DATA ASSETS
PROTECTING AND DRIVING VALUE IN A DIGITAL AGE

Edward du Boulay, Miriam Everett, Kyriakos Fountoukakos, Andrew Moir and Rachel Montagnon of Herbert Smith Freehills LLP explore the key legal considerations for organisations looking to develop or refine a data commercialisation strategy.

Faced with the exponential rise of data as an asset class in its own right, organisations are now taking a fresh look at the data that are available or accessible to them and the ways in which the value of those data can be safeguarded, unlocked and maximised. Data have become a strategic and valuable asset for many organisations but protecting and exploiting that asset is not always simple.

This article considers data as an asset, how they can be used effectively and how to minimise associated legal risks. It explores key legal considerations for organisations looking to develop or refine a data commercialisation strategy, including:

- The concept of so-called data "ownership".
- Intellectual property rights.
- Contractual rights.
- Information governance.
- Competition law.
- Corporate transactions.

DATA OPPORTUNITIES

Data, in the widest sense, are simply pieces of information collected together for reference or analysis, and have always underpinned business success. In every industry, the effective use of data enables organisations to increase profitability, including by: generating new revenue streams; reducing costs; informing decisions; expanding reach; and facilitating improvements in quality and efficiency. At the same time, the value of data can be eroded and they can expose organisations to significant risks and liabilities if they are not handled with care (*see feature article "Data use: protecting a critical resource", www.practicallaw.com/w-012-5424*).

There is a surfeit of bold statistics and predictions regarding the scale of actual and imminent data opportunities. In April 2018, the European Commission predicted that, by 2020, the EU data economy could be worth €739 billion, representing 4% of overall EU gross domestic product (*https://ec.europa.eu/digital-single-market/en/towards-thriving-data-driven-economy*). In its research report published on 7 September 2018, Accenture suggested that, by 2030, data marketplaces might facilitate the exchange of data worth more than $3.6 trillion in value (*www.accenture.com/gb-en/insights/high-tech/*

Personal data and the GDPR

To the extent that the data in question contain personal data relating to citizens in the EU, the General Data Protection Regulation (*2016/679/EU*) (GDPR) will generally apply. The GDPR goes beyond its predecessor, the Data Protection Directive (*95/46/EC*), by imposing obligations over the confidentiality, integrity and availability of personal data. Some common GDPR issues that arise in the context of data commercialisation are considered below.

Security

The GDPR refers to the need to implement appropriate technical and organisational measures, which are broadly equivalent to controls in an information security context. However, the GDPR does not specify what controls should be in place. To determine what controls are appropriate, an organisation should first conduct an information security risk management process that entails undertaking a risk analysis to identify particular threats and vulnerabilities, and their likelihood of occurrence.

The organisation can then implement appropriate controls to mitigate those risks to an acceptable level, to otherwise manage the risks, for example, by buying cyber insurance, or to avoid the risk altogether. A combination of controls is most effective, including administrative controls (for example, policies and training), technical controls (for example, passwords, biometrics and network firewalls) and physical controls (for example, access cards and security guards), often using a "defence-in-depth" approach in which controls are applied over the data being protected in a series of layers.

Certification standards such as ISO 27001, which is a best-practice information security management system, can assist in achieving the requisite GDPR compliance. However, the GDPR does not specify any appropriate security specifications so it is not possible to guarantee that adherence to any particular security standard alone will satisfy the requirements of the GDPR.

Security controls are also relevant from an intellectual property (IP) perspective: organisations need to protect their own IP and ensure that it is neither misused nor leaked. For example, under the Trade Secrets Directive (*2016/943/EU*), whether the owner has taken reasonable steps to keep information secret is a key part of whether IP can constitute a trade secret (*see feature article "Trade secret protection: guarding against a global threat", www.practicallaw.com/5-637-7032*).

Purposes

It is also important to bear in mind the purposes and uses to which data are put. Under the GDPR, for example, a careful consideration of the lawful bases and specific purposes for processing is essential before collecting and using personal data since it is far more difficult to use data for other purposes at a later point in time. Mapping out data, where they are, what they are used for and what the business wants to use them for is therefore imperative.

