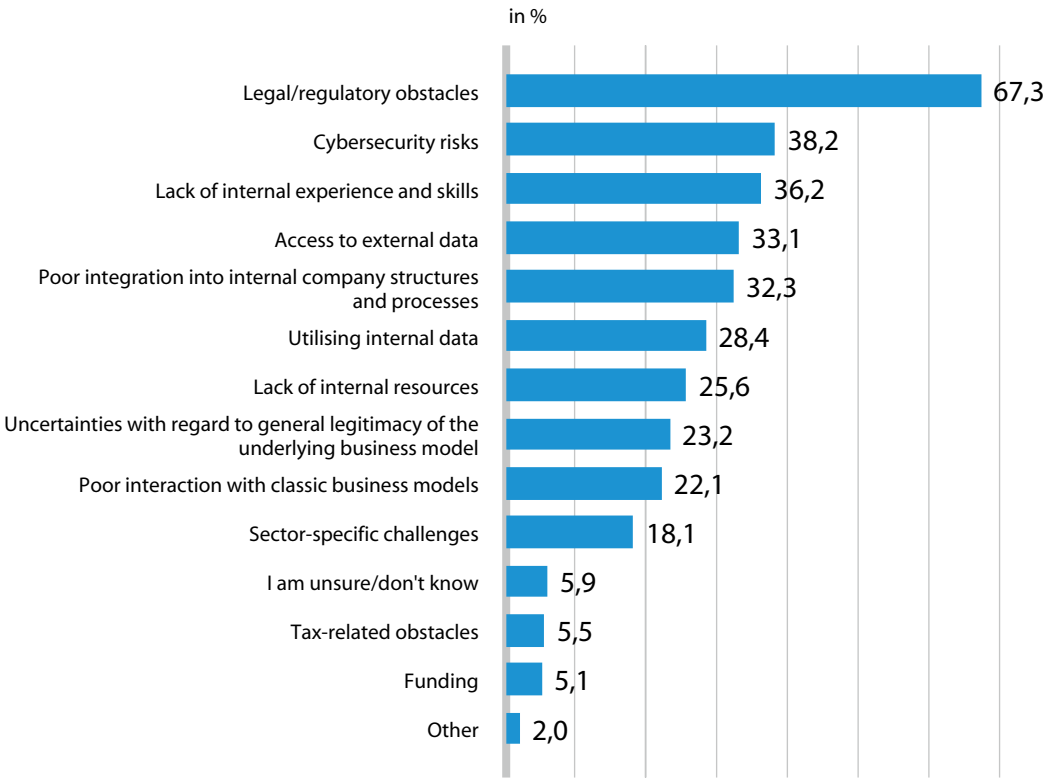


Figure 1.3.1

tion, 32,3% of companies see the integration of data-driven business models within their internal company structures and processes to be lacking. 22,1% of respondents report poor interaction between the data-driven business models and the classic business models upon which the company is set up. 23,2% of participating lawyers also work for companies that are concerned about the legitimacy of the data-driven business model.

That one in three responding lawyers currently considers their organisational structure and processes to be deficient in introducing data-driven business models is concerning. This could indicate that such companies do not have adequate data retention and organisational practices in place to facilitate the necessary data collection activities. In contrast to a lack of expertise, which can be improved by introducing key personnel, changing company structure and culture can be an uphill battle that has been a focal point in the discussion on disruptive innovation within business communities for the past two decades.

Limitations with data: A significant proportion of companies see access to external data, at 33,1%, and utilising internal data, at 28,4%, as some of the biggest obstacles their businesses face when implementing data-driven business models.

Sector-specific challenges: 18,1% of businesses have identified challenges specific to their industry as hindering the implementation process.

In your experience, what are the biggest obstacles to implementing data-driven business models?

Energy & Utilities: Top 5 options chosen

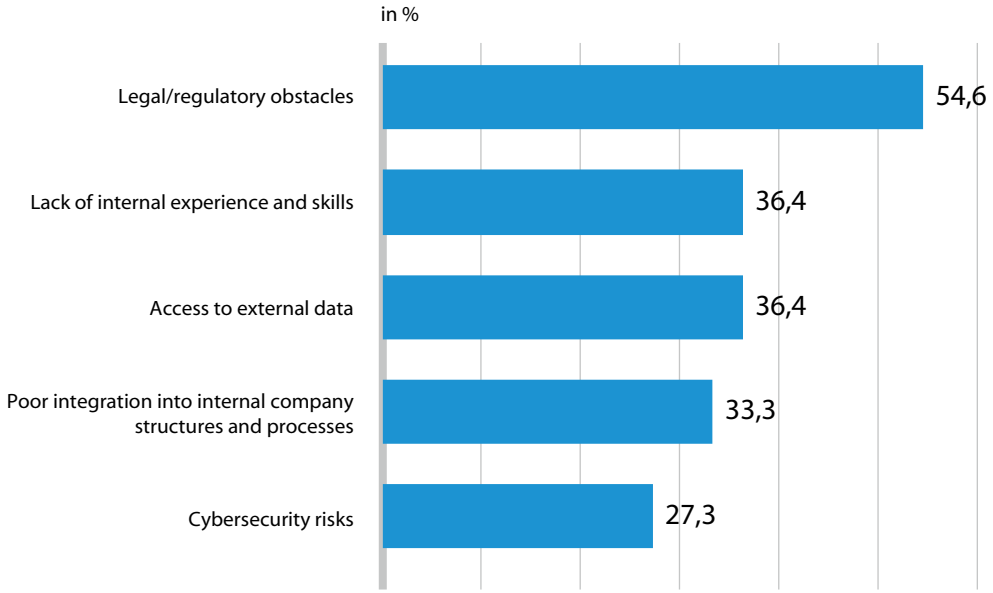


Figure 1.3.2

In your experience, what are the biggest obstacles to implementing data-driven business models?

Financial Services: Top 5 options chosen

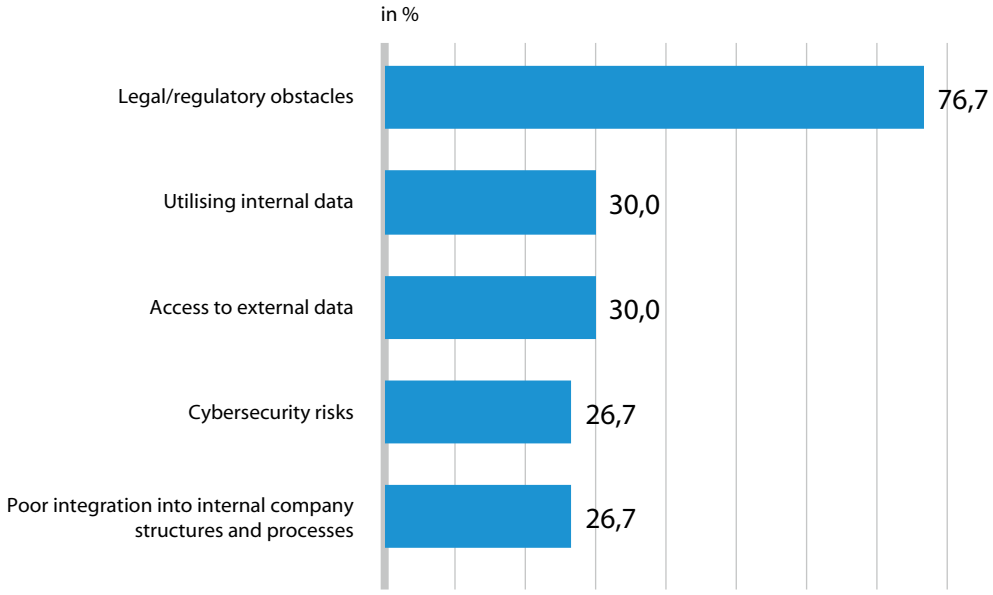


Figure 1.3.3

Financial backing: Just 5,1% of companies report funding to be one of the five biggest obstacles their organisations are concerned about when implementing data-driven business models.

Energy & Utilities: 54,6% of responding companies have identified legal and regulatory obstacles as a constraint for their businesses. 36,4% of respondents see external data access as a major obstacle. A lack of internal experience and skillsets required for implementing data-driven business models is reported by a further 36,4% of participating companies. Poor integration of data-driven business models into internal company structures and processes is an issue for 33,3% of companies within the sector. 27,3% of companies also see cybersecurity risks as a major obstacle for a proper implementation process.

Financial Services: 76,7% of companies have identified legal and regulatory obstacles as one of the five biggest issues. 30% of companies are also concerned about access to external data. A further 30% see improper internal data utilisation as a hindrance. 26,7% of respondents report poor integration into internal company structures as a challenge. In addition, cybersecurity risks are also one of the five biggest obstacles for 26,7% of participating companies. However, it sees the lowest proportion of companies reporting it as a major obstacle across the surveyed sectors. This could indicate how cybersecurity-related concerns have been at the forefront within the industry for a longer period in comparison with other sectors and how companies in the Financial Services industry have already addressed a large proportion of the challenges that cybersecurity risks bring. Furthermore, the sector sees below-average representation of companies that are concerned about a lack of internal experience and skills, as it is not one of the five most popular options. This highlights the maturity that the industry enjoys, given that it was one of the earliest sectors to target data-related activities.

"There is a trend across all the industries showing a high degree of uncertainty around the regulation of data usage. We can see a clash between tech and media businesses that operate under a data monetisation model and principles-based regulations like GPDR. Alot of regulations are still in their infancy regarding their applicability to areas like AI. By necessity, businesses must interpret new regulations across technologies and techniques that may not have been contemplated by the regulators in drafting the laws. Thus far, the guidance we see coming from Europe and from regulators on implementation does not delve deeply enough into the technical nuances of possible data usage. Without more technical guidance, these businesses will have to continue operating with great uncertainty, which is of course not hugely conducive to innovation or competition, especially for SMEs in the space."

Sally-Anne Hinfey PhD,
Vice President and Deputy GC Legal
(Global Privacy), Momentive-AI

In your experience, what are the biggest obstacles to implementing data-driven business models?

Life Sciences & Healthcare: Top 5 options chosen

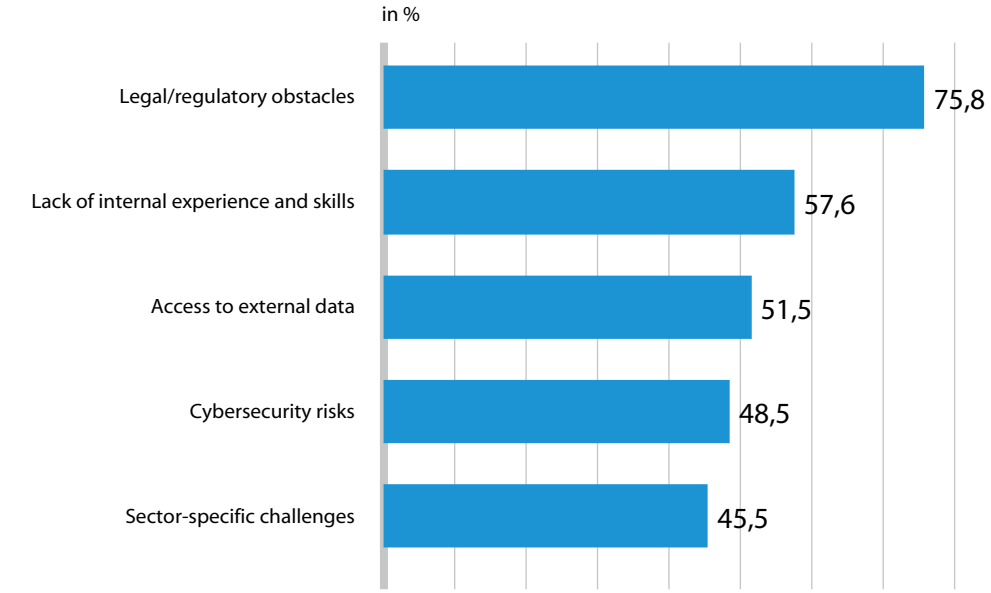


Figure 1.3.4

In your experience, what are the biggest obstacles to implementing data-driven business models?

Real Estate & Infrastructure: Top 5 options chosen

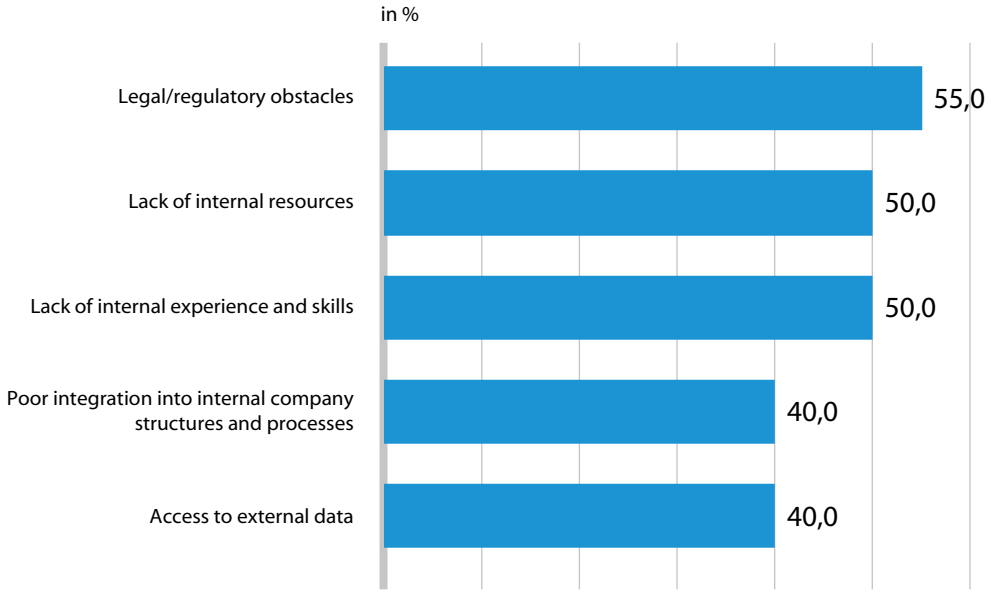


Figure 1.3.5

In your experience, what are the biggest obstacles to implementing data-driven business models?

Retail & Consumer Goods: Top 5 options chosen

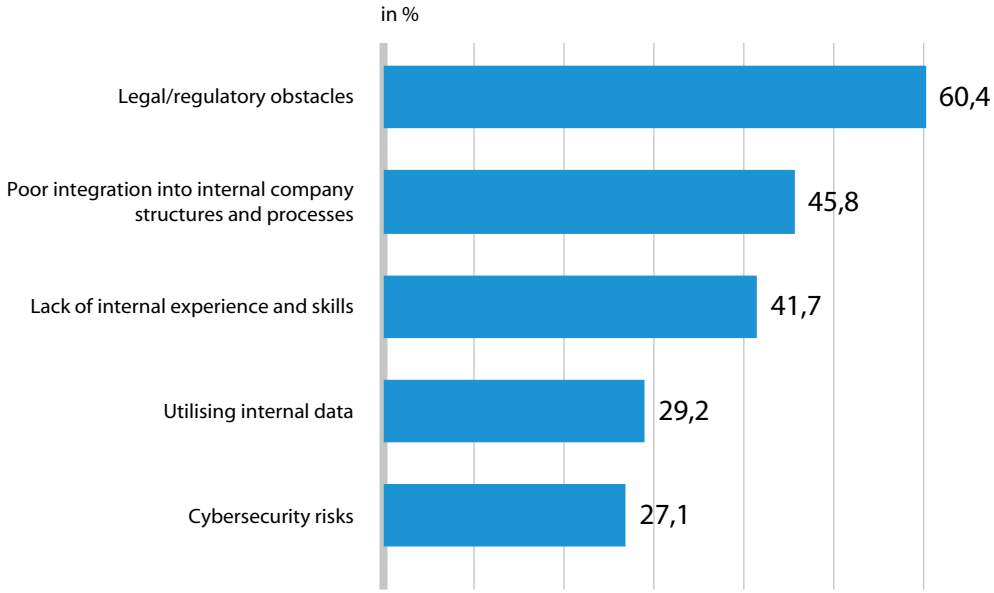


Figure 1.3.6

Life Sciences & Healthcare: 75,8% of participating lawyers see legal and regulatory obstacles as one of the five biggest concerns to introducing data-driven business models within their companies. In addition, 57,6% of participants have identified the internal experience and skills within their units as lacking. 51,5% of participants report access to external data as a hindrance. 48,5% of respondents see cybersecurity risks as a major obstacle. 45,5% of companies also report sector-specific challenges as a major obstacle, the only industry where this is reported as one of the five most common options. The cybersecurity concerns within the industry stand at 10 percentage points above the general results, demonstrating the threat that targeted attacks bring to the sector.

Real Estate & Infrastructure: 55% of companies consider legal and regulatory issues as a major obstacle. 50% of companies also report a lack of internal experience and skills as an issue. A further 50% of respondents are concerned with a lack of internal resources. This is double the proportion that the general results highlight and it is the only sector where internal resource concerns exceed a 30% threshold. 40% of companies within the industry report access to external data as one of the five biggest challenges. Another 40% consider the integration of data-driven business models into internal company structures and processes as challenging.

Retail & Consumer Goods: 60,4% of companies report legal and regulatory obstacles as a point of concern. 45,8% of participating lawyers also see poor integration of data-driven business models into internal company structures and processes as an obstacle. 41,7% of participating companies report a lack of internal experience and skills as hindering the implementation process. 29,2% of respondents also see internal data utilisation as a challenge. 27,1% also report cybersecurity risks as one of the five biggest challenges.

In your experience, what are the biggest obstacles to implementing data-driven business models?

Technology, Media & Telecoms: Top 5 options chosen

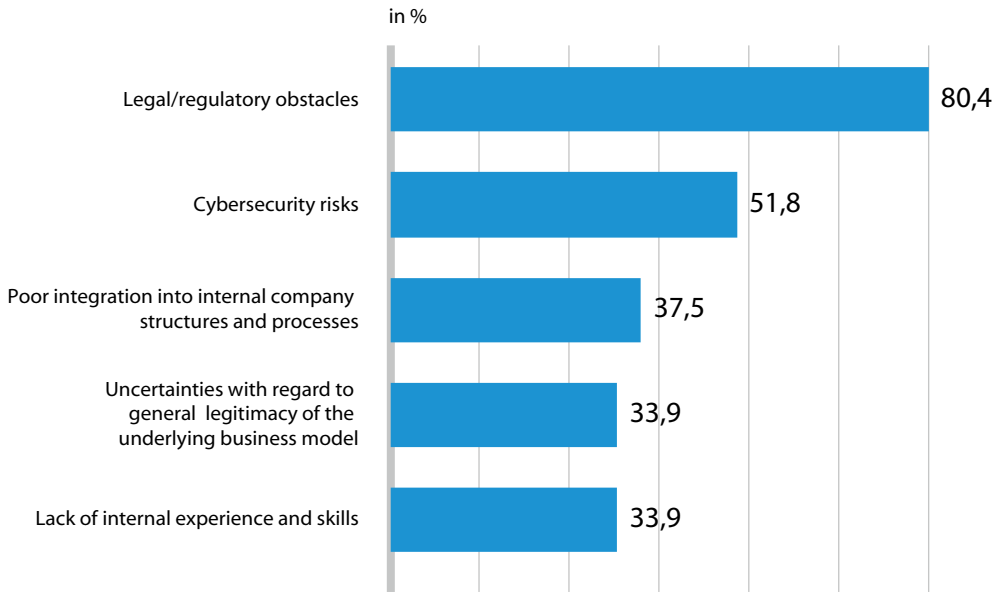


Figure 1.3.7

Technology, Media & Telecoms: 80,4% of responding companies report legal and regulatory obstacles as one of the five biggest challenges. A further 51,8% of participants identify cybersecurity risks as an obstacle. No other sector saw legal/regulatory obstacles exceed the 80% threshold, and no other sector saw cybersecurity concerns highlighted by over 50% of the responding companies. 37,5% of lawyers see poor integration into internal company structures and processes as a hurdle. 33,9% of companies report a lack of internal experience and skills as an obstacle. Another 33,9% work for companies that see uncertainties regarding the general legitimacy of the underlying business model.

The high proportion of responding lawyers reporting legal/regulatory issues could reflect the fact that innovation in this sector is often in areas where there is no bespoke regulation and so a risk-based assessment has to be made about whether and how regulation designed for other scenarios might nevertheless be relevant. The response may also reflect regulators' and policymakers' focus on this sector. Currently, there are multiple major legislative proposals being discussed, both at EU level, such as the Digital Services Act and the Digital Markets Act, and at national level across Europe.

Transport & Automotive: 67,4% report legal and regulatory obstacles as one of the five biggest obstacles to implementing data-driven business models. 46,5% report cybersecurity risks as concerning. 44,2% also report a lack of internal experience and skillset within their businesses. In addition, 39,5% see a lack of access to external data as a major hurdle. 34,9% consider the implementation of data-driven business models to integrate poorly with existing internal company structures and processes.

In your experience, what are the biggest obstacles to implementing data-driven business models?

Transport & Automotive: Top 5 options chosen

Figure 1.3.8

Osborne Clarke view

Dr Jens Schefzig ✉
Partner
Germany
Further information

"Businesses across Europe are struggling to navigate the regulatory landscape when implementing data-driven business models. This is an important and worrying finding. A sound understanding of the applicable legislation is key to the efficient development of successful data-driven business models. Companies that lack this understanding risk investing in business models that cannot then be implemented as planned, wasting valuable resource in a competitive global market. This finding is all the more concerning given upcoming EU legislation, including the Digital Markets Act, the Data Act and the Artificial Intelligence Act, which could be perceived as adding further complexity. Current and future data regulation should be proactively considered when making all decisions regarding data-driven business models."

B. The outlook of company lawyers on the legal framework and on their businesses regarding data-driven business models

Having established the most concerning obstacles for companies surveyed across Europe, participants were given several statements and asked to rate them. In the first statements, participants were asked to voice their opinion regarding the current legal and regulatory framework concerning the implementation of core data-driven business models. The statements aim to establish whether participating lawyers consider the framework to be either well-structured or too complex, clearly understandable or confusing, supportive or obstructive, and stable or unstable.

Two-thirds of businesses say the legal framework is too complex

68,1% of respondents consider the framework to be too complex for implementing data-driven business models, with just 11,1% seeing it as well-structured. A further 20,9% of participating lawyers are unsure about the statement. In addition, 63,4% consider the framework to be confusing, with 15,7% seeing it as being clearly understandable and a further 20,8% being unsure. Both the positive responses are surprisingly low and highlight the discontent that

How do you assess the current legal/regulatory framework with regard to the implementation of core data-driven business models?

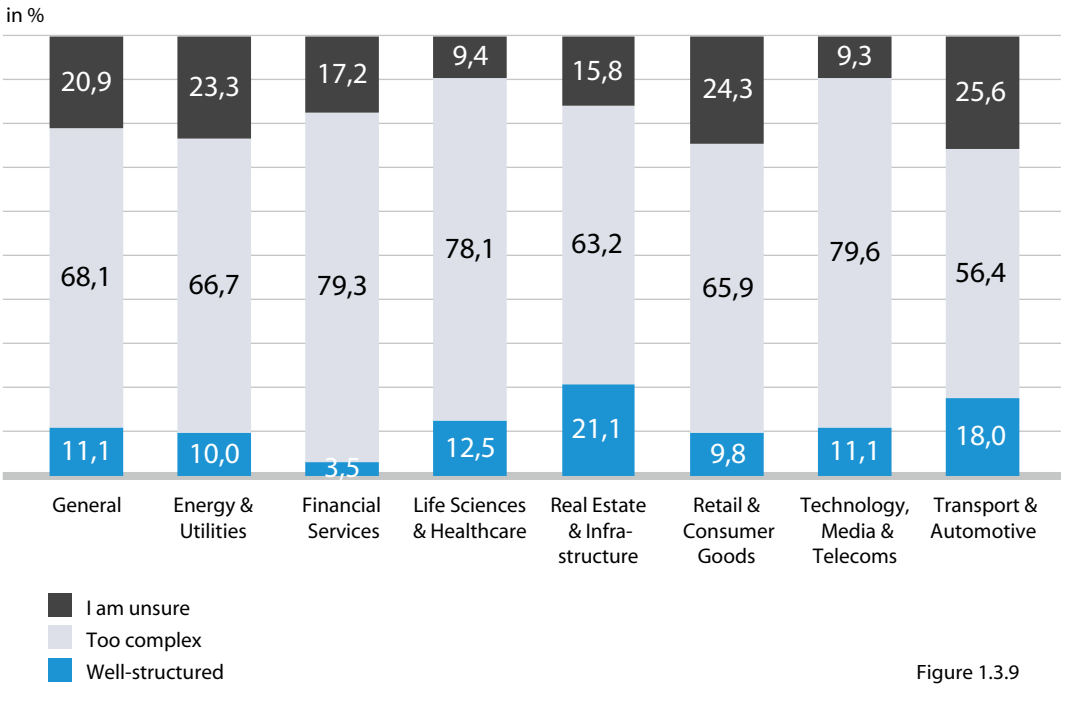


Figure 1.3.9

How do you assess the current legal/regulatory framework with regard to the implementation of core data-driven business models?

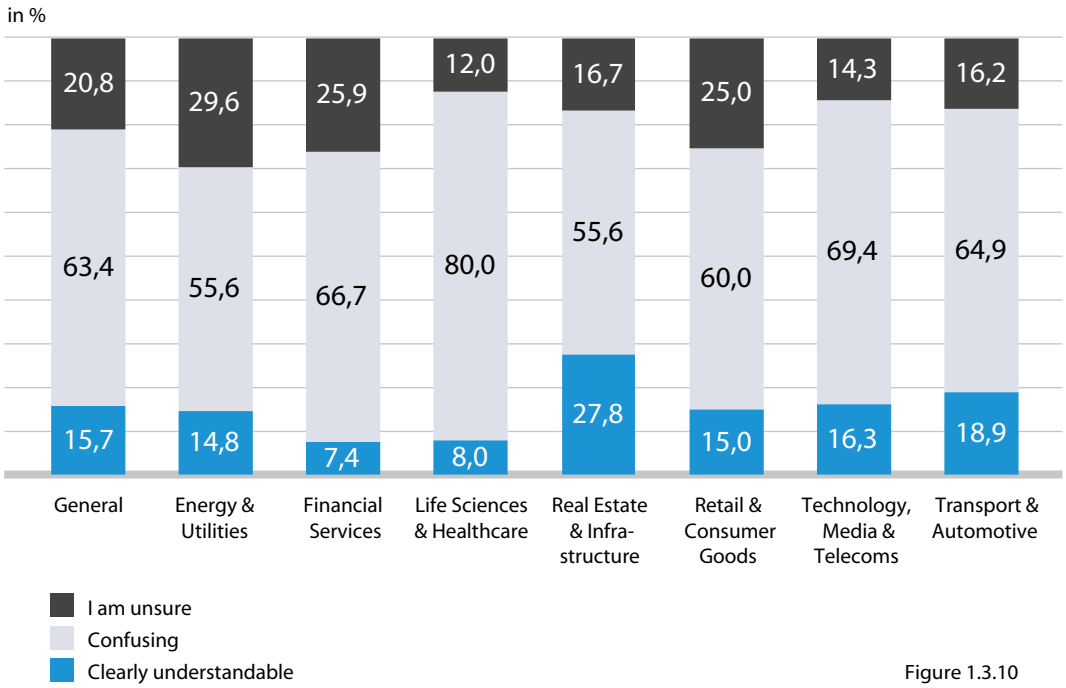


Figure 1.3.10

lawyers across Europe feel towards the legal/regulatory framework in place. That just one in ten company lawyers consider the framework in which they must work in to be well-structured should be a point of concern for European lawmakers. That two-thirds of respondents consider the framework to be confusing may reflect the shift in skills that is needed for in-house lawyers when their businesses are digitalising their operations.

In addition, just 11,4% of respondents consider the legal/regulatory framework to be supportive, with a further 55% considering it to be obstructive. A third of respondents were unsure about the assessment. The Transport & Automotive industry was the only surveyed sector where the Supportive proportion exceeded the general averages by 10 percentage points, at 21,2%. Three sectors saw a single-digit positive assessment, with Energy & Utilities and Financial Services at 3,7% and Real Estate & Infrastructure at 6,7%.

Furthermore, 22,6% of general respondents see the legal/regulatory framework to be stable, with a further 49,5% considering it to be unstable. Another 27,9% were unsure. The Transport & Automotive sector saw the Stable proportion exceed the general average by at least 10 percentage points, at 37,5%. In contrast, 70% of companies in the Technology, Media & Telecoms industry consider the framework to be unstable for the purposes of implementing core data-driven business models, 20 percentage points above the general averages.

Next, participants were given two True or False statements regarding data utilisation within their organisations. The first statement concerns whether companies have either already been involved in a dispute on data rights or access to data.

How do you assess the current legal/regulatory framework with regard to the implementation of core data-driven business models?

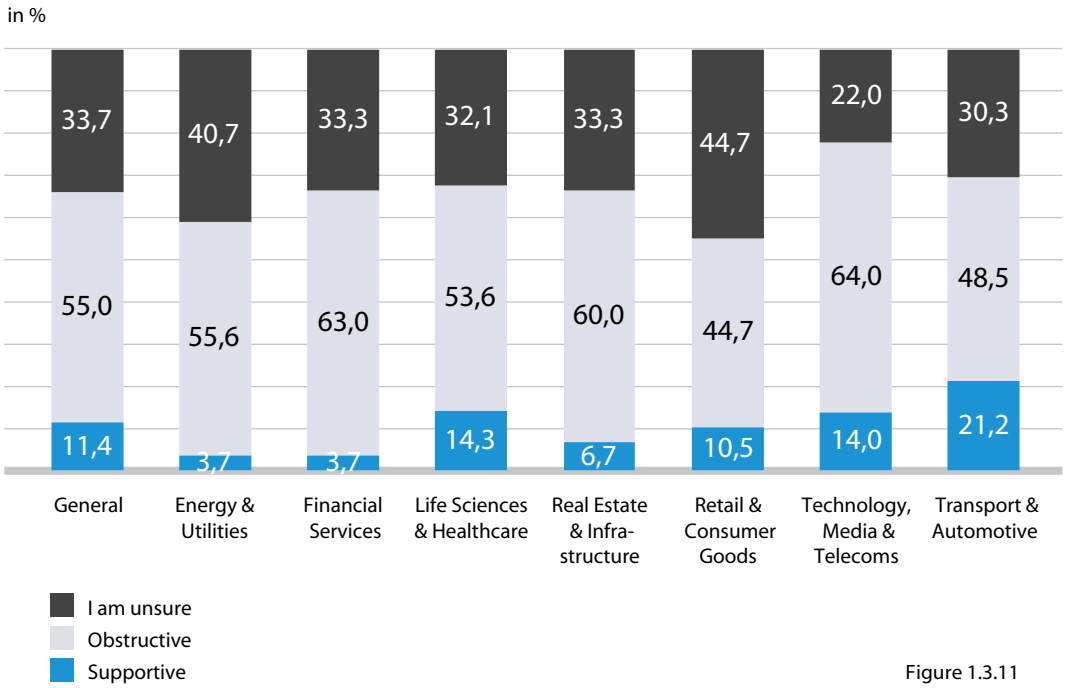


Figure 1.3.11

How do you assess the current legal/regulatory framework with regard to the implementation of core data-driven business models?

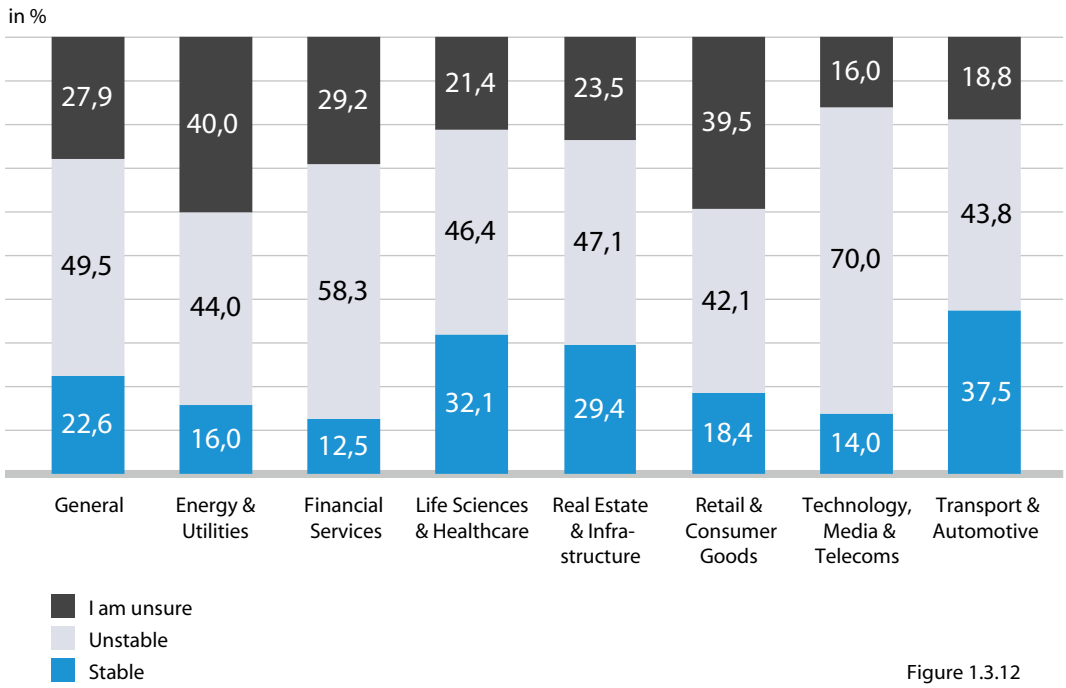


Figure 1.3.12

Which of the following statements apply to your company?

Your company has been involved in a dispute on data rights and/or access to data before:

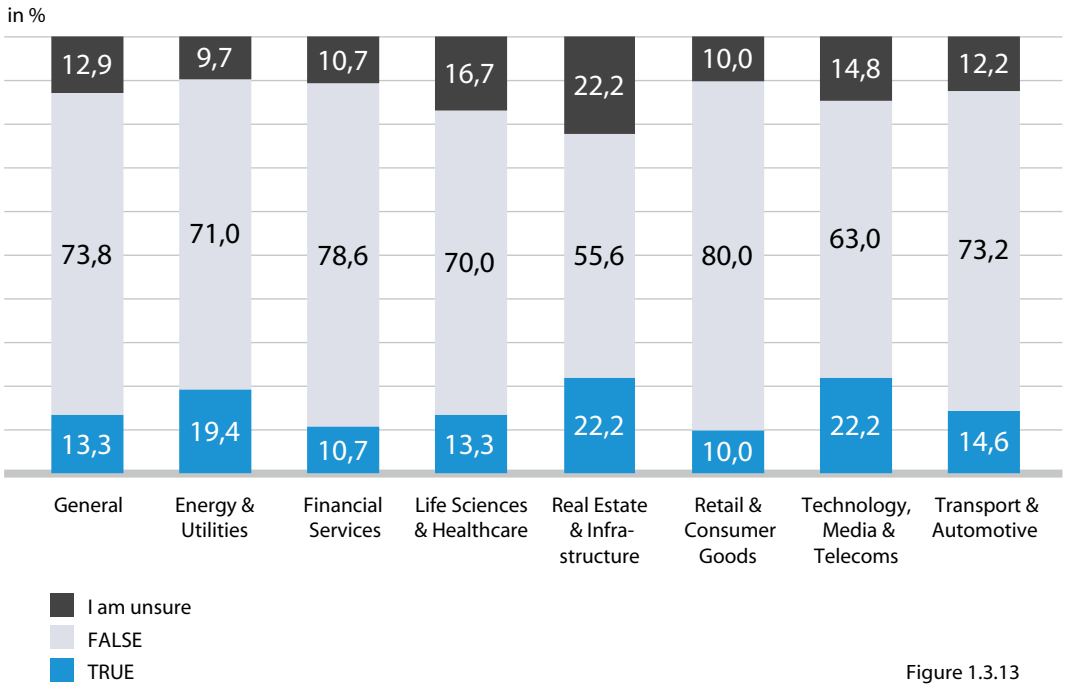


Figure 1.3.13

Which of the following statements apply to your company?

Your company has already been involved in the strategic acquisition of data

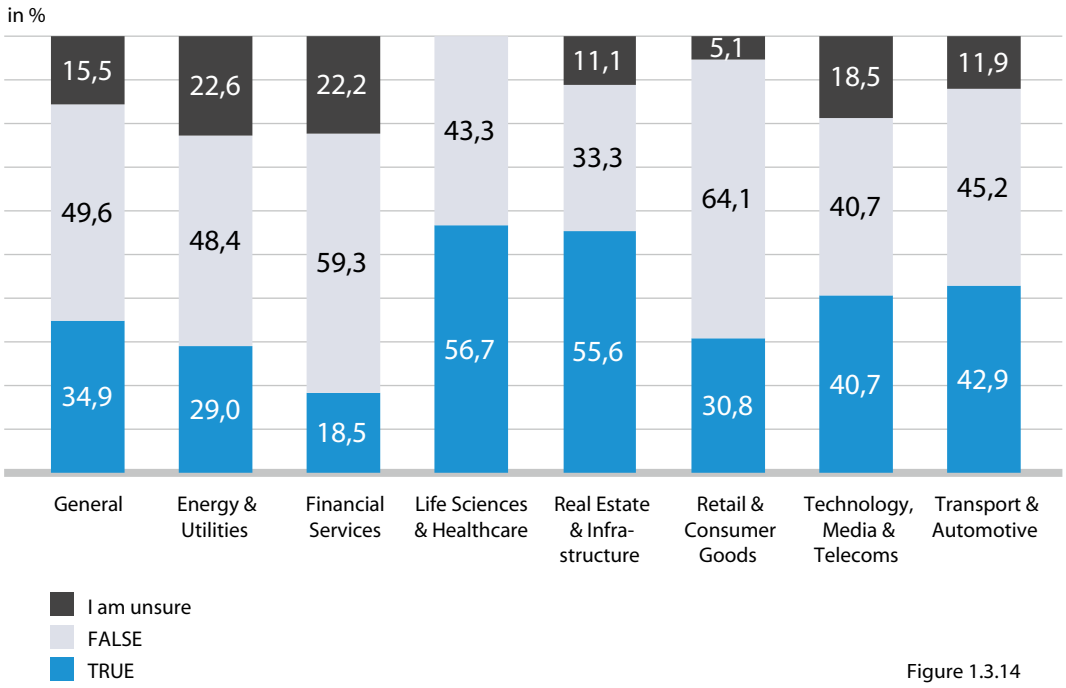


Figure 1.3.14

One in five businesses in Energy & Utilities, Real Estate & Infrastructure and Technology, Media & Telecoms sectors have been involved in a data dispute

Just 13,3% of participating lawyers answered True, with a further 73,8% answering False. 12,9% of respondents were unsure whether their company had been involved in such disputes. Three sectors demonstrate an increased proportion of True answers, with Energy & Utilities, at 19,4%, Real Estate & Infrastructure at 22,2%, and Technology, Media & Telecoms at 22,2%. Even though most companies across Europe have yet to face such a challenge, it should be considered a significant proportion that certain sectors already have one in five companies that have been involved in disputes on data rights/access to data. It will be interesting to revisit this topic once data-driven business models become more embedded in corporate structures and see how the proportion of True answers increases over time.

The second statement concerns whether responding companies have already been involved in the strategic acquisition of data.

One-third of businesses have been involved in the strategic acquisition of data

34,9% of respondents answered True to this statement. A further 49,6% answered False. 15,5% of respondents were unsure whether their company had been involved in strategic data acquisition.

Over one-half of Life Sciences & Healthcare and Real Estate & Infrastructure businesses have been involved in the strategic acquisition of data

There are notable sectoral differences regarding this statement. In the Financial Services sector, only 18,5% of responding lawyers have been involved in strategic data acquisition. In contrast, 56,7% of companies in the Life Sciences & Healthcare and 55,6% of companies in the Real Estate & Infrastructure industries have already been involved in the strategic acquisition of data. These are also the only two sectors where the proportion of True answers exceeds the proportion of False statements. The largest share of False statements can be found in the Retail & Consumer Goods sector, where 64,1% of respondents answered in the negative.

Osborne Clarke view

Karima Lachgar ✉
Partner, France
Further information

"The potential to exploit data (particularly when combined with AI) to produce new products and improved business models is well known within the financial services industry, as the rise of FinTech demonstrates. But the use of new technologies and business models in a heavily regulated industry, where the regulations don't contemplate this technology, can be challenging both for businesses and regulators. Financial services businesses and regulators need to take a collaborative approach and evolution is more likely than revolution."

Regarding the low proportion of True answers in the Financial Services sector, one must consider that the companies operating in the sector already collect a large volume of data tailored to their needs. Often, considering the cost involved, it is not reasonable for businesses in the industry to obtain additional datapoints externally, as companies can internally obtain the data in a much more effective manner. The regulatory framework also restricts the industry in sharing various datapoints of interest, which in turn encourages companies to set up internal processes to facilitate their needs.

Regarding the Retail & Consumer Goods industry, it is notable that it is the sector with the second lowest proportion of uncertainty amongst lawyers, as most respondents were able to provide a definitive answer. However, the proportion of True answers is slightly below average, with the proportion of False answers being 15 percentage points above the general results. This highlights the general sentiment found across this study: that the industry is trailing other surveyed sectors in many respects in the context of data-driven business models.

Next, participants were asked to rate statements about the activities of their company on a numbered scale, with 1 being the lowest score and 6 being the highest. The goal is to establish how strongly European companies feel about specific aspects about data related activities within their organisations. To provide clarity to the results displayed, the scores "1" and "2" have been consolidated into "Strongly disagree", the scores "3" and "4" into "Neutral", and the scores "5" and "6" into Strongly agree. Specific scores on a statement are elaborated to provide further insights whenever relevant. Participants were also able to choose Unsure/Not relevant if they deemed the statement to be inapplicable to their businesses.

The first statement asked participants to rate how relevant of a role real-time data is either currently playing or will play for their companies. 30,9% of respondents rated the statement with the highest score of "6", with a further 24,8% of participants rating the statement at "5", which amounts to 55,7% of respondents who strongly agreed. Just 9,6% of respondents disagreed with the statement. The average score across participants for this statement amounted to 4,6. In every sector except Life Sciences & Healthcare, at least 50% of respondents rated the statement either a "5" or "6", indicating a strongly positive result.

Over half of responding businesses have a data strategy in place

The second statement concerns whether companies currently have a data strategy in place. 36,1% of respondents strongly agreed with the statement. The average score for this statement amounted to 3,96. The Energy & Utilities and the Real Estate & Infrastructure sectors have the highest proportion of respondents strongly disagreeing with the statement, at 27,6% and 27,8%, respectively. The Financial Services industry sees the highest proportion of companies strongly agreeing with the statement, at 42,9%, and the lowest proportion of companies strongly disagreeing with the statement, at 10,7%. Most industries, however, largely resemble the general results.

The third statement elaborates on whether legal teams have implemented data strategies for companies that have one in place. 42,2% of respondents were neutral about the statement. Just 16,1% of participants strongly agreed with the statement, with a further 25,7% strongly disagreeing. The average score for this statement amounted to 3,3. Though there is some variance in the distribution of scores across the surveyed industries, most respondents across industries are neutral towards the statement. The Technology, Media & Telecoms industry, at 20,8% and the Financial Services industry, at 21,4%, are the only two sectors where at least 20% strongly agreed with the statement.

Which of the following statements apply to your company?

Real time data plays a relevant role for your company or will play a relevant role in the future:

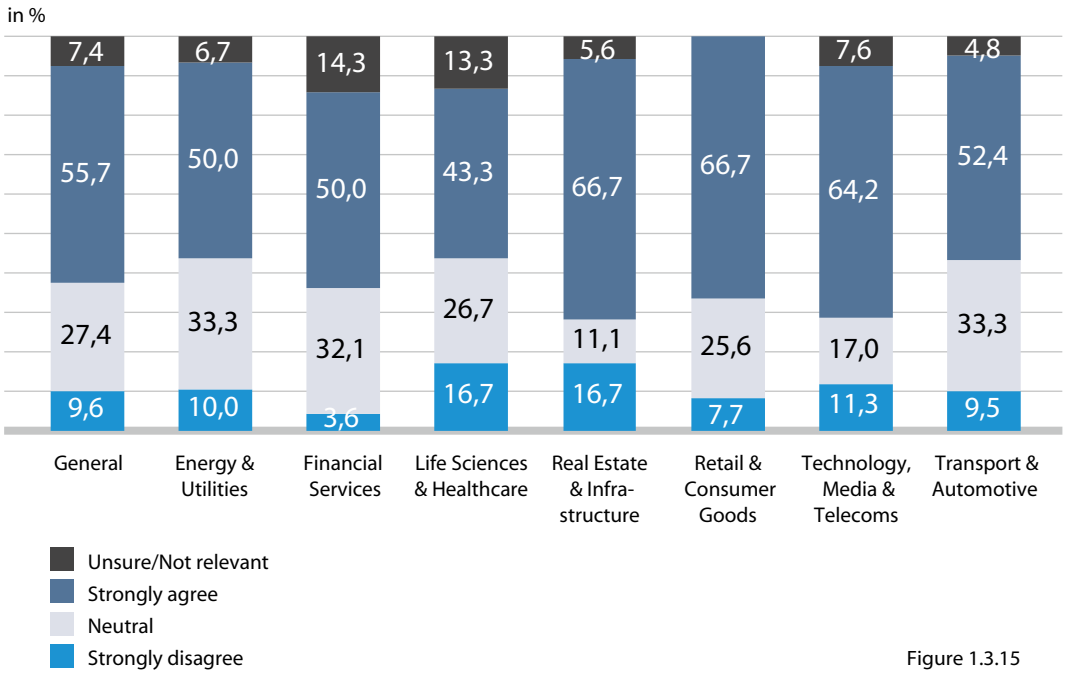


Figure 1.3.15

The fourth statement asked whether companies use contract templates that include provisions on data usage beyond data protection compliance issues. 40,2% strongly agreed with the statement. The average score for this statement amounted to 3,9. The only industry where at least 50% of participants strongly agreed concerns the Technology, Media & Telecoms sector. Companies in the Life Sciences & Healthcare industry see above average representation of neutral and strongly agreed responses, with a below average proportion of companies that

Osborne Clarke view

Philip Meichssner ✉
Partner, Germany
Further information

"While those surveyed indicate that Retail may be behind other sectors, our observation is that the industry is, in fact, quite sophisticated in their approach to data driven business models. However, there may well be a disconnect between the operational side of these businesses and their legal teams. We have definitely seen evidence of this."

Which of the following statements apply to your company?

Your company has a data strategy

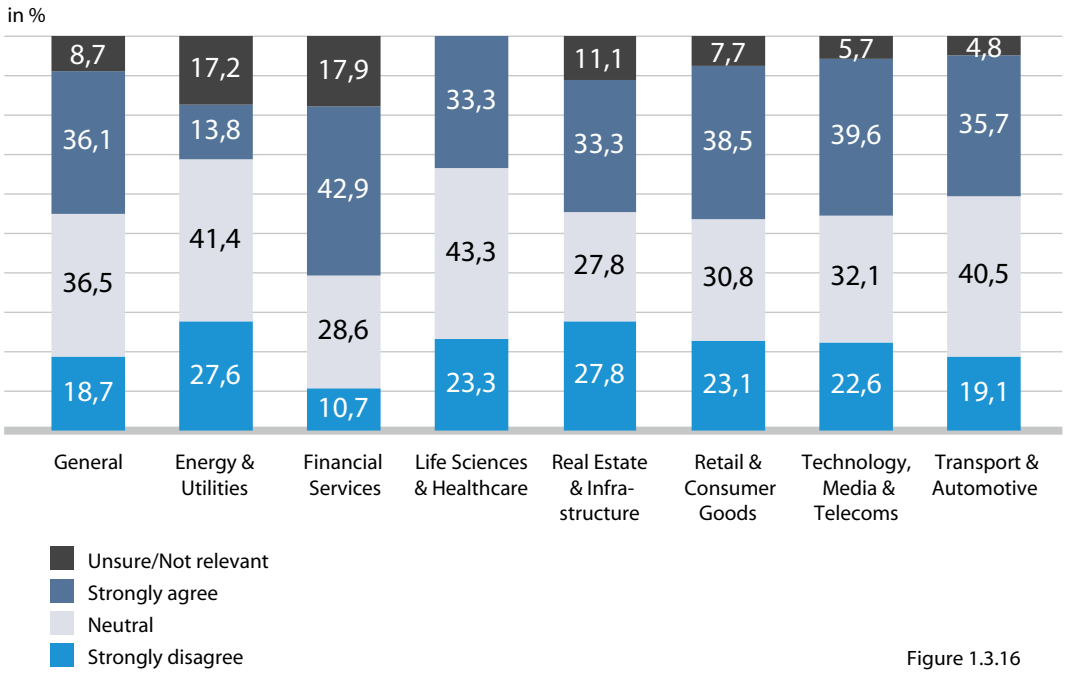


Figure 1.3.16

disagree with the statement. This could reflect the type of data that the industry is typically concerned with. Sensitive medical data will carry regulatory protections and businesses will need a comprehensive framework to obtain and utilise such data. The Financial Services industry sees the lowest proportion of companies that strongly disagree with the statement, at 10,7%.

The next statement concerns the readiness for the legal challenges that arise from data-driven business models. Just 11,4% strongly agreed with the statement, of which just 1,75% rated the statement at a "6". 49,3% of respondents were neutral about the statement. The average score for this amounted to 3,1. It is noteworthy that the Energy & Utilities, the Financial Services sector, and the Real Estate & Infrastructure see a considerable proportion of respondents answering "Unsure/Not relevant" to the statement. This could indicate the awareness that legal departments in these industries have about the risks and complexity that implementing data-driven business models brings to their operations.

The sixth statement concerns companies accounting for ethical aspects in data usage, in addition to practical concerns. 47% of respondents strongly agreed with the statement. The general score for this statement amounted to 4,4. This was one of the highest general averages among the statements given and illustrates how, in the view of the legal department, their employers operate with a high standard when it comes to data processing. The high ratings also indicate that companies are aware of the potential backlash unethical data processing can bring to their organisations. That the sector with the lowest averages concerns the Energy & Utilities industry supports this argument, given that the sector deals less with individual backlash in contrast to other industries.

Which of the following statements apply to your company?

If your company has a data strategy in place, the legal team has already implemented that strategy:

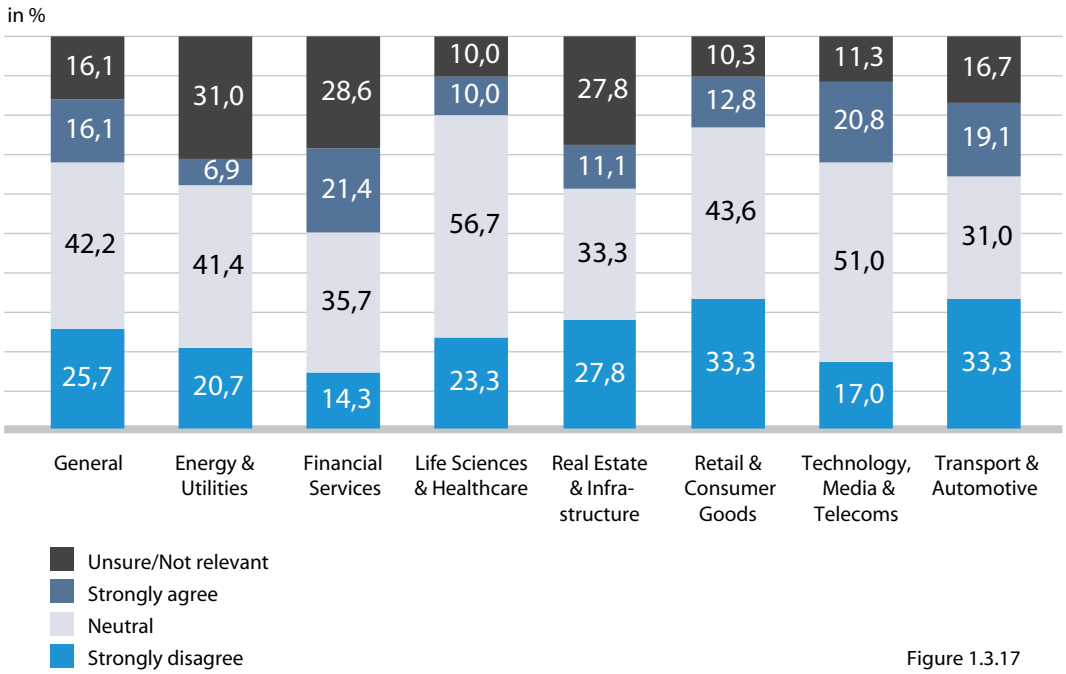


Figure 1.3.17

Which of the following statements apply to your company?

Your company uses contract templates that include provisions dealing with the use of data (beyond provisions dealing primarily data protection compliance)

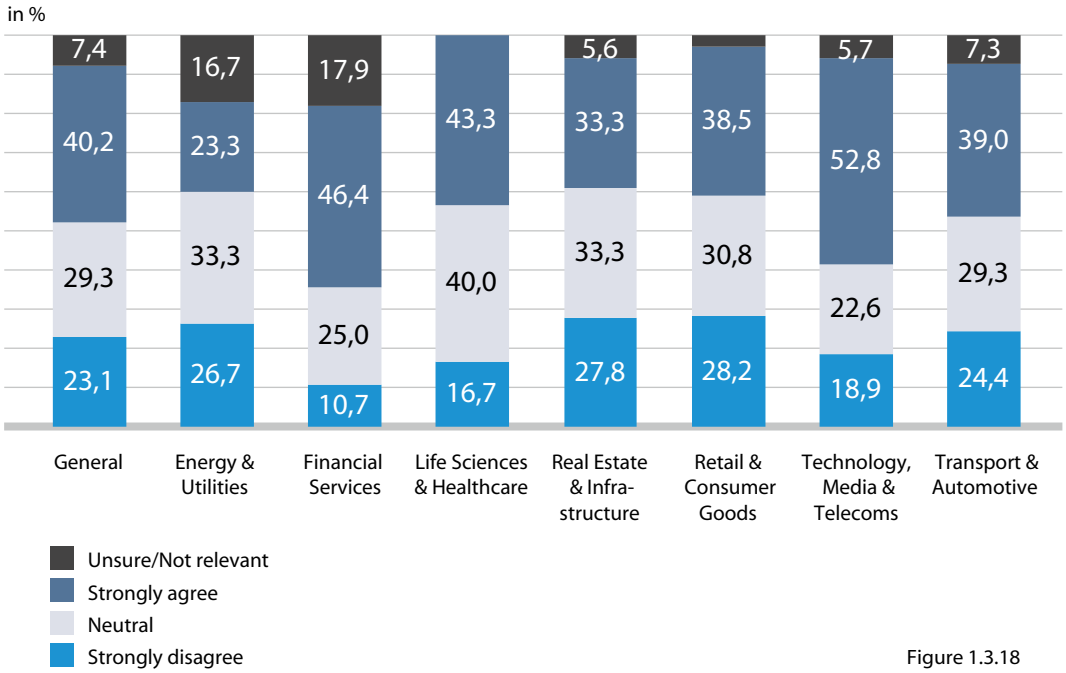


Figure 1.3.18

The next statement asked participants to rate whether their companies have board-level expertise with regards to data-centric business models. One in four companies strongly agreed with the statement, with a further 31,7% being neutral and another 29,6% strongly disagreeing. The average score for this statement amounted to 3,3. Across industries, the Financial Services industry and companies in the Technology, Media & Telecoms sector exceed the general averages by a considerable margin, with 39,3% of companies in the former and 43,4% of businesses in the latter strongly agreeing with the statement, respectively. Conversely, sectors such as Energy & Utilities, Life Sciences and Healthcare, Retail & Consumer Goods and Transport & Automotive have over a third of companies that strongly disagree with the statement. The results here signify the variance between the different sectors and highlight how certain industries are further along in establishing effective and supported data-driven business models within their organisations.

Participants were also asked to rate whether their companies take an open approach to data, to create value through collaboration, in contrast to a proprietary approach. For the general results, the answers are rather equally distributed among the possible scores, with both the highest score of "6" and the lowest score of "1" standing at 8,3%. Overall, 26,6% of participants strongly disagreed with the statement", with another 30,1% being neutral and 23,6% strongly agreeing. The average score for this statement amounted to 3,4.

The differences can be seen in the surveyed industries, however. Energy & Utilities stands out with the sector with the lowest scores, with 46,7% of respondents strongly disagreeing. Financial Services sees the highest proportion

Which of the following statements apply to your company?

Your company is well prepared for the legal challenges of data-driven business models:

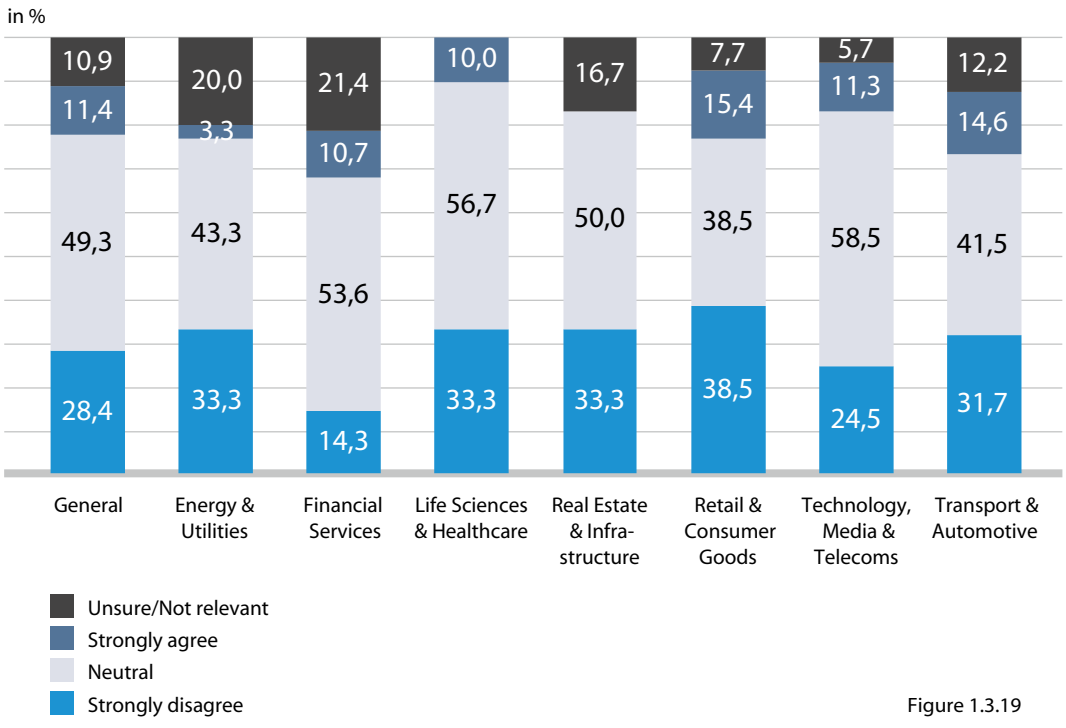


Figure 1.3.19

Which of the following statements apply to your company?

Your company thinks about the ethical and reputational angles of the use of data, as well as the practical ones.

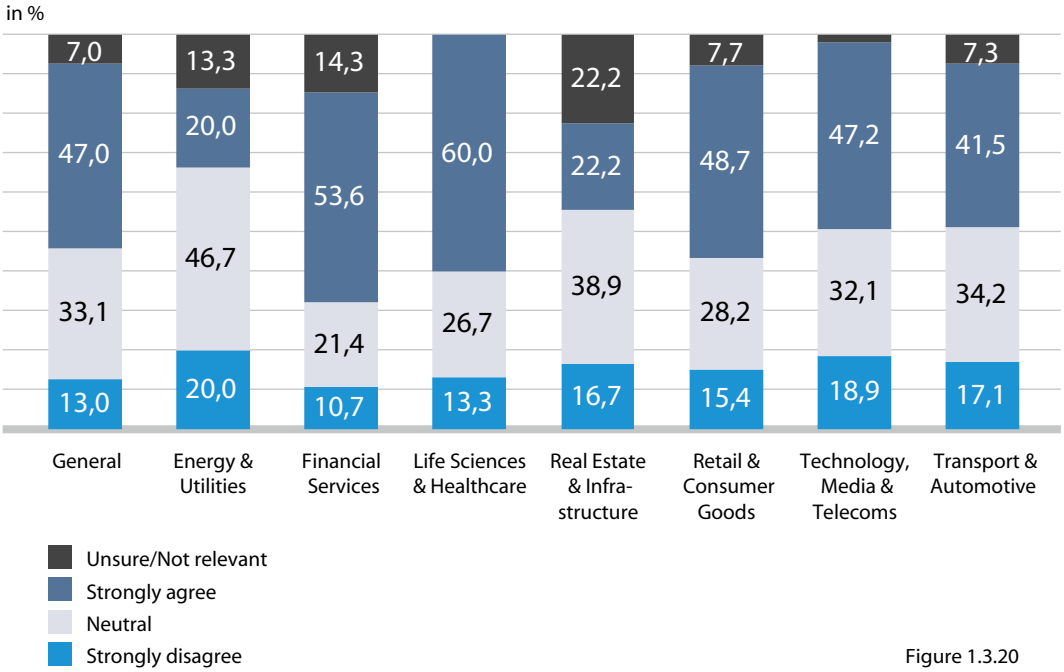


Figure 1.3.20

Which of the following statements apply to your company?

Your company has board-level expertise around data-centric business models

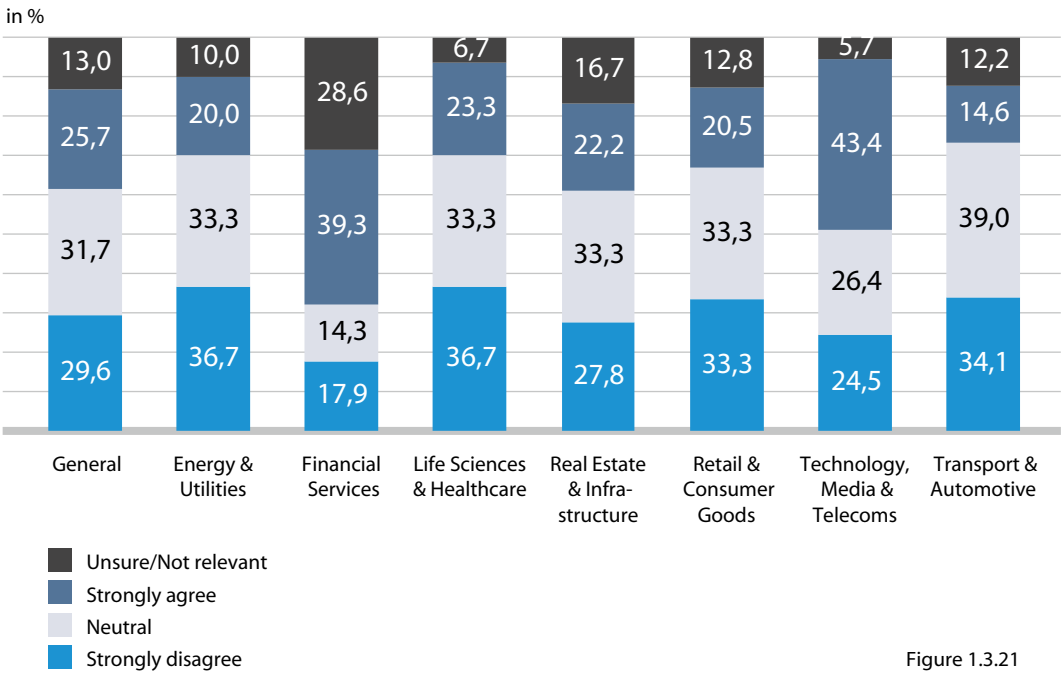


Figure 1.3.21

Which of the following statements apply to your company?

Your company tends to take an open approach to data to create value through collaboration, rather than a proprietary one to preserve its value for our business

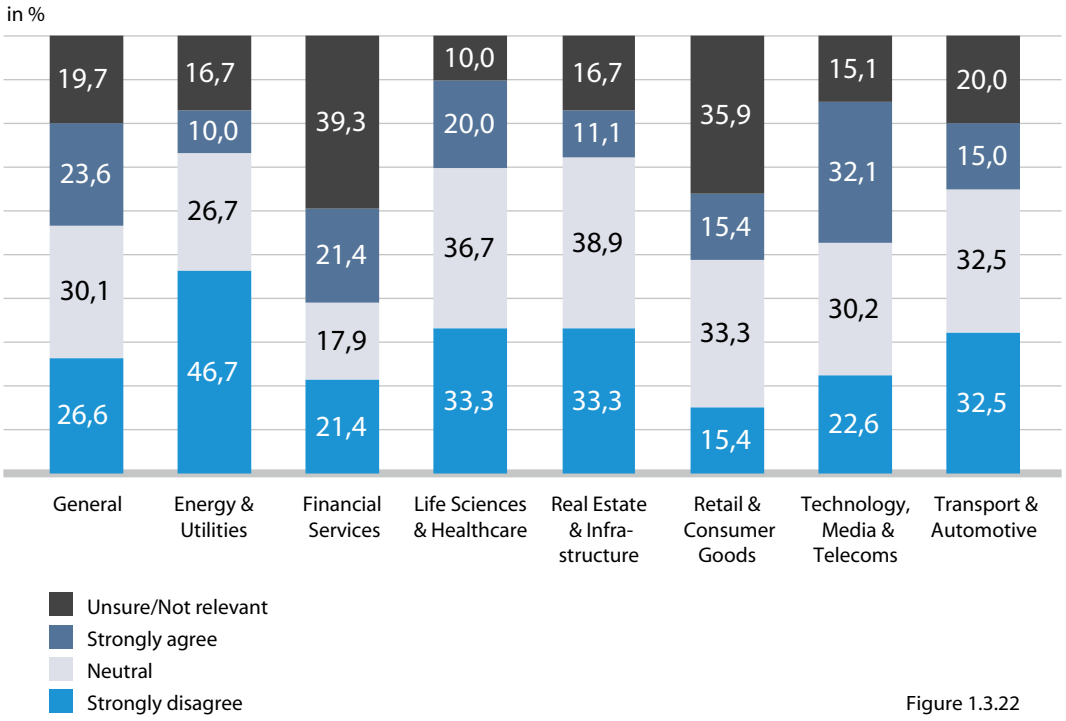


Figure 1.3.22

of uncertainty, with 39,3% of respondents being unsure about the statement or deeming it irrelevant. Technology, Media & Telecoms, however, is the only industry with a higher proportion of participating companies having a more open approach to data, with 32,1% of respondents strongly agreeing with the statement.

The ninth statement asked companies whether their companies aim to increase the usage of artificial intelligence in their business development operations. 39,9% strongly agreed with the statement. The average score for the statement amounted to 4,1. There is some notable variance in the definitiveness of some sectors, namely the Technology, Media & Telecoms industry, where 35,9% of respondents rated the statement at a score of "6" and a total of 43,4% strongly agreed. Similarly, companies in the Financial Services industry see an above average representation of a score of "5", at the expense of lower scores, amounting to a 50% proportion of companies that strongly agreed. Businesses in the Energy & Utilities and Real Estate & Infrastructure sectors are the most hesitant in introducing AI elements to their business development, with 46,7% and 33,3% strongly disagreeing, respectively.

Finally, we asked participants to rate their current AI skills within their legal departments. Participants were given an interactive slider with no visible scores to remove any scoring biases from their opinion. Underneath, the slider represented a range from -10 being the lowest score to +10 being the highest score. Most respondents moved the slider to the lower edge of the spectrum, indicating low AI skills within their departments. The mean position of the slider amounted to -3,7. This, combined with

Which of the following statements apply to your company?

Your company will increase the usage of artificial intelligence (AI) in business development

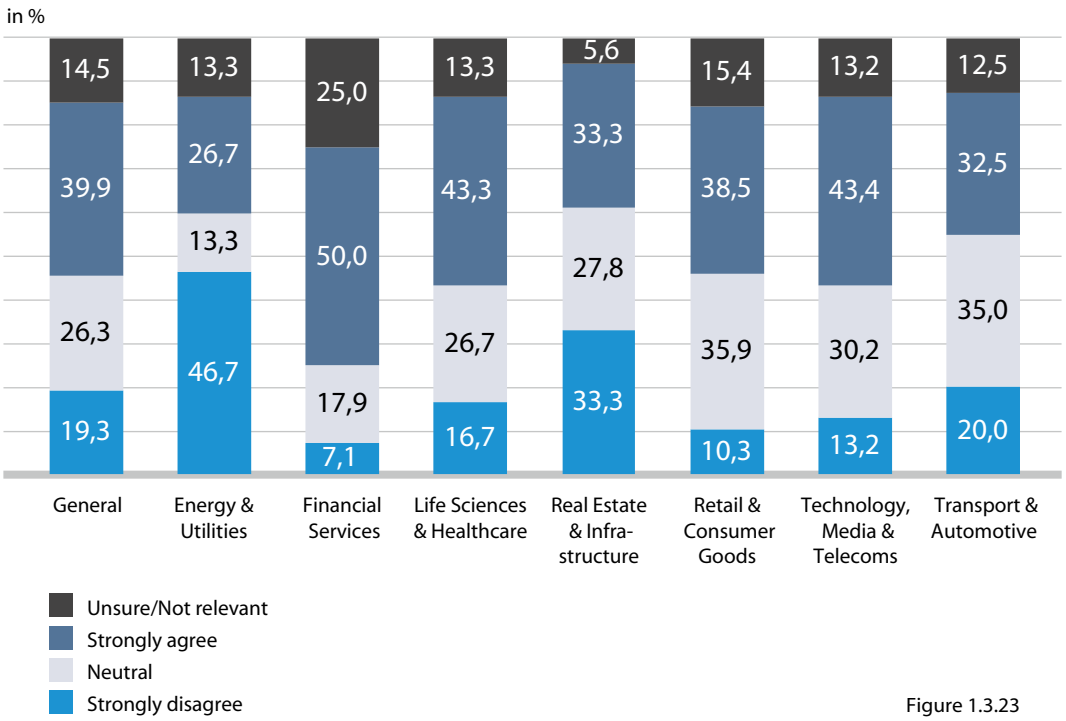


Figure 1.3.23

the previous statement, highlights the desire and interest that European companies have in introducing innovative approaches to their operations, but suggests that in-house legal departments have not yet developed skills and expertise specific to procuring and using AI.

Which of the following statements apply to your company?

How would you rate the AI skills in your legal department?

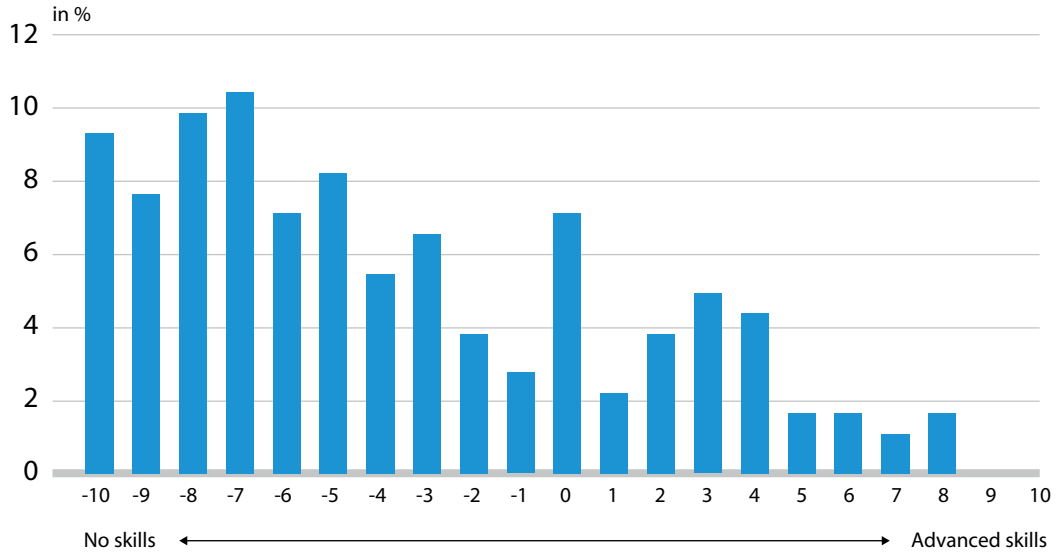


Figure 1.3.24

Osborne Clarke view

Nick Johnson ✉
Partner
United Kingdom
Further information

"We see a growing awareness by legal teams of the need for data-related skillsets that go beyond data privacy, and of the gathering storm of new data legislation. These can be blind-spots for a company's board, and in-house legal teams may need to work hard to explain their concerns and demonstrate the need for action. However, businesses that empower their legal teams to take a leadership role in planning and rolling out data-driven business models will reap clear rewards: legal teams are uniquely well-placed to see the bigger piture, and to help drive the changes necesssary for new data initiatives to achieve their potential."

1.4
SECTOR ANALYSIS

52,2% of responding companies in the Transport & Automotive sector (T&A) already offer data-driven products and services. 40,3% are currently planning to do so soon, the highest result for an intended launch of such products among the surveyed industries.

ENERGY & UTILITIES

...half (49,9%) offer data-driven products/services, and 23,8% have no plans to adopt them.

The most striking survey results from respondents in the Energy & Utilities (E&U) sector include the result that only half (49,9%) offer data-driven products/services, and 23,8% have no plans to adopt them. This is the largest group with no plans in any of the sectors.

This is an interesting result. One of the biggest challenges in the E&U sector is the shift to renewable generation. These sources of energy are often much more difficult to control than fossil-fuel-powered generation – the sun or wind cannot be switched on or off in line with demand levels, in the same way that gas- or coal-powered generation can. Moreover, whereas traditional generation was done at scale, concentrated in the hands of a limited number of suppliers, generation assets can now range from nuclear power stations to a couple of solar panels on the roof of a domestic dwelling – there are many more sources of supply to the grid. For both reasons, balancing supply and demand on the grid is becoming ever more complex. Tech-driven tools are an important part of how this complexity can be managed, including data flows, data analysis, AI-driven predictions for demand levels, or for weather conditions and resulting renewable generation power outputs.

The need for transparency of demand flows right down to the end consumer level. Moreover, at that end of the supply chain, smart meters have, for some time, enabled much more granular data about energy use to be captured. The significance of customer data and flows of data due to contractual or legal obligations is reflected in the survey findings that the main external sources of data for this sector are customers (a source of data for 79,2% of respondents with data-driven business models) and legal or contractual obligations (29,2%).

... it is striking that almost half (46,7%) of E&U respondents did not expect their business to increase its use of artificial intelligence

Against this backdrop of increasing complexity in the system, it is striking that almost half (46,7%) of E&U respondents did not expect their business to increase its use of artificial intelligence.

Notably, in this context only 11,1% of E&U respondents that offer or plan to offer purely data-driven services aim to provide products and services to improve decision-making capabilities – this is some 22 percentage points below the general, cross-sector result. Against the backdrop of the switch to renewables, this low figure seems surprising, but perhaps is indicative – as in many traditional industries undergoing transformation – of the range of engagement with digital technology in this traditional sector with many long-standing incumbents facing seismic change in their industry.

The coming changes to EU data regulation, creating extensive data access rights, may necessitate a shift in expectations

Interestingly, a significantly higher proportion of respondents in this sector take a proprietary approach to data compared with the general results, with the figure some 20 percentages points higher at 46,7%. Only 10% responded that they take an open, collaborative approach to data. The coming changes to EU data reg-

ulation, creating extensive data access rights (see Chapter 2.2) may necessitate a shift in expectations.

In terms of challenges for legal departments in implementing data-driven business models, legal and regulatory obstacles were felt less widely to be an obstacle than for the cross-sector results. Cybersecurity also scored less strongly as an obstacle. Although these results may at first sight seem surprising in a heavily regulated sector that is centred on critical infrastructure, perhaps the lower level of concern reflects greater familiarity with these issues to the point that they are not seen as problems by as many. That said, in many jurisdictions the treatment of data and technology by energy sector regulation regimes is considered to be outdated and out of step with current technology – so a higher level of concern over the challenge of regulation might have been expected. Indeed, only 3.7% of respondents thought the regulatory framework in the E&U sector was supportive of data-driven business models. In the future, managing baseload, the intermittency of renewables, and the use of battery and other storage technologies within the context of outdated grid networks is going to require an appreciation of all contributing assets in real time. Systems operators, networks, generators and suppliers will all need access to curated data sets to ensure efficient operation and revenue maximisation.

Perhaps the most notable result from the survey was a higher level than the general results of "Unsure" responses in relation to various aspects of the regulatory regime for the E&U sector, including how stable it is, how confusing or clear it is, and how well structured it is. These results appear to indicate a general lack of familiarity. This is reinforced by 36,4% of E&U respondents considering that there is a lack of internal experience and skillsets required for implementing data-driven business models in the sector.

Corporate data strategies appear to be the exception rather than the norm...

Corporate data strategies appear to be the exception rather than the norm in this sector, with only 13.8% of respondents answered positively that their business has one (compared with 36,1% across all sectors), and 27,6% answering that they do not (compared with 18,7% across all sectors). Only 20% of respondents' businesses have board-level expertise around data-driven business models – one of the lower results across the sectors.

FINANCIAL SERVICES

Unsurprisingly, given that figures, accounts and spreadsheets sit at the heart of the Financial Services (FS) sector, most companies in this sector already offer data-driven products/services, at 60,4%, with 30.2% planning on introducing such offerings soon. That said, the focus for most respondents is on improving existing products and services (69,7% of companies that offer/plan to offer hybrid service bundles), with a much smaller number focused on innovating with new products or services (24,2% of companies that offer/plan to offer hybrid service bundles). This is a notable result in the context of the UK's open banking initiative (discussed further in Chapter 2.3), and the thriving field of fintech. The results should certainly not be read as reflecting a lack of disruptive innovation in this sector as a whole.

..there are a number of indicators in the survey results of a more advanced understanding of data-driven business models..

Indeed, there are a number of indicators in the survey results of a more advanced understanding of data-driven business models amongst FS respondents than many other sectors. 39,3% of FS respondents confirmed board-level expertise on data-driven business models, second only to the Technology, Media and Communications sector. 42,9% have a data strategy (the strongest response in any sector by some margin). 46,4% include provisions dealing with data in their contract templates. 53,6% think about the ethical and reputational angles of the use of data (second only to the Life Sciences and Healthcare sector). 50% of FS respondents expect to make more use of artificial intelligence. These are all strong results, above the cross-sector findings. Cybersecurity risks are still considered one of the sector's five biggest obstacles to implementing data driven business models, but the number of respondents citing this concern (26,7%) was lower than in any other sector, arguably reflecting familiarity with these concerns over a longer period than other sectors. Similarly, the sector was less concerned about a lack of internal experience and skills (23,3%) or internal resources (23,3%) than any other sector.

...the FS sector responses indicated the highest diversity of data sources among any of the surveyed sectors...

The FS sector also stands out for the variety of sources of data that are used by respondents. 84% use customer-sourced datasets. 48% report using public datasets (6 percentage points higher than the next highest sector result), 44% purchase databases, 44% obtain data through contractual or legal obligations, and 24% source it from social media and APIs. The only category where the FS sector responses are slightly lower than the general response is for web-crawled or internet-scraped data. This result indicates a more developed ecosystem for data than in most other sectors – indeed, the FS sector responses indicated the highest diversity of data sources among any of the surveyed sectors, including even Technology, Media and Communications.

... businesses must carefully consider whether and how existing financial regulation frameworks apply to them ...

However, the picture regarding legal and regulatory frameworks for data-driven business models in the FS sector is less positive. This is, of course, a heavily regulated sector. 76,7% of FS respondents consider legal/regulatory obstacles as one of their five biggest challenges,

and it was by far the most commonly selected obstacle by respondents. The dominance of legal obstacles over other concerns is demonstrated by the spread of 50 percentage points between the first and fifth most cited obstacles (compared with a spread of 35 percentage points for the cross-sector results). Just 3,5% of responding companies consider the current legal/regulatory framework in Europe to be well-structured, only 7,4% consider it to be clearly understandable, and only 3,7% consider it to be supportive of data-driven business models – the lowest proportions for these statements across the surveyed industries.

These are interesting results as the FS sector regulators, particularly in the UK, have been at the vanguard of initiatives such as regulatory sandboxes, which enable regulators to learn about tech innovations, and innovators to learn about regulation. These survey results may reflect the potential disruption from initiatives such as open banking, and from new technologies such as blockchain and cryptocurrency, which take a fundamentally different approach to structuring interactions compared with institutional financial transactions. Bespoke regulation is not yet in place for these innovations, meaning that businesses must carefully consider whether and how existing financial regulation frameworks apply to them – which can be difficult and contentious.

LIFE SCIENCES & HEALTHCARE

The Life Sciences and Healthcare (LSH) sector is another where the survey results indicate a more advanced state of the market as regards data-driven business models. Most companies in the sector responded that they already offer data-driven products/services, at 57,7%, and 24,4% plan to offer them soon.

… innovation is clearly a focus with 51,9% of responding companies using or planning to use data to provide novel products or services…

In this sector, innovation is clearly a focus with 51,9% of responding companies offering or planning to offer hybrid service bundles to provide novel products or services - the highest proportion among the surveyed industries and 17 percentage points above the general average. Unsurprisingly for a sector which is focused on medicine and human health, 91,3% of companies use customer-provided datasets. Purchased databases are much more widely used in this sector than others, with 60,9% of companies reporting this as an external source – almost double the general cross-sector result. Similarly, the score of 56,7% for respondents who have been involved in the strategic acquisition of data is the highest result in any sector.

Notwithstanding these strong results, lack of access to external data was cited as an obstacle to the development of data-driven business models by 51,5% of LSH respondents. This may reflect the availability of public datasets. Public healthcare services have a central role in this sector in many jurisdictions, yet only 30,4% of respondents reported using freely available public data sets. The sector's reported frustrations in accessing data, notwithstanding apparent widespread use of external data sets, may therefore concern freely available public datasets. For EU companies, this may ease with the enactment of the EU's Data Governance Act (see Chapter 2.12), which is designed to make it easier to share public data, and with the EU's initiative to open up access to public health data through recent proposals for a European Health Data Space.

…the only sector where respondents felt that sector-specific challenges are a significant concern.

The LSH sectors stands out for having a much greater focus on joint development of data-driven products and services than other sectors. Indeed, joint development with a commercial third party (64%) is more common than in-house development (60%), and the sector has by far the strongest relationship with academia and public research institutions for the development of data-driven products and services (48%). Advances in this intellectual property-rich field often involve complex cutting-edge research over many years, so this result is perhaps not surprising given the nature of how innovation is achieved. The results for the LSH sector are also notable for the number of obstacles that were identified, with most of the survey options for different obstacles being selected by proportionately more LSH respondents than the general cross-sector answers. This includes legal/regulatory challenges (cited by 75,8% of LSH respondents), lack of internal experience and skills (57,6%), access to external data (51,5%, as already noted), cybersecurity risks (48,5%), sector-specific challenges (45,5%), poor integration into internal company structures and processes (36,4%) and poor interaction of data-driven business models with classic business models (30,3%). This is the only sector where respondents felt that sector-specific challenges are a significant concern.

The reason for this overall sentiment that data-driven business models face more hurdles in the LSH sector than others is unclear, but may be because digital transformation is not yet embedded and familiar through the sector, notwithstanding that digital health was significantly boosted during the pandemic; that much of the data in this sector concerns the health of individuals and may be treated as 'special category' data, which is heavily regulated under the GDPR; and that the sector as a whole is regulated, particularly as regards medical products and devices. The landscape is therefore complicated. Indeed, 78,1% of responding lawyers in the LSH industry consider the current legal/regulatory framework regarding the implementation of core data-driven business models to be too complex, and 80% consider it to be confusing.

...60% of respondents think about the ethical use of data – the highest score of any sector...

Consistent with those findings, only 10% of LSH respondents felt their company was well prepared for the challenges of data-driven business models. Although the number of respondents in this sector reporting that their company has a data strategy (33,3%) was in line with the cross-sector result (36,1%), only 10% of those with a data strategy answered that the legal team had already implemented it. On the other hand, there is clearly data-related activity involving the legal team in the LSH sector. 43,3% reported that their contract templates include data provisions. Notwithstanding the difficulties reported in obtaining external data, as discussed above, 56,7% of participating companies have already been involved in the strategic acquisition of data, the industry with the highest proportion. Notably, 60% of respondents think about the ethical use of data – the highest score of any sector, which may reflect the significance of ethics across all activity in this human-centric sector. However, only 23,3% reported board-level expertise around data-driven business models. So, as with many other sectors, there is a mixed picture around strategy and governance, with some elements in place, but clear potential for the legal team to take the lead in delivering a considered and joined-up approach across the business.

REAL ESTATE & INFRASTRUCTURE

Most respondents ...already offer data-driven products and services

Most responding companies in the Real Estate and Infrastructure sector (REI) already offer data-driven products and services, at 70,4%, second only to the Technology, Media and Communications sector. 15% are planning to introduce such products and services. These are, in many ways, surprising results[1] for a sector that is still considered very traditional in its approach to business, particularly when compared with the Technology, Media and Communications sector. There is increasing use of technology and data to increase the efficiency of buildings as a significant aspect of climate change-driven green tech. Measurement of the environmental performance of buildings is also an area of regulation-driven growth of digital tools for this sector.

The REI supply chain is certainly seeing digitalisation at all levels, from data-driven construction techniques to Internet of Things-based digital tools for building and asset management (including, at the most sophisticated end of the scale, digital twins, discussed in Chapter 2.8), to apps and digital interfaces with tenants, occupiers, and people passing through the built environment (for example, free WiFi and an app for shoppers visiting a mall). The strong result for the use of real time data from this sector (66,7%) may reflect the use of real time management tools such as building automation systems. We are seeing an emerging use of tech and data, not only in support of real estate planning, valuation, and transactions, but also around strategies to improve the accessibility, sustainability, and social impact of the built environment. Nevertheless, the overall strength of the results for this survey were greater than we expected. We are encouraged but have to acknowledge that the results may have been impacted by a smaller sample size than other sectors.

...high levels of data deals and litigation may indicate a more developed understanding of the raw value of data and databases...

68,8% of REI companies selling or planning to offer raw data and other data products as intangible goods reported that they either already do or plan to collect, analyse, process, and sell raw data as a commodity, which is not surprising given the scale of data already being collected across the built environment, and 21 percentage points above the cross-sector figure. The sector also shows the highest rates of repurposing data originally collected for a different objective for use in a new purpose. At 81,3%, this is some 10 percentage points above the next highest sector score, and 17 percentage point above the general results. As regards external sources, respondents indicated a similar level of use of customer-provided datasets (82,4%), freely available public data acquisition (35,3%) to the cross-sector results, but a much higher level of acquiring or purchasing databases at 47,1% (the highest of any sector) and 15 percentage points higher than the general results. Much of this activity will be in line with the sector's move towards more informed urban planning, design, and investment decisions.

Consistent with this result, respondents indi-

1 There was a smaller number of responses from REI businesses compared with other sectors (see Methodology and acknowledgements), which may have impacted on these results.

cated that 55,6% of REI respondents have been involved in the strategic acquisition of data (the second highest result). The sector also gave the second highest response for using data required to be provided through contractual or legal obligations at 41,2% (second only to the Financial Services Sector). 22,2% of companies within the industry have already been involved in data disputes, the joint highest proportion amongst the different sectors. The high levels of data deals and litigation may indicate a more developed understanding of the raw value of data and databases than in other sectors. This inference appears to be reinforced by the result that only 11,1% of REI respondents answered that their business takes an open approach to data.

For the development of data-driven products and services, REI was one of only two sectors where respondents indicated that developing new data-driven products and services jointly with commercial third parties (70,6%) is more popular than in-house development (64,7%) – although REI respondents are also the most likely to use arms-length group companies for their tech development (35,3%). Joint development was more likely than outsourcing, which received notably low support – at 17,7%, the lowest of any sector.

...reduced focus on legal and regulatory obstacles for REI respondents...

Regarding the challenges that the legal department experiences when implementing data-driven business models, the results are far more balanced than in other sectors, where legal and regulatory constraints tend to dominate. While this is still the primary concern of respondents at 55%, 50% of companies reported a lack of internal experience and skills as a concern; and 50% of respondents are concerned with a lack of internal resources. In addition, 40% of REI respondents cited poor integration into internal company structures and processes as a concern and 40% also cited access to external data as an obstacle. This spread of only 15 percentage points between the first and fifth concern compares with a spread of 35 percentage points for the cross-sector results, and 50 percentage points for the sector with the largest spread.

...not a single respondent in the REI sector considered their business to be well prepared for the challenges of data-driven business models...

The reduced focus on legal and regulatory obstacles for REI respondents may reflect the fact that this is not a regulated sector into itself, and that a significant proportion of the data collected and used in this sector will not be personal data and will not be subject to privacy regulation. In line with this relative lack of concern, 21,1% of REI respondents consider the legal and regulatory framework for data-driven-business models in their sector to be well-structured, the highest proportion among the surveyed industries. In addition, 27,8% consider it to be clearly understandable, the highest result by 9 percentage points. On the other hand, not a single respondent in the REI sector considered their business to be well prepared for the challenges of data-driven business models – a striking result.

...respondents who consider the regulatory framework for data-driven business models to be stable may need to reconsider.

Caution is wise given the change that is coming to the regulation of data-driven business models. The 29,4% of REI respondents who consider the regulatory framework for data-driven business models to be stable may need to reconsider. For businesses in the EU, the Data

Act (discussed in Chapter 2.2) proposes to open up access to data collected by Internet of Things systems, including where they are embedded in immovable objects such as real estate, infrastructure such as roads or bridges, or large machinery such as wind turbines. Providers of such systems will be obliged to give access to data to the users whose interactions with the system generated that data. A framework of regulatory obligations will be created around data collected by connected products or structures and related services.

There was more clarity in this sector than others about whether the respondents' businesses had a data strategy with an overall positive response of 33,4%. This is slightly below the general result (36,1%) but within that, the highest level of confidence expressed about this question of any sector. Again, this a might suggest a strong understanding amongst the respondents of the value of data and how to realise it.

...a more strategic approach to the use of data may be needed...

However, REI respondents gave a very low response to whether the legal team has implemented the company's data strategy (if it has one) with only 11,1% answering positively, and the second lowest response to whether the company uses contract templates incorporating provisions dealing with data (33,3% responded positively, compared with the general response of 40,2%). Only 22,2% responded that their company has board-level expertise around data-centric business models, and only 22,2% of REI respondents' companies think about the ethical and reputational angles of data use as well as the practical ones. Given the disruption that is likely to come to this sector, certainly to REI businesses in the EU and those selling products and services into the EU, a more strategic approach to the use of data may be needed, with stronger top-down governance and monitoring of how regulation will impact on their current understanding of the value of data and how to protect it.

RETAIL & CONSUMER GOODS

... lower enthusiasm than in most other sectors for data-driven business models...

The Retail & Consumer Goods (R&C) sector generated results indicating lower enthusiasm than in most other sectors for data-driven business models, with only 48,7% of respondents companies in the industry already offering data-driven products/services (one of two surveyed industries that does not reach the 50% threshold). 20,8% of respondents report no formal plans for introduction, the second-highest proportion among the surveyed sectors.

For external data sources, customer-provided datasets are the most popular option, at 81,6%. This is not a surprising result, given that the consumer-facing part of this sector is rich in customer data from, for example, loyalty programmes, till receipts and online retail sales. Freely available public datasets are used by 42,1% of R&C respondents, and the sector makes above average use of data from social media and other applications via APIs, at 31,6%. The latter may reflect the extensive use of social media for marketing brands in this sector.

...cybersecurity risks appear to be one of the concerns...

Regarding the challenges that legal teams are faced with when implementing data-driven business models, 60,4% of companies report legal and regulatory obstacles as a point of concern. Many of the other most-cited concerns are inwards facing: 45,8% of participating lawyers see poor integration of data-driven business models into internal company structures and processes as an obstacle; 41,7% report a lack of internal experience and skills as hindering implementation; 29,2% see internal data utilisation as a challenge; and 27,1% are concerned about lack of internal resources. At 27,1%, cybersecurity risks appear to be one of the concerns in this sector. Given the amount of customer data, including payment data, which may be held by retail businesses, particularly those using online sales channels, strong awareness of data breach risks is understandable.

... a higher proportion of "unsure" responses in relation to many of the survey questions...

In addition to these concerns about internal obstacles, there are a number of further signs in this sector that the in-house legal teams are less involved in the business's data-driven business models than in others. It is striking that there is a higher proportion of "unsure" responses in relation to many of the survey questions from this sector compared with others, including those around the nature of the data-driven business models used. Similarly, questions looking at the legal and regulatory framework for data-driven business models – including how well structured, understandable, supportive or stable it is – all receive a large number of "unsure" responses. Only 10% of R&C respondents have been involved in a dispute around data rights or access. 23,1% don't know whether their business takes an open or proprietary approach to data, with a further 12,8% deeming it not relevant. Again, there is a sense that many in-house counsel in this sector are not familiar with data-driven business models.

R&C respondents indicated that 38,5% of their companies have a data strategy, a little above the cross-sector figure of 36,1%. Of those that do have one, their legal teams have implemented the strategy in only 12,8% of cases. Only 20,5% of R&C respondents indicated that they have board-level expertise around data-driven business models. 38,5% of R&C respondents lacked confidence about their business's readiness for the legal challenges of digital transformation.

Given the importance of digital interactions in this sector – not least for e-commerce and digital sales channels – the apparent unfamiliarity of many R&C legal counsel with how their companies are using data-driven business models is somewhat unexpected for an industry known to be technology savvy. It may indicate that the understanding of data-driven business models sits within pockets within these businesses, rather than being disseminated throughout the organisation.

This is, of course, not a universal finding. Many in-house legal teams will have been closely involved in ensuring that retail websites are designed to be in compliance with regulation around e-commerce and payment services. Innovations such as adding connectivity to existing products to make 'smart' consumer products (explored in Chapter 2.4) will have necessitated careful legal analysis to ensure compliance, as well as a contractual framework to create the necessary underlying digital infrastructure. Subscription pricing models, often supported and managed through a digital platform, require assessment against a number of different areas of law. Pooling data from different sources, for example to build customer profiles for marketing or advertising, will have needed advice from the in-house team (as explored in Chapter 2.5).

...changes on the horizon for digital and data regulation create an opportunity for R&C counsel...

For those who are less familiar, the many changes on the horizon for digital and data regulation create an opportunity for R&C counsel to get closer to the data-driven business models used in their companies to evaluate how those changes will impact on their businesses. As explained previously, the new laws will create rights as well as obligations, so an awareness of where the business sits within these new frameworks will ensure that its interests can be fully protected and exercised. Moreover, where digital products and services need to be compliant with regulation, it is typically better to design compliance into them from the outset rather than trying to retrofit, which tends to cause expense, delay, and disruption. As such, the legal team needs to be at the heart of innovative data-driven projects from the outset, which will in turn build a strong understanding of the business model.

TECHNOLOGY, MEDIA & COMMUNICATIONS

As would be expected for this data and digital technology-focused sector,[1] substantially all companies in the Technology, Media & Communications (TMC) sector industry offer (87%) or plan to offer (10,9%) data-driven products or services, the highest proportion among the surveyed industries. The share of companies not planning on doing so is negligible. 75% of respondents that offer or plan to offer data infrastructure solutions said that their business offers data-related analysis and consulting services – perhaps a natural focus for this sector, particularly as digitalisation spreads to all sectors.

Regarding external data acquisition, 91,4% of TMC respondents use customer-provided datasets, and that 27,6% of companies obtain web-crawled data, the highest proportion among the surveyed industries. A relatively low number (26,8%) of TMC respondents cited access to external data as an obstacle.

...the most extensive in-house tech development skills...

In relation to the development of data-driven products/services, TMC sector responses indicate the most extensive in-house tech development skills, with 83,9% of respondents selecting this answer, 14 percentage points above the cross-sector average. In addition, 32,1% also used group companies that operate at arm's length. Again, this result is to be expected – although conversely 33,9% of TMC respondents report a lack of internal experience and skills as an obstacle.

In terms of the biggest obstacles when implementing data-driven business models, 80,4% of TMC companies highlight legal and regulatory obstacles. 51,8% of TMC participants identify cybersecurity risks as an obstacle. Both results were the strongest for the sectors.

Another notable result for this sector is that 33,9% of TMC respondents are concerned about uncertainties regarding the general legitimacy of the underlying business model. This is a much bigger percentage than the next largest sector result at 23,3%. It perhaps reflects the fact that innovative and transformative tech will often first be developed in this sector, which must grapple with the question of whether and how existing regulation relates to it. Where the regulatory position is unclear, compliance becomes a matter of risk management. There is always a concern that if the business has taken an overly robust approach to regulation in an innovative field, or if regulation is introduced that takes an approach that was not anticipated, the foundations of the new business model may be found to be non-compliant and fall away.

When considering the existing legal and regulatory framework for data-driven business models, responses from the TMC sector were typically more negative than from other sectors, finding it more complex (79,6%) more confusing (69,4%), more obstructive (64%) and more unstable (70%) than other sectors. Again, this may reflect the fact that a significant proportion of tech innovation starts in the TMC sector before spreading out to other sectors, so lawyers in this sector may well be at the vanguard of trying to map out and understand the likely regulatory analysis of a transformative new business model under old regulation that was shaped to apply to a previous generation of technology.

1 It is worth noting that the "Media" part of this sector includes businesses that are not entirely tech-focused, such as printed media and publishers.

… only 39,6% of respondents already have a data strategy in place…

Perhaps surprisingly for a sector that includes many of the pioneers in understanding the revenue-generating potential of data, only 39,6% of respondents already have a data strategy in place (placing second to the Financial Services sector). The corporate data strategy (for those businesses that have one) has only been implemented by 20,8% of TMC legal teams, but 52,8% use contract templates that have detailed provisions on data usage. Interestingly, only 47,2% of TMC companies reported thinking about the ethical and reputational angles of the use of data, and only 43,4% reported having board-level expertise on data-driven business models – the latter result seems particularly surprising. EU regulation of this sector, particularly of large digital platforms, is being rethought and strengthened (see Chapter 2.13), along with the regulation of data (see Chapters 2.2 and 2.12) and new regulation for artificial intelligence (see Chapter 2.7). Ensuring consumer trust and the respect of fundamental rights is a theme running throughout all of these regulatory initiatives. It may be that data strategy and data governance need to be given more prominence within TMC organisations, whether in reaction to the new regulatory landscape, or as a sensible approach in itself.

…respondents take an open, collaborative approach to data…

The strength of the open source philosophy, born in the TMC sector, is evident in the result that 32,1% of TMC sector respondents take an open, collaborative approach to data, versus 22,6% who prefer to keep data proprietary. This is the strongest support for open data of any of the sectors by some 11 percentage points – the general score is lifted by the TMC score above the level in any other individual sector. It is also the industry that sees the strongest positive interest in increasing the usage of artificial intelligence for business development purposes, with 43,4% of TMC respondents strongly agreeing with this statement.

…negligible level of concern… about sector-specific obstacles may well change in the coming years…

Unsurprisingly, the survey results indicate strong familiarity in the TMC sector with data-driven business models, although there is also evidence of scope to strengthen data strategy and governance. The regulatory changes for this sector under the European Digital Strategy shift this sector from being unregulated, in the sense of being subject only to universal legal regimes, to having policy-driven sector-specific regulation, which is actively intended to shape these markets going forwards. The negligible level of concern in the TMC sector about sector-specific obstacles may well change in the coming years – although, as is always the case, new obligations for some create new opportunities for others. The enduring characteristics in this sector of rapid change and constant innovation will undoubtedly endure.

TRANSPORT & AUTOMOTIVE

52,2% of responding companies in the Transport & Automotive sector (T&A) already offer data-driven products/services. 40,3% are currently planning to do so soon, the highest result for an intended launch of such products among the surveyed industries. This signifies the changing landscape within the sector although also perhaps indicates that it is somewhat behind in its digitalisation journey.

... second-highest proportion of companies using data to offer novel products and services...

73,7% of companies that sell or plan to offer purely data-driven products and services plan to improve ongoing activities/processes, with a further 21,1% offering purely data-driven products and services to support decision-making. Although the sector sees the lowest proportion of companies planning to use hybrid service bundles to extend existing products/services (37,2%) it sees the second-highest proportion of companies planning to offer novel products and services, at 48,8%, reinforcing the inference that the industry is still undergoing transformation from harnessing data. This inference certainly aligns with what is happening in this sector. Vehicles are shifting to becoming connected and electric-powered, with longer term research into autonomy. Meanwhile transport services have seen extensive disruption from digitalisation with the emergence of digital platforms to support mobility, as well as the development of integrated Mobility as a Service offerings across public and private transport options. Connectivity of vehicles has raised the issue of access to data flowing from vehicles by third parties as an issue (explored more generally in Chapter 2.2). Digital twins in the urban environment (discussed in Chapter 2.8) can extend to traffic management, with data flowing from vehicles, trains and other forms of mobility moving though the city streets.

...80% of responding T&A companies generate new data internally for new applications...

Previously a sector focused on very physical products and industry, this transformation phase is perhaps reflected in the statistics that 80% of responding T&A companies generate new data internally for new applications – the highest result of any sector. Creativity about data use is also present though, with 57,5% repurposing existing data for novel purposes. For external data sources, customer-provided datasets remain the most popular option, at 80%, with the remainder of the results for external data sources broadly tracking the general cross-sector results. 42,9% of T&A respondents report that their companies have been involved in the strategic acquisition of data. This is an above-average proportion and the third-highest score among the surveyed industries. Real time data plays a significant role within the sector, with 52,4% of respondents answering positively to this question. Again, this may reflect the growing importance of real time data flows from connected vehicles, as well as real time data that powers many of the innovative services in this sector, such as the location of scooters, bikes or cars that are available on the streets for public hire.

This sector stands out for its collaboration with academia...

Respondents in the sector have built in-house expertise around tech development, with 66,7% reporting fully integrated internal development teams, and 28,2% reporting that development is undertaken by arms-length group companies. On the other hand, 44,2% of T&A respondents report a lack of internal experience and skillsets within their businesses as an obstacle. This sector stands out for its collaboration with academia, coming second only to the Life Sciences

and Healthcare sector in using this option for development (25,6%). This well may reflect the complexity and extended time span for research into autonomous driving, the leading edge of data-driven change in this sector.

In terms of obstacles that T&A legal departments face when implementing data-driven business models, 67,4% report legal and regulatory challenges as one of the five biggest hindrances, and 46,5% report cybersecurity risks as concerning. The latter is a high score, second only to the TMC and Life Sciences sectors. This may reflect the focus on safety in this sector – historically this has been around the safety of vehicles, but as they move to being integrated with digital software and connectivity, cybersecurity is becoming a significant aspect of operating safety.

...this is a sector where policymakers are actively engaged and clearly future-focused.

With regards to the current legal and regulatory framework for data-driven business models, although the majority (as in all sectors) have difficulties with the framework, 21,2% of T&A respondents consider it to be supportive of these new business models, and 37,5% consider it to be stable. 56,4% of participants report the regime to be too complex. While this still represents the majority of respondents, it is nevertheless the lowest proportion among the surveyed industries. These results may reflect the fact that there is extensive product regulation in this sector, including type-approval requirements and health and safety standards and obligations, as well as close policy attention to liability, with mandatory insurance or compensation regimes in many jurisdictions to ensure victims of harm from vehicles have recourse to remedies. Moreover, lawmakers in many countries have started to consider the impact of autonomous vehicles on the liability regime. So overall, this is a sector where policymakers are actively engaged and clearly future-focused. This is also evidenced by the European Commission choosing the T&A sector as one of the areas in which sector-specific legislation should be implemented in addition to the proposed Data Act. On the other hand, only 14,6% of T&A respondents consider their company to be well prepared for the legal challenges of data-driven business models – the least confident response of any sector – so there is clearly awareness of the impending legal and regulatory consequences of data-driven transformation in this sector.

...only 35,7% reported having a data strategy in place...

While data is clearly a focus for many businesses in this sector, only 35,7% reported having a data strategy in place. Of those respondents, only 19,1% reported that the legal team have already implemented the strategy. Only 14.6% of T&A respondents have board-level expertise around data-driven business models – perhaps a reflection of the speed of change in this sector, where the incumbents will have needed very different expertise to steer strategy until recently.

2

HOW IS LAW AND REGULATION SHAPING SUCCESS FOR DATA-DRIVEN BUSINESS MODELS?

OSBORNE CLARKE'S EXPERT LEGAL COMMENTARY

2.1 SHAPING SUCCESS FOR DATA-DRIVEN BUSINESS MODELS

OSBORNE CLARKE AUTHORS

Catherine Hammon
Digital Transformation Knowledge Lawyer, United Kingdom

Catherine.Hammon@osborneclarke.com

Further information ›

Nick Johnson
Partner, United Kingdom

Nick.Johnson@osborneclarke.com

Further information ›

Dr Jens Schefzig
Partner, Germany

Jens.Schefzig@osborneclarke.com

Further information ›

HOW TO IMPLEMENT DATA-DRIVEN BUSINESS MODELS

As data and digital technology transform businesses, an opportunity is emerging for in-house legal teams to embed themselves at the heart of the business. The increasing complexity and scope of data and digital regulation mean they will need new skills and a 'hands-on' mentality. The proposed new and reworked regulatory frameworks aim to reshape the data ecosystem. Data-driven business models will need to be designed with this new legal environment in mind.

KEY TAKEAWAYS

- → Data regulation is poised to expand far beyond privacy and personal data into new, previously unregulated areas.
- → The EU legislators are seeking to reshape the EU data ecosystem to open up access to data and to ensure alignment with EU values and fundamental rights.
- → Digital regulation is evolving into a legal specialism in itself, and expanding in impact as digital transformation spreads across sectors.

A. The challenge

It is not difficult to find examples of businesses that have harnessed data in order to create business models that have profoundly changed their markets, or created entirely new ones.

But equally, data-driven business models can be complex to implement – not least where they are part of a digital transformation strategy. The survey results show that although the adoption of data-driven business models is widespread across sectors, many in-house legal teams find supporting their implementation to be complex and confusing. Digitalisation often completely changes the legal skillset needed to support a business initiative: for example, a bridge operator that collects tolls in the form of cash from motorists will need completely different legal advice if it launches an app for digital payment. Digitalisation and data-driven business models often rest on a foundation of tech procurement contracts, with an associated digital supply chain.

Not only can the legal relationships in any particular data-driven business model be complex, but the regulation of digital products, services and processes – and of data itself – is ever expanding. There are a number of radical legislative changes to digital regulation on the table, particularly from the European Commission, both overhauling existing legislation and introducing completely new regulatory frameworks in a number of areas. This matters because the legal and regulatory context for data-driven business models is fundamental to their viability.

In this introduction to Part 2 of this report, we offer an overview of the issues that are explored in more detail in the following chapters.

B. The variety of data-driven business models

Digital transformation means that every sector is embracing digital tools, boosted by technologies such as the Internet of Things (IoT) and artificial intelligence (AI). Data is critical, whether as a raw material, an output, or even as a means of payment. Data is increasingly referred to as an 'asset' in its own right, reflecting the value that it can generate. Data-driven business models seek to harness that value, in some cases in the form of separate revenue streams.

I. Data as an enabler

Sometimes a dataset itself carries financial worth, but the value in data can also flow from its power as an enabler: reducing costs, boosting productivity or facilitating innovation. The transformation that has been enabled by the open banking and wider open finance initiatives in financial services markets is a prime example (see Chapter 2.3).

Business processes can be improved by tracking performance and/or the conditions in which they are operating. Data about past breakdowns and repairs can be fed into AI systems to generate predictions about when a machine will next break down. Data about customer behaviour and decisions can both feed into personalised offers and marketing, and inform design decisions to hone a product or service to address customer demand and preferences.

Data from different sources can be pooled to enhance these applications further (see Chapter 2.5).

II. Digital platforms

Data-driven business models are often built around a digital platform to hold data and generate insights from it. For some markets, the

platform is the interface with consumers, hosting the digital services that they wish to acquire or use. Such platforms often amass data about their users, which can then be used to power advertising sales, to boost personalisation of marketing, product design and development, or to power other enhancements to the core services.

Other platforms support digitally connected products, enabling data flows to and/or from them, potentially powering analysis of the collected data.

Accordingly, data-driven business models tend to have a strong digital aspect, and data regulation has to be considered alongside the wider field of digital regulation.

III. Connected devices

Connected devices and IoT systems are growing in every sector, from wearable health devices to wind turbines, to vehicles, to building management systems, to smart home systems, to children's toys, to infrastructure such as bridges (see Chapter 2.4).

Where data flowing from a connected product or service has competitive value – perhaps offering insight into demand levels in neighbouring markets such as repairs and maintenance or spare parts – access to that data can become a competition law or intellectual property (IP) issue. And new laws, like the recently proposed EU Data Act[1] , are likely. This will mean a new regulatory landscape for the fight for data flowing from connected devices (see further Chapter 2.2).

1 See https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113 Osborne Clarke's summary of the European Commission's proposed Data Act is available here: https://www.osborneclarke.com/insights/eu-data-act-proposal-commission-plans-comprehensive-right-data-access

IV. Digital twins

Digital twins are a particularly advanced example of data powering insight and efficiency. IoT systems and data flows can turn a digital model of the shape of something into a digital twin that also mirrors its functionality, physical properties and performance and integrates data flows so that the digital twin becomes a virtual replica of the physical thing.

Such digital twins are an integral part of digital industry systems (see further Chapter 2.6), but can also be created to support collaborative projects with many stakeholders (see Chapter 2.8). These twins, often modelling the built environment, can for example boost the understanding, operation and optimisation of smart cities.

V. Cybersecurity

Data-driven business models depend on a constant flow of data. But each digital connection is a new cybersecurity access point into the connected business or home. This is an operational risk for IT professionals, but also generates legal risk that can be managed through contractual frameworks, proper IT security management systems and supply chain terms of procurement (see further Chapters 2.9 and 2.9.1).

VI. The interface of data-driven business models with decarbonisation

The overarching imperative of decarbonisation is also driving a new regulatory approach (discussed in Chapter 2.11). The easy availability and scalability of cloud-based processing services can make energy conservation a low priority in designing technology. Some jurisdictions are starting to address this with requirements to minimise the environmental impact of technology. France is taking a lead, with requirements

and enforcement structures for the eco-design of digital services.

C. An emerging new legal framework

The dynamic environment for technological development is accompanied by equally dynamic regulatory developments. Case law around data continues to evolve but entirely new frameworks for data regulation are being enacted and existing digital regulation is being overhauled. The European Commission, in particular, is seeking to expand the scope of data regulation far beyond privacy, with the objective of ensuring consumer trust and engagement and also the availability of data as a resource for new business models. Businesses that are delivering data-driven business models in Europe or for EU customers need to be aware of how the regulatory landscape for data and digital products and services is changing. We are on the cusp of a major reset.

Europe is at the forefront of this development but it is not limited to Europe (see further Chapter 2.14). And although the focus for this report is Europe, data flows and digital products and services are often global in nature, with regulation from other jurisdictions impacting directly on exports from European businesses and their processing activities. Digital regulation and local compliance around the world can shape export priorities or even determine certain aspects of a business model.

I. The EU Digital and Data Strategies

Data and digital regulation in the EU is being driven by the European Commission's European Digital Strategy of February 2020.[2] Its objective is to maximise the potential benefits to the economy and society from data and digital technology, noting in particular the role of data as a "key factor of production", or a raw material, for digital products and services.

Alongside its digital strategy, the Commission has also published the European Data Strategy.[3] The latter also emphasises the role of data at the centre of digital transformation and states:

> "... data should be available to all – whether public or private, big or small, start-up or giant. This will help society to get the most out of innovation and competition and ensure that everyone benefits from a digital dividend. This digital Europe should reflect the best of Europe – open, fair, diverse, democratic, and confident".

The data strategy goes on to identify various issues that need to be tackled, including the availability of data, particularly for innovative re-use. It notes that business-to-business sharing can be hampered by a lack of economic incentives, including the fear of losing a competitive edge. It notes that there are imbalances in market power as regards data holdings. It also cites the need to empower individuals to exercise their rights as regards data portability, noting that an absence of technical tools and standards can make such rights burdensome and not simple to use.

There is a data-centric logic across the raft of new regulation coming out of the EU. If the

2 Commission Communication, "Shaping Europe's digital future", available at https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf We discussed the strategy announcement in this article: https://www.osborneclarke.com/insights/eu-digital-strategy-tech-sovereignty-common-eu-values

3 Commission Communication, "A European strategy for data" (COM(2020) 66 final) of February 2020 available at https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data-19feb2020_en.pdf

Digital Services Act and Digital Markets Act are seeking to remould aspects of established digital markets, the proposed Data Act and Data Governance Act seek to influence the characteristics of the data ecosystem that should start to thrive as data becomes more accessible. The overarching digital and data strategies set the tone and direction for the regulatory approach as a whole. In the EU, the themes of consumer trust, data accessibility and respect for fundamental rights are now set at the heart of digital regulation.

Although the EU cannot boast many major global tech players, the Commission is seizing the opportunity to set the global gold standard for digital regulation. Moreover, there are signs of a new trend for centralising enforcement to Brussels. Currently, regulatory enforcement in all fields except competition law is devolved to national Member State authorities. However, the Commission will itself take responsibility for enforcement of the reformed legislative framework for the largest digital platforms (see Chapter 2.13). This change in approach can be seen not only as a move to ensure consistent and coherent enforcement, but also as an indication of the strength of the EU's intention to influence how global data and digital markets develop in the future.

The ambitions of the EU digital and data strategies are being progressed on various fronts.

II. Growing the data ecosystem

New legislative frameworks have been proposed by the Commission to shape the data ecosystem, open up the availability of data held by public and private entities, and boost consumer trust in data sharing, including the proposed Data Act (see Chapter 2.2) and the proposed Data Governance Act (see Chapter 2.12).

The Data Governance Act[4] envisages a strong ethical framework, limiting the ability of profit-making data intermediaries to use the data that they collect and sell for their own purposes, and imposing a fiduciary duty to act in the best interests of the data subjects. The proposals also envisage new structures for "data altruism", enabling individuals to donate their data to not-for-profit organisations to be used in pursuance of defined objectives (see further Chapter 2.12).

The Data Act will create a new right of access to data for businesses using digital tools that collect data about their activities (see Chapter 2.2). For example, tenants might be able to obtain data collected about their premises by systems run by building management, or the users of smart devices might have the right to access the data that their use generates (see further Chapter 2.4).

The interface between these proposals to open up access to data and the protections under intellectual property that may, for some data and datasets, protect their value is an important one (explored in Chapter 2.10).

III. Rethinking regulation of digital platforms

In addition, the Commission has undertaken reviews of existing regulation of digital services markets to ensure that these frameworks are as effective as possible in light of developments since they were first issued. These reviews have resulted in the European Commission's proposals for the Digital Markets Act and the Digital Services Act (discussed in Chapter 2.13), both of which involve significant changes for the regulation of digital platforms, with specific obligations being imposed on specified

4 See https://digital-strategy.ec.europa.eu/en/policies/data-governance-act Our summary of the proposals is available here: https://www.osborneclarke.com/insights/eu-data-governance-act-creating-european-regulation-data-ecosystem

platform market "gatekeepers" and very large digital platforms.

IV. Ensuring trustworthy artificial intelligence

AI is another field of data-rich technology receiving close regulatory attention to ensure that the technology is developed in alignment with the values that the EU wishes to embed across data-driven products and services. The European Commission's proposals for their entirely new field of regulation are currently making their way through the legislative process. The AI Act[5] proposes burdensome obligations in relation to data used in AI systems, as well as the AI technology itself Agreed and its implementation (see Chapter 2.7).

Artificial intelligence is built in a fundamentally different way to other software and systems, and the interface with intellectual property rights is not yet settled (as is explored in Chapter 2.10).

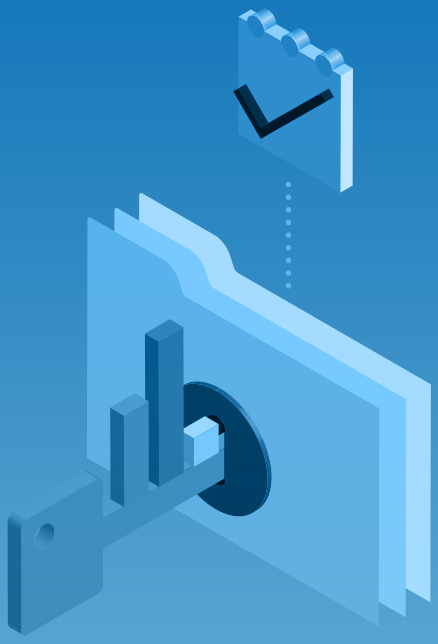
D. Conclusion

The regulatory landscape around data-driven business models is set to become fundamental to how they are built and operated. As noted, keeping on top of both the current position and the known changes is important because the legal and regulatory context for data-driven business models is fundamental to their viability. As such, compliance increasingly needs to be designed into products and services from the outset.

Although the extent of change can be daunting, in-house counsel need to embrace this opportunity to put themselves at the heart of innovation in their businesses, delivering the advice needed to shape the success of their organisation's data-driven products and services.

5 See https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence Osborne Clarke's summary pf the proposals is available here: https://www.osborneclarke.com/insights/european-commission-proposes-new-regulatory-framework-artificial-intelligence

2.2 ACCESS TO DATA (AND HOW TO ENFORCE IT)



OSBORNE CLARKE AUTHORS

Dr Sebastian Hack
Partner, Germany

Sebastian.Hack
@osborneclarke.com

Further information

Catherine Hammon
Digital Transformation Knowledge Lawyer, United Kingdom

Catherine.Hammon
@osborneclarke.com

Further information

Katherine Kirrage
Partner, United Kingdom

Katherine.Kirrage
@osborneclarke.com

Further information

Elisabeth Macher
Counsel, Germany

Elisabeth.Macher
@osborneclarke.com

Further information

Paul Schmitz
Associate, Germany

Paul.Schmitz
@osborneclarke.com

Further information

ACCESS TO DATA (AND HOW TO ENFORCE IT)

For most data-driven business models, access to data is key. If a supplier holds data that gives it a competitive advantage (for example on an aftermarket), its competitors will need to find alternative or equivalent datasets or seek to secure access to the first supplier's data. In practice, securing access is not always an easy undertaking. For effective competition on such markets, legal options for gaining access to data for all market participants are crucial.

KEY TAKEAWAYS

- → Access to data can be crucial for effective competition. Some datasets give advantages that others cannot replicate.
- → Legal options to secure access to data today include complaints to competition authorities, litigation based on antitrust law, unfair competition law, or sector-specific legislation.
- → In future, regulatory efforts such as the European data strategy aim at facilitating data exchange, and will lay the foundation for new data-driven business models.

A. Access to data and competitive advantage

Many suppliers and manufacturers now offer connected products, and many of those products collect data.

Often the data is not about the user, but is about performance or wear and tear. It can be valuable data where it supports aftermarket services associated with the main product, such as repair, maintenance or servicing, or supply of spare parts or additional consumables needed to use the main product. Having access to this data can enable a number of aftermarket actions. For example, it might give the supplier a clear indication of when the customer is likely to need aftermarket services. This might, in turn, enable the supplier to schedule pre-emptive maintenance at the user's convenience, avoiding wear and tear breakdowns and unexpected call-outs for emergency repairs, and facilitating efficient deployment of its workforce. The data might also enable the supplier to order replacement parts or new consumables in good time. This data-driven business model is seen in the automotive industry for cars and car servicing, in the energy sector for smart meters and boiler servicing, and for some connected consumer products that regularly need new supplies of a consumable (such as ink and paper for a printer).

However, where there is a downstream market for the supply of aftermarket services such as repairs and maintenance, or for the associated consumables, access to the data from connected products becomes a strategic issue. If competitors cannot access the data, and cannot access an equivalent or alternative dataset, they may find it more difficult to win that customer for their alternative aftermarket products and services. Access to data from the main product becomes a barrier to entry for aftermarket competitors.

In addition, in some markets collected data is considered to be proprietary by the business that holds it, and not shared. This may mean that third parties have no possibility of using it innovatively to develop new products and services that the incumbents do not offer.

Is it possible for a business using a product to gain access to data generated by its use? Can a third party gain access to the data? Or is the supplier that holds the data free to decide to retain it – and any competitive advantage that flows from the data – for itself?

B. Legal options to get access to data today

I. Complaint to a competition authority

European legislators have repeatedly acknowledged and stressed the relevance of data for competition. In this vein, there have been several amendments to national competition laws expressly focusing on the relevance of data. In Germany, with the 10th Amendment to the Act against Restraints of Competition (Competition Act – GWB), the legislator clarified that companies owning certain data can qualify as being dominant and restricting access to such data is abuse. Competition authorities have also not been shy to initiate investigations into practices where the use and access to data has been at the core of the case. An investigation by a competition authority has certain advantages due to the extensive investigatory powers of competition authorities. Therefore, companies seeking access to data may ask authorities for help by lodging a complaint. Such complaints can be by an individual company, a group of companies, a trade association or even anonymous.

However, given that authorities have a discretion regarding if and when to open an investigation, authorities will balance their available resources with (among other things) the complexity of the case, the expected investigatory efforts

required, and the economic importance and general relevance of the issues at hand. Against this background, complaints tend to be more successful when the complainant has already built a convincing case setting out the legal issues, providing corroborating evidence and showing the general importance for a wider group of companies or a sector. Should a competent national competition authority or the European Commission initiate an investigation and conclude that the data holder has infringed competition law by restricting access to the data, the authorities can impose remedies on the data holder that not only affect the complainants, but may also benefit other companies.

II. Direct claims based on competition law

Competition law provides not only for public enforcement but also for private enforcement through litigation. Therefore, companies seeking access to data may alternatively choose to assess a direct civil claim against the data holder. Such claims can be brought as follow-on litigation on the back of a decision from a competition authority or as a stand-alone claim. Follow-on litigation has certain advantages as there is some relaxation of the burden of proof (the decision of the authority is binding for courts with regard to the infringement). However, in most of the cases there is no authority decision on which claimants can rely.

Stand-alone litigation can be based on specific competition law, such as that in Germany dealing with access to data, but also finds support in seminal court decisions on European competition law like the Magill (cases no. C-241/91 P and C 242/91 P) and IMS Heath (case no. C-418/01) cases of the Court of Justice of the European Union. On this basis a claimant may have a right to access if the access to the specific data is indispensable in order to compete on a downstream market. Given that in a civil claim the burden of proof is on the claimant, it is our experience that the prospects of a successful claim hinge on the diligent preparation of facts, in particular with regard to the type of data, the replicability of data and relevance of that data for the products and services that the claimants offer.

III. Direct claim based on sector-specific legislation

The EU and national legislators have introduced specific legislation on access to data for certain economic sectors. For example, in the automotive sector, Regulation (EU) 2018/858 contains specific obligations for car producers to provide technical information on their vehicles to the independent aftermarket (repair shops, spare parts providers and so on). The Regulation also provides for a right of independent operators to access the vehicle data stream. As a Regulation, these rules are directly applicable in EU Member States, and independent operators can enforce rights in court based on this sector-specific legislation.

The European Commission envisages further regulation of access to in-vehicle data via sectoral legislation, which is to be specifically tailored to the distinctive characteristics of the automotive industry and will serve to supplement the broader approach of the Data Act (see Chapter 2.10).

IV. German particularity: Unfair competition law in connection with sector-specific legislation

In Germany, in addition to basing claims directly on sector-specific legislation, claimants may also enforce such legislation through competition law. The German Unfair Competition Act contains a provision whereby, among other things, competitors and associations may base unfair competition claims on a violation of a market conduct rule. Legislation on access to information or data will often constitute such

a market conduct rule. The German Federal Court of Justice has explicitly confirmed that the rules on access to information in the automotive sector constitute a market conduct rule (Federal Court of Justice, decision of 30.1.2020 – I ZR 40/17).

Basing claims on unfair competition law has several procedural benefits. In particular, these claims can be raised by associations (despite the fact that typically only their members, not the associations as such, will be legal beneficiaries of access rules); claimants may select among several local jurisdictions; and provisional injunctions can be granted by the courts without prior substantiation that the matter is urgent.

Where there is no sector-specific legislation in place, claimants may still try to rely on IP and property rights where their own machinery is concerned. Arguably, the producer of a machine cannot prevent the purchaser of said machine from accessing data generated by it, since the purchase will include rights to use and access the software on the machine. This principle has now also been enshrined in the Data Act (see Chapter 2.10).

C. Legal options to get access to data in the future

The importance of data-driven business models means that these issues are now at the forefront of regulators' and policy-makers' attention. New legislation and regulatory frameworks will make it more difficult for suppliers of connected products to refuse to share the data that they generate. These changes are driven both by competition policy and by a broader desire to build data economies that offer enhanced potential for innovation and new data-driven products and services.

In the UK, we have already seen data access and interoperability as a competition remedy in open banking, which has given challenger financial services and software companies the ability to offer competing banking services based on compulsory application program interfaces (APIs)/data interoperability (see Chapter 2.3).

This is likely to be reflected in the upcoming EU Digital Markets Act, which will regulate companies acting as "gatekeepers" (likely to include the Big Tech players) in EU digital markets. Parallel regulation is planned in the UK, to be enforced by the new Digital Markets Unit within the UK competition authority.

In particular, the Digital Markets Act proposals include obligations on gatekeepers to allow third parties to interoperate with the gatekeeper's own service in certain specific situations and to allow business users to access data that they generate in their use of the gatekeeper's platform. On the flip side, gatekeepers will be prohibited from usage of certain data, including taking non-public data from business users on their platform to compete with those businesses, and combining personal data obtained from the core platform services with any other service unless in accordance with the General Data Protection Regulation (GDPR).

While these proposals are currently targeted at the leading tech players, they will provide a clear precedent on the usage of data and the requirements of interoperability where players have a strong market position and so may provide useful grounds for bringing complaints in other markets.

More broadly, the EU Commission's Data Act proposals, published in February 2022, envisage creating rights for users of connected products and services to have access to the data held by the supplier but generated from their use of the product or service. The proposals enabling the user to require access are extended to identified third parties. These are radical proposals that will significantly impact on the current ability

of suppliers to keep such data as proprietary. In the UK, the concept of 'smart data' is being actively explored. The example of open banking is being extended into other areas of consumer finance, such as open pensions. But more generally, policymakers are exploring how opening up access to consumer data could power innovation for the benefit of consumers.

As with all regulatory shifts, some businesses will find that longstanding strategies – or less considered default approaches – will need to be reconsidered. Other businesses and start-ups will find new opportunities are created. We expect the opening up of data from these new initiatives to offer the raw material for a new wave of data-driven business models.

2.3 HOW OPEN BANKING HAS FACILITATED DATA-DRIVEN BUSINESS MODELS, AND WHAT'S NEXT

OSBORNE CLARKE AUTHORS

Paul Anning
Partner, United Kingdom

Paul.Anning@osborneclarke.com

Further information

Jonathan Hazlett
Partner, United Kingdom

Jonathan.Hazlett@osborneclarke.com

Further information

Karima Lachgar
Partner, France

Karima.Lachgar@osborneclarke.com

Further information

Maia Steffan
Associate, France

Maia.Steffan@osborneclarke.com

Further information

Mark Taylor
Partner, United Kingdom

Mark.Taylor@osborneclarke.com

Further information

Seirian Thomas
Senior Knowledge Lawyer, United Kingdom

Seirian.Thomas@osborneclarke.com

Further information

Dr Daniel Walter
Partner, Germany

Daniel.Walter@osborneclarke.com

Further information

HOW OPEN BANKING HAS FACILITATED DATA-DRIVEN BUSINESS MODELS, AND WHAT'S NEXT

Open banking offers opportunities for data-driven business models by allowing customers to share their banking data securely with third parties. We explore examples of business models successfully using data shared under this framework.
The next step is unlocking customer data across the financial sector. Open finance has the potential to promote innovation and benefit customers, but effective and ethical implementation will be challenging.

KEY TAKEAWAYS

- → Open banking gives customers control of their bank data, helping them manage their money and access better products.
- → Mandating participation by banks and a standardised technical approach has been key to open banking's success.
- → Opening up customer data across the broader financial sector is next on the horizon, with challenges to be navigated.

A. What is open banking?

Open banking is a framework allowing customers to share access to their bank accounts and data with trusted third-party providers.

In the past, the relationship between bank and customer was private, with the bank controlling customer data. 'Screen scraping' offered customers a workaround to aggregate their financial data by sharing bank log-in details with unregulated third parties, but was plagued by security concerns and lack of trust, as well as constituting a breach of customers' terms and conditions with banks in some cases.

Under open banking, the customer gains control of their banking data and can choose to share it securely with regulated third parties. Importantly, banks are legally required to permit and facilitate this data sharing. Open banking has unlocked opportunities for innovative business models in the Financial Services sector, ultimately enabling customers to access more and better products and services.

In the EU, the key legislation underpinning open banking is the EU's second Payment Services Directive[1] (PSD2), which took effect on 13 January 2018. PSD2 was implemented[2] in the UK before the UK left the EU. Separately, the UK Competition and Markets Authority (CMA) has been instrumental in driving the UK's open banking initiative from an early stage, as open banking is seen as key in promoting competition and innovation in the retail banking sector.

B. Account information services and open banking

PSD2 created two new regulated payment services:

- account information services[3] (AIS), where the customer gives a trusted third-party provider (TPP) access to information on their payment accounts held at account servicing payment service providers[4] (ASPSPs); and
- payment initiation services[5] (PIS), allowing customers to make payments to third parties directly via a TPP, as an alternative to paying online with a credit or debit card.

Firms carrying out AIS and PIS need to be regulated or registered with their local financial regulator and must comply with certain obligations when providing these services. The PSD2 framework has enabled the growth of new business models, including those making use of customer data shared via AIS.

I. AIS providers and models

AIS is generally provided by three categories of market players:

- Traditional or established payment service providers (e.g. credit institutions, electronic money institutions (EMIs), and payment institutions);

1 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (implemented separately in each EU Member State) – available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015L2366-20151223 (last accessed 10 March 2022).

2 Primarily by the Payment Services Regulations 2017 (SI 2017/752) – available at https://www.legislation.gov.uk/uksi/2017/752/contents (last accessed 10 March 2022).

3 Defined in Art. 4(16), PSD2: "an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider".

4 Defined in Art. 4(17), PSD2: "a payment service provider providing and maintaining a payment account for a payer".

5 Defined in Art. 4(15), PSD2: "a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider".

- Fintechs and other technology companies offering innovative solutions based on AIS; and

- Marketplaces and other businesses looking to enrich their existing offering and add value to their core services.

In practice, companies utilising data collected through AIS operate under various business models, including:

- **White labelling:** the company offers a combined service of data collection and utilisation under its brand and contracts with the customer, while a partner behind the scenes provides technological capabilities;

- **Co-branding:** the company provides a combined data collection and utilisation service and uses the services of an account information service provider (AISP) as an outsourced service provider to collect the required data; and

- **A redirection framework:** the company only utilises the customer data. The customer signs up for AIS directly with an AISP and agrees that the AISP may share their data with the company.

Depending on the business model used and the service offered, firms operating in this sector must be appropriately authorised in the relevant jurisdiction(s); both AIS and PIS activities may be "passported" from a firm's "home" state into the rest of the EU and European Economic Area on either a cross-border services or establishment basis.

II. AIS use case: online financial dashboards

AIS facilitates an increasingly popular personal financial management tool: online dashboards that provide a consolidated view of a customer's finances across their accounts and/or banks. Providers, which include firms such as Emma, Money Dashboard, and Plum Analytics, may offer free and/or paid-for options for their dashboard service, depending on their business model and the range of tools provided.

This type of service allows customers to review their spending in the round, without having to log in to separate online banking portals and record the data manually. This can help the customer manage their finances effectively. This service also makes it easier for a customer to manage accounts at multiple banks, thereby promoting competition in the retail banking sector.

Dashboards can offer numerous money management tools, including:

- viewing the total balance across all accounts in one place;
- alerts for low balances and bills falling due; and
- other budgeting tools, such as categorising spending, setting savings goals, and recording 'streaks' to motivate saving.

Some dashboard services use the customer's transactional data to suggest which subscriptions the customer may not need and could cancel, flag bills which would be cheaper with alternative providers, and offer vouchers or deals for businesses at which the customer shops frequently.

III. AIS use case: loan eligibility

Another use case for AIS is to support creditors assessing the loan eligibility of new borrowers. Credit scoring is carried out by creditors to assess their risk exposure on credit to be granted. In addition, for consumer loans, the EU's

Consumer Credit Directive[6] requires creditors to assess the consumer's creditworthiness on the basis of sufficient information, to be obtained from the consumer and a relevant database. In consequence, obtaining information about the consumer's income and regular spending allows the creditor to fulfil its legal obligations.

The AIS model allows account information to be provided to the customer, but also gives the option to send the information to a third party at the customer's instruction. The customer can therefore instruct their bank to send specific account information to potential creditors looking to assess the customer's creditworthiness. This service simplifies the process for the customer to provide information to a potential creditor, and also benefits the creditor as they can obtain the required information directly from the bank.

Using AIS to check loan eligibility is growing more widespread, with the service being offered by providers such as finAPI and FinTecSystems. In contrast to online financial dashboards, which are usually targeted at consumers, use of AIS for loan eligibility checks is typically offered to creditors. This means that while the AISP has a regulatory relationship with borrowers, its commercial relationship (from which it derives its revenue) is with creditors.

IV. AIS use case: accountancy services for small and medium enterprises (SMEs)

A third core use case for AIS is its use in accounting and banking management solutions. Here are three examples of innovative French companies with this AIS use case:

- **Expensya:** this company has entered into a partnership with an EMI authorised to provide AIS and uses the information collected via the EMI in order to provide automated business spend management solutions for its large corporate and SME customers. The solution allows Expensya's customers to manage their employee expenses, reports and follow-up more easily;

- **Pennylane and its sister company REV:** this company is an accountancy firm providing automated solutions for accounting operations, using the information collected either by its sister company, the fintech REV acting as AISP, or by third parties such as Budget Insight or Fintecture; and

- **Indy:** this company has developed solutions enabling automated book-keeping, generation of tax returns, and other finance management tasks (much like QuickBooks in the UK).

AIS has allowed these companies to aggregate data on a customer, using the information from their bank accounts. In support of AIS, the technology companies have developed technical solutions, such as operating systems and algorithms allowing utilisation of the data.

Technology firms are also exploring the commercial possibilities offered by AIS. For example, some companies are considering using a customer's banking data to offer new products and services in a targeted manner, based on the customer's purchase history. Naturally, the utilisation of data in this context raises questions regarding the application of data protection rules.

6 Directive (EU) 2008/48 of the European Parliament and the Council of 23 April 2008 on credit agreements for consumers (implemented separately in each EU Member State) – available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0048&from=en (last accessed 14 March 2022).

C. Beyond open banking: open finance

In the EU and UK, open banking only applies to payment accounts[7] (most typically, current accounts), whether held by individuals, SMEs, corporates or institutions. Payment accounts represent a small subset of the financial products a customer might hold, such as insurance, mortgages, personal loans, investments and pensions.

The success of open banking is prompting governments and authorities to consider broadening the initiative to other parts of the financial services sector, looking to open banking as one model for how this could work. The move to open finance would create even more opportunities for successful data-driven business models, as customers would be able to share significantly more data across a range of financial products.

I. Progress in the UK

Regulators are working on how best to bring about open finance. The UK Financial Conduct Authority (FCA) has run a Call for Input process on open finance, concluding in its feedback statement (March 2021) that "[o]pen finance has the potential to transform the way consumers and businesses use financial services" and "help unlock the value of data across the economy".[8]

Authorities are also working on initiatives for sharing customer data beyond the financial sector. The UK government calls this "smart data", defined as "the secure and consented sharing of customer data with authorised third-party providers".[9] In future, customers may be able to benefit from services driven by simple, secure sharing of their data, such as automatic switching between providers and better management of accounts and bills, across sectors like energy and communications. The extension of smart data is expected to promote innovative services, stronger competition, and improved customer outcomes.

II. Challenges for open finance

In the UK, the FCA considers that open finance "would create or increase risks and raise new questions of data ethics",[10] ranging from the use of artificial intelligence, machine learning and data bias, to potential discrimination in favour of open finance customers and how to ensure an equitable distribution of risks and benefits.[11] These questions would need to be considered upfront as part of system design, and risks managed with appropriate regulation. Customers would need to be confident their data is being used ethically and in line with their expectations and consent.

It remains to be seen whether participation in all future open finance initiatives will be mandated, and how firms will be incentivised to participate. For example, the UK government has indicated its intention to introduce primary legislation to "improve [its] ability to mandate participation in smart data initiatives".[12] Legislative compulsion, whereby ASPSPs are required to facilitate data sharing in line with PSD2 rules and using standardised application program interfaces (APIs), has been a key factor in the success of open

7 Defined in Art. 4(12), PSD2: "an account held in the name of one or more payment service users which is used for the execution of payment transactions".

8 FCA Feedback Statement on open finance (FS21/7, March 2021), para. 1.13 – available at https://www.fca.org.uk/publication/feedback/fs21-7.pdf (last accessed on 10 March 2022).

9 Department for Digital, Culture, Media and Sport (DDCMS) policy paper, "National Data Strategy" (last updated December 2020), Glossary – https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#glossary (last accessed on 15 March 2022). See also section 6 on smart data.

10 FS21/7, para. 5.2.

11 Ibid., para. 3.37 et seq.

12 DDCMS paper, section 6.1.1.

banking, and could be crucial to ensuring open finance is taken up by a sufficient proportion of the market to be useful to customers. This would impose costs on smaller firms with fewer resources, but would benefit businesses seeking to capitalise on the newly unlocked data.

Another challenge will be whether a central standards body is established to support the delivery of open finance, similar to the UK Open Banking Implementation Entity or the Berlin Group in the EU, and if so, how this will be funded.

III. Open finance in action: the Pensions Dashboard

In the UK, the open banking concept is being taken forward into the world of pensions: UK law will require pension providers including pension trustees to feed data into pensions dashboards. The requirements are being introduced with effect from April 2023 and will be staged according to scheme size. Pensions dashboards will allow savers to see at a glance how their investments are performing and how much they will need to save for their future retirement.

A public body, the Money and Pensions Service (MaPS), has been tasked with designing and implementing the digital infrastructure that will make pensions dashboards work. MaPS will also establish and operate the first non-commercial dashboard. Providers will be able to establish their own commercial versions later, provided they are regulated by the FCA.

Pensions dashboards will not store data themselves; data will continue to be held by providers. The dashboard ecosystem will act like a search engine following a saver's request. A key concern for providers is to ensure that the data they hold is accurate, readily available and in a form that will be compatible with dashboards. MaPS has published a comprehensive data standards guide which provides details of what data providers must hold. Data cleansing work is now being undertaken because the provider's liability in case the data provided by the dashboard is wrong remains unclear.

Pension providers are also concerned about their potential liability for data breaches if their systems are not robust enough to prevent or mitigate a cyber attack. Providers are, therefore, looking closely at contractual relationships with pension scheme administrators and/or software providers. Providers will also face civil penalties for failing to comply with pensions dashboard requirements as well as reputational damage.

While the initiative will need time to bed down, dashboards will help savers take control of their pensions and make better informed decisions about their money.

2.4 OUR NEW PRODUCTS ARE CONNECTED – WHAT IMPLICATIONS DOES THAT HAVE?

CASE STUDY

OSBORNE CLARKE AUTHORS

Victoria Gwynedd-Jones
Legal Director,
United Kingdom

Victoria.G-Jones
@osborneclarke.com

Further information

Samuel Martínez
Lawyer, Spain

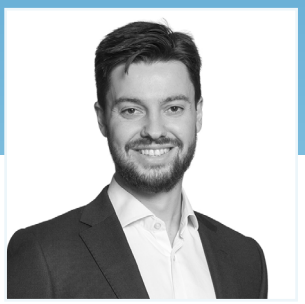
Samuel.Martinez
@osborneclarke.com

Further information

Dr Jens Schefzig
Partner, Germany

Jens.Schefzig
@osborneclarke.com

Further information



Thomas Stables
Associate, United Kingdom

Thomas.Stables
@osborneclarke.com

Further information

OUR NEW PRODUCTS ARE CONNECTED – WHAT IMPLICATIONS DOES THAT HAVE?

Introducing connected products into a business's product range may on some level appear straightforward, but the fact that the products are connected to the internet and can share information about themselves, their usage and their environment means that there are numerous legal implications. Here we consider some of the key legal consequences and outline how legal counsel can guide a business through this strategic transformation.

KEY TAKEAWAYS

- → Be aware that introducing a new connected functionality will change your business model in a fundamental way
- → Be prepared for your business requiring direct contractual relationships with many more parties such as developers and hosting providers
- → Understand how else to support your business in the successful launch of new connected products

A. The business and its products

Consider a business that produces tools and machinery that are to be used by other businesses in their manufacturing processes. The products are sold globally, either directly to customers, or indirectly via dealers or distributors.

The newest generation of these products is capable of connecting to the internet, and transferring data collected by sensors in the products to an online service. The business intends to provide this online service to end users of the products. The users will be able to log into the online service, see their fleet of products, and view certain information collected about those products such as malfunctions, battery status and location. The business intends to develop functionality in the future which will also allow users to manage their manufacturing process, or third party machinery, remotely using the service.

The fact that this new generation of products is connected (that they are 'Internet of Things' or 'IoT' devices) has numerous implications for the business and its legal position. What would this business need to do in order to implement this new connected business model?

B. The evolving business model

Often a business which is introducing IoT products into its product range will be able to provide a high level description of the service and its plans. But a common challenge is understanding the key issues and risks that the IoT element introduces from a legal perspective.

To better understand these issues and risks, running a workshop for the key stakeholders will be helpful. The business should establish a team including perhaps the C-level executive who is responsible for pushing the project forward internally; the head of the design or engineering department which developed the products; the head of the IT-development team which developed the online service; a project manager; and in-house or external legal counsel specialising in data, commercial contracts and the regulatory environment.

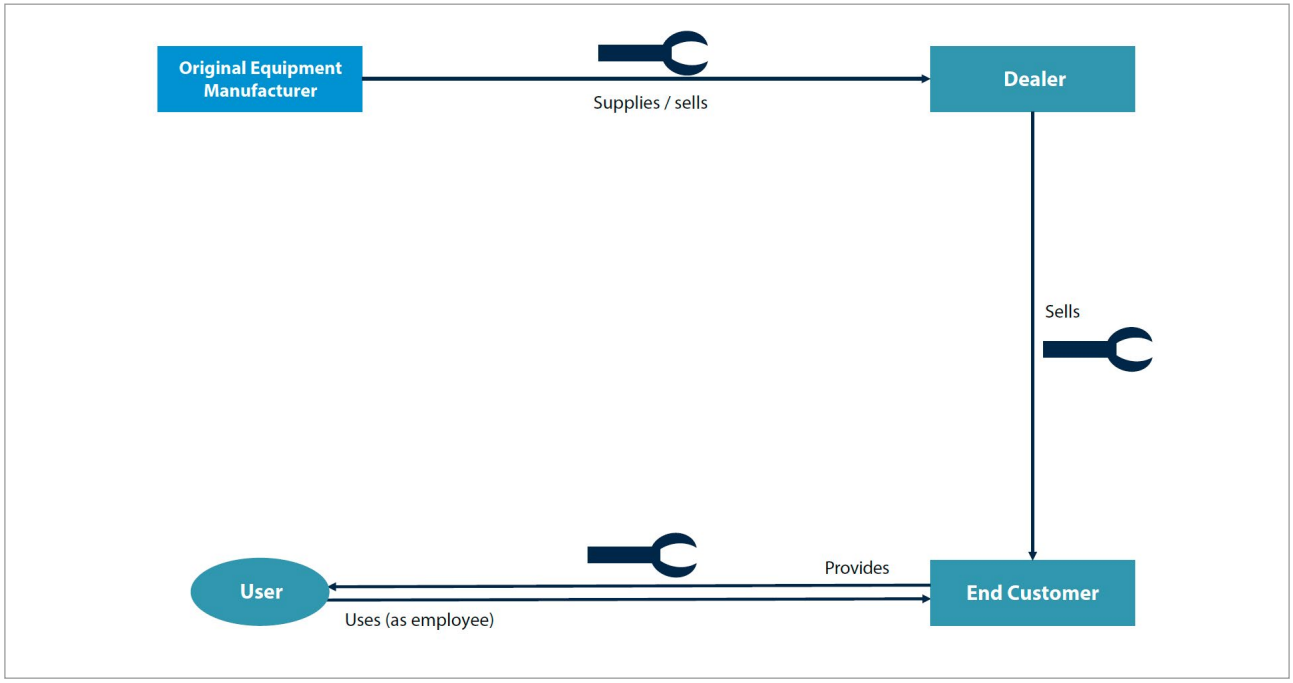
The key aims for the legal counsel at the workshop would include:

- Finalising the new business model from a legal perspective, and assisting the business in understanding all of the elements involved (including the relevance of the intervention of third party suppliers, and considering whether the business would be provided as an operational expense solution, as a service model including software and devices, or as a capital expense solution just for the devices);
- Defining the legal deliverables to be included in the project plan; and
- Defining the key objectives for the project team in delivering the project.

For these exercises, a usual starting point is a white board! Legal counsel should describe the business model from a legal perspective, and then help the project team to understand how the new IoT functionality of the products, despite being a simple addition, changes the business model in a very fundamental way.

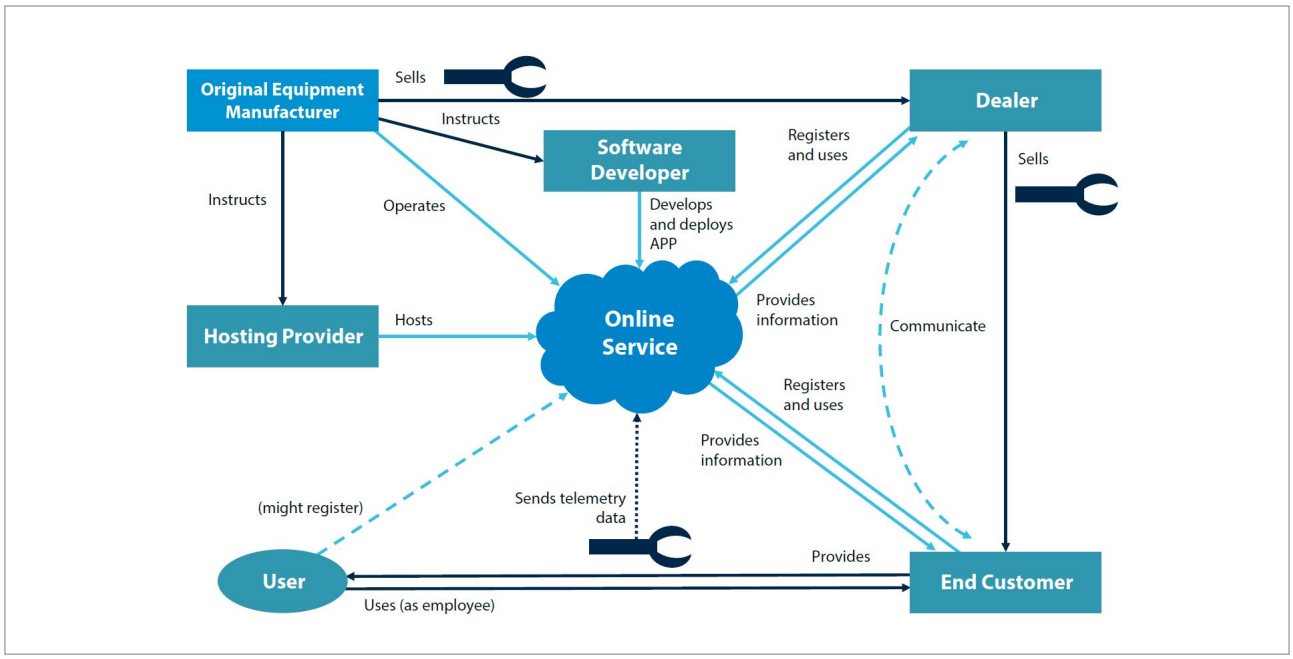
This might be the original business model:

The traditional business model



However, by connecting the products to the internet, and providing an online service directly to the end users, the legal relationships can become a lot more complex, as demonstrated below:

The connected product



C. Key insights

The number of important legal relationships that the business has multiplies in the new business model. Previously the business had a traditional linear sales model, but now that the products are IoT devices, and have digital services associated with them, the business will have direct contractual relationships with all end users. This will be the case even if the end user does not purchase directly from the business.

And some of the contractual relationships are with entirely new categories of partners with which the business is unlikely to have dealt in the past. Alongside the end users of the products, the business also has new contracts to establish with software developers and hosting providers.
These relationships will involve new kinds of risks and require detailed due diligence in legal areas with which the business may not previously have had to grapple, such as complex data protection issues.

For example, something the business may not previously have had to consider is who has the right to use the data which is generated by and collected from its IoT products. This data will be valuable information, and is likely to provide useful insights for both the end user and the business itself.

Other issues to consider include which legal entity will provide the online service; where that entity will be established; where the data associated with the service would be hosted; and how this would be related to the sales organisation, which is likely to be organised on a country-by-country basis.

D. Continuing the project

Following any workshop, the legal elements necessary for the business to successfully launch the new IoT products, and the accompanying service, will need to be integrated into the overall project. Moving forwards, legal counsel is likely to need to support the business with a number of legal deliverables including:

- A risk matrix on providing the online service, covering tax, data protection, commercial and consumer law, intellectual property, and competition law.
- An assessment of the business under applicable data protection laws.
- Drafting terms and conditions and privacy policies for the new relationships being established.
- Negotiations with some of the essential dealers.
- An evaluation of the necessity to amend current insurance policies or to take out a cybersecurity insurance policy.
- The provision of the relevant documentation required, if applicable, for the certification of IoT products, according to standard market practices.
- Setting up the proper contractual structures with suppliers involved in the business model, ensuring, among other things, a proper allocation of responsibilities, reliable connectivity, detailing the ownership of IP assets and data and ensuring adequate service level agreements are in place.
- An assessment on potential restrictions to the import/export of the IoT products to any of the countries where the business model will be offered.

E. Developing compliant connected products in the future

As with other aspects of legal risk, although the addition of IoT sensors into products may, in a practical sense, be straightforward, there are numerous implications when it comes to ensuring that safe and compliant IoT products are placed on the market.

Existing product safety laws were not written in the context of modern connected technology. Although connected products must comply with the Radio Equipment Directive[1], potentially other CE marking directives, and even applicable technical standards, product safety laws generally do not contemplate connected products and the Internet of Things.

This means that it is often difficult: (i) for a business to know whether it is acting in compliance with applicable requirements; and (ii) for end users to know if they are purchasing products which represent best practice in terms of security and system integrity.

There are also risks introduced at both ends of the supply chain. The data collected by the products is valuable, however it might also be confidential, and the business must ensure that the cybersecurity of the products does not leave its users vulnerable.

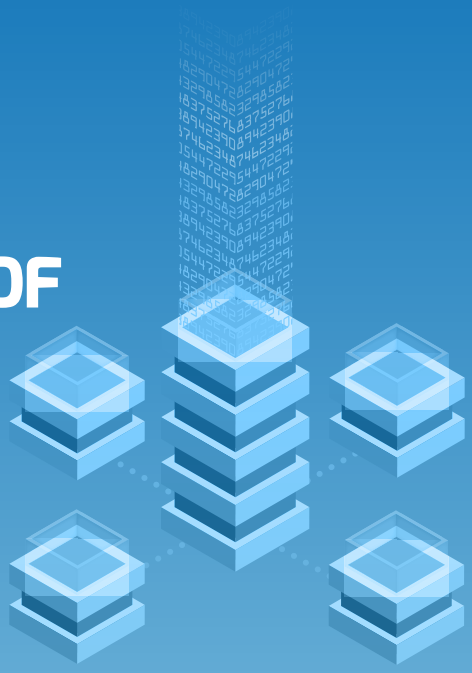
In response to these risks and regulatory uncertainties, the EU has begun to introduce initiatives to ensure that connected devices are safe for both businesses and consumers.

Amendments to the Radio Equipment Directive mean that, by mid-2024, manufacturers of connected devices will need to incorporate features to avoid harming or disrupting the networks they connect to, protect personal data that they might collect, and minimise the risk of monetary fraud.

A proposal for a European Cybersecurity Resilience Act is also anticipated for the second half of 2022, which is expected to establish harmonised standards for connected products throughout their lifecycle.

1 Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment

2.5 DATA POOLING AND DATA INTEGRATION IN GROUPS OF COMPANIES



OSBORNE CLARKE AUTHORS

Victoria Gwynedd-Jones
Legal Director,
United Kingdom

Victoria.G-Jones
@osborneclarke.com

Further information

Gianluigi Marino
Partner, Italy

Gianluigi.Marino
@osborneclarke.com

Further information

Dr Flemming Moos
Partner, Germany

Flemming.Moos
@osborneclarke.com

Further information

Gemma Nash
Associate, United Kingdom

Gemma.Nash
@osborneclarke.com

Further information

Joanne Zaaijer
Partner, The Netherlands

Joanne.Zaaijer
@osborneclarke.com

Further information

DATA POOLING AND DATA INTEGRATION IN GROUPS OF COMPANIES

There are various stages in the life-cycle of a dataset. First, the dataset must be created, whether this is achieved organically, or through merger, acquisition or asset transfer. Then the dataset may be enhanced through the addition of data available from external sources. Thorough analysis of the combined dataset can lead to a deeper understanding of a group's customers, their needs and interests, with resulting benefits. But understanding the limitations on data use at each of these stages is critical to the success of a data pooling project.

KEY TAKEAWAYS

- → Careful due diligence is vital prior to any proposed database acquisition to establish any potential legal or contractual restrictions on usage
- → Upfront definition of the use cases of pooled data can be important, and requires close co-operation between data scientists, business stakeholders and the legal team
- → Clear and robust data governance structures can help to mitigate risk

A. Building a data pool through mergers, acquisitions and other transactions

When a business wishes to build a database or expand an existing database into a data pool, it will commonly consider merging with or acquiring another company, or purchasing specific databases through asset transactions. Before doing so, it is crucial to establish that applicable laws (including those relating to data protection, intellectual property and competition) as well as contractual restrictions will not hinder or prevent a business from achieving the ultimate goal of creating a combined data pool. Conducting careful due diligence is therefore of utmost importance.

The acquisition of a database may in certain cases be subject to prior requirements and approvals. Depending on the nature of the data included in the database it may be necessary to obtain prior consent from data subjects (for example, where the transaction involves health data) or to offer data subjects the possibility of an opt-out. Additionally, where the transaction involves personal data, both the purchaser and the target company will be required to inform the data subjects of the transfer as soon as reasonably possible.

In order to avoid unnecessary barriers and delays, we often advise clients to agree joint statements and consent forms prior to completion of the transaction and to include the drafts in the transaction documentation. Another helpful strategy can be to agree arrangements for some key processes in advance, for example, about how data subjects are to be given the opportunity to supplement or correct their data prior to the transaction. Obtaining accurate and up-to-date data will contribute to an increase in the value of the database.

B. Enriching internal databases with data available on the market

One way in which a business's databases can be enriched is by combining the personal data held by the business internally with data from external sources, most notably statistical data. Useful statistical data may be that relating to the geographical distribution, or the socio-demographic, structural or economic characteristics of the local population. This information, once cross-referenced, can make it possible to identify new evaluation parameters that enable the business to categorise its customers into different clusters (that is, groups of customers that have similar characteristics).

Following this enrichment process, the business's clusters would not be configured exclusively on the basis of the potential client's behavioural analysis but would be redistributed by means of socio-demographic categories provided by the external source of data. This allows the business to identify new, and increasingly defined, sets of potential users to which to address more targeted and therefore more effective promotional campaigns.

This process of association is based on probability and aims to maximise the likelihood of attributing particular characteristics to a certain category of users. Such processing requires the evaluation of the company's legitimate interests and a thorough scrutiny of the new information that is selected, to ensure it is relevant to the purposes for which it is collected.

Data enriched in this way should also be subject to a limited retention period, given its probabilistic nature, subject to possible subsequent irreversible anonymisation. Furthermore, users must be adequately informed of this processing and given a right to object. From a technical point of view, systems should ensure logical and/or physical separation of information,

segregation of duties, and access on a need-to-know basis only. To ensure legal and regulatory compliance of a project such as this, co-operation between the marketing, commercial, IT and legal functions is essential.

C. Creating profiles from data pools for personalised service and marketing

The combination of databases and datasets across separate entities in a group of companies or across different business segments can very often lead to greatly improved insights into how the group's products and services are used. These insights, gained through a deep analysis of the data pool, can provide various benefits to a company: they can allow a business to improve its products and services (for example, by designing them to better meet their customers' needs), or they can be used to make advertising more targeted (for example, by better focusing on what the customer might be interested in).

However, a company can usually only benefit from these advantages if it stays within the narrowly defined legal framework; especially if personal profiles are to be created in the process. One crucial aspect is to find an appropriate organisational structure for the data pool. This is not only necessary in terms of defining the responsible entities: it can also allow certain processing activities to be carved out from the strict requirements of applicable data protection law by anonymising data through an appropriate organisational setup, for example, by making use of a data trustee.

Another important step in order to ensure the success of a data pooling project, is to define the use cases from the outset, as specifically as possible. This is because the legal requirements can vary significantly depending on the actual data used, the specific purpose pursued and the entity that will benefit from the analysis. Defining the use cases accurately requires a close co-operation between data scientists, business stakeholders and legal experts.

D. Data pooling governance and management

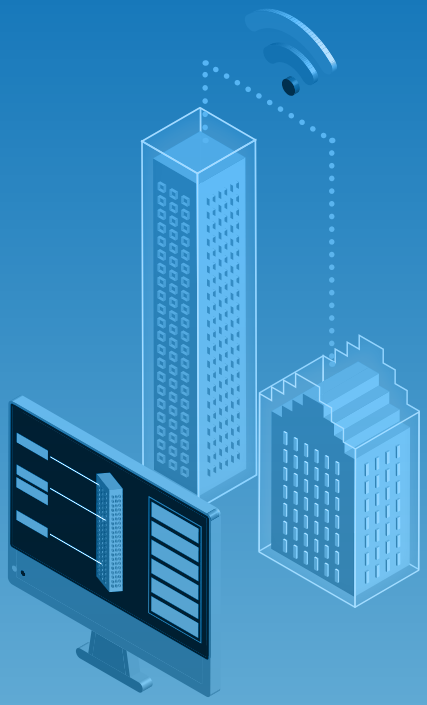
A key legal risk relating to data pooling is unrestricted access to a large amount of data: this can result in abuse, such as using the data in ways that breach legal or contractual restrictions. Depending on the nature and source of the data, use of that data may be restricted due to intellectual property rights (for example, licence restrictions), contractual restrictions (including on use, transfers and storage location), privacy requirements (for example, purpose limitation) and data localisation laws restricting the transfer of data outside the territory in which the data was generated. Such use may also give rise to competition issues (for example, information exchange between competitors).

Understanding the limitations on data use at the outset of a data pooling project is critical to determining how best to structure, manage and govern such use in a way that minimises risks to the business but maximises the value of the data. This includes determining where to store the data (central lake vs. local hosting environments), setting clear parameters on purposes for use, establishing access controls, implementing the right security measures and/or anonymisation techniques.

Challenges seen in practice include identifying exactly which restrictions apply to which data, understanding how the data can be used without breaching these restrictions, and subsequently managing this at scale. Difficulties with overcoming these challenges can cause a data pooling project to subsequently fall apart. The most successful projects are those that understand the limitations on data use at

an early stage of implementation (and critical to this is a process for mapping data flows and labelling data according to use) and that build a clear and robust data governance structure.

2.6 DIGITAL TWINS: ENABLING SALE OF A SERVICE, NOT AN ASSET



OSBORNE CLARKE AUTHORS

Catherine Hammon
Digital Transformation Knowledge Lawyer, United Kingdom

Catherine.Hammon@osborneclarke.com

Further information

Will Robertson
Partner, United Kingdom

Will.Robertson@osborneclarke.com

Further information

Mark Taylor
Partner, United Kingdom

Mark.Taylor@osborneclarke.com

Further information

Joanne Zaaijer
Partner, The Netherlands

Joanne.Zaaijer@osborneclarke.com

Further information

Laurène Zaggia
Senior Associate, France

Laurene.Zaggia@osborneclarke.com

Further information

DIGITAL TWINS: ENABLING SALE OF A SERVICE, NOT AN ASSET

Digital twins are increasingly used in industrial systems. They can be transformative, enabling optimisation of efficiency and output. They can also shift the entire business model for a supplier from selling an asset to selling the service provided by the asset. The contractual relationship between supplier and customer shifts from the sale of goods to the provision of a service, becoming a much closer and potentially more enduring arrangement.

KEY TAKEAWAYS

- → Digital twins are an advanced form of the Internet of Things, a virtual replica of a physical asset synchronised through data flows.
- → Twins can be used to monitor the use of an asset installed with a customer, charging the customer only for the service provided.
- → Although machine data is largely outside current data regulation frameworks, this will change with the proposed EU Data Act.

A. What is a digital twin?

Digital twins use connectivity, Internet of Things (IoT) technology and data flows to turn a straightforward digital model of something physical into a virtual mirror of not only its shape but also its movement, the processes that it undertakes, how it performs, and associated data such as consumption of inputs and production of outputs. Data flows between the physical and digital versions of the asset keep them synchronised. Performance of the physical asset can be mapped onto the virtual one, facilitating real time or slower analysis and optimisation.

In themselves, digital twins can be transformative, particularly in manufacturing, processing and (as discussed in Chapter 2.8) in the built environment. But they are also enabling a fundamental shift in how assets are supplied to customers, supporting data-driven 'Assets as a Service' business models and the 'servitisation' of the provision of physical goods – i.e. selling the service provided by the asset, rather than the asset itself.

B. Digital twins in industry systems

I. Digital twin applications

In industry, processing and manufacturing, digital twins are an advanced application of digital technology – sometimes called 'Industry 4.0'. Anything from single machines, to individual production lines or whole factories can be digitally modelled and connected to create their virtual mirror.

Digital twins are typically hosted in the cloud and so can be accessed and controlled from anywhere. Where a digital twin sends and receives data to and from the physical twin with real time data flows, it can be used to monitor or control the physical asset remotely. Real time digital twins can be used as an early warning system for problems with machinery or infrastructure. They can be integrated with augmented reality tools to enable visualisation of the data flows and information about output and performance against each piece of machinery as someone walks the factory floor. Digital twins can also integrate with additive manufacturing systems (industrial 3D printing), enabling the manufacture of bespoke repairs based on the digital model and insights into the malfunctioning parts.

Alternatively a digital twin can be run separately to the physical twin. Such systems might be used for training purposes, for example to teach repair or maintenance routines for remote or dangerous assets such as wind turbines. Financial risk can be considerably reduced by building, testing and finessing a prototype as a digital twin before any expenditure or investment is made in building a physical prototype. When the physical prototype is built, it is much less likely to need radical modifications. When the new product is ready for production at scale, its digital twin is already in place.

New hardware or software can be tested and commissioned on a digital twin, rather than the physical machinery. Performance can be tested and optimised on the digital twin. Once perfected, the finely tuned improvements can be transferred across to the physical machinery with minimal disruption to production schedules. Historical data about performance can be analysed to understand patterns of wear and tear or asset failure, enabling predictive maintenance and more efficient deployment of maintenance staff, and correspondingly reducing unexpected downtime and emergency call-outs.

For all of these reasons, digital twins are increasingly an integral part of software systems for industry and manufacturing.

II. Legal issues

Digital twins typically need collaboration with a number of providers.

Most smaller businesses will procure the core technology from an external source. Many of the traditional industrial engineering conglomerates have transformed themselves into digital industry specialists, turning their in-house technical expertise into third party offerings and new revenue streams. Cloud-based hosting services may be provided by that business or a third party. Building the digital twin, installing the new systems and establishing the data flows may well need consultancy services from the software provider or another specialist.

Depending on the sophistication of the twin, collaboration may be needed with research bodies (for example, the digital twin might include scientific data about the physical properties of its moving parts such as friction or vibrations).

All of these relationships will need to be documented and shaped with procurement and/or consultancy agreements. Depending on the complexity, value and degree of customisation of the systems being installed, these projects can require bespoke negotiation of contractual relationships.

In particular, care will be needed to define responsibilities and liability. These will often become ongoing commercial relationships once the initial development and installation is complete, and may become business-critical, particularly if production depends on them. For that reason, expertise in tech dispute resolution can be essential if such relationships break down at any point – replacing technology systems can be extremely disruptive. It may be sensible to agree up front provisions to deal with below-par service or performance to minimise disruption should disputes arise.

It may also be sensible to consider enhanced cybersecurity provisions across these relationships. Digital connections into third parties constitute a new avenue of attack and cyber risk. Agreeing key performance indicators for cyber and information security management from suppliers is recommended, backed up with periodic reporting requirements and audit rights.

C. Digital twins powering assets as a service

I. The 'servitisation' model

Digital twins of an asset can power an even greater transformation where they enable a manufacturer or supplier to switch from selling the asset itself to selling the service that it offers.

This model is used across a range of valuable assets, from aircraft engines sold on the basis of the power delivered, to packaging machinery at the end of a production line sold on the basis of the number of wraps made. The asset is installed with the customer – at their premises, on their production line or on their aircraft – but title over the asset does not pass to them and remains with the supplier.

Pricing is based on the service provided: a price per use is multiplied by the number of times the customer uses the asset. The price can be bundled to include repairs and servicing of the asset, additional consumables or an allowance for spare parts. Insurance may well remain the responsibility of the supplier, in which case it becomes part of the cost base for providing the service.

A bundled pricing structure often lends itself to a subscription model with a fixed price per day, week or month, based on projected use or consumption over that period. Digital twins enable a different approach. Very granular pricing can be calculated based on actual operation of the physical asset, monitored by data flows back to

its digital twin. The data enables the supplier to issue invoices for the exact amount of the service that has been consumed by the customer.

For the customer, this can be a powerful shift, particularly where the asset concerned is of high value. In particular, it transforms what would have been capital investment in acquiring the asset into operating expenditure that is a variable cost driven by actual consumption. No asset finance is needed to procure the asset; it will not appear on the balance sheet; there will be no depreciation charges; and, overall, there will be reduced financial risk. This change flows into corresponding differences in tax treatment of the asset and the service provided by it.

II. Legal issues

At its most basic, the shift from selling an asset to selling the functionality that it offers changes the legal relationship between supplier and customer from a contract for the sale of goods to an agreement for the provision of services.

In particular, the relationship between supplier and customer moves from being primarily a relatively time-limited interaction of ordering, delivering and perhaps installing the asset, to a closer relationship over a much longer period. Performance of the ongoing interaction between supplier and customer becomes more significant. Key performance indicators will need to be agreed – both what to measure and how to measure it. They may be needed in relation to both the output of the asset and associated services such as repairs and maintenance. It could be prudent to anticipate how any disputes should be dealt with, to minimise as far as possible the risk of any escalation of disputes in a relationship which may be business-critical, for example for maintaining production output levels.

The digital twin of the supplied asset will be the property of, and/or controlled by the supplier (at least as far as the customer is concerned). If the customer is to have access to the digital twin for the asset and/or access to the data collected from the asset, terms and conditions around data flows and associated digital services will need to be agreed. Cyber and information security provisions may also need to be included. To the extent that the digital connections between the parties create risk for each other, the parties may wish to include cybersecurity performance levels in the agreement, which might be reinforced by agreed audit and reporting processes.

Given the industrial context, the data protection regime for personal data is not likely to be in play. However, the customer may wish to include confidentiality or ringfencing provisions in relation to data collected by the supplier's digital twin, since it may provide valuable insight into its business's performance. It may also wish to constrain any wider use of data flowing from its use of the asset by the supplier.

A clear liability framework will need to be agreed between the parties to ensure that responsibility for any issues such as breakdowns, faulty operation, problems with the data flows or functioning of the digital twin is clearly allocated. If the day-to-day operation of the asset is carried out by the customer's staff, the supplier may require the customer's staff to undergo specified training to ensure that the asset is used correctly. Allocation of liability between the parties will need to include situations where the asset is damaged or underperforms due to errors by the customer's staff, or the damage is otherwise caused by them.

As regards pricing, the supplier will need to consider whether the costs of installation are charged up front, or recouped during the lifetime of the contract as part of the cost base for the services supplied. If the latter, would a pro rata penalty for early termination be needed to recoup upfront costs that had not yet been clawed back? Terms of renewal will need to consider how the absence of installation costs affects pricing for the second contractual term,

as well as any adjustments for changes in other costs. Although concerns tend to be less acute in relation to business-to-business relationships, fairness in pricing where contracts roll over into new terms has been a focus for competition and consumer authorities.

On termination, ongoing access for the customer to historic data collected by the supplier about the performance and output of the installed asset will need to be considered, as well as arrangements for timely recovery of the asset by the supplier.

As regards financing the asset, this will no longer be needed by the customer. Any asset finance will instead be needed by the supplier, perhaps to fund manufacture of the new asset, to be serviced by the future revenue stream from the customer. Potentially, the need to service debt may necessitate a minimum purchase obligation on the customer to ensure that a lower level of use of the asset by the customer than forecast does not create risk of default by the supplier under the financing arrangements.

As with any commercial relationship, the extent to which the supplier is prepared to negotiate its standard terms and conditions around the supply of an asset provided on an 'as a service' basis will depend on the value of the contract and of the wider commercial relationship with the customer. The larger the installed asset base of the supplier, the less it will want different terms of service provision with different customers.

D. Future regulation of IoT data flows

At present, there is minimal regulation around non-personal data flows. The performance of machinery is unlikely to reveal information about identifiable individuals so data privacy regulation will not usually be a prime consideration in relation to an industrial digital twin or a servitisation business model.

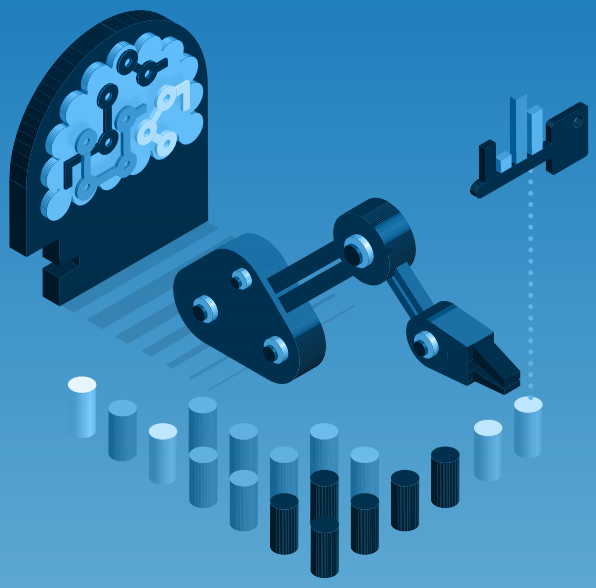
However, the European Commission's recent proposals for a Data Act[1] would extend the scope of data regulation to include swathes of non-personal data generated in a business context.

Manufacturers of data-collecting connected products and providers of related services will be required to make the data generated by their use easily accessible to the user, whether a business or a consumer, potentially in real time as it is collected. The user will be entitled to pass the data on to third parties or use it for their own purposes. Users may also demand that the data is made available directly to third parties. The manufacturer or supplier's own use of that data will be limited and need to be contractually agreed with the user.

The Data Act, which is intended to reshape the European data ecosystem, is discussed in more detail in Chapter 2.10. It remains some way off from becoming law, and is expected to be changed as it makes its way through the legislative process. But it is extremely likely that the ability to comply with the new regime – including the capability to pipe data out to users and third parties – will need to be designed into all new data-collecting business models, and retrofitted into existing ones. Digital industrial systems will be no exception.

1 The Commission's proposals are available at https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113 Osborne Clarke's summary of the proposals is available at https://www.osborneclarke.com/insights/eu-data-act-proposal-commission-plans-comprehensive-right-data-access

2.7 REGULATING DATA-POWERED ARTIFICIAL INTELLIGENCE



OSBORNE CLARKE AUTHORS

John Buyers
Partner, United Kingdom

John.Buyers@osborneclarke.com

Further information

Catherine Hammon
Digital Transformation Knowledge Lawyer, United Kingdom

Catherine.Hammon@osborneclarke.com

Further information

Dr Sabine Von Oelffen
Counsel, Germany

Sabine.Vonoelffen@osborneclarke.com

Further information

REGULATING DATA-POWERED ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is an increasingly powerful and pervasive tool being used to boost productivity across all sectors. Data is its essential fuel. A wave of new regulation is coming at EU level both for AI specifically and for the data needed to feed it. The latter will boost availability of data, but compliance will need to be built – or retrofitted – into AI tools to avoid the risk of enforcement action and fines.

KEY TAKEAWAYS

- → AI regulation is a new field but a policy focus area for legislators.
- → The EU's cross-sector proposals are working through the legislative process, while the UK is still at the policy-development stage.
- → Suppliers and developers of AI should monitor developments: regulatory compliance will become a design consideration.

A. The importance of data for artificial intelligence systems

AI, in its machine learning and deep learning forms, depends on data.

AI systems are trained to perform their allocated tasks using vast quantities of information. The systems are set up to identify and map patterns in the training data, creating a huge matrix that is subtly recalibrated and refined with each new piece of data that passes through the system. Once trained, the AI system can be used to classify new pieces of data based on the data that it has been trained on, or to generate data that is similar to its training data.

AI is used for a vast range of commercial applications. It can be used for decision-making – this information matches that grouping and so produces that outcome; this person can be classified as low risk so can be given consent for a new credit card; this candidate matches the preferred characteristics so should be interviewed; that customer query corresponds to this answer. It can also be used for interpretation of visual images or text – this image is a dog; that scan has cancerous cells; this sentence in one language translates into that sentence in another; there is a person on that crossing. It can also be used for prediction tasks – this drug may match that medical problem; this new text answers that question; this machine part is likely to break down around that date; these related website links may be useful for someone reading that webpage.

The applications that AI can be put to are hugely varied, but each individual tool has only 'narrow' intelligence, in the sense that it is trained for a very specific task and objective. Although AI systems can sometimes find patterns in data that humans had not spotted, and so generate outputs that humans did not expect, they are entirely constrained by the scope of the data that has been passed through them. A system for recognising apples that has not been shown enough pears or oranges would not be able to distinguish between them. AI systems cannot map ideas, concepts or data that they have not been shown through the training datasets, and have no wider common sense or understanding of the context in which they are deployed.

Accordingly, AI systems can only reflect and replicate the data passed through them. If the training data is poor quality, unrepresentative or biased, then the resulting AI will very likely reproduce those problems and generate outputs that are poor quality, unrepresentative or biased. As the data scientists put it, "Garbage in, garbage out".

For all these reasons, the availability of data, its quality, and its appropriateness for the task in hand, are all key considerations when developing and using AI tools. Given the breadth of applications of AI, poor decision-making could clearly generate harm to businesses or individuals in a myriad of ways.

B. Regulation to ensure trustworthy AI

I. The proposed AI Act

In April 2021, the European Commission published proposals for a new cross-sector regulatory regime for AI.[1] The legislation takes a risk-based approach:

- AI tools in a limited number of defined areas (such as social scoring or real time facial recognition surveillance systems in public areas for law enforcement) will be prohibited, subject to exceptions;

1 The proposed legislation and wider documents on "A European approach to artificial intelligence" can be found at https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence. Osborne Clarke's summary of the legislative proposal is available here: https://www.osborneclarke.com/insights/european-commission-proposes-new-regulatory-framework-artificial-intelligence

- AI systems considered to be "high risk" will be subject to extensive regulation with an enforcement framework at national level that includes the potential for heavy GDPR-style fines for non-compliance;

- AI systems designed to interact with humans will be subject to transparency requirements to make sure the person concerned knows they are dealing with an AI tool, not a human; and

- Other AI applications are left unregulated.

Broadly speaking, the "high risk" categories are focused on AI tools used in health and safety systems, or which impact on fundamental human rights – in both cases the focus is on the risk of harm to natural persons. For example, the proposed high risk categories include biometric ID systems, credit scoring systems, a number of HR systems such as job application sifting, work allocation or employee performance measuring, as well as AI systems used in the public sector such as social security assessments, border control checks or asylum eligibility systems. The draft recitals highlight the risk that AI systems could perpetuate historical patterns of discrimination, create new discriminatory impacts, or result in injustices against individuals.

National regulators will be created (or powers extended) to ensure enforcement of the new regulatory framework. Businesses will be required to undertake conformity assessments and in most cases will be able to self-certify compliance. AI tools in conformity will carry the CE mark, and must be registered on a central register maintained by the Commission. In addition to the data provisions discussed below, high risk AI must also meet mandatory requirements in relation to technical documentation, record-keeping, wider transparency issues, human oversight, plus accuracy, robustness, and cybersecurity.

The EU's approach can be seen as another example of its strategic ambition to set the gold standard for digital regulation around the world. It is certainly the most advanced legislative proposal in this field and is ambitious in its aim to create a single horizontal regime, rather than more tailored regulation for different sectors or risk areas.

II. The proposals regarding data

Since data is the fuel for AI, the provisions regarding data are likely to be correspondingly significant in their impact. Obligations for high risk AI systems concerning data and data governance training are addressed in Article 10 of the proposed regulation. The proposals are demanding and extensive:

- Data governance and management practices must cover design choices; data collection; relevant data preparation processes; the assumptions about what the data measures and represents; prior assessment of the availability, quantity, and suitability of the required datasets; examination for possible bias; and the identification of possible gaps or shortcomings in the data and how those gaps and shortcomings can be addressed.

- Datasets must be relevant, representative, free of errors, and complete, and must have appropriate statistical properties for the intended application of the AI tool concerned.

- Where appropriate, datasets must take into account the particular characteristics or elements of the specific geographical, behavioural, or functional setting in which the high-risk AI system will be deployed.

The standard required of data is important because this is one of the limited areas where the highest level of fines envisaged under the proposals for non-compliance – up to six per cent of global turnover – will apply.

The intention of these provisions is to ensure that datasets are properly and responsibly curated to minimise the risk of poor quality data resulting in a poor quality tool more likely to cause harm. But the final provisions are likely to incorporate amendments. The Commission's proposals are demanding to a point that many commentators consider both unrealistic and disproportionate, requiring a near-perfect standard of data, which may simply not be achievable. Given the severity of the potential fines, it is important that compliance does not involve disproportionate difficulty or burdens on businesses.

III. Opening up access to data

As well as quality of data, access to data is essential for a thriving AI ecosystem. The AI Act does not address this issue, but it is one of the focuses of separate legislative initiatives at EU level, flowing from the European Data Strategy.[2]

The Commission's November 2020 proposal for a Data Governance Act seeks to shape the data ecosystem by encouraging the availability of public sector data, by regulating for-profit intermediaries that supply data to optimise consumer trust, and by providing for new data sharing structures for individuals to "donate" their data to not-for-profit organisations that will be able to supply data for defined purposes. The Data Governance Act is discussed in Chapter 2.12.

Separately, the Commission's proposed Data Act of February 2022 makes provision for opening up access to privately held datasets, and for enhanced portability of data. The Data Act is discussed further in Chapter 2.10.

The Commission is also seeking to develop "European Data Spaces", with pools of data for particular sectors, including healthcare and energy. These initiatives are intended to ensure the availability of data across a wide range of areas to fuel innovation and advances – including developing new AI tools, or improving or updating existing ones.

IV. UK plans to regulate AI

Post-Brexit, the EU legislative initiatives discussed above will not apply directly in the UK (although they will, of course, affect UK and other third country businesses that sell to EU customers).

The UK is not currently planning to take a similar horizontal, one-size-fits-all approach to regulating AI. It is moving somewhat slower than the EU in developing its policy. A White Paper and consultation on how to approach the UK regulation of AI is expected during the course of 2022 (delayed from the first quarter, which the UK's National AI Strategy[3] had signalled). Although the UK had previously indicated that a "vertical", sector-specific approach to AI regulation was preferred with policy development led by sector regulators, the White Paper is expected to reopen that decision and seek views through consultation on whether a horizontal approach would be desirable, particularly to ensure conformity of approach between sectors.

2 Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

3 Available at https://www.gov.uk/government/publications/national-ai-strategy

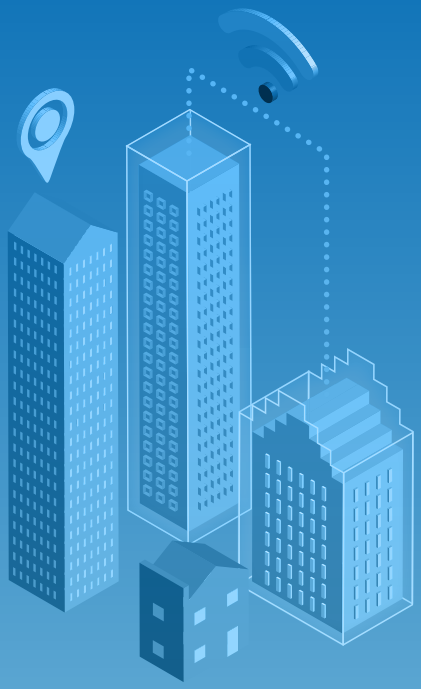
C. Be ready for increasing regulation of AI

Currently, these new areas of legislation are still making their way through the legislative process. Once finalised, each will incorporate a time period for transition before compliance is required. Change is not imminent – but there is no doubt that it is coming.

The regulation of both AI tools and the data that shape them will significantly impact on AI developers, suppliers and organisations using AI. Each of these legislative initiatives from the EU is novel, ground-breaking, and extends digital regulation into new areas where legal compliance had previously been much more limited.

As with so much digital technology, compliance by design will be extremely important. AI-centric business models that do not yet incorporate regulatory compliance – in both product design and data procurement and curation – may require disruptive and potentially costly rethinking. Although the new EU regulations are not yet in force, their future scope and impact needs to be monitored by all those operating and developing AI-centric data-driven business models.

2.8 DIGITAL TWINS IN THE BUILT ENVIRONMENT



OSBORNE CLARKE AUTHORS

Catherine Hammon
Digital Transformation Knowledge Lawyer, United Kingdom

Catherine.Hammon@osborneclarke.com

Further information

Jonathan Mills
Partner, United Kingdom

Jonathan.Mills@osborneclarke.com

Further information

Tamara Quinn
Partner, United Kingdom

Tamara.Quinn@osborneclarke.com

Further information

Steven Verschuur
Partner, Belgium / The Netherlands

Steven.Verschuur@osborneclarke.com

Further information

Laurène Zaggia
Senior Associate, France

Laurene.Zaggia@osborneclarke.com

Further information

DIGITAL TWINS IN THE BUILT ENVIRONMENT

Digital twins can offer powerful insights into the built environment, including ensuring optimised energy use or enabling visualisations of environmental data. The collaboration of a number of stakeholders will need a clear governance framework, including allocation of liability, ownership of intellectual property and arrangements about data sources, flows and access rights. Legal and regulatory compliance will need to be incorporated by design from the outset.

KEY TAKEAWAYS

- → Clarity around data and intellectual property being put into the digital twin or being created by it is critical to the success of the collaboration.
- → If the project involves public sector bodies, public procurement rules and State aid/ subsidy rules may need to be considered.
- → Competition law compliance may shape data flows and feed into whether third parties are given access to the digital twin.

A. Modelling physical assets and infrastructure

I. The digital twin concept

A digital twin is a virtual model of something physical. The starting point is typically its physical shape, but any other aspect of the physical thing can be modelled into the digital version. Real-time data about any aspect of the asset can also be fed into the digital twin so that it becomes a synchronised virtual mirror of key aspects of the physical thing, its performance or its processes.

Digital twins are an extension of the Internet of Things (IoT) technology that underpins many real estate solutions. For example, building automation systems can monitor and automatically adjust the settings for heat, ventilation or light within a building to ensure that it is operating efficiently and maintaining the desired parameters for temperature and air quality.

Digital twins take the concept further by modelling a broader range of features, potentially with more complex analytics, to enable a more complete representation of the physical asset. As explained in Chapter 2.6, digital twins can be used to monitor actual operations, to optimise efficiency and performance, to flag future performance problems and to undertake analysis of different situations or scenarios without interrupting or disrupting the operation of the real assets.

II. Ambitious projects

Digital twins need not be limited to single buildings but can encompass a particular estate, a district of a town or city, a whole city or even a whole country. They are often part of 'smart city' initiatives.

For example, Singapore is developing a digital twin of the whole city-state. "Virtual Singapore" offers a three-dimensional model of the physical city and a collaborative data platform for use by public, private, and research sectors. The UK has a hugely ambitious "National Digital Twin programme"[1], initially set up by a partnership between the government and academia with extensive collaboration with private and public sector organisations. It is intended as "an ecosystem of connected digital twins to foster better outcomes from our built environment".

Digital twins of the built environment can be used, for example, to monitor pollution and air quality but also to understand how wind and airflows through the city impact on pollution dispersion. A digital twin focused on traffic management might show the road network through the centre of a town and be integrated with the traffic management system to optimise traffic light phasing, or to redirect traffic away from a congested area following an accident. Sophisticated data analytics such as artificial intelligence (AI) can be integrated with digital twins, enhancing the insights that the digital twin can deliver, such as generating predictions and forecasts or spotting anomalies in the data.

III. Sustainability and decarbonisation objectives

Digital twins can play a powerful role in delivering energy efficiency, decarbonisation and sustainability objectives. Osborne Clarke recently published research in partnership with Econ-

1 https://www.cdbb.cam.ac.uk/what-we-do/national-digital-twin-programme Osborne Clarke's work on the legal aspects of the National Digital Twin programme is discussed in this article: https://www.osborneclarke.com/insights/shaping-future-success-uks-national-digital-twin-early-legal-input The National Digital Twin Programme is now part of the UK's Connected Places Catapult accelerator hub: https://cp.catapult.org.uk/news/the-cdbb-digital-twins-hub-at-the-connected-places-catapult/

omist Impact[2] seeking to identify "impactful, scalable and investable technologies to drive urban decarbonisation". As the report notes, digital twins can be used to plan efficiencies in a city space, to make construction more efficient, or to make buildings more sustainable and to reduce their energy consumption.

It must not be overlooked that digital twins may themselves require significant processing capacity which in turn may consume significant energy. Analysis is needed of whether the environmental benefits that the digital twin can deliver outweigh the carbon footprint of the technology itself. But – particularly with the growth of green cloud services and renewable energy more generally (discussed in Chapter 2.11) – delivering a net benefit appears to be an achievable goal.

B. Collaborative structures

The success of digital twins of the built environment is often driven by bringing a variety of different stakeholders into the arrangement. This is in contrast to digital twins created for industrial applications or which drive 'Asset as a Service' business models (discussed in Chapter 2.6), which may need commercial partnerships to build and deliver, but can be characterised as private, closed systems. Collaborative arrangements across a sector, by their nature, need to be more open – and regulation may also push in the direction of openness rather than exclusivity.

Chapter 2.6 discussed the legal considerations around the development of digital twin systems in an industrial context. Many of the same considerations will apply to digital twins for the built environment. This chapter discusses the additional legal issues that flow from the wider collaboration that is usually needed for the broader and more complex alliance of stakeholders that are typically involved in a smart cities project or similar digital twins of the built environment.

I. Co-operation frameworks

Collaborative projects involving the investment of time, money, expertise and – given the digital context – data, require a contractual framework to set up the terms of governance of the partnership or alliance. In some situations, a self-standing corporate vehicle might be appropriate, in which case key terms will tend to be set out in a shareholders' agreement. Alternatively, the collaboration might be looser and less permanent, with contractual provisions governing the commercial partnership.

Either way, it is important not to underestimate the time needed to negotiate and sign such an agreement. Our experience of digital collaborations is that reaching a consensus on the contractual framework is often at least as complex as building the technology itself.

Consortium arrangements will typically deal with issues such as:

- the respective roles and obligations of the various parties;
- governance provisions for the project, including what it will or could be used for, oversight of the system, third party access provisions;
- provisions for distribution of any revenues or profits from the project;
- the arrangements for the licensing of intellectual property into the project and ownership of any intellectual property resulting from the project;

2 See Osborne Clarke's report with Economist Impact on "Sustainable disruption: 12 decarbonising technologies for cities" (November 2021), available here: https://www.osborneclarke.com/insights/sustainable-disruption-12-decarbonising-technologies-cities-report

- where data is to be shared, terms governing the use, storage or access rights in relation to the data, as well as ownership of and access to data generated by the project;
- arrangements for the day-to-day running of the project;
- responsibility for issues such as cybersecurity, maintenance and upgrades to the digital twin system;
- the split of liability between the partners for any harm caused by reliance on the digital twin, or on data contributed;
- provisions concerning any reserved decisions;
- provisions dealing with the change of control of participants; and
- terms for exit from the arrangement and for entry of new partners.

II. Standards and interoperability

The parties to a digital twin project will need to consider at the outset the question of standards and interoperability. Technical specifications will need to be clear and universally understood. Cybersecurity standards, data formats and integration issues are all crucial.

These are not legal considerations. But operational issues around the architecture and specifications of the digital twin technology could readily become a source of disagreement, disruption or delay to the project. In order to avoid disputes, it would be sensible to consider and agree these issues up front, and include the agreed technical specifications in the framework agreement between the parties. Securing consensus to ensure interoperability and smooth data flows is a valuable investment of time and effort.

III. Public sector involvement

Where the collaboration involves public sector bodies and organisations, additional legal and regulatory considerations may come into play. Public bodies have many key roles in relation to the built environment both as decision-makers in areas such as planning, and through their responsibilities for running urban infrastructure and services. The public sector, moreover, may be the custodian of key data and data feeds that are needed, or would be desirable, to inform a digital twin of an urban area. Digital twins of the built environment may well, therefore, involve the participation of public sector bodies.

Firstly, if goods or services are being provided to public entities, the parties will need to consider whether regulated public procurement regimes are triggered. These rules govern the processes by which public bodies decide who to contract with, with the objective of ensuring that public sector contracts are awarded in a way that is open, competitive and non-discriminatory. A public procurement regime applies across the EU, and very similar rules remain in force in the UK post-Brexit (pending wider reforms). The public procurement regime only applies where financial thresholds for particular types of contracts are met, but basic standards of transparency and impartiality apply for lower value contracts, so fixed procedures may still need to be followed.

Secondly, if public funding or financial support in other forms is being put into the collaborative project, state subsidy rules may need to be considered, such as the EU State aid rules or the UK's public subsidy regime. Both regimes seek to ensure that a business does not gain an unfair competitive advantage from financial support from the public purse that is not available to its competitors.

IV. Competition law issues

Collaboration within a particular sector may involve businesses that are competitors, or that are active in related markets – such as one operating at a different level in the same supply chain. Where this is the case, care must be taken that the competition rules are respected as regards the terms of the collaboration and in relation to the exchange of data. Additionally, enforcement authorities tend to be concerned that collaboration in one area could spill over into other, more contentious issues, resulting in cartel-like behaviour and harm to competition or consumers.

Information flows – at the heart of many digital twin projects – can be considered a serious breach of competition if the information gives a business insight into another's competitive position or strategy and results in muted competition or even aligned behaviour between them. Each situation needs to be assessed on its facts but in some cases it may be necessary to restrict certain categories of data from being shared, or to implement data ringfencing provisions within the competing businesses so that the circulation of competitor data accessed via a digital twin is strictly limited and does not influence competitive strategy.

This can be complex territory, but guidance from the enforcement authorities can help. In particular, there are useful developments where digital twins are being used to generate energy efficiencies, or as a delivery mechanism for net zero strategies. The EU and UK competition authorities are currently developing guidance for businesses in relation to the application of competition law to sustainability agreements. The aim is to offer clarity in the interpretation of competition law so that it does not create unnecessary complication or caution in environmental or sustainability-focused projects where the collaboration is not focused on the parameters of competition.[3]

More generally, collaborative digital twins within an industry sector raise the possibility that they create an asymmetry of advantage for those who are part of the project over those who are not. Care is needed in such situations that the collaboration does not create market distortions which might amount to a competition infringement. This may mean that although a digital twin has been created by a limited group of stakeholders, others in the market need to be able to access the model, or its outputs, on fair, reasonable and non-discriminatory terms, to avoid distortions of competition. Any pricing strategy for access will also need to be reviewed for its impact on competition.

V. Intellectual property, data and access

Ensuring robust provisions around the contribution and licensing of existing intellectual property rights (IPRs), and the ownership of any rights created from the collaboration or from the use of the digital twin, will be fundamental to the success of a collaborative digital twin. Digital twins will generate a range of IPRs, from copyright in software, patents covering sensors and integration systems, to confidential information and database rights in the generated data.

The consideration of IPRs will need to extend to the data being put into, and generated by, the digital twin.

As regards the data being put into the digital twin, parties will need assurance, probably in the form of warranties, that each entity supplying data for the initiative has the right to do so,

3 https://www.osborneclarke.com/insights/uk-and-eu-regulators-offer-further-detail-how-competition-law-can-support-sustainability (April 2022)

and does not infringe any third parties' rights by sharing the data. Agreement will need to be reached between the parties as to the level of warranties about the accuracy and completeness of the data. Liability for the data going into the digital twin, and for data generated by it, will also need to be considered.

As regards the data and analysis flowing from the digital twin, rights in that data will need to be set out clearly, as well as the term of access to the data both for the parties to the agreement and any third parties. Data generated from digital twins has the potential to be very valuable for use in training AI systems. The machine-learning systems which typically underlie many AI systems are developed and honed by feeding them vast datasets. This includes the AI systems which will, in future, be integrated into the digital twins themselves.

Where the digital twin involves the development of new software, or adaptation of existing software or AI systems, the parties will need to be clear about ownership of the IPRs in the finished software. Thought should also be given as to whether the software itself can be further commercialised beyond use for the digital twin. The technology underlying the digital twin might be very valuable – on the one hand, that value needs to be protected and preserved but, on the other, if it could be used for digital twins of other aspects or geographies of the built environment, then commercialising it could offer a material further revenue stream.

It must not be overlooked that data used in or generated by digital twins may include personal data which may be subject to the EU or UK data protection regimes if it concerns an identifiable individual. This could include data from door access systems, information about electricity use in a domestic dwelling, images picked up by cameras monitoring particular areas, or even temperature changes created by the presence or absence of a person in a particular zone.

C. Compliance by design driving success

As with so many of the data-driven business models explored in this report, there are many different legal angles to be considered around collaborative digital twins for the built environment. Compliance needs to be designed into the project from the outset, with an early injection of legal advice. This will ensure that the project is not hampered by late consideration of regulatory issues and having to retrofit compliance into the arrangements, potentially causing delay and costs that could have been avoided.

2.9 HOW TO RESPOND TO A RANSOMWARE ATTACK – AN ILLUSTRATIVE EXAMPLE

CASE STUDY

OSBORNE CLARKE AUTHORS

Grégoire Dumas
Counsel, France

Gregoire.Dumas@osborneclarke.com

Further information

Nina Lazic
Associate Director, United Kingdom

Nina.Lazic@osborneclarke.com

Further information

Xavier Pican
Partner, France

Xavier.Pican@osborneclarke.com

Further information

Dr Tobias Rothkegel
Counsel, Germany

Tobias.Rothkegel@osborneclarke.com

Further information

Adrian Schneider
Partner, Germany

Adrian.Schneider@osborneclarke.com

Further information

Olgierd Świerzewski
Co-Managing Partner, Poland

Olgierd.Swierzewski@osborneclarke.com

Further information

HOW TO RESPOND TO A RANSOMWARE ATTACK – AN ILLUSTRATIVE EXAMPLE

Cyber attacks have become a fact of life. They are a persistent and real risk for any business, with the frequency and severity of attacks increasing dramatically over the past few years. Our case study illustrates how to navigate a cyber attack: to ensure that operational impact, reputational damage, financial loss, and legal liability are minimised, and the potential fallout is managed to the greatest extent possible.

KEY TAKEAWAYS

- There are jurisdictional nuances, even as between the UK and EU interpretations of the GDPR, which mean that the approach and strategy in one country may not be the right approach to take elsewhere.
- Investigations need to be carefully managed, to ensure that the relevant issues are addressed and any written report does not inadvertently increase legal liability. Expert legal and cyber forensics advice should be sought at the earliest opportunity.
- It's not all about the GDPR. Cyber attacks might trigger additional legal and regulatory obligations. Make sure that these are fully considered, alongside any GDPR analysis.

A. Fictional scenario

TechCo, a London-headquartered technology company, with subsidiaries in France, Germany and Poland, has suffered a ransomware attack. The ransomware attack has encrypted a large tranche of the data held by TechCo (including personal data). The type and quantity of affected personal data is unknown at this stage. It is also not yet clear whether TechCo's back-ups have been affected.

The hackers have contacted TechCo's CEO, threatening to release personal data onto the dark web if a ransom payment of the bitcoin equivalent of $500,000 is not made within 72 hours, in exchange for the return of the data.

TechCo's IT team has started investigating the incident. Investigations have not yet confirmed whether the hackers have, in fact, exfiltrated data (including personal data) from TechCo's systems.

B. Factual investigations and operational issues

TechCo should consider at the earliest opportunity whether it may be necessary to appoint an expert cyber forensics firm to assist with any investigation. Internal IT teams may not have the necessary time and expertise and there can be questions in relation to independence.

If TechCo instructs a cyber forensics expert, it should consider whether it is possible to instruct that expert in a way which means that any reports produced are privileged (to the extent that this is possible in individual jurisdictions). If it is not possible to produce a report under privilege, then TechCo (and its lawyers) should exercise careful control over the production of the report to ensure that it does not increase TechCo's legal liability for the incident.

C. Legal and regulatory issues

I. Article 33 GDPR – notifying the relevant supervisory authority

Under Article 33 of the General Data Protection Regulation (GDPR), a data controller must notify a personal data breach to the relevant data protection authority no later than 72 hours after having become aware of it unless the breach is unlikely to result in a risk to the rights and freedoms of those affected. At present, there is no divergence between the UK GDPR and the EU GDPR, but the manner in which Article 33 is interpreted does vary across jurisdictions.

If there has been unauthorised access to, and encryption of, large volumes of personal data (as well as the potential exfiltration of this data) by a hacker, it is likely that the Article 33 threshold for notification to a data protection authority will be met.

TechCo does not have an obvious "main establishment" in the EU. As such, it cannot reliably take advantage of the EU's 'one-stop shop' system, where one competent data protection authority acts as the lead supervisory authority in relation to the incident. This means that, if Article 33 is triggered, TechCo must report the incident to the supervisory authority in each affected jurisdiction. And, of course, the UK is no longer in the EU, so even if there were a "main establishment" in the EU, the UK would need to be dealt with separately. From a practical perspective, if multiple jurisdictions are involved and the decision is made to notify in one jurisdiction, it is sensible to notify the relevant supervisory authority in all relevant jurisdictions.

1. UK

The UK's data protection authority, the Information Commissioner's Office (the ICO), has various guidance on its website with respect to how it expects data controllers to assess whether any breach is likely to result in a risk to the rights and freedoms of those affected including, most recently, new guidance in relation to ransom attacks.[1] If TechCo determines that Article 33 has been triggered, it should make an initial notification within the 72 hour period (the ICO has not, to date, fined data controllers who make this notification a few minutes or a few hours late). This could then be followed by an update as the situation progresses. While the ICO has a specific form on its website for reporting data breaches, the use of this form is not mandatory (breaches can be notified via email).

2. France

If personal data of the French subsidiary is affected by the incident, TechCo would have to make an initial notification of the incident to the French data protection authority (the CNIL), directly on the CNIL's website using the standard online form. When TechCo has gathered more comprehensive information about the incident, it will be able to update its initial declaration with an additional and final declaration. The CNIL is usually keen to claim jurisdiction over certain incidents. So, in case of doubt, it would be sensible for TechCo to notify the CNIL, even if investigations at a later stage reveals that the French subsidiary was not affected.

3. Germany

As TechCo has an establishment in Germany, the supervisory authority of the state in which it is located would be the competent data protection authority provided that the establishment was affected by the incident. Germany has 16 independent supervisory authorities for each state (Bundesland) and one federal supervisory authority. Some supervisory authorities tend to be stricter with regard to incident reports than others. Many supervisory authorities have published guidance notes on their approach to data incidents and on when they expect to be notified.

4. Poland

The Polish data protection authority, the Urząd Ochrony Danych Osobowych (UODO), would expect TechCo to notify them of this incident, if data related to the Polish subsidiary is affected. The notification can be submitted either by filling in a dedicated electronic form available on their website, or by sending the completed form to the ePUAP electronic message box (which is a specific system for communicating with government bodies) or via traditional post to their address.

II. Article 34 GDPR – personal data – notifying the relevant data subjects

Under Article 34 of the GDPR, data subjects must be notified "without undue delay" where a "personal data breach is likely to result in a high risk" to their rights and freedoms. There are certain instances where communication to data subjects is not required: (1) where the data controller has previously taken measures to protect its data in the event of a breach, thus rendering the exfiltrated data useless (such as encryption); (2) the controller has taken measures since the breach to combat the likelihood of a high risk to the rights and freedoms of the data subjects; and (3) it would involve disproportionate effort, and a public communication or similar would be equally effective.

1. UK

On the facts of this scenario, we do not know what volume or types of personal data have been affected, how they have been affected, and for which data subjects. TechCo will need

1 Ransomware and data protection compliance | ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ransomware-and-data-protection-compliance/ (last accessed 1 April 2022).

further information in order to assess whether Article 34 has been triggered, and will need to consider what proportionate investigations it should carry out. Once it has further information, TechCo will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. It should refer to the ICO's guidance on personal data breaches in making this determination and consider preparing a risk assessment.[2]

2. France

The CNIL adopts a conservative approach and tends to have a broad interpretation of situations that are considered as "high risk". An assessment of the risk/high risk situation would need to be made on a case-by-case basis by TechCo, taking into account the relevant factors (see CNIL's website for guidance).[3] In many cases, following CNIL's approach, it will be necessary to notify the data subjects. Data controllers will have to carefully weigh the pros (compliance from a regulatory perspective) and cons (potential bad publicity) of notifying in case of doubt as to whether the "high risk" threshold is met or not.

3. Germany

The assessment as to whether to notify data subjects depends to some degree on which supervisory authority will be competent for TechCo's establishment in Germany. Many supervisory authorities in Germany have published guidance notes with practical examples when they usually see a likely risk.

4. Poland

In carrying out the assessment of whether to notify data subjects, we would recommend carrying out a risk assessment. Given that the UODO usually follows a formalised risk-based approach, documentation of the impact analysis would be an important part of any discussions with the UODO.

C. Ransom payments

The payment of a ransom raises legal, practical, and ethical considerations. These include: whether payment of a ransom will be effective (for instance, will it result in the provision of decryption tools and will the attacker abide by assurances?), the potential that payment of a ransom will attract further ransom attacks, possible criminal liability, and whether there is any negative reputational impact for a business in paying.

I. UK

Under English law, the payment of a ransom is not of itself illegal. However, the payment of a ransom may be illegal and constitute a criminal offence if it breaches anti-money laundering legislation, anti-terrorism laws, or breaches sanctions. If TechCo wishes to consider paying the ransom, it will need to conduct due diligence regarding the payee before any payment is made.

The ICO has recently issued new guidance on the payment of ransoms, and the impact that this has on a data controller's regulatory duties.[4] The ICO's position is that payment of a ransom does not affect the position that personal data has been compromised.

Businesses in certain regulated sectors may be subject to additional obligations and restrictions.

2 Personal data breaches | ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#whatinformationmust (last accessed 1 April 2022).

3 Homepage | CNIL, https://www.cnil.fr/en/home (last accessed 1 April 2022).

4 See, supra n. 1.

II. France

Both the CNIL and the ANSSI (governmental agency for IT security) warn against paying a ransom. The CNIL does not permit controllers to view the risk to data subjects as being lower by virtue of having paid a ransom (no weight is given to a cyber criminal's promise of returning data). Moreover, French insurers are usually very reluctant to cover payment of ransom.

III. Germany

It is unclear whether paying ransom would constitute a criminal offence under German law. The payment could potentially infringe anti-money laundering regulations. German law enforcement agencies as well as the German Federal Agency for Information Security (BSI) warn companies not to pay in the case of a ransomware attack. However, German law enforcement agencies also usually have a clear focus on the actual perpetrators and the practical risk of prosecution is rather low if a company actually pays ransom.

IV. Poland

There is no direct legal regulation in Poland governing the payment of ransoms. However, the ethical and legal assessment of the payment of the ransom may be considered from the point of view of the concept of a state of necessity, in which it is necessary to eliminate a danger directly threatening the personal well-being of a person, which is recognised by Polish law.

If the ransom were to be paid by the Polish branch of TechCo, TechCo would be advised to cooperate with the special cyber department of the Polish police, especially in order to avoid doubts related to the transfer of payments in cryptocurrency, a tool which is often used in criminal activities related to money laundering.

D. Potential follow-on claims

Under Article 82 of the GDPR, data subjects that suffer material or non-material damage as a result of an infringement of the GDPR are entitled to compensation.

This means that TechCo faces the prospect of potential claims against it by affected data subjects. The likelihood of potential claims against it being threatened varies by jurisdiction, with certain jurisdictions having developed a 'claims culture'.

I. UK

In England, there has developed a 'class action' or claims culture.[5] If TechCo were to notify data subjects of a personal data breach, it can expect to receive claims for compensation from a certain number of data subjects. In order for any claim for compensation to succeed, a data subject must demonstrate that: (1) TechCo has breached the UK GDPR and (2) as a result, the data subject has suffered material or non-material damage (such as distress).

II. France

France has not yet fully developed a claims culture. Nonetheless, over the past few years, consumer associations are slowly integrating the fact that some of them can now act to claim damages in cases of alleged breach of data protection obligations. Indeed, in France, the law extended "collective action" (action de

5 Privacy & Data Protection journal - Volume 21, Issue 8, https://www.osborneclarke.com/system/files/documents/21/10/25/UK%20data%20protection%20litigation%20-%20a%20burgeoning%20market%20that%20needs%20rebalanci.... pdf (September 2021) (osborneclarke.com) (last accessed 1 April 2022); Supreme Court in Lloyd v Google dismisses data protection class action - Osborne Clarke | Osborne Clarke, https://www.osborneclarke.com/insights/supreme-court-lloyd-v-google-dismisses-data-protection-class-action (last accessed 1 April 2022).

groupe) to cover the compensation of material and moral damages suffered due to a breach of data protection obligations incumbent to a data controller or processor (as provided for by French data protection law and by the EU GDPR).

Under French law, each person participating in a collective action has the right to be compensated individually. The compensation that TechCo may be liable to pay corresponds to the economic loss suffered; it is a matter of compensating the loss actually suffered by the person concerned.

III. Germany

Germany does not recognise representative actions. German civil law is very much focused on the compensatory effect of damages claims. Therefore, claimants will have to provide evidence that damage has actually occurred. Although it is possible to claim for non-material damages, German courts tend to grant relatively small amounts compared to other jurisdictions. Typical damages granted by courts for data protection infringements have varied between zero and €5000 (per data subject). The claims that TechCo may face very much depends on the nature of the data affected by the attack, whether the data has actually been exfiltrated and the impact the incident has on the data subjects.

IV. Poland

Poland is not a country with a high culture of lawsuits. The compensation awarded by courts for damages is generally low, limited to actual or future monetary losses, with little regard for victims' suffering and indirect effects. The main concern for TechCo in relation to personal data breaches is the risk of administrative fines and the loss of customers (rather than claims for compensation under the GDPR). In addition, the nature of personal data can cause serious reputational damage to data subjects, which can translate into high claims.

E. Other legal, regulatory and reputational considerations

TechCo should consider how the incident affects data for which TechCo is acting as data processor, as TechCo will have GDPR obligations to notify relevant data controllers.

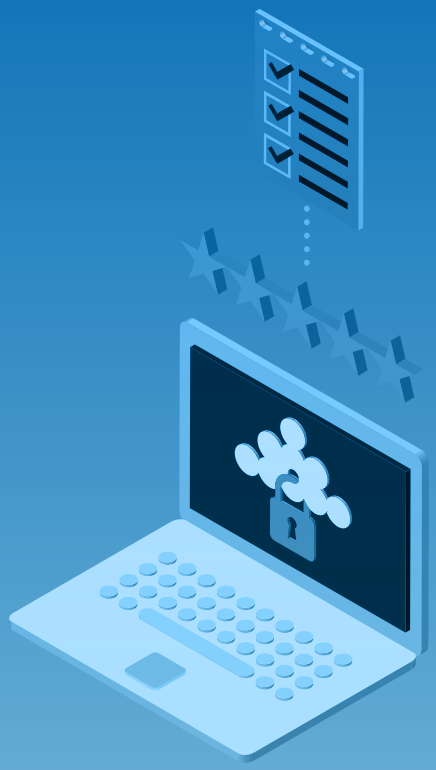
Aside from the GDPR, TechCo will need to consider whether the incident gives rise to any other legal and regulatory considerations. This could include regulation under the NIS Regulations, regulation by other professional bodies (such as the Financial Conduct Authority, in the UK), rules which may apply if it is listed on a stock exchange, and/or contractual obligations (under insurance contracts or to commercial counterparties).

Further, if it transpires that the cyber incident has arisen as a result of any breach by a third party supplier, TechCo should consider whether it is able to bring a claim against that third party supplier to recoup its losses arising from the incident.

TechCo should also be careful to ensure that communications, both internal and external, follow a narrative designed to protect the company's interests and reputation. Inadvertent admissions of liability can and will result in regulatory scrutiny and open the door for follow-on claims.

TechCo may also wish to notify the relevant law enforcement authorities.

2.10 CYBERSECURITY GOVERNANCE– ARE YOU PREPARED?



OSBORNE CLARKE AUTHORS

Olgierd Świerzewski
Co-Managing Partner, Poland

Olgierd.Swierzewski@osborneclarke.com

Further information

CYBERSECURITY GOVERNANCE – ARE YOU PREPARED?

For many European companies, a cyber attack is inevitable. The question is not if, but when and how the company will become a target. If company boards think that appointing a Chief Information Security Officer (CISO) is their sole responsibility, absolving them of legal, reputational and incident management responsibilities, nothing could be further from the truth. Cybersecurity has become the responsibility not only of the IT department, but more importantly of the company's board, which must coordinate the activities of individual managers and look at the issue of cybersecurity in a holistic way.

KEY TAKEAWAYS

- → Having a CISO does not relieve the board of its responsibility in managing cybersecurity and potential legal liability.
- → The demonstration of due diligence by management is key to minimising the financial, legal and reputational consequences in the event of an incident.
- → Preparing your company for incident management means carefully selecting the composition of your cyber incident management team.

A. Cyber threat seems imminent

The FIREEYE website[1] has a map that monitors live attacks and cyber threats. At any one moment, hundred of thousands of attacks are taking place around the world.

The war in Ukraine, which is also taking place in cyberspace, is a new factor that is both important and dangerous. Many hacking activities are funded and commissioned by nation states – the North Korean regime has even made cybercrime a source of budgetary revenue. Companies operating in NATO countries will be particularly vulnerable to attacks. This is another reason why directors should consider creating a cybersecurity governance structure within their organisations.

B. Pure formality or effective approach?

For some companies operating within so-called critical infrastructure, legislation may mandate that cybersecurity be addressed. This means that there is a legal obligation to establish responsibilities and procedures related to cybersecurity risk management and business continuity planning. This legal reason has some pros and cons in terms of awareness of the importance of cybersecurity in an organisation. The benefits of the legal pressure are related to the mandatory preparation of procedures including governance, internal policies, minimum training requirements, and use of defensive technologies. The possible downside of legal requirements may manifest itself in a strict, formal approach to filling out policies without focusing on creating an internal cybersecurity culture that is shared by all employees and the entire company. In a very formal approach to regulatory compliance, the natural temptation is to shift all responsibility for cybersecurity onto the shoulders of IT staff and chief information security officers (CISOs). Understanding cyber threats and their implications for the company and its shareholders is key to board engagement. This must be the principal driver for engagement, not the legal obligation in itself.

Therefore, properly established cybersecurity governance and training programmes should be a positive impetus to engage all levels of employees, including board members, which also means the implementation of a more holistic approach that could be supported by a clear definition of the CEO (Chief Executive Officer)'s role and the board's involvement in the cybersecurity process. The central role for cybersecurity should be placed in a Cybersecurity Committee led by the CEO with input from the CISO and other board members. This committee should meet quarterly to discuss all important processes and policies related to security, cybersecurity and business continuity of the company. In this way, companies can achieve 'management buy-in'. Some corporate practices are not consistent with the stated declaration of the importance of cyber threats. Management board members need to ensure that they have appropriate cybersecurity training and develop a channel of communication with the CISO.

C. Role of management board

The aim of actions taken by the management board in the field of ensuring information security, including information processed in connection with the provision of the key service, is to achieve an organisational and technical level that:

- Ensures full implementation of applicable legal requirements in the field of cybersecurity;
- Guarantees confidentiality of information constituting critical data for the enterprise;

1 https://www.fireeye.com/cyber-map/threat-map.html

- Ensures the integrity of business data;
- Mitigates threats, and if they occur, limits their impact;
- Ensures readiness to take appropriate action in crisis situations;
- Enables learning and improvement of the information security management system; and
- Raises awareness of employees and users in information security.

D. Cybersecurity governance and incident response management

Cybersecurity governance is also intimately connected with the organisation of incident response teams. Depending on the size and scope of an incident, the list of people on a corporate security incident response team (CSIRT) might need to include some or all of the following:

- CEO - the key person who takes responsibility for the critical, final decisions of the team based on reports and recommendations provided by the other CSIRT members.
- CSIRT Leader (CL) - board member responsible for IT infrastructure and operational support. Should coordinate internal and external forces involved in the incident response process. Their role should also include the preparation phase, including training and simulation exercises, checklists, procedures, and CSIRT war room organisation.
- CISO - cybersecurity team leader managing the entire process from an IT and cybersecurity perspective, responsible for threat analysis from detection systems, reporting to CSIRT, containment, eradication, recovery process, and development of lessons learned.
- Chief Operating Officer (COO) - the board member responsible for business and production operations who is responsible for analysing the business impact of emergency processes and communicating with operations managers and external business partners on operational details related to the business flow.
- Control System Engineer - responsible for analysing the potential impact of an attack on maintaining operations, as well as shutting down certain production processes. Their role should include reporting to the CSIRT on possible business and operational scenarios related to attacked critical assets and production systems.
- Data Protection Officer - a person responsible for monitoring compliance with data protection regulations. Their tasks include determining the impact of a cyber attack on data protection and making recommendations to the CEO and the board of directors on how to communicate the data protection breach to state authorities.
- IT cyber defence specialists, dedicated to the containment and elimination stages.
- Individuals in charge of the IT area business units who are responsible for the daily maintenance of operations and are involved in monitoring and detecting threats and recovery planning. These should be network and system administrators who should provide information to the CSIRT related to possible vulnerabilities, interconnections, and the impact of the incident on business continuity.
- IT Service Desk team, which collects all signals from employees regarding anomalies

in the normal functioning of systems and is required to report them to the CISO.

- General Counsel - responsible for legal assessment of the situation and advising on regulatory obligations. The key to the role of general counsel in CSIRT is a proper value matrix based on customer interest, regulatory obligation, and shareholder expectations. Short-term interests of the board (and self-interest) should be placed at a lower level: there should be no pressure to sweep problems under the carpet with the naive hope that they never materialise. Strong legal advice helps in proper prioritisation of actions, especially towards customers, government bodies, shareholders (especially in listed companies that also report serious incidents to meet European Market Abuse Regulation requirements).

- Head of Security - who, as the physical security officer, should take full responsibility for arranging access for CSIRT members to the affected infrastructure, as well as for securing critical assets and infrastructure from intrusion if some security systems are disabled.

- Public relations professional - who should have a communication scheme in place in advance for various threats and impacts. However, PR specialists should not act alone as their words are crucial for business, social and political reactions, and the share value of a company. It is crucial to get CSIRT approval before any public statements. Therefore, communication should be part of training based on cyber attack scenarios.

- HR director - should be the source of internal communication for employees. They have the best knowledge about the possible reception of the communication by the employees. It should be emphasised that internal communication must also be agreed within the CSIRT and be consistent with external communications, as journalists will immediately notice the discrepancy and contrast the official statements with the knowledge of the employees.

- Support staff - the list of additional support staff should include forensic experts, representatives from IT vendors and application developers, engineers responsible for critical manufacturing processes, sales managers with relationships with key customers, a management assistant who should be responsible for having and updating all contact information and assisting in organising a 'war room' meeting physically or virtually.

What needs to be added to the discussion of cybersecurity in organisations is real engagement of leaders and periodic training based on case studies, especially in the area of phishing and spear phishing-based social engineering techniques. This training and education programme should also be dedicated to the external contractors and vendors, especially to the franchisees who operate within part of the common network. It is a common perception within businesses that cybersecurity is solely a priority for the IT security staff, not an issue which should be tackled by everyone. And this should be changed by training. Cybersecurity should be spread beyond the IT community to all employees, through the greater awareness of the business, operational and legal managers.

2.11 FUTURE IP ISSUES RELATING TO DATA-DRIVEN BUSINESS MODELS

OSBORNE CLARKE AUTHORS

Dr Johannes Graf Ballestrem
Partner, Germany

Johannes.Ballestrem@osborneclarke.com

Further information

Valentin de le Court
Counsel, Belgium

Valentin.Delecourt@osborneclarke.com

Further information

Tim Harris
Partner, United Kingdom

Tim.Harris@osborneclarke.com

Further information

Robyn Trigg
Knowledge Lawyer, United Kingdom

Robyn.Trigg@osborneclarke.com

Further information

FUTURE IP ISSUES RELATING TO DATA-DRIVEN BUSINESS MODELS

This article delves into a selection of future IP issues that owners of data-driven businesses should be aware of. Firstly, we will assess whether the recent EU Data Act proposal can coexist with the existing rules protecting trade secrets. Then, we will look into the hot topics of the patentability of AI-generated inventions, copyrightability of AI-generated works, and the text and data mining copyright exceptions.

KEY TAKEAWAYS

- → The EU Data Act proposal aims to foster access to and use of data, while still ensuring legal protection of trade secrets is preserved.
- → Autonomously computer-generated works are not copyrightable under EU law, whereas the UK does grant protection.
- → AI can be a helpful tool to invent but is not itself an "inventor" for the purpose of patent filing.

A. The EU Data Act: a single market for data versus trade secrets?

On 23 February 2022, the European Commission officially presented its proposal for an EU Data Act,[1] which aims to establish a European single market for data – a core component of the digital economy. The proposal sets out a cross-sectoral and harmonised legal framework for the access to and use of data, both personal and non-personal, whether by individuals, businesses, public sector bodies or European public authorities.

The proposed regulation mainly applies to manufacturers and users of connected products and providers of related services within the EU. It governs rights and obligations with respect to the data generated by the use of connected devices and related services.

A key element is that manufacturers of such products and providers of related services would have to make data generated by their use easily accessible to users, businesses or consumers alike.

Users would have the right to share this data with third parties or demand that the data is made directly available to third parties. By doing so, the stated aim is to foster access to and use of data and to ensure fairness in the allocation of value from data among actors in the data economy.

The proposed regulation has the potential to change the ecosystem for data-driven business models in the EU and it is hoped that it will foster innovation and preserve incentives to invest in ways of generating value through data.

I. Conflicting objectives?

At first blush, the objectives of the proposed regulation and existing trade secrets protection may seem at odds. The Data Act seeks to facilitate the sharing of and access to data. While the Trade Secrets Directive[2] aims to harmonise protection of confidential information across the EU, thereby recognising that ensuring control on undisclosed information is particularly important for business competitiveness and innovation-related performance.

Despite the desire to facilitate more open access to data, the Data Act states that existing rules for the legal protection of trade secrets should not be affected. Trade secrets must be respected in the context of data use between businesses or by consumers and their confidentiality preserved. They should only be disclosed provided that "all specific necessary measures are taken to preserve [their] confidentiality",[3] particularly with respect to third parties.

Where data disclosure to a third party is requested by a user and trade secrets are involved, disclosure shall be limited to the extent strictly necessary to fulfil the agreed purpose and only provided where specific confidentiality measures are agreed between the data holder and the third party. Moreover, the obligation to make data available to a data recipient does not oblige the disclosure of trade secrets, unless otherwise provided by EU law.

1 Proposal for a Regulation of the European Parliament and of the Council on harmonised rules for fair access to and use of data (Data Act), COM(2022) 68 final, https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data 23 February 2022.

2 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157, 15.6.2016, p 1-18. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943

3 n 1, Article 4(3).

II. Practical tips for data holders – maintaining trade secrets protection

With respect to direct disclosure to third parties, data holders should consider whether the disclosure of any trade secrets is strictly necessary for the purpose agreed between the user and the third party. If not, the data holder should resist such disclosure.

In doing so, the data holder will need to prove the data at stake qualifies as a trade secret and that reasonable steps have been taken to protect the confidentiality of the data. This will require having a proper trade secrets management and protection policy in place. Data holders should anticipate the receipt of access requests and prepare for them by conducting a trade secrets audit, maintaining a trade secrets register, and having all reasonable confidentiality measures in place.

Where trade secrets should be disclosed, the proposal emphasises the need to ensure that appropriate confidentiality measures are in place between the parties. Such measures will need to be agreed and implemented before any trade secrets are disclosed (and any related data shared). They should set out the obligations imposed on the receiver, be appropriate to the information being shared, address the specific purpose of providing the data, and set out the outcomes and remedies available should the measures be breached.

Implementing monitoring and other technical protection measures, such as smart contracts, to ensure compliance with the agreed measures may be prudent. These are explicitly permitted by the proposal, provided that such measures are not used to hinder a user's right to provide data to third parties.

If many access requests involving trade secrets are anticipated, data holders might want to formulate a uniform confidentiality policy to ensure consistent steps are followed for each access request and trade secrets appropriately protected in each instance.

It is important to bear in mind that the Data Act aims to prevent the unilateral imposition of unfair contractual terms on micro, small or medium-sized enterprises by rendering any such terms non-binding. To assist in this regard, the Commission has committed to developing non-binding model contractual terms. It remains to be seen whether these will involve model provisions aimed at ensuring the confidentiality of trade secrets. If they do, these will serve as a good starting point for considering what measures to put in place.

III. Practical tips for users and other data recipients – accessing trade secrets

Users and other data recipients should firstly consider whether receiving trade secrets is necessary for the purposes they wish to pursue. If possible, any data qualifying as trade secrets should be avoided as this may involve limitations on the use of the shared data.

If such data needs to be received, users and other data recipients must ensure they understand the implications of receiving the trade secrets, including putting in place proper processes for their handling and to ensure compliance with any agreed protective measures.

Challenging whether specific data qualifies as a trade secret may also be well advised as the data holder will bear the burden of proof of such qualification.

As to third parties, they should ensure they are aware of the obligations the Data Act places on them, including, for example, the restrictions on the purposes for which the data can be used.

IV. Next steps

At present, the Data Act remains a proposal and the draft is likely to be subject to change. We would expect the progress of the Data Act to become clear over the next year. However, the Commission's intentions are apparent: it intends to create a European data economy. All parties involved in the access to data need to be alert to the interplay between the desire for openness and existing protection of trade secrets.

B. Patentability of AI-generated inventions (inventorship and entitlement): the state of play in the EU and UK

In the EU, inventions generated by artificial intelligence (AI) are presently not patentable. The European Patent Office has rejected the notion that an AI system can be regarded as an inventor.[4] Only humans can be named as inventors on a patent application. As a result, an invention generated autonomously by an AI system without human involvement will not be attributed to any inventor and will not be patentable.

The sole ownership of the AI system generating the invention is not sufficient to determine inventorship. Any European patent application treating such an owner as the inventor will be rejected. Further, a machine cannot legally transfer any rights under EU law and therefore the owner of an AI system cannot be the machine's successor in title to apply for a patent.

The debate heats up when considering AI as a tool for the human inventor. If AI is used in the process of developing an invention, the assessment of inventive step may be challenging: the higher the degree of autonomy, the more difficult it will be to speak of the AI as a tool.

Similarly in the UK, the Court of Appeal has also recently held that an AI system cannot be an "inventor" for the purposes of filing a patent.[5] Nor is the owner of an AI machine entitled to any intangibles produced by the machine. However, the owner of the AI system in question before the Court of Appeal (known as "DABUS") has sought leave to appeal this judgment to the UK's Supreme Court. The UK Intellectual Property Office (UKIPO) also recently closed a second consultation on whether an AI-devised invention should be patentable in the UK, and we currently await the government's decision in response.

Even more recently, the German Federal Patent Court provided a pragmatic solution to obtaining patent protection for inventions created by AI and gave clarity on how to correctly register inventions created by AI.[6] The court held that the listed inventor on a patent application must be a human, even when the AI system devised the invention. However, the AI system can also be named on the patent application.

C. Copyright protection for computer-generated works: contrasting positions in the EU and UK

AI is increasingly used to generate creative works, but are those works protected by copyright? In the EU, the short answer is no. Although the Court of Justice of the European Union (CJEU) has not yet dealt with the copyrightability of computer-generated works, previous judgments have confirmed that copyright

4 J 8/20, https://register.epo.org/applicationdocumentId=KXGBKNEA11IZE8D&number=EP18275163&lng=en&npl=false and J 9/20, https://register.epo.org/application?documentId=KXGCDC30B4X4NRA&number=EP18275174&lng=en&npl=false

5 *Thaler v Comptroller General of Patents, Trade Marks and Designs* [2021] EWCA Civ 1374.

6 German Federal Patent Court (BPatG), Judgment of 11 November 2021, ref. 11 W (pat) 5/21.

protection requires some form of human input because it must reflect the author's personality. Purely computer-generated works, by definition, lack any form of human contribution and are, as such, not eligible for copyright protection. If a computer program is copyrightable, such protection is separate from any protection that could potentially be afforded to any works it autonomously creates.

In contrast to the position under EU law, the UK has expressly provided for copyright protection of computer-generated works (which would include works generated by AI) by the Copyright, Designs and Patents Act 1988.[7] Care must be taken to distinguish between works that are created by a computer or AI, which have a 50 year protection from the date the work is made, and works created by a person using a computer (or AI) as a tool, which will have a longer copyright protection.

D. Exemptions to copyright protection for text and data mining – the EU and UK positions

Data mining – the extraction of certain contents from a database – is useful to provide AI systems with large datasets from which to learn. EU law provides for two exemptions to copyright protection of works for the sake of text and data mining (TDM).[8]

The first exemption is for a specified class of users, applying only to research organisations and cultural heritage institutions, including universities, libraries, museums and archives. These institutions may conduct TDM of copyrightable works. Copies of mined works must be securely stored and may be retained by these institutions for the purposes of scientific research, including the verification of research results.

However, this exception only applies to works or databases to which the extractor has lawful access. The extracted works must therefore be freely available online or made accessible to the extractor via the rightsholder, for example through a subscription service. It is not possible for rightsholders to contractually rule out TDM of these types of organisations and no financial compensation is provided.

The second exemption to copyright protection for TDM under EU law applies to everyone and provides for TDM and retention of lawfully-accessed copyright-protected works for non-research uses. The rightsholder does, however, have the possibility to opt-out of this exemption to copyright protection, thereby prohibiting the collection and extraction of the relevant copyrighted works for commercial purposes. In order to opt-out, rightsholders must reserve their rights in the specified manner. For example, this can be declared by machine-readable means, including metadata and terms and conditions of a website or a service, or by a contractual agreement or unilateral declaration.

At present in the UK, a specific copyright exception exists but, as for the EU exception, a number of specified conditions must be met including that the TDM must be for non-commercial research. The copyright exception also does not apply to database rights so TDM on databases that qualify for database right protection require a licence.

However, the UKIPO's second recent AI consultation also asked for comments on whether to amend the existing TDM exemption.[9] The

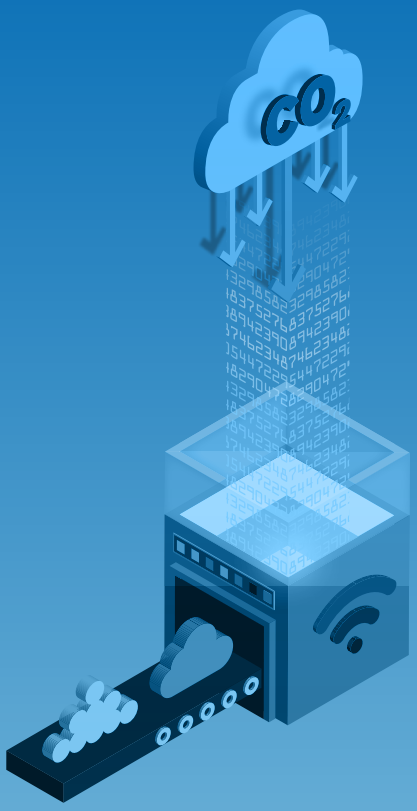
7 See ss 9(3) and 12(7).

8 Articles 3 and 4, Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130, 17.5.2019, p 92-125.

9 Artificial intelligence and intellectual property: copyright and patents. https://www.gov.uk/government/consultations/artificial-intelligence-and-ip-copyright-and-patents/artificial-intelligence-and-intellectual-property-copyright-and-patents

consultation asked for responses on various options including whether to widen the existing TDM exception to cover commercial research and database rights, and whether rightsholders should be able to opt-out their works from the exception. We await the government's response to the outcome of the consultation.

2.12 CHALLENGING THE ENVIRONMENTAL IMPACT OF DATA-DRIVEN BUSINESS MODELS



OSBORNE CLARKE AUTHORS

Dipika Keen
Head of Business Transactions Knowledge, Co-Lead of Tackling the Carbon Challenge – Policy & Regulation, United Kingdom

Dipika.Keen@osborneclarke.com

Further information ›

Claire Bouchenard
Partner, France

Claire.Bouchenard@osborneclarke.com

Further information ›

John Buyers
Partner, United Kingdom

John.Buyers@osborneclarke.com

Further information ›

CHALLENGING THE ENVIRONMENTAL IMPACT OF DATA-DRIVEN BUSINESS MODELS

Net-zero goals have become a strategic priority for many businesses and so the carbon footprint of data-driven business models has strategic relevance. However, technology typically used in data-driven business models has the potential to involve significant carbon emissions. While technology suppliers are themselves taking steps to reduce their environmental impact, there is also a new body of law seeking to bring about green choices and design.

KEY TAKEAWAYS

- → Make sure your data-driven business model strategy dovetails with your net-zero strategy
- → 'Green' your IT procurement process by scoring on environmental performance and including contractual obligations
- → Understand the impact of new green-focused laws on the cost and provision of technology services

A. Carbon footprint of a data-driven business model

Big data and data analytics are crucial to the delivery of a successful model but they often rely on IT infrastructure which require large amounts of energy.

The carbon footprint of a data-driven business model is relevant in two ways. First, many businesses are making net-zero commitments. Any data-driven business model strategy will therefore need to dovetail with the business's own net-zero strategy. Second, legislative and regulatory pressure to make sustainable choices in tech design are starting to develop. Businesses need to be aware of the legal framework within which they will be required to operate.

B. Data-driven business models and Net Zero

IT services used to deliver data-driven business models have a high level of energy consumption. One study estimated that data centres accounted for between 1,1% and 1,5% of global electricity use.[1] Visual display units (VDUs) such as smartphones and screens have an even greater impact: a recent report by ARCEP, the French telecoms regulator, revealed that they are responsible for 64-92% of the environmental impact of digital, while data centres "only" account for 4-22%.[2] It is necessary to consider all aspects of the IT system being used to deliver the model.

Thankfully, high energy consumption does not necessarily translate into a high carbon footprint as energy generation continues to shift away from fossil fuels to low carbon sources. Many IT providers have committed to decarbonise. AWS and Microsoft Azure aim to use 100% renewable energy by 2025, and Google Cloud by 2030. The corporate power purchase agreements that enable these transitions are dominated by IT companies: Google was the largest corporate purchaser of renewable energy on the planet in 2018.[3]

IT infrastructure is also becoming more efficient. For example, hyperscale data centres are operationally optimised and data centres located in colder parts of the world, or even underwater, facilitate cooling.

Indeed, IT changes as a result of a data-driven business model may have a positive effect on a business's emissions profile. For example, shifting 'on-premise' processing into the cloud is itself often cited as a greener option, since cloud servers tend to be more up to date and efficient, and overall less hardware is required.[4]

A business seeking to implement a data-driven business model should assess the carbon emissions of its own IT infrastructure and those of its suppliers when making procurement decisions. Some businesses are starting to include 'green' obligations in their supply contracts.

C. Changing legal framework

I. General decarbonisation law

International and national laws that require countries to decarbonise have existed for a number of years. The legal framework as it applies to individual businesses is now being developed and tightened.

1 https://energyinnovation.org/2020/03/17/how-much-energy-do-data-centers-really-use/ (Last visited 23 Feb 2022)

2 https://www.arcep.fr/uploads/tx_gspublication/etude-numerique-environnement-ademe-arcep-note-synthese_janv2022.pdf (only available in French)

3 https://www.nature.com/articles/d41586-018-06610-y (Last visited 23 Feb 2022)

4 https://atos.net/en/blog/how-cloud-services-can-securely-advance-your-low-carbon-digital-transformation-strategy (Last visited 23 Feb 2022)

In the EU and UK, companies of a particular size already have to report publicly on their greenhouse gas emissions.[5] Soon companies will be required to report publicly on the climate-change risks facing their business in accordance with the Taskforce on Climate-related Financial Disclosures. Mandatory TCFD reporting has just been introduced in the UK and is being considered in the EU as part of the European Green Deal.

II. Green tech law

New laws and regulations are encouraging the design of digital systems that minimise their environmental impact.

In France, a new law was adopted on 15 November 2021 to reduce the environmental impact of digital technology; Article 28 of which requires data centres to comply with quantified indicators in terms of both power and usage. A second new law, adopted on 23 December 2021, is aimed at empowering the ARCEP to collect information on the environmental footprint of the electronic communications sector. This broadens the scope of the digital actors that can come under the ARCEP's control and extends the ARCEP's powers (such as its powers of surveillance, control and sanction) over those actors, including data centres.

In parallel with these provisions, there has been a movement towards ecodesign. A discussion platform organised by ARCEP has led to the proposal to create charters and/or codes of conduct to encourage ecodesign which may be voluntarily adopted by companies.

Separately, UNESCO's recent global agreement on the ethics of artificial intelligence (AI) notably included a strong environmental angle, urging AI actors to "favour data, energy and resource-efficient AI methods" and asking governments not to invest in AI systems which would have a disproportionate impact on the environment. The most recent draft of the proposed EU AI regulation adds emission and pollution control systems to the categories of "high risk" AI that will be regulated.

D. Looking ahead

As many of the large IT providers achieve 100% renewable energy consumption, attention will shift to the level of embodied carbon – the carbon emitted during the manufacture or construction of IT infrastructure[6] - and also to sustainable plans for lifecycle and end-of-life management.[7] Here too there are sustainability laws which will need to be considered, such as the application and development of anti-waste/circular economy laws.

Now and in the future, the development of a data-driven business model must go hand in hand with a business's net-zero strategy if both are to succeed.

5 EU Directive 2014/95/EU on the disclosure of non-financial information

6 https://www.datacenterdynamics.com/en/analysis/sustainable-data-centers-require-sustainable-construction/ (Last visited 23 Feb 2022)

7 See https://www.simslifecycle.com/resources/white-paper-data-center/ (Last visited 23 Feb 2022)

2.13 TRUST AND LEGAL CERTAINTY FOR THE DATA-DRIVEN ECONOMY?

A LOOK INTO THE EU DATA GOVERNANCE ACT

OSBORNE CLARKE AUTHORS

Benjamin Docquir
Partner, Belgium

Benjamin.Docquir
@osborneclarke.com

Further information ⊙

Jeremy Godley
Associate Director,
United kingdom

Jeremy.Godley
@osborneclarke.com

Further information ⊙

Catherine Hammon
Digital Transformation
Knowledge Lawyer,
United Kingdom

Catherine.Hammon
@osborneclarke.com

Further information ⊙

TRUST AND LEGAL CERTAINTY FOR THE DATA-DRIVEN ECONOMY? A LOOK INTO THE EU DATA GOVERNANCE ACT

The EU sees a bright future for a European data economy. The ambition of the Data Governance Act (DGA) is to enhance legal certainty by defining governance mechanisms for the sharing of data. The DGA focuses on certain forms of data sharing, especially for data held by the public sector. But it will also be relevant for the private sector and could be supplemented by sector-specific rulemaking such as the European Health Data Space.

KEY TAKEAWAYS

- → The DGA aims to enable access to data and interoperability, while safeguarding personal data, confidentiality and intellectual property rights.
- → The DGA defines a governance framework for data pooling and data sharing initiatives in both public and private sectors.
- → Trust and effective means of protection are essential conditions for data sharing initiatives, both for commercial and non-commercial purposes.
- → Innovative services and data markets could emerge and flourish, leveraging the legal certainty and the governance framework laid down by the DGA.

A. Scope

The DGA[1] is part of a wider EU policy effort to regulate the data-driven economy. The EU's ambition is to promote data sharing, and ensure that data is and remains findable, accessible, interoperable and re-usable (referred to as the FAIR acronym). In short, the EU wants businesses to compete on their intrinsic merits, rather than on the amount of data they happen to possess or control. But in order to achieve that purpose, there is a need for increased legal certainty, in particular with respect to data that is protected or restricted under data protection law, intellectual property or trade secrets rules.

In that context, 'data governance' is to be understood as a set of rules, structures, processes and technical means to share and pool data.[2] The goal of the DGA is to lay down a level playing field for data sharing and pooling, with all relevant stakeholders (including data subjects and data holders) being represented and engaged, so that the rules of the sharing game become clearer, and businesses in turn benefit from greater access to datasets that they can re-use lawfully.

The DGA will create a common minimum legal regime (governance) across the EU in respect of three key areas: (i) the re-use of certain data held by public sector bodies, (ii) the provision of data intermediation services and (iii) the provision of services based on "data altruism". In addition, it allows for the adoption of sector-specific data spaces through implementing legislation, in areas such as health, mobility, climate, financial services, agriculture and manufacturing. In so doing, the DGA lays important foundations for data sharing beyond those three specific areas, through a focus on salient cross-sector issues such as promoting openness and transparency, implementing technical means to preserve the integrity of data, and ensuring effective protection for third parties' rights. The first sector-specific regulation could be the Regulation for a European Health Data Space, the draft of which has just been officially published.[3]

B. Interaction with other legislation

As a general rule, the DGA is not intended to change or amend existing legislation, nor to create any obligation to share or allow re-use of data. Its provisions must be applied in combination with existing primary and secondary sources of EU law and with national law. Several commentators have highlighted, though, that combining the DGA with other rules on data sharing is not exactly frictionless, and that many questions arise.[4]

For instance, the DGA defines new forms of data intermediaries, but it is unclear how and to what extent the responsibilities of those entities apply with respect to other kinds of intermediaries, in particular platforms and other gatekeepers as regulated under the coming Digital Services and Digital Markets Acts. Another example is the interaction with data protection rules.[5] The DGA clearly states that the EU and national rules on data protection must be complied with, and even prevail in the event of conflict. It also clari-

1 Official published version available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868

2 See the Commission's comments about the proposal, available at https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2103; As noted by D. Amran, the concept of data governance actually encompasses additional dimensions: "Governance (of Personal Data Flows)", in G. Commandé (ed.), Elgar Encyclopedia of Law and Data Science, Edward Elgar, 2022, p. 186.

3 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197

4 See J. Baloup, E. Bayamlioglu, A. Benmayor, C. Ducuing, L. Dutkiewicz, T. Lalova, Y. Miadzvetskaya, B. Peeters, "White Paper on the Data Governance Act", available on https://ssrn.com/abstract=3872703; R. Gellert, I. Graef, The European Commission's proposed Data Governance Act: some initial reflections on the increasingly complex EU regulatory puzzle of stimulating data sharing, TILEC Discussion Paper, DP 2021-006, available on https://ssrn.com/abstract=3814721.

5 See the EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), version 1.1., available on https://edpb.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf.

fies that the DGA does not create an additional legal basis for the processing of personal data nor alter any obligations and rights laid down in the General Data Protection Regulation (GDPR) or the e-Privacy Directive. It remains to be seen, though, whether this will suffice to define clearly which rules apply in respect of mixed datasets (containing both personal and non-personal data), or in situations where advanced analytics and machine-learning techniques enable the re-identification of previously anonymised data. In such cases, it might be difficult to assess whether only the data sharing rules of the DGA apply, or must be combined with the more demanding requirements of the GDPR.

The same difficulty can be seen with respect to the international transfer of non-personal data to third countries. In this regard, the DGA sets new restrictions and rules inspired by the GDPR provisions on international data transfers. The DGA requires those sharing data to obtain contractual assurances on confidentiality and, in respect of intellectual property law, to assess the risk of government access to data. It limits the cases where data sharing entities may comply with requests for access from third country authorities. The combination of those new obligations with existing post-Schrems II[6] transfer impact assessment and risk mitigation exercises, will leave practitioners and privacy professionals with many unanswered questions.

C. A wealth of new data sources?

The text of the DGA focuses on certain categories of entities that are likely to authorise the re-use of data: (i) public sector bodies, (ii) data intermediaries and (iii) data altruism organisations. In the short-term, these can be labelled the potential new sources of data for businesses, keeping in mind that the DGA also provides a general framework for data sharing beyond those three categories of data sources, through implementing legislation.

- Public sector bodies are authorities or entities established for purposes of general interest with no industrial or commercial character, having legal personality and funded or controlled by public authorities. The DGA does not create a new obligation to allow the re-use of data but creates a framework to facilitate the sharing of such data when it is protected under confidentiality obligations, intellectual property or data protection laws and hence falls outside the scope of the Open Data Directive.[7] It should be noted that the DGA has a carve-out for public undertakings, broadcasters and cultural establishments. Outside these categories, the general range of public sector bodies that possess datasets and have not yet made these available for re-use, could now be requested to share them and would then need to comply with the specific requirements set out in the DGA to accommodate the protection of confidentiality, intellectual property or personal data.

- Data intermediaries are a new category of provider that facilitate the sharing of data and aim to establish commercial relationships between several data holders and categories of data users. On the face of it, the DGA targets three forms of intermediaries: (i) data exchange services or platforms, (ii) services that enable individuals to control the sharing of their personal data, and (iii) "data cooperatives" that support their members in exercising their rights with respect to data. Categories of traditional services such as web browsers, email services, cloud storage, analytics or data sharing

6 We discuss Schrems II and the current state of play for cross-border data transfers in this article: https://www.osborneclarke.com/insights/cross-border-data-transfers-whats-the-state-of-play

7 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, O.J., L-172, 26 June 2019, p. 56-83.

software are excluded, as are services used in a closed group such as those ensuring the functioning of Internet of Things (IoT) devices or objects. All of this seems to refer to new business models or innovative data services such as implementations of the Solid protocol[8] or the MyData movement.[9] But existing marketplaces or consent management systems could fall under that definition as well, and be subject to the same general obligations as imposed upon all data intermediaries: prior notification to a competent authority of the intention to operate as a data intermediary, based on a mandatory disclosure of data sharing services and activities, rules on independence, and requirements to ensure that the data sharing activities are carried out in an open and transparent manner.

- Data altruism is defined as the voluntary sharing of personal or non-personal data without seeking a reward and for purposes of general interest, such as healthcare, combating climate change, or improving mobility. The DGA requires data altruism organisations to be registered, imposes a not-for-profit corporate structure, and mandates an independent functioning and functional separation from other activities, as well as a number of requirements to safeguard transparency and data subjects' rights. The Commission may also lay down further rules regarding information requirements, technical and security measures and interoperability standards.

D. Common issues for data sharing

While the DGA creates specific rules and enforcement or monitoring systems for these various categories of data sources, it is useful to highlight three common themes in the regulation of data sharing. These could also become recurring themes when implementing legislation is enacted to foster data sharing in specific sectors or for specific purposes, such as the European Health Data Space.

- First, the goal to ensure that data be **"as open as possible, as closed as necessary"**. In order to maximise openness, the DGA requires the sharing of data to be done on a non-discriminatory and non-exclusive basis. Exclusive re-use arrangements with public sector bodies are generally prohibited, subject to a very narrow exception tied to the provision of a service of general interest. The conditions and fees for re-use of public sector data must be proportionate and justified on the basis of objective grounds, and fees must remain limited to the necessary costs. The same ambition inspires rules for data intermediaries and data altruism organisations: they must ensure interoperability of data formats and interoperability with other similar providers, and ensure their services are available on a fair, transparent and non-discriminatory basis. In addition, implementing legislation can be enacted to promote the availability of data or to facilitate the obtaining of consent, for instance.

- Secondly, the willingness to ensure an **effective protection of third parties' rights** such as confidentiality, intellectual property or data protection laws. Throughout the DGA, entities that benefit from an access to data, and those that facilitate such access, are made accountable and must preserve the confidential nature of data, ensure anonymisation of personal data or protection against disclosure of commercially sensitive pieces of information, including by implementing appropriate organisational and technical measures or passing on the same requirements to their contractual counterparts involved in the data sharing.

8 See https://solidproject.org/.

9 See https://mydata.org/.

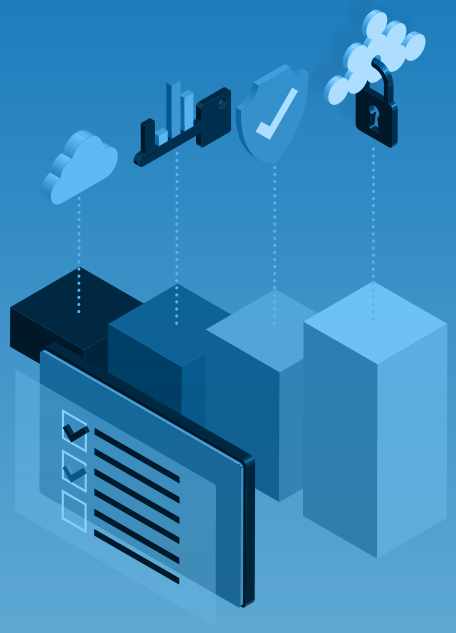
For public sector bodies, that includes the ability to prohibit the use of results that contain information jeopardising the rights and interests of third parties, or to prohibit re-identification of data subjects, for instance. Where data intermediaries are able to facilitate data sharing, this remains subject to the purpose-limitation principle and they must act "in the data subjects' best interest" when facilitating the exercise of the data subjects' rights under data protection legislation. For data altruism organisations, in addition to the layer of transparency requirements, they must provide tools for granting and withdrawing permissions to process data.

- Thirdly, the notion of **"secure processing environments"**, highlighting the need to implement a combination of legal, contractual, technical and organisational measures in order to preserve the integrity of the data. The notion of a secure processing environment is even defined as both the physical or virtual environment and the organisational means to ensure compliance with applicable Union or national law at large, allowing the entity to determine and supervise data processing actions, going from display and download to "calculation of derivative data through computational algorithms". Public sector bodies have a specific obligation to use such secure processing environments, and the recitals refer to techniques such as anonymisation, differential privacy, randomisation (again, these principles could be extended through implementing legislation for dedicated European data spaces). But data altruism organisations and even data intermediaries might also find themselves under a duty to use secure processing tools, either under the general obligation to implement adequate measures to prevent unlawful transfer or access to data, or pursuant to national implementing legislation.

E. A new regulatory regime for the data ecosystem

There is no doubt that the DGA represents a significant extension to the framework for data regulation in the EU. Its impact will not be limited to businesses located within the EU – it will also apply to data intermediaries providing services into the EU, and data altruism organisations that are collecting data from within the EU. The EU is seeking both to support businesses by boosting the data ecosystem with these measures, and also to control it and ensure the trust of consumers by laying out a clear framework for governance. Alongside the proposals for the Data Act, which will create new rights for data subjects to secure access to non-personal data (see further Chapter 2.10), and proposals for governing the data used to train AI deep learning systems (see further Chapter 2.7), the European Data Strategy will lead to wide-ranging changes in the landscape for data in the EU. There will be significant new opportunities for businesses and for individuals, but also sweeping expansion of data regulation, including full regulatory enforcement frameworks to ensure compliance.

2.14 RETHINKING REGULATION OF DATA-DRIVEN DIGITAL PLATFORMS



OSBORNE CLARKE AUTHORS

Henrik Bergström
Managing Partner, Sweden

Henrik.Bergstrom@osborneclarke.com

Further information

Konstantin Ewald
Partner, Germany

Konstantin.Ewald@osborneclarke.com

Further information

Catherine Hammon
Digital Transformation Knowledge Lawyer, United Kingdom

Catherine.Hammon@osborneclarke.com

Further information

Nick Johnson
Partner, United Kingdom

Nick.Johnson@osborneclarke.com

Further information

RETHINKING REGULATION OF DATA-DRIVEN DIGITAL PLATFORMS

The European Union is about to enact the Digital Markets Act and Digital Services Act. Both are focused on reshaping the regulation of digital platforms – hugely important and impactful data-driven business models for today's society.

KEY TAKEAWAYS

- → The DMA and DSA seek to impose granular obligations and restrictions on designated "gatekeepers" to digital markets and on the biggest online platforms.
- → Enforcement will be centralised, with the Commission having sole jurisdiction to take action against market "gatekeepers" and the biggest digital platforms, and to impose heavy fines.
- → As well as a proactive – not reactive – approach, the new laws take a tiered approach, and focus on compliance by design. Retrofitting compliance to existing platforms may be complex.

A. Bringing the regulation of digital platforms up to date

Cross-sector interest in data-driven business models is inspired, in no small part, by the success of the businesses that first identified how to turn reams of data into scalable revenue streams. Many of these models are platforms that facilitate the coming together of different parties who wish to interact, whether for social or commercial reasons, including social media, marketplaces and search engines. Many are now at the heart of the digital and online economy.

Over the last few years, the European Commission has reviewed the existing regulatory framework for digital markets to ensure that these frameworks are as effective as possible in light of developments since they first emerged, in the early years of the internet. These reviews have resulted in a number of legislative proposals from the Commission, including among others the Digital Markets Act (DMA) and the Digital Services Act (DSA). At the time of writing, political agreement has been reached between the Commission, the Council of Ministers and the European Parliament in relation to the fundamentals of the DMA and the DSA, but the technical detail is still being finalised and the final texts are not yet available. Both are currently expected to become law in autumn 2022, with a further period for compliance.

These two pieces of legislation sit front and centre in a shift in the approach to the regulation of digital platforms, products and services in the EU.

B. A new approach to regulation

I. Proactive regulation

The DMA is focused on ensuring "contestable and fair markets in the digital sector".[1] Digital platforms, like all businesses, are subject to competition law. But over time policy-makers and legislators in Europe started to question whether the usual toolbox of powers and sanctions were sufficient to maintain effective competition in these markets, and whether more could or should be done to support European competitors (given that businesses from the USA and China are often in the vanguard of these markets). As noted in Chapter 2.1, the European Commission considers data to be a "key factor of production" and so the accessibility of data in digital platform markets has been a particular area of focus.

The Commission has concluded that the particular economics of digital markets have caused some platforms to become "gatekeepers", able to influence the fairness and contestability of their markets in a structural way. In the Commission's view, these issues have proved difficult to address using general competition law, either because the actions are not illegal in themselves under those laws, or because investigating and remedying infringements after the event has proved complex and cumbersome, particularly in the context of what are often fast-moving markets. Moreover, it considers that reversing any harm caused can be difficult. A similar conclusion was reached by policymakers in the UK, which is also planning specific legislation to deal with digital markets to be overseen by a new Digital Markets Unit.

1 The key provisions of the Digital Markets Act, as they stood at the beginning of 2022, are summarised in this article: https://www.osborneclarke.com/insights/digital-markets-act-eus-new-regulation-gatekeepers-pushes-ahead-2022

General competition law sets out overarching prohibitions applicable to all businesses. Case law and enforcement has built up understanding over time of the types of commercial behaviour or agreements that will fall within the prohibitions. The DMA, by contrast, sets out detailed provisions specifying actions that "gatekeepers" must or must not take. Gatekeepers will be formally designated as such by the Commission, on the basis of parameters set out in the DMA.

As regards data, the DMA seeks, first, to limit the extent to which datasets about an individual are combined, requiring consent or another lawful basis for processing under the EU's General Data Protection Regulation. In addition, it seeks to increase the portability of data about an individual user from one platform to another, with the intention of making it easier for customers to switch to an alternative provider, or to use a number of providers at the same time (known as "multi-homing").

The DSA, similarly, imposes much more granular expectations on online platforms regarding illegal online content than the previous approach of the e-Commerce Directive[2] (which currently governs liability of platforms for online content). The new regulation will require active monitoring of risk, adoption of effective mechanisms to remove illegal content or to verify the identify of traders using online marketplaces and includes requirements for reporting to the Commission. It will also require transparency around certain algorithms such as recommendation engines, and will impose controls on the use of data-driven profiling of users.

II. Tiered regulation

The DMA and DSA represent a significant increase in regulation of digital businesses. Both are notable in being uniform across the EU, but not uniform in their application to businesses. As noted, the DMA will apply only to businesses designated as gatekeepers, while the DSA contains fewer burdens for smaller businesses which will, moreover, be given a longer period for compliance once the legislation is in force.

In addition, the mechanics of enforcement of the DSA are also impacted by the scale of the business concerned, as explained below.

III. Centralisation of enforcement

Currently, the only area where the Commission has direct powers to enforce EU law is in the field of competition law.[3] Both the DMA and the DSA will create new, exclusive areas of jurisdiction for the Commission – a rare and significant extension of its role.

As regards the DSA, this role was not included in the Commission's original proposals for the legislation but was added by the European Parliament and Council of Ministers during the legislative process. It is in notable contrast to the decentralised approach of other European legislation, including the General Data Protection Regulation (GDPR)[4], that is enforced by national regulators.

The DMA applies only to designated gatekeepers with a certain scale and impact, and will be enforced entirely by the Commission. For the DSA, the Commission will take over enforcement in relation to very large online platforms, meaning those with over 45 million users in the

2 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32000L0031

3 The Commission currently has enforcement powers in relation to general competition/antitrust law under Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12016E%2FTXT&qid=1651153217851 merger control law under Council Regulation (EC) No 139/2004 of 20 January 2004, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32004R0139 and State aid law under Article 107 TFEU.

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 https://eur-lex.europa.eu/eli/reg/2016/679/oj

EU, i.e. roughly 10 per cent of the population of the EU. The finalised text of the legislation is not available at the time of writing but it has been reported that such platforms will also be required to pay a yearly fee of up to 0,05% of their global turnover to fund enforcement by the Commission – again, a new approach to enforcement of EU law.

It remains to be seen whether the approach in the DSA, entrusting enforcement of the most significant cases to the Commission, is the beginning of a new trend in digital regulation enforcement. A recently leaked draft suggests that the European Parliament will seek to amend the proposed AI Act (see Chapter 2.7) to provide for a similar centralised approach in relation to breaches that meet specified thresholds indicating a significant EU dimension.

This shift in approach can be interpreted as a desire for consistency across the EU. It will reduce the risk of diluting the impact of enforcement by being split across numerous national regulators – a criticism which is sometimes made in relation to the track record of enforcement under the GDPR. Potentially, it puts considerable power in the hands of the Commission to shape digital markets going forwards.

As an aside, it is worth noting a significant ramification of centralising EU enforcement. Where the Commission undertakes an investigation under EU-level powers, the EU rules of legal professional privilege will be in play. This means that legal advice from in-house counsel (or from non-EU-qualified lawyers) will not be considered privileged[5] and will not, therefore, be protected from disclosure to the Commission. In some Member States, the advice of in-house lawyers is not privileged in any case, but in those where it is (for example, many Member States with a common law legal system), the loss of such protection from disclosure in a Commission investigation is a significant point to bear in mind in terms of risk management for the legal team.

IV. Compliance by design

The nature of data-driven business models such as digital platforms, products and services is that the software that underpins or delivers them is often automated, whether in a simple way or using complex AI systems. As such, regulatory compliance will typically need to be designed into the system from the outset.

This is a trend that has been seen increasingly for digital regulation,[6] and the DMA and DSA continue the theme. For example, where provisions create rights of access to data, this will need to be integrated into the structure of the system, building the technical functionality needed to fulfill the regulatory requirement. Retrofitting compliance into existing systems can be difficult – the relatively short deadlines for compliance in the DSA and DMA once the two regulations are in force are particularly noteworthy in this context.

5 See Case 155/79, AM&S Europe Ltd v Commission (EU:C:1982:157) https://curia.europa.eu/juris/showPdf.jsftext=&docid=90571&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=378263 and Case C-550/07 P, Akzo Nobel and Akcros Chemicals v Commission (EU:C:2010:512) https://curia.europa.eu/juris/document/document.jsf?text=&docid=82839&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=378530

6 We discussed the growth of "compliance by design" in our Technology, Media and Communications Annual Review 2022. https://explore.osborneclarke.com/tmcannualreview2022/legislators-worldwide-move-to-adopt-regulation-by-design/

2.15 DATA LAW LANDSCAPES BEYOND EUROPE

OSBORNE CLARKE AUTHORS

Felix Hilgert
Partner, US

Felix.Hilgert@osborneclarke.com

Further information

Vikram Jeet Singh
Partner (BTG Legal), India

Vikram@btg-legal.com

Further information

Guohua Zhang
Managing Partner,
Co-founder, China

Guohua.Zhang@oclegalchina.com

Further information

DATA LAW LANDSCAPES BEYOND EUROPE

European businesses with an appetite for global growth cannot afford to ignore the data law landscape in other markets. Regulation on privacy and artificial intelligence (AI) is developing at rapid speeds in other key markets such as the US, China and India. The latter two in particular require certain types of data to be stored locally, and regulators are cranking up the enforcement.

KEY TAKEAWAYS

- → Data laws in the US are fragmented but rapidly expanding, and already more protective of consumers than their reputation.
- → India is moving towards a much more structured data regulation framework, modelled after the GDPR.
- → China's data protection and cybersecurity regime has evolved to its final form, a three-pillar regulatory framework.

A. Expanding and enforcing privacy law

Privacy regulation worldwide is evolving to become more protective of individuals, with more comprehensive enforcement to boot.

I. US

The American privacy regulation landscape has historically been fragmented, with individual and highly divergent laws for certain sectors, situations or types of data.

1. Fragmented privacy regime

Depending on business models, companies may need to comply with well-known federal laws like the Children's Online Privacy Protection Act,[1] which protects children's information in online environments, the Health Insurance Portability and Accountability Act[2] for health information, and more obscure legislation such as the Video Privacy Protection Act,[3] which makes it illegal for video rental businesses to disclose their customers' rental history (and has been applied to streaming services as well).[4]

State laws can add even more complexity. In Illinois, the Personal Information Protection Act[5] imposes breach notification and data-security obligations on any organisation that collects personal data, and the Biometric Information Privacy Act[6] specifically regulates the collection and use of biometric information by private corporations.

2. US states limit data sharing

Recently, several US states have passed more comprehensive consumer privacy legislation, with California leading the charge, with its consumer privacy legislation[7] and, more recently, a privacy rights act,[8] followed by Virginia, Colorado and Utah (their statutes come into effect in the course of 2023). Many other states, including New York, Texas, Illinois and Florida, have also introduced new draft consumer privacy legislation.

These laws aim to limit the "sale" of consumer information by the companies that gather it – with the definition of "sale" being broad enough to include some situations where no money changes hands. Letting consumers opt out of data sharing can also impact the utility of datasets, which will come with a self-selection bias built in.

These laws have unmistakable similarities, despite differing nuances. They apply to entities doing business in the respective states, subject to various thresholds, including overall company revenue, the number of concerned data subjects, and the portion of revenue derived from data sharing.

However, unless a business intends to remain small, it would be short-sighted to ignore privacy regulation entirely in business and product decisions that may be hard to change once a business does have enough traction to cross the thresholds.

1 Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6505

2 Health Insurance Portability and Accountability Act, 110 Stat. 1936

3 Video Privacy Protection Act, 18 U.S.C. § 2710

4 Eichenberger v. ESPN, Inc., 876 F.3d 979 (9th Cir. 2017), https://casetext.com/case/eichenberger-v-espn-inc-1

5 Personal Information Protection Act, 815 ILCS 530

6 Biometric Information Privacy Act, 740 ILCS 14

7 California Consumer Privacy Act, California Civil Code s. 1789.100

8 California Privacy Rights Act

3. Enforcement risk

While California will have a dedicated privacy regulator,[9] other states rely on lawsuits brought by their Attorney General or private citizens. Fines and damage claims can add up quickly for structurally non-compliant products or services, as they can be calculated per concerned customer.

II. India

India's privacy laws are in the process of being overhauled, following a 2017 ruling of the Indian Supreme Court holding that all individuals are entitled to informational privacy. The last version of the proposed law, the Personal Data Protection Bill was released in December 2019. After almost two years of discussions, a joint parliamentary committee of the Indian Parliament adopted its report on the 2019 Bill, in November 2021, and this report was placed before the Parliament on 16 December 2021.

1. Data subject rights

Closely following the General Data Protection Regulation formulation, data subjects in India will have extensive rights under the new law. These include the "right to be forgotten" and data portability, which were not available under the older data law. These rights will increase the regulatory compliance burden on data processors, particularly since some of them may be exercised through the offices of the Indian government and data protection authority.

2. Localisation mandates

The proposed privacy law requires entities to store a copy of "sensitive personal data" (for example, financial data, biometrics and health information) within India whenever cross-border transfers are undertaken. Further "critical personal data" (which remains to be defined) is to be stored only in India. As such, entities hosting sensitive and critical personal data outside of India may be required to formulate procedures to mirror such data within India.

3. "Significant" data fiduciaries face more regulation

"Significant" data fiduciaries will be classified on the basis of factors such as volume of data processed, nature and sensitivity of data, etc. These entities will have additional compliance obligations under the new law, including appointing a data protection officer and maintaining records of processing activities.

III. China

The year 2021 was remarkable for China's data protection and cybersecurity regime, as we eventually saw the completion of the three-pillar regulatory framework: alongside the Cybersecurity Law (CSL) (effective as of 1 July, 2017), the People's Republic of China (PRC) enacted the Data Security Law (DSL) and the Personal Information Protection Law (PIPL). In addition to such cornerstone basic laws, multiple implementation rules or national standards were also issued either as binding rules, or drafts for public comments, intended to provide more practical guidance for implementation.

1. The Personal Information Protection Law

The long-awaited PIPL, known as the "Chinese GDPR", took effect as of 1 November 2021. Unlike the security-oriented CSL and DSL, this law particularly focuses upon the protection of personal information. While there are many similarities between GDPR and PIPL, there are also noteworthy differences, or China-specific features (for example, legitimate interest is not

9 How California Is Building The Nation's First Privacy Policy, https://www.nytimes.com/2022/03/15/technology/california-privacy-agency-ccpa-gdpr.html

a legal ground for processing, requirements on cross-border transfers, etc).

2. Localisation and cross-border transfer

Cross-border data transfer (CBDT) has been a hot topic since the CSL, in which critical information infrastructure operators (CIIOs) are subject to an express data localisation requirement. The PIPL provides further restrictions on CBDT by non-CIIOs, thus in a sense providing more clarity on the issue. Notably, non-CIIOs may now also be subject to mandatory security assessment with PRC authorities before transferring data out of China.

The latest development in this regard was the issuance for public comments of the draft measures of security assessment for CBDT rules. The draft CBDT rules set out a more detailed and broad scope of CBDTs by non-CIIOs, which are subject to mandatory security assessment, by reference to the number of data subjects whose personal information (or sensitive personal information) is processed and will be transferred out of China. Businesses, especially multinational companies in China, are hoping to see the final form of these CBDT rules soon.

3. Enforcement

The year 2021 was a busy year for PRC regulators for the enforcement of data protection laws and regulations.

While both the DSL and PIPL were relatively new, PRC regulators have focused on specific areas of enforcement. For instance, an unprecedented number of websites and apps were identified as non-compliant with data protection requirements, and either disabled and removed from app stores or suspended from operating for violation of applicable data protection laws and regulations (for example, excessive data collection, collection and processing without obtaining valid consent, unlawful sharing). This represents a very strong indication by the regulator that data protection is no longer an issue that a business in China could possibly ignore and a high price could be paid for non-compliance.

B. Regulating artificial intelligence

Regulation of AI is developing at very different speeds around the world. While this does not appear to be a priority in India, both China and the US are following ambitious, if slightly different, goals.

I. The US

A large number of initiatives are currently under way on a federal and state level to regulate the use of AI, in particular with a view to ensuring ethical decision-making and mitigating actual or perceived risks for consumers.

Legislators are trying to tackle the issue that machine learning from actual data may result in a perpetuation of existing biases by imposing transparency requirements. Most of the proposed federal and state legislation would force companies to self-audit their algorithms and AI applications, proactively counter any algorithmic discrimination on grounds of protected categories such as ethnicity, gender or disability, and provide disclosures explaining each decision to enable affected consumers to contest the validity of the data used in its making.

These initiatives would complement existing sectoral laws that already limit or regulate the use of AI for certain situations. In some states, using AI in the recruiting process is subject to information and consent requirements and, in New York City, the technology must be regularly subjected to bias audits. If eligibility decisions, such as for loans, but also housing or employment, are based on AI analysis, this may

already trigger certain notification obligations and correction rights for consumers.

But there are also some encouraging signals: the federal government and many states are actively promoting education and research into AI and improving related policy-making. Alabama has created a special council to advise legislators and the government about AI and, in Mississippi, machine learning and AI are now part of the state's official school curriculum.

II. India

India does not have an overarching law governing AI, and it is not likely that such a law will be formulated any time soon. That said, sector-specific laws still have bearing on how an AI enterprise can function in the Indian context.

The Indian government's strategy papers over the past decade call for sector-specific "tweaks" for AI, as opposed to a bespoke law. For example, provisions in any data privacy law can be calibrated to deal with AI issues. In December 2021, in fact, in response to a question in Parliament the Indian government stated that there are no plans to regulate AI and matters such as facial recognition are and will be covered under other laws.[10]

As in many fields, regulation will likely lag behind innovation. It remains to be seen whether the Indian government's stance on regulating AI changes, having regard to developments in other jurisdictions as well as emergent public uses. As things stand, AI-based systems will still need to abide by current laws that may define or even limit their development. For instance, Indian law is particularly sensitive around sharing images of children, and any 'machine learning' product may need to account for local privacy and child protection regulations.

III. China

The latest Chinese law, the Administrative Measures on Algorithm Recommendation of Internet Information Services (effective as of 1 March 2022) regulates the use of algorithms to recommend information to internet users.

These measures require AI algorithms used in the recommendation must be moral, accountable, and transparent, which is not dissimilar to the principle for automated decision-making under PIPL.

Like PIPL, the measures also prohibit algorithms from processing personal information to apply differential pricing between users. Businesses are also required to be transparent about the purpose of basic rationale, the intent and the main mechanism for operating the algorithms.

The measures require the algorithms to be trustworthy AI and, from a regulatory perspective, they set up concrete rules on what, in many other jurisdictions, is more of a concept.

These measures represent China's ambitious approach in regulating AI technology and will bring changes to and impact upon a wide range of businesses, especially where an algorithm is a key element in its pricing strategy and business model.

10 Parliamentary Responses Reveal How The Government Thinks Of AI Regulation, https://www.medianama.com/2021/12/223-ai-regulation-india-government-parliament/

ECLA AND OSBORNE CLARKE

EUROPEAN COMPANY
LAWYERS ASSOCIATION

ABOUT ECLA

The European Company Lawyers Association (ECLA) was founded in 1983 and is the umbrella organisation of 22 different national associations of in-house counsel working in companies and organisations.
For more than 39 years, ECLA has been committed to the profession of company lawyers throughout Europe and accounts for approximately 68,000 professionals in its network and represents the more than 150,000 company lawyers across Europe.

www.ecla.eu
www.inhouse-legal.eu
www.corporatecounselacademy.com

ABOUT OSBORNE CLARKE

Helping you succeed in tomorrow's world

Osborne Clarke is a future-focused international legal practice, with 300+ partners and more than 1,080 talented lawyers working together across 26 offices around the world.

Our three-dimensional approach to client service combines legal expertise, in-depth understanding of our clients and the sectors they operate in, together with insight into the global issues that are transforming the landscape of how we live, work and do business: decarbonisation, digitalisation and urban dynamics. Looking around corners to help our clients solve legal and business challenges, big and small, and harness the opportunities of change – together we'll be ready for what's next.

Visit osborneclarke.com to find out more.

Osborne Clarke is the business name for an international legal practice and its associated businesses.

Full details here: osborneclarke.com/verein