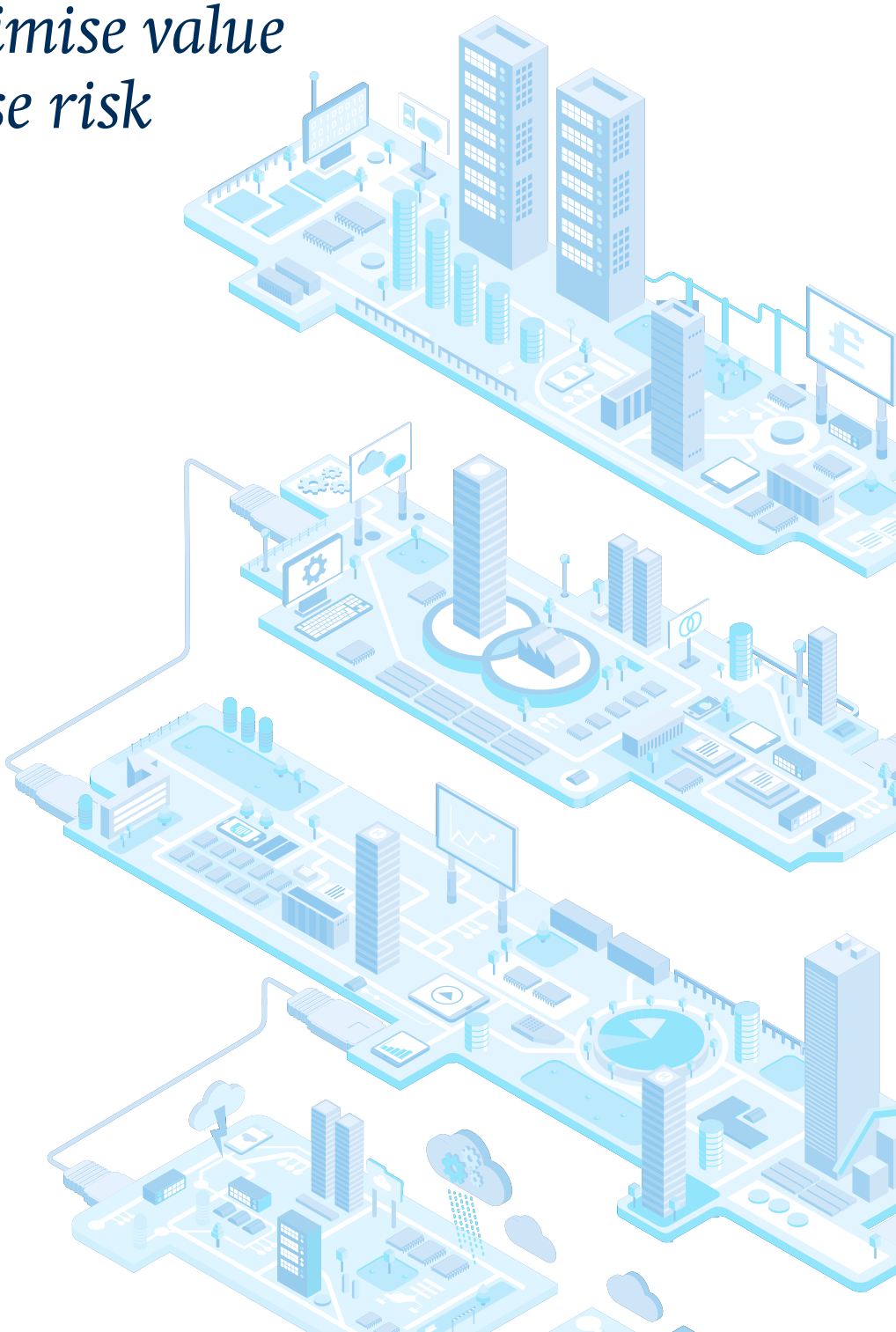
Freshfields Bruckhaus Deringer

Dealing with data – *how to maximise value and minimise risk*



On 2 February 2016, Alphabet – Google's parent company – revealed its latest financial results.

The resulting share price spike turned it into the world's most valuable company.

Much of the buzz comes from its 'moon shot' ventures, which are exploring everything from robotics to a cure for ageing. But data is the principal driver of Alphabet's financial success.

Encompassing everything from internet search to Gmail, YouTube and Android, Google contributes more than 99 per cent of Alphabet's revenues.

Why data innovation is not just for tech companies

While data underpins many of the 21st century's fastest-growing businesses, it is not the sole preserve of the tech industry.

Telecoms companies, manufacturers, pharmaceutical businesses, carmakers, utilities and financial services providers are all collecting vast quantities of data and exploring how they can use it to drive growth.

> Ericsson's latest Mobility Report reveals that there are 2.6 billion smartphone users globally – and that by 2020 this will have swelled to 6.1 billion.

The opportunity – and the risk

To understand how businesses are harnessing the power of data and managing its risks, Freshfields surveyed 200 senior executives at major businesses across the US, Europe and Asia. In partnership with YouGov we designed a study that explores the data that businesses collect, how they use it and what legal structures they have in place to manage it.

The results paint a fascinating picture of data's potential to disrupt established business models and reshape global commerce.

Our main findings

The overwhelming majority of businesses recognise data as a crucial input for competitive advantage and use advanced tools in an attempt to harvest its benefits.

89%
of respondents say access to data is critical to being competitive in their industry.

90%
are working on their data with smart analytics.

A majority see the potential of data to transform their operations.

- **72%** say greater use of data is likely to change the products and services they offer.
- **60%** say greater use of data could change profit centres.
- **58%** say greater use of data could change business models and **28%** say it could change job descriptions.

But many companies still have a long way to go to harness data's power.

- Just **45%** use data to enhance the quality and scope of current products and services.

Most of the respondents to our survey are looking to build their data portfolios in the coming year, but there is uncertainty surrounding the valuation of data assets.

- **60%** of businesses are considering acquiring data companies, assets or capabilities in the next year.
- However **more than one-third** of those businesses say they have no way of valuing data in a potential target.

Many are yet to implement a comprehensive data strategy, despite such strategies radically improving the probability of extracting value from data and minimising its risks. Implementing a comprehensive strategy requires a significant investment of time.

- **53%** say they have a fully comprehensive strategy in place right across their business.
- **37%** have a partial strategy in place.
- Those with a comprehensive strategy are **more than twice as likely** to use data to develop new products and services.
- But **45%** of these businesses are missing important elements of their strategy.
- **52%** say implementing a comprehensive strategy took them more than two years.

Businesses recognise antitrust as an issue in data-driven markets – but many are yet to raise it up the risk agenda.

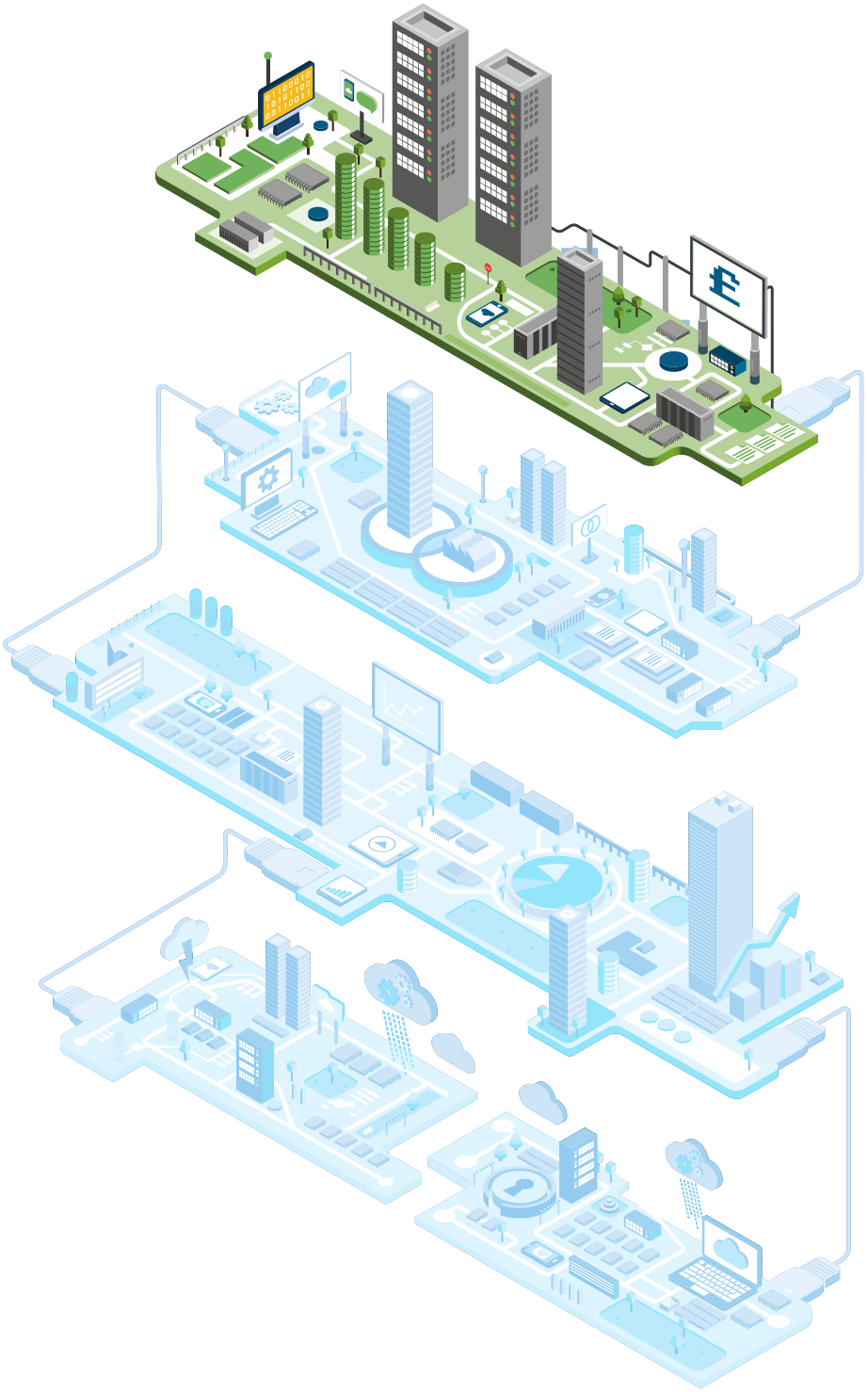
- **67%** say antitrust is a medium to high risk factor with the data they hold.
- **62%** say access to data is a problem for new entrants in their industry.

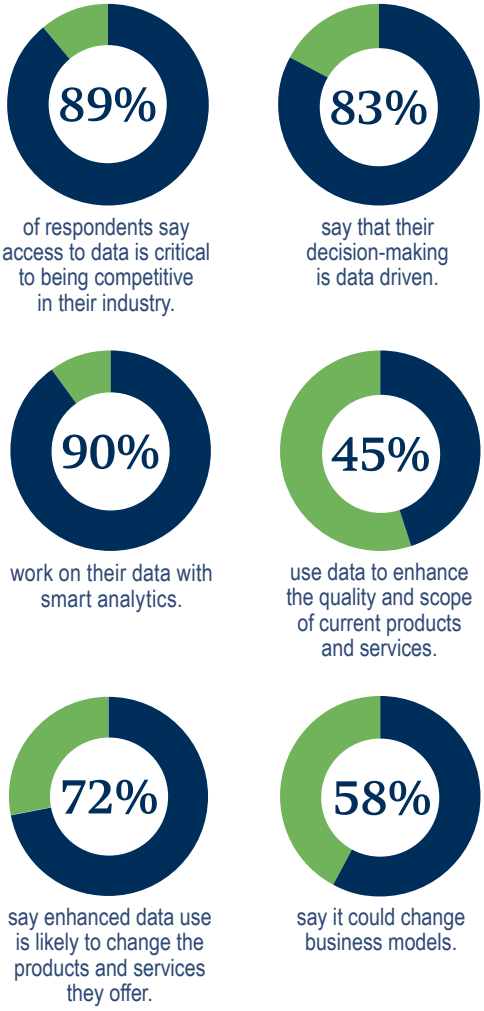
The often conflicting and disparate array of regulatory regimes appears to act as a barrier to harnessing the benefits of data. Regulation is rated by businesses as the main obstacle to fully exploiting their data. Data protection and cyber security regulations are in focus, and cyber security is seen as a significant risk factor.

- **83%** rate cyber attacks as a medium to high risk factor.
- **13%** say data leaks occur frequently in their industry.
- **26%** say leaks have become more common in the past three years.
- **13%** say they have been involved in litigation related to data.
- **70%** say compliance with data protection/privacy regulations is a medium to high data risk.

1

The value of data and how to realise it





“

The volume of data stored around the world is growing exponentially. KPMG predicts that by 2020 there will be 35ZB (zettabytes – 1 billion terabytes) in existence. Just two years ago the entire World Wide Web comprised just 4ZB.

Our survey shows data is increasingly valuable to all businesses, with nearly 90 per cent of respondents saying access to data is critical to being competitive in their industry. Our results also reveal the huge variety of data sources companies use and the types of data they collect. Seven in 10 respondents gather productivity or output data from machines, and more than 60 per cent collect data from external sources such as business partners or weather forecasters.

The benefits of smart analytics

One of the keys to extracting value from data is the use of smart analytics – advanced algorithms that can make sense of vast pools of disparate information.

Recent research by McKinsey shows that big data analytics have ‘substantial’ profitability and productivity benefits. McKinsey reports that the average business investing in big data analytics experiences an initial 6 per cent increase in profits, which rises the longer the investment continues.

It is therefore not surprising that over 90 per cent of respondents to our survey are using these smart tools. However, less than half (45 per cent) say they use data to enhance the quality and scope of their current products and services.

Just 27 per cent are using data to develop new products and services, despite 81 per cent saying they collect data expressly for this purpose.

But when asked how enhanced use of data could reshape their organisations, 72 per cent say it could change the products and services they offer – and 58 per cent say it could change entire business models.

Our survey shows that businesses recognise data’s value. They are collecting lots of it and analysing it with advanced tools. They can see its potential to transform what they do and how they do it. Yet today, most are not using data to improve their products or to develop new ones. So how can they make the leap?

How to use data to create value

With so much data available it's tempting to start analysing it without a clear view of what's being searched for – or what data and tools will produce the right result. One of the defining characteristics of businesses that derive value from data is a data strategy with defined goals.

> The companies that make the most of their data have a clear data strategy aligned to their business objectives.
>
> Bertram Burtscher, Partner

'The companies that make the most of their data have a clear data strategy aligned to their business objectives,' says Bertram Burtscher, a Freshfields partner who has been advising many of the world's most advanced businesses on how to harness their data assets.

'They know where they want to go and what data will get them there. The businesses without a robust data strategy risk wasting time and money and any success they do have is likely to be the result of luck.

'Businesses should consider what they want to achieve on a sliding scale of importance and cost and then focus on the things that are most important and least costly. They should start small, go through rapid prototyping and only scale up once they've proved their concept works.

'They also need to be clear whether they need personal data to achieve their objectives. Personal data can be a "poison pill" because of the regulatory burden that it places on analytics tools – and in many cases the same results can be achieved without it.'

The benefits of a holistic approach

And monetising data isn't just about having clear goals. Preserving the value in data means taking into account multiple legal issues that often play out differently across the world. Giles Pratt, a Freshfields partner who advises businesses across a range of data issues, says: 'The most successful data businesses take a holistic approach that goes beyond data privacy and cyber security.

'These two issues are already high up the corporate agenda, but generating real value from data – and managing the risks – requires a joined-up approach that considers everything from antitrust risk to tax, intellectual property, employment law and sector-specific regulations.

> Data privacy and cyber security are already high up the corporate agenda. But generating real value from data – and managing the risks – requires a joined-up approach that considers everything from antitrust risk to tax, intellectual property, employment law and sector-specific regulations.
>
> Giles Pratt, Partner

‘Incorporating these into a data strategy isn’t just about the lawyers and compliance team. It’s critical to get input and buy-in from, among others, senior management, HR, public affairs, media relations and IT. But by considering all of these things a business can structure its operations and its contracts in a way that delivers competitive advantage.’

And Natasha Good, a partner in Freshfields’ technology, media and telecoms group, adds: ‘There is real excitement about what data can offer a business, but it’s hard for many to harness that potential.

‘This is particularly acute for companies where data is important but isn’t yet an essential building block of their offering – such as consumer products businesses, financial services companies or telcos.

‘Newer tech businesses – where data has been central in early stages of growth – have fewer of the issues that more mature companies face, such as institutional investor expectations and long-term planning horizons. It’s harder for mature businesses to be as entrepreneurial with data.’

“

There is real excitement about what data can offer a business, but it’s difficult for many to harness that potential. It can be harder for mature businesses to be as entrepreneurial with data.

Natasha Good, Partner

Data and tax

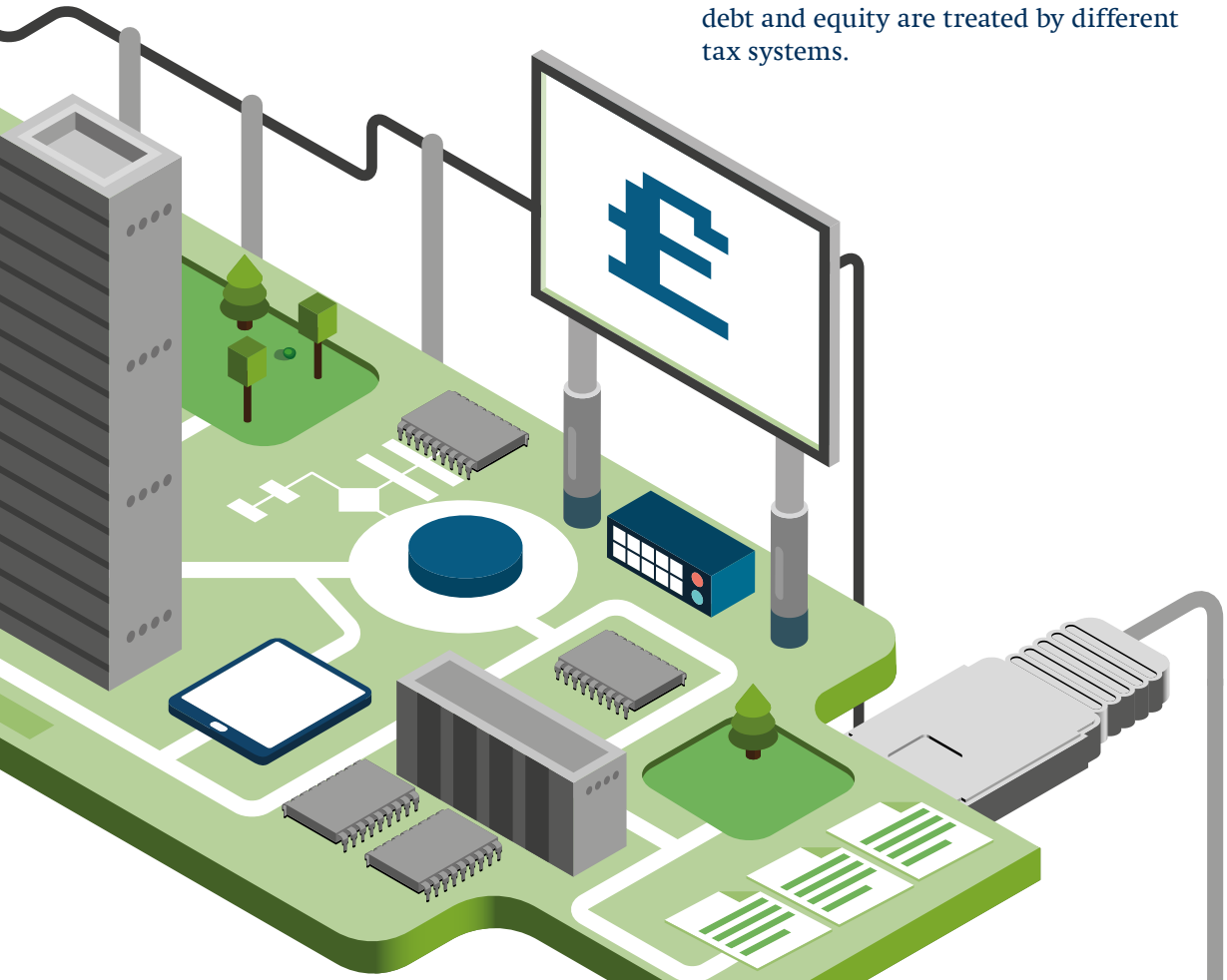
Our survey reveals that more than half of businesses expect enhanced use of data to shift profit centres. So what are the consequences for their tax position?

60%
of respondents say greater use of data could change profit centres within their business.

Digital companies such as Amazon and Google have recently been in the spotlight over their tax affairs. Much of the controversy surrounds the way revenues flow around data-driven businesses, which makes it hard to tax profits at source. But new rules are set to be implemented across the world that will change the landscape for everyone.

The OECD's Base Erosion and Profit Shifting (BEPS) proposals – supported by the G20 and accepted in principle by all members – aim to align tax more closely with value creation.

'Many tax structures rely on authorities not knowing what's going on in other jurisdictions,' says Freshfields Tax Counsel Job van der Pol. 'For example, "hybrid instruments" take advantage of the way debt and equity are treated by different tax systems.



> Many tax structures rely on authorities not knowing what's going on in other jurisdictions. The BEPS recommendations aim to eliminate this asymmetry.
>
> Job van der Pol, Counsel

'To eliminate this asymmetry, the BEPS recommendations include country-by-country reporting. Companies will have to include in their annual accounts their effective tax rate in different jurisdictions. This information can be measured against sales volumes, which makes it easy to see whether a company is paying the statutory rate of tax.'

New rules threaten more investigations and disputes

This increased transparency is likely to lead to more investigations and tax disputes, particularly in relation to double tax treaties. Existing structures are currently being challenged by the EU under state aid rules and the changes could see this activity grow.

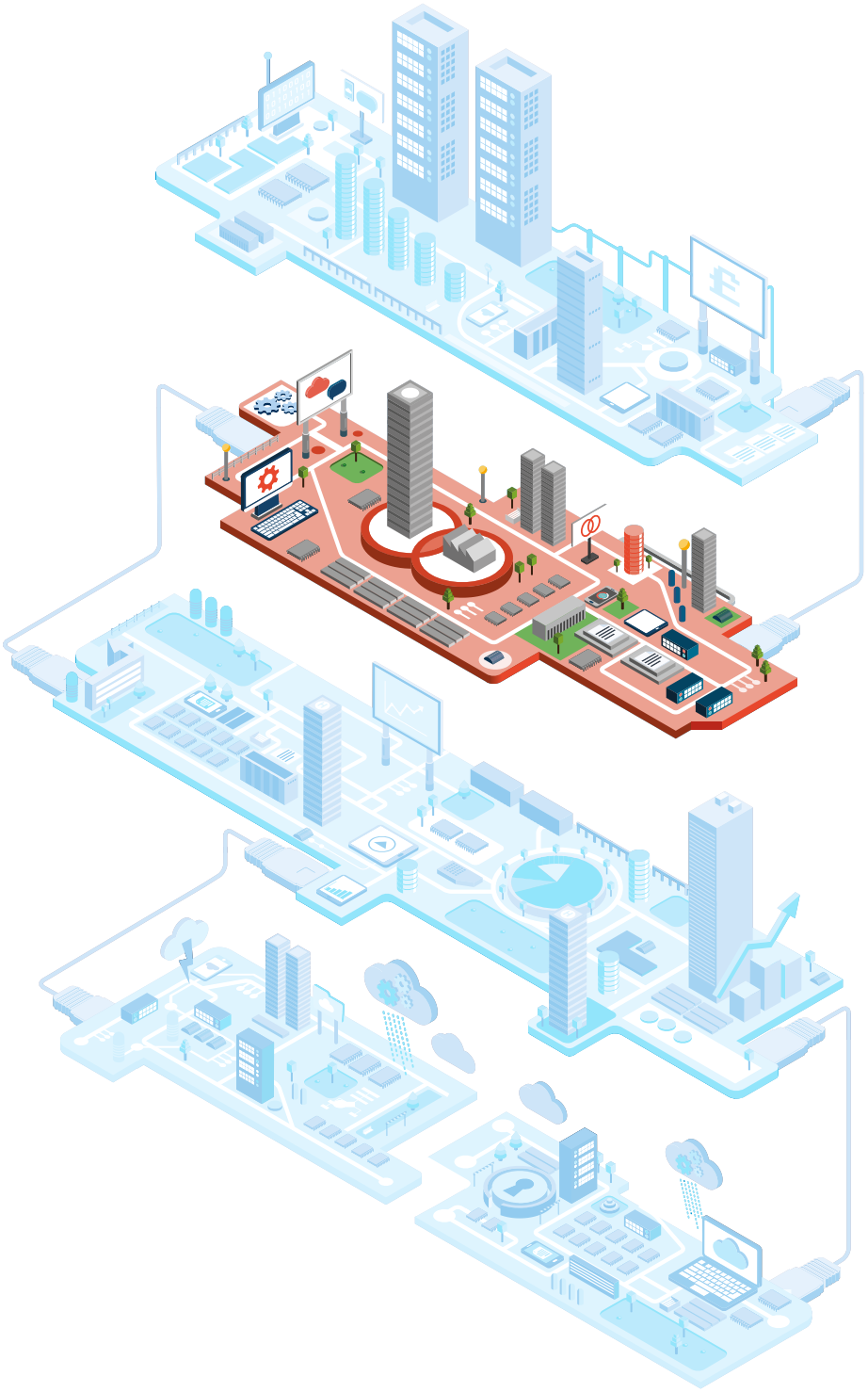
The new rules will prevent businesses locating value-creating intellectual property in low-tax regimes unless the underlying R&D and the control over the intellectual property also take place in the same jurisdiction. Businesses therefore face a choice: relocate people or IP assets – or lose their tax benefits.

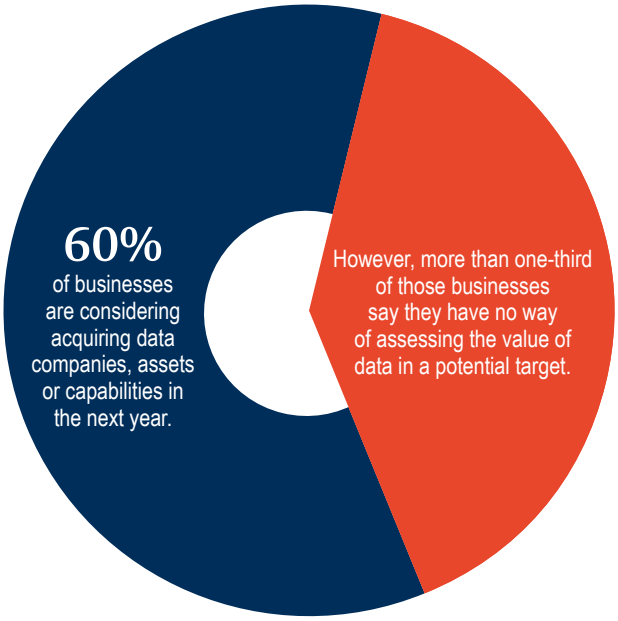
For businesses that create value from data analytics, this raises a number of questions. If data is purchased from or licensed to a company in one jurisdiction and processed in another, how does that affect the tax position of each? And where is value created?

Job says: 'It may be possible to argue that value is created at the processing stage, when essentially worthless streams of raw information are brought together to generate insight. With a well-thought-through strategy that locates sensors and storage in the right places, a business should be able to move data across borders without transfer pricing issues and process it in the optimal location where the value-added processing actually takes place.'

2

How to treat data in M&A





The value of a business can be calculated in a number of ways. As a multiple of profits. As a multiple of revenues. By reference to estimated future cashflows. Risk plays a role, as will the value of the company's assets. So with data becoming an increasingly important asset, how should it be treated in an M&A transaction?

As our survey shows, most businesses are looking to build their data portfolios. More than half (60 per cent) of respondents confirm they are looking to acquire data companies, assets or capabilities in the next year – yet more than one in three say they have no way of assessing the value of data in a potential target.

Data is now a red flag issue for many deals

It is possible to assess the legal value of data as part of due diligence. Corporate Partner Natasha Good says: 'The most important considerations are usually whether you as the buyer or the target company have the rights to use that data in the way it's currently being used, and can develop further use cases to expand and develop the business.'

And Giles Pratt, a Freshfields IP partner, explains: 'This is partly about data privacy, but it is also about contractual rights and IP protection. Cyber security procedures and evidence of previous cyber incidents are also important factors. Buyers are now much more focused on making sure they're not on the hook for data sins of the past, and want to make sure their financial projects for data use won't be derailed by future regulation.'

> The most important considerations are usually whether you as the buyer or the target company have the rights to use the data in the way it's currently being used.
>
> Natasha Good, Partner

How to treat data *in M&A*

The legal structures that enhance data's value

Specific legal structures that can be put in place pre-sale, during a deal or post-transaction reinforce data's value and give all parties greater flexibility. Data sharing agreements – a vital component of an effective strategy – define usage rights for both the seller and the buyer. They can also minimise risk should the deal attract the attention of antitrust regulators.

Data is increasingly in the spotlight from an antitrust perspective, and many businesses now need to consider whether they might need to make certain data sets available to competitors as part of merger control remedies. Laurent Garzaniti, a Freshfields antitrust, competition and trade partner, says: 'If an antitrust regulator rules that data should be handed over as part of a deal, the way a data set has been designed and existing data sharing agreements can give parties more flexibility to deal with regulatory requests. If access rights are clearly defined, they may be able to open up segments of the data in line with the sharing agreement rather than the whole pool.'

Assessing value

Putting a specific cash value on data is a much trickier task. There have been a number of attempts to solve this puzzle but no definitive answer. As Doug Laney, a senior analyst at technology research company Gartner, says: 'We are in the midst of the information age – yet information is still considered a non-entity by antiquated accounting standards.'

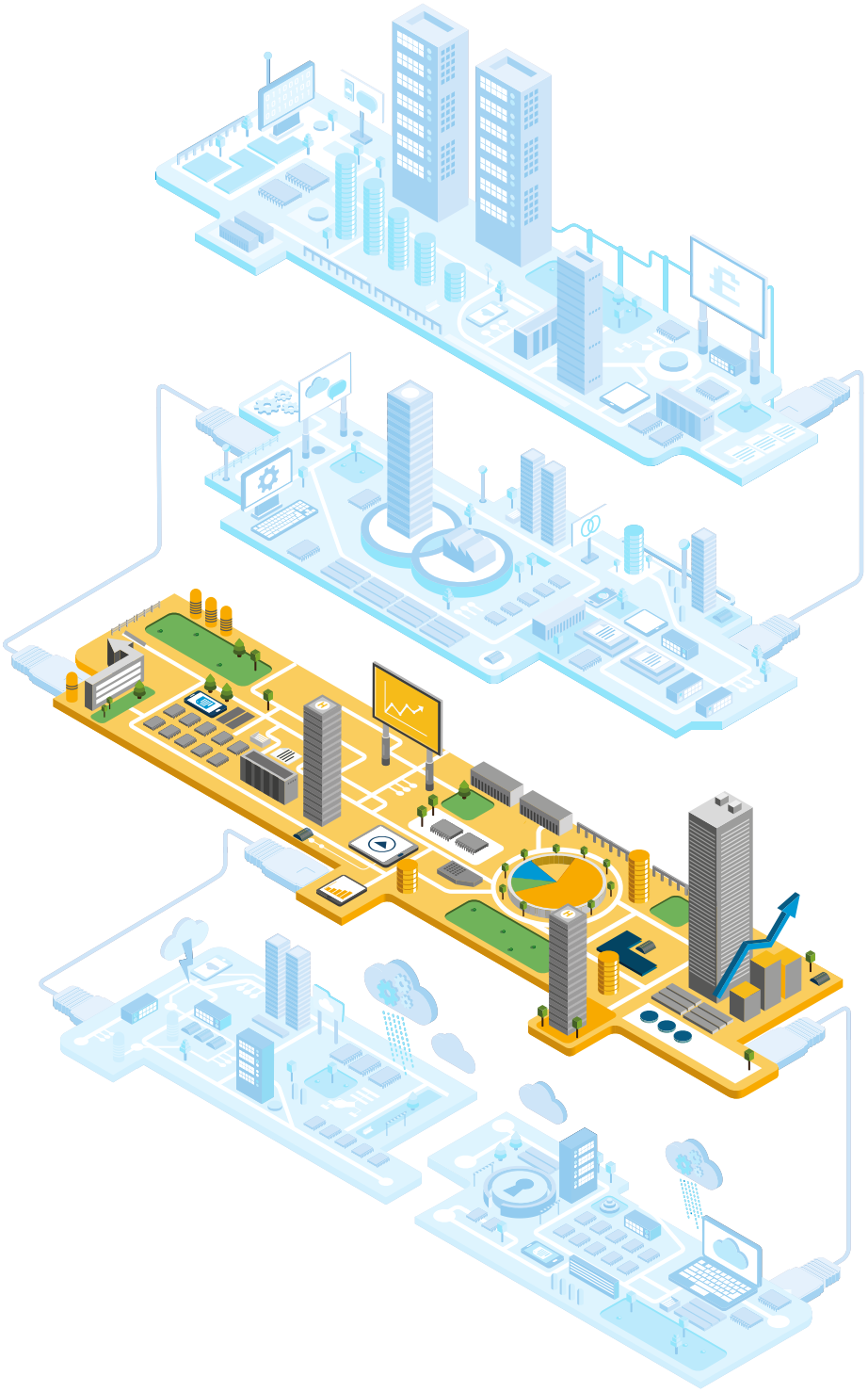
Corporate Partner Bertram Burtscher adds: 'You can calculate enterprise value using revenue derived from products based on data, but there's no established methodology that can set a plausible monetary value on raw data itself.

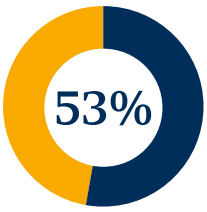
> Investors in data-rich companies often need bank financing to pay for acquisitions, yet data is not included on the target's balance sheet.
>
> Bertram Burtscher, Partner

'This is an issue for investors interested in data-rich companies. They often need bank financing to pay for acquisitions, yet data is not included on the target's balance sheet. We're working with the Fraunhofer research institute on ways to get businesses "data ready" in a more holistic way. This will help make data a more tangible asset and get investors closer to the assurances they need.'

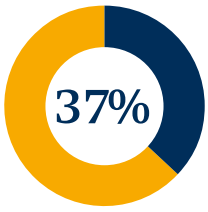
3

How to create a data strategy that works



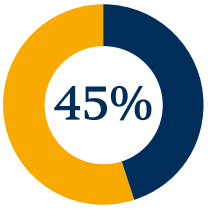


of respondents say they have a fully comprehensive strategy in place right across their business.

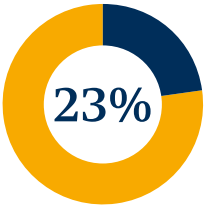


have a partial strategy in place.

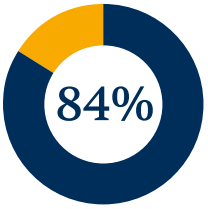
Those with a fully comprehensive strategy are more than twice as likely to use data to develop new products and services.



However, almost half of the 'fully comprehensive' businesses (45%) have some important elements of their strategy missing.



Of the 'partial strategy' businesses, just 5% have the essential building blocks in place, and just 23% have implemented effective governance procedures.



However, many of these businesses are already collecting large volumes of data and analysing it with smart analytics (84%).

To create value from data a business needs a comprehensive strategy containing specific legal structures. Our survey reveals companies that have implemented what they regard as 'fully comprehensive' strategies right across their operations are more than twice as likely to use data to develop new products and services.

Yet even these strategies are often not as comprehensive as they could be – almost half (45 per cent) of this 'fully comprehensive' group are missing at least one of five essential building blocks.

What a data strategy needs to do

Effective data strategies define what data will be analysed, how it will be analysed and what it will be used for. They also ensure personal data is anonymised, reducing the risk of breaching data privacy regulations.

They establish parameters for sharing data within groups. And when combined with effective data governance, they ensure only the highest-quality and most relevant data is being analysed – and that it's protected from cyber attacks.

The five essential building blocks of an effective data strategy

1	Rules for selection of data to be processed	Of the data available to your business, which will give you the best chance of achieving your objectives?
2	Rules for mining data for business purposes	Which of the data available to your business can be manipulated and analysed in line with antitrust constraints as well as data privacy, security and sector-specific regulations?
3	Rules for data use	Is the way you want to use the data (including the way you make it available to others) compliant with legal requirements? How do you allocate the responsibilities and risks of non-compliance within the company?
4	Rules for effective anonymisation	Do you need to use personal data to achieve your goals? If so, effective anonymisation will take it out of the scope of privacy regulations and give you greater flexibility to process it and develop different use cases for it.
5	Rules for sharing data intra-group	Which entities in your group contribute data to a pool? Which group entities will process the data? Who in your group has access to it? How do you distribute value created from the pool between group entities?

In the 'fully comprehensive' group, around nine in 10 have rules for data selection, data use and data mining. But fewer have rules for sharing data intra-group and effective anonymisation.

Of the 37 per cent of respondents with a partial strategy in place, these numbers drop to around 50 per cent, with just 38 per cent effectively anonymising the personal information they hold.

Despite this, a significant proportion of companies in this latter group are collecting many different types of data and 84 per cent are already using smart analytics – potentially explaining why so many are yet to really use data to create value.

Implementing a strategy takes time

More than four in 10 respondents with a data strategy (43 per cent) report that it took between one and two years to implement, and 52 per cent say it took even longer. So where do you start?

Technology, media and telecoms Partner Bertram Burtscher says: 'It's about getting the right people in place and thinking about what you want to achieve.

'You need strategic people who understand the company's objectives and can ensure board support. You need operational people who know what data the business generates, or could generate if necessary. You need technical people who understand how to access and manipulate data, and legal people who understand how to do all this within the scope of regulatory restrictions.

'In legacy structures these people often report into different C-level functions and don't work together effectively. Many companies will therefore need an "external prophet" such as a data scientist who can help them overcome the structural hurdles that are standing in the way of understanding data's potential for the business.'

Why it's important to share (with the right rules)

In complex multinational groups, different entities are likely to generate data that could benefit the business as a whole. Using that data to create long-term value while reducing legal risk requires a data sharing arrangement formalised in contracts.

These arrangements take into account sector-specific regulations, privacy regimes and the compliance rules of the jurisdiction in which data is stored and processed. They define what data is available for analysis and who has access to it. And if value is created from collaborations, they govern where that value arises and how it's shared within the group.

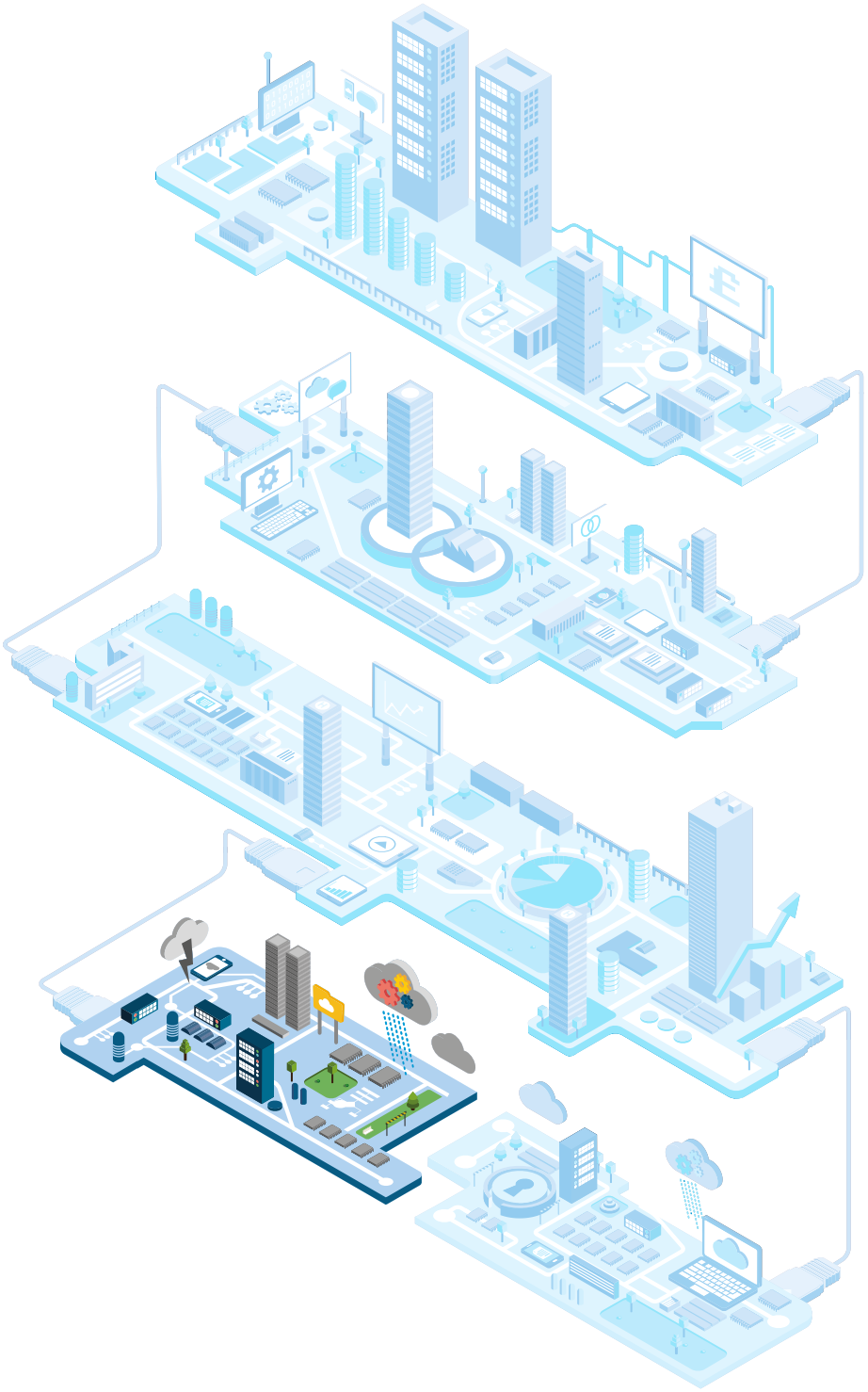
Bertram says: 'Data sharing arrangements are complex to design and implement, and even some of the most sophisticated data businesses don't have them. But they're vital in large, complex companies, particularly if they're active in M&A.

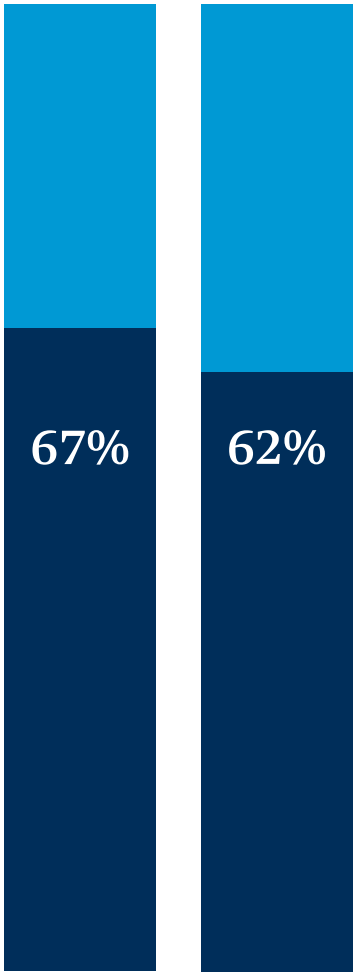
'If a group business is carved out and sold, that entity instantly becomes an independent partner or even competitor yet it may still be dependent on access to shared data. Solid sharing arrangements, particularly in multinational conglomerates, need to cater for the implications associated with businesses joining or leaving the group – including in terms of data.'

> The right strategy will get you where you want to go more quickly, more effectively and more cheaply. Without a proper strategy, you're much less likely to get what you want. And you'll waste time, money, resources and credibility in getting there.
>
> Bertram Burtscher, Partner

4

Data, antitrust and consumer protection





say antitrust is a medium to high risk factor.

say access to data is a problem for new entrants in their industry.

Antitrust regulators are taking an increasing interest in data and examining whether some companies have collected so much customer data that their rivals are unable to compete. There are also concerns about the impact of combining large data sets in M&A transactions and joint ventures, from both a pricing and a consumer protection perspective.

Regulators in France, Germany, the US and the UK – where the Competition and Markets Authority recently published a report on the commercial use of customer data – have launched investigations, leaving companies vulnerable to multiple actions.

The spotlight is also on particular industries. The UK Financial Conduct Authority, for example, is examining whether insurers' use of big data analytics could be harmful to consumers.

EU Competition Commissioner Margrethe Vestager, speaking in January 2016, said: 'If just a few companies control the data [needed] to satisfy customers and cut costs, that could give them the power to drive their rivals out of the market.

If just a few companies control the data [needed] to satisfy customers and cut costs, that could give them the power to drive their rivals out of the market.

Margrethe Vestager, EU Competition Commissioner

'And with less competition, there's a risk that there won't be enough incentive for companies to keep using big data to serve customers better.'

Almost two-thirds of respondents agreed that access to data was a problem for new entrants, reflecting Ms Vestager's concerns.

Data, antitrust and *consumer protection*

And while 67 per cent rate antitrust as a medium to high data risk, it should probably be higher up the agenda considering the current regulatory trend.

Laurent Garzaniti, head of Freshfields' technology, media and telecoms group, says: 'More businesses should be aware of data's antitrust implications. Companies are yet to fully appreciate the antitrust risk connected to data, but when enforcement actions begin it will be impossible to ignore.'

Which industries are in the regulators' sights?

Antitrust is a particular risk for any consumer-facing businesses. France's competition regulator for example recently ordered a former state-owned energy company to open its data to competitors, arguing that it has such detailed information that its rivals are unable to compete with its targeted tariffs.

Laurent says: 'Utilities, insurers and banks have access to extremely valuable data – for example health and financial information – simply by providing a service. There are also digital platforms that provide services for free in exchange for personal information, which they then effectively sell to advertisers.

'Some of these platforms risk being subject to an antitrust investigation for abuse of dominance. Competitors are alleging that they have become so powerful that they are almost an essential facility. We're seeing a lot of regulatory attention in Europe, particularly as many of these companies are based in the US.

'It's very difficult to know where to draw the line. Regulatory action may discourage investment, and unfairly penalise those who have first-mover advantage.'

Focus on data pooling

The pooling of data is also in the regulators' sights, both via M&A and in joint ventures. Data is being analysed as part of merger control proceedings to ensure the combination of large data sets does not lead to dominance.

And businesses involved in developing new technologies such as the Internet of Things are also under scrutiny. They could find themselves at risk because the systems will generate huge volumes of data and involve extensive collaboration across industries.

Regulators' concerns will not be solely linked to competition. There will also be interest in whether some deals could reduce consumer privacy where the merging parties have divergent standards.

As Tom Ensign, a Freshfields antitrust partner based in Washington, says: 'The US agencies do not perceive big data to present any significant competition issue. Instead, the focus has been on potential discrimination against certain socio-economic groups, privacy, and deceptive practices.'

> Companies should ask themselves whether they need users to make their data available on an exclusive basis. If not, it's harder to argue that your data is unique.
>
> Sascha Schubert, Partner

But in Europe, action is already being taken. The EU has introduced 'data portability' in an attempt to encourage competition, allowing individuals who may have been discouraged from switching providers because their incumbent held so much personal information to take their data elsewhere.

How can businesses mitigate their risk?

To reduce antitrust risk, data management should be part of a business's antitrust compliance procedures – particularly if they're using advanced analytics.

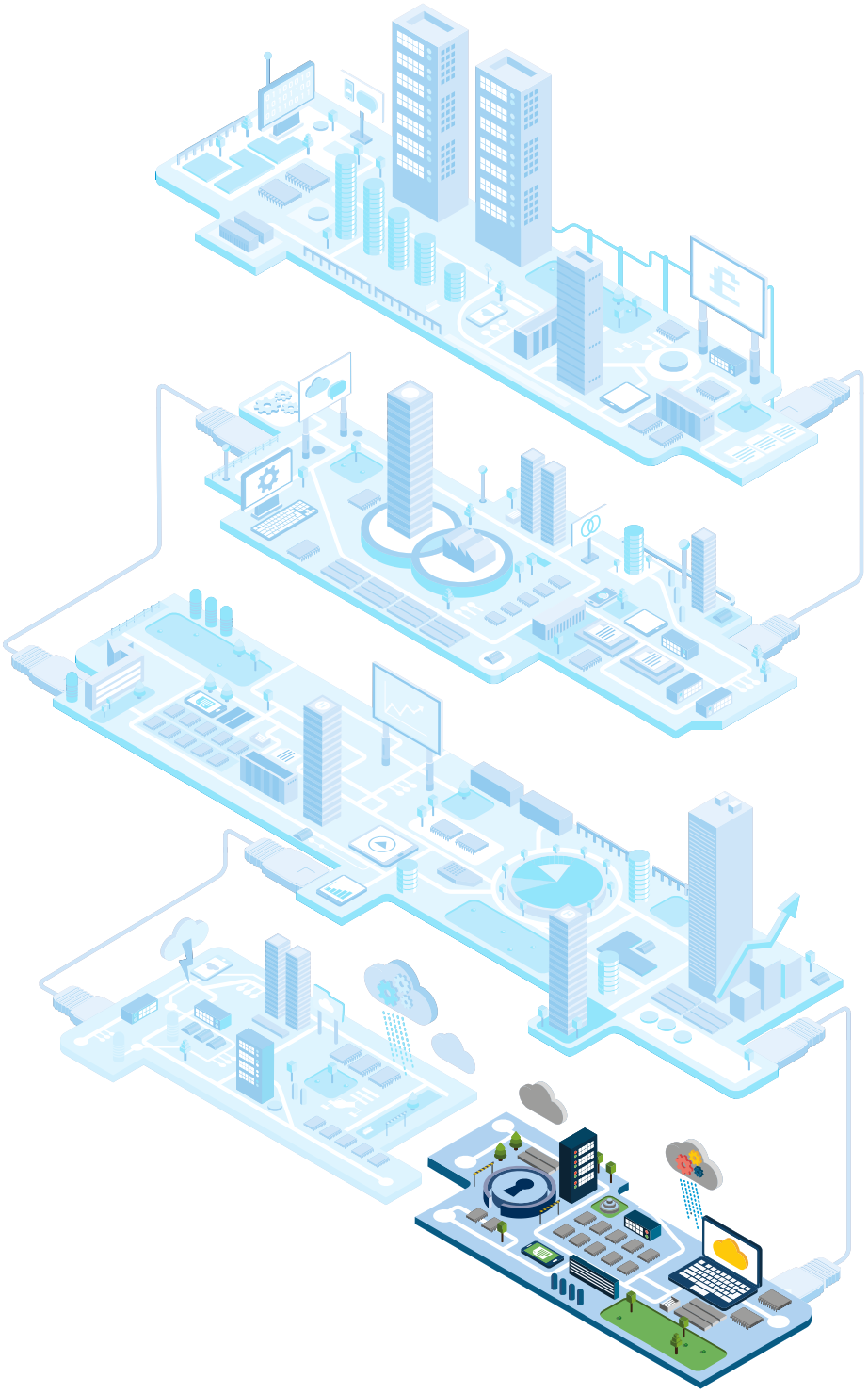
Sascha Schubert, a Freshfields partner who has advised clients on the antitrust issues associated with big data analytics, says: 'One thing that companies should ask themselves is whether they need users to make their data available on an exclusive basis.

'If not, it's harder to argue that your data is unique because it's possible for your competitors to get it themselves.'

For a more detailed look at antitrust and data, click here.

5

Cyber security and regulatory constraints



Any company that holds data is under threat from hackers and either malicious or careless employees. But while cyber security emerges as the biggest threat to the data companies hold, it is surprising that the proportion who deem it a medium to high risk factor (83 per cent) isn't higher.

Just 13 per cent of respondents say that data leaks occur frequently in their industry, and 26 per cent acknowledge that they are becoming more frequent. This, too, is a cause for concern.

“

There still appears to be a degree of complacency about the risk of data leaks, with a perception that they are something that affects others.

Jane Jenkins, Partner

Jane Jenkins, a partner who leads Freshfields' cyber security group, says: 'There still appears to be a degree of complacency about the risk of data leaks, with a perception that they are something that affects others. But cyber attacks are happening in every sector and companies need to be alive to the threat they face.'

Cyber security and *regulatory constraints*

The consequences of a cyber attack

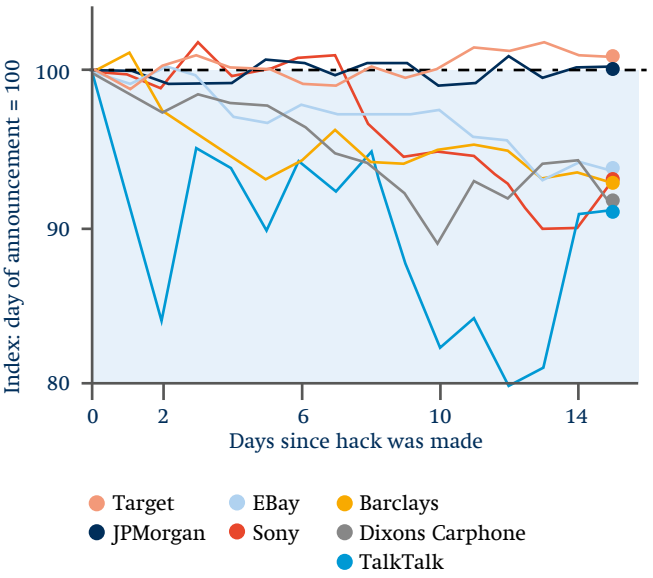
The regulatory risk of suffering a data loss is growing around the world. Under the new EU Data Protection Regulation for example, companies can be fined up to 4 per cent of global group-wide revenues for a breach.

Financial liabilities are growing in other jurisdictions, too. US identity theft protection company LifeLock was recently fined $100m for failing to protect customer data, the biggest ever US penalty. And US retailer Target's cyber attack has cost the company hundreds of millions of dollars, both in defence costs and in repaying banks that compensated its customers.

Litigation risks are highest in the US, but Europe now has a class-action regime. In many jurisdictions company directors are held personally liable if they fail to implement effective security standards.

Then there are the reputational consequences. Cyber attacks that target personal data can destroy consumer trust. UK broadband provider TalkTalk lost more than 100,000 customers when hackers stole vast quantities of personal information and its share price fell more than 20 per cent.

How company shares have fared after cyber attacks



Source: City AM

But while the media and political focus has been on losses of consumer data, in many cases the most valuable information a company holds is not personal. Where an attack targets essential business information, a cyber attack can bring a company to its knees. Cyber security should therefore be seen as a general business continuity risk.

Tim Harkness, who leads Freshfields' US cyber security group, says: 'There is a political demand that regulators focus their attention on personal data. But that's not the most valuable information for a lot of businesses.

'Imagine a hacker stole your company's living will. If it ends up with a competitor it could destroy you. You need to think about how you protect your formulas and non-patented trade secrets.'

Are your cyber protections sufficient?

In countries such as the UK and the US, regulators judge preparedness by industry standards. Directors therefore need to know what their competitors are doing. If they don't, they could to be sued for failing to protect the company.

Authorities are also pushing for greater transparency. The US Securities and Exchange Commission, for example, is considering making certification of internal controls mandatory in financial statements.

Justin Watts, another partner in Freshfields' cyber group, says: 'Governments are encouraging businesses to share information on threats and how they protect themselves as a way of driving higher standards.

> The general trend is towards greater awareness, greater governance, greater investment in cyber security and greater transparency.
>
> Justin Watts, Partner

'Companies also need to be aware of regulatory debate. The EU for example considered whether to require the appointment of a dedicated data protection officer during discussions on the data protection regulation. Businesses should therefore think hard about whether they need one.'

How to make yourself cyber secure

Freshfields Partner Klaus Beucher, who advises multinationals on cyber security issues, says there is a set of steps that companies must take to protect themselves.

'Firstly, conduct a thorough risk assessment of your business. Map your data so you know where it is and what you're doing with it. Don't just look at your technical infrastructure, review your legal risks as well. Look at everything from IP protections to your obligations under data privacy and employment law.

'Then, ensure you have effective data governance policies in place. Finally you should draw up a crisis plan and practise it. All of this should be done in partnership with the board.'

Tim Harkness adds: 'Directors have personal risk, particularly in the US. Good governance is therefore vital and boards need to decide who is responsible for data security.'

Navigating global regulation

Our respondents consider regulatory restrictions to be the biggest obstacle to fully exploiting their data. There is huge uncertainty about what companies can do with their data within the scope of global regulations.

Limitations on the use of personal data, for example, vary greatly between jurisdictions. The rules are constantly shifting to address new developments in technology and are inconsistent across geographical boundaries, putting them at odds with the inherently borderless nature of data.

Cyber security and *regulatory constraints*

The EU/US Privacy Shield

In February the EU and the US announced that they had concluded negotiations on a successor to the Safe Harbor regime, which allowed companies sending personal data from Europe to the US to self-certify that they were compliant with European privacy rules.

The regime was invalidated last year by the European Court of Justice, which ruled that Safe Harbor did not sufficiently protect Europeans' personal data from US state surveillance. But the new deal – Privacy Shield – is itself expected to be challenged.

The conflict between international conceptions of privacy is already being tested in the courts. Microsoft is challenging a request from US prosecutors to access personal emails held on an Irish server, and has handed control of its European data to a subsidiary of Deutsche Telekom in Germany in an attempt to keep its customer data out of the reach of US state surveillance. In response we expect more companies to review which entities in their corporate families control data.

Asia has become a pioneer for data-driven businesses

It's not just in the West that the regulatory environment is changing. Richard Bird, a Freshfields partner who works with tech businesses across Asia, says: 'Investment restrictions in the e-commerce and internet services sectors are gradually being peeled away in Asia, encouraging further investment by international and regional tech players.

'At the same time the data privacy landscape grows more complex. Asian countries are taking differing approaches to the protection of personal and consumer data and to cyber and data security. Some countries are adopting liberal data privacy regimes to encourage data analytics, data-driven business models and supporting infrastructure, while others are taking a strict line to data sovereignty and cross-border data transfers. Adoption of the Trans-Pacific Partnership Agreement will only go so far to harmonising these approaches.

'We are advising many established international and Asian companies looking to build out mobile and data ecosystems across Asia. Many of these deals involve partnering with local, data-rich companies.

'Multinationals need sophisticated advice to close these deals and to avoid the many pitfalls in a continually evolving regulatory landscape. This advice needs to combine the highest levels of deal execution capability with deep, specialist expertise at local level.'

For more on the legal aspects of cyber security, click here.

“

Asia has become an incredibly exciting innovation sandbox in the data and tech field. This presents huge opportunities for overseas investors. But with divergent data privacy and regulatory approaches, tapping into local expertise remains critical.

Richard Bird, Partner

Methodology

The survey was conducted via telephone interviews with 206 businesses across Europe, the US and Asia.

The respondents performed a variety of roles:

- CIO – **46 per cent**;
- CTO – **31 per cent**;
- general counsel – **15 per cent**; and
- COO – **9 per cent**.

The interviews were evenly split by region:

- US – **33 per cent**;
- Europe – **34 per cent** (UK – 12 percent; France – 11 per cent; Germany – 12 per cent); and
- Asia – **32 per cent**.

The businesses were from a variety of sectors:

- financial services;
- pharmaceutical, life sciences and healthcare;
- consumer products and automotive;
- technology, media and telecoms;
- utilities;
- transport; and
- retail.

They had market capitalisations of $500m and over:

- $500m–$999m – **42 per cent**; and
- $1bn+ – **58 per cent**.

Respondents all have substantial decision-making input over their companies' data arrangements.

YouGov plc makes every effort to provide representative information. All results are based on a sample and are therefore subject to statistical errors normally associated with sample-based information.

All fieldwork was completed between 2 and 27 November 2015.

Percentages may not always add up to 100 due to rounding.

Contacts

Richard Bird
Partner, IP

T +852 2913 2660
E richard.bird
@freshfields.com

Tim Harkness
Partner, Dispute Resolution
– Litigation

T +1 212 230 4610
E timothy.harkness
@freshfields.com

Klaus Beucher
Partner, IP

T +49 221 20 50 71 13
E klaus.beucher
@freshfields.com

Jane Jenkins
Partner, Dispute Resolution

T +44 20 7832 7280
E jane.jenkins
@freshfields.com

Bertram Burtscher
Partner, Corporate

T +43 1 515 15 119
E bertram.burtscher
@freshfields.com

Giles Pratt
Partner, IP

T +44 20 7716 4339
E giles.pratt
@freshfields.com

Tom Ensign
Partner, Antitrust,
Competition and Trade

T +1 202 777 4527
E thomas.ensign
@freshfields.com

Sascha Schubert
Partner, Antitrust,
Competition and Trade

T +32 2 504 7039
E sascha.schubert
@freshfields.com

Laurent Garzaniti
Partner, Antitrust,
Competition and Trade

T +32 2 504 7115
E laurent.garzaniti
@freshfields.com

Job van der Pol
Counsel, Tax

T +31 20 485 7648
E job.vanderpol
@freshfields.com

Natasha Good
Partner, Corporate

T +44 20 7832 7659
E natasha.good
@freshfields.com

Justin Watts
Partner, IP

T +44 20 7716 4296
E justin.watts
@freshfields.com

freshfields.com