In addition, for controllers of personal data, privacy by design must be included as an integral part of processing, especially for anticipated or new uses of data with privacy risks attached (*see feature article "Data protection: privacy by (re)design", www.practicallaw.com/w-018-6087*). In these cases, data protection impact assessments will be essential for evaluating, managing and recording associated privacy risks. Similarly, from an IP licensing perspective, where data are licensed to an organisation, it is essential to stay within the scope of the licensed purposes for those data. In the cases of both personal data and licensing obligations, commercial needs must be balanced against legal obligations.

Retention

There are also restrictions on how long data can be retained. The GDPR has led to a drive for organisations to retain data for only as long as needed and to then delete them, which often presents technical and practical hurdles, given how data proliferate. Conversely, an organisation can be subject to a multitude of EU, national and international legislative requirements that require certain types of data to be retained. Identifying and complying with these, particularly where data are commonly intermingled, can be a significant challenge.

dawn-of-data-marketplace). An article published in Forbes grandly describes data commercialisation as "the next frontier in digital transformation" (*www.forbes.com/sites/forbestechcouncil/2018/05/08/what-should-be-your-data-monetization-strategy-to-compete-in-the-borderless-economy/#20bb49ac4095*).

Beneath the hype, however, it is clear that businesses are currently presented with unprecedented opportunities for creating, collecting, analysing and using data. This is, in large part, due to the maturation of several key technologies such as data virtualisation and cloud computing, and improved analysis through machine learning, and will continue with the rapid development of the internet of things. Much has been written about each of these developments in separate contexts but it is widely accepted that businesses are now operating amid a data revolution.

It is therefore unsurprising that data assets have become a board-level issue for many companies, even for those not traditionally perceived as digital businesses. Every business in today's modern and digital economy is increasingly a data business in some sense. At the same time, uncertainty remains as to how best to harness the value of data proliferation. Research by Ernst & Young in 2015 found that 81% of senior executives agree that data should be at the heart of decision making but only 31% have actually restructured their operations to do this (*www.ey.com/Publication/vwLUAssetsPI/Becoming_an_analytics_driven_organisation_to_create_value/$FILE/ey%20big%20data%20report_low-res.pdf*).

From a legal perspective, organisations have devoted significant resources in recent years to adopting or revisiting strategies to

promote the protection of personal data, largely as a result of the implementation of the General Data Protection Regulation (*2016/679/EU*) (GDPR) in May 2018 or similar legal developments elsewhere (*see box "Personal data and the GDPR"*) (*see feature article, "GDPR one year on: taking stock", this issue and News brief "EU General Data Protection Regulation: on your marks, get set, go!", www.practicallaw.com/w-014-9290*). However, data are about more than just legal or regulatory compliance. In order to design, implement and manage effective data activities, organisations need to consider the wider legal landscape, and rights and responsibilities affecting all data, not only personal data.

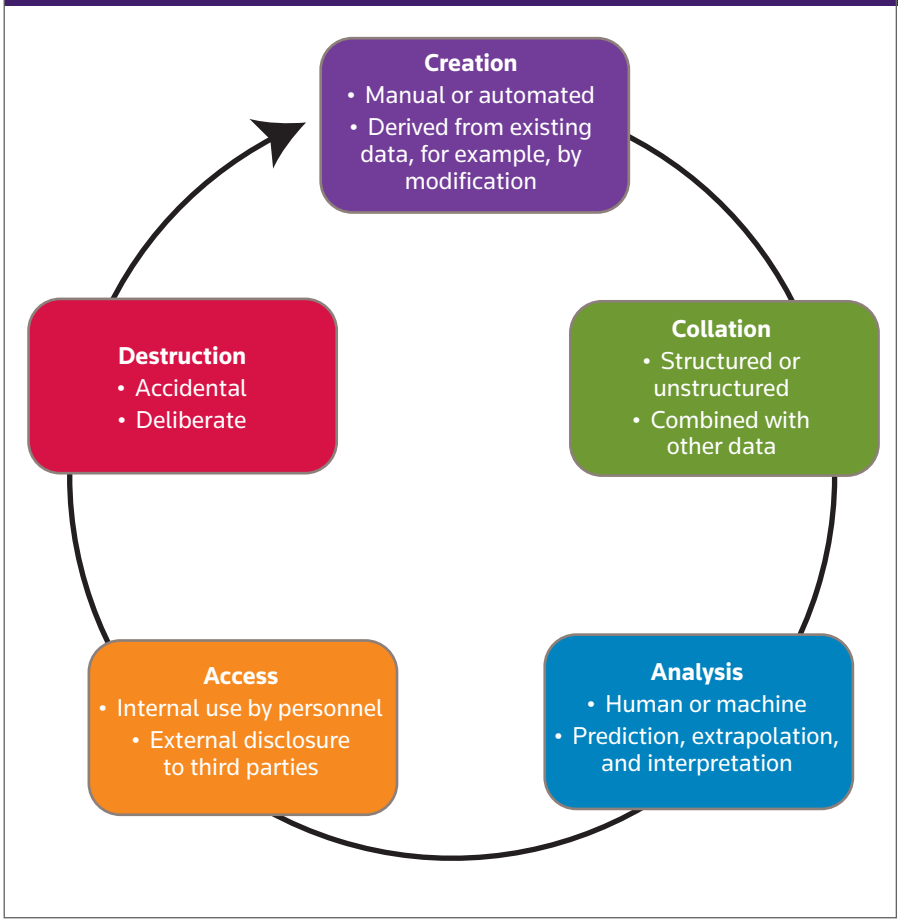
VALUE OF DATA

In general terms, the issue of how businesses can derive value from data depends on the nature of the data in question and what can be done with them. Clearly, many data are inherently valuable and can be recognised as balance sheet items in their own right. The International Accounting Standards recognise that value can be held in an identifiable non-monetary asset without physical substance. These assets can be difficult to value, however, as their potential benefits and useful life can be uncertain. For this reason, most balance sheet data assets, such as structured databases, trade secrets and proprietary know-how, typically have a longer lifespan than more transient forms of data.

Other data, such as unstructured sets of big data, are less obviously valuable (*see feature article "Big data: protecting rights and extracting value", www.practicallaw.com/1-595-7246*). Many raw data are worthless until they are reviewed or analysed to derive insights or to guide commercial decisions, or until they can be tested against planned use cases. In order to derive commercial benefits from these data, it is usually necessary to collate them and subject them to software processing in order to extract actionable intelligence or gain any efficacy which is itself valuable.

Regardless of whether data are structured or unstructured, value can typically be derived at each stage in the common lifecycle of data (*see box "The data lifecycle"*). This is especially true at the stages of collation and analysis, including data mining, modelling and interpretation, which offer perhaps the greatest opportunities for organisations to enhance and extract the value of data.

The data lifecycle



Once valuable data have been identified, organisations need to assess whether their value is of an internal or external nature. Internal value can be derived by using data to inform strategic commercial, operational or technical decisions to enhance profitability. External value can be realised by using data as a commercial asset, for example by licensing or selling them to third parties or contributing them in return for other value.

DATA OWNERSHIP

The maxim that there is no such thing as data ownership is, in the most general sense, true from an intellectual property (IP) point of view at least. The moral philosophy behind IP rights (IPR) is to create monopolies as a reward and incentive for creative effort or adding to the body of human knowledge. IPR provide protection against unfair advantage being taken of another's efforts or, in return for the revelation of the secret of an invention, are given so that the next step can begin to be taken by others to the overall benefit of the community at large.

If data are pieces of information, pure and simple, there is no moral or political incentive to allow restrictions on their access or use. The other IP maxim that an idea cannot be protected, only the expression of that idea, exemplifies this concept. There is an argument that information, once released into the public sphere, is, and should be, available for all. However, given the value of data across every aspect of business and personal life, these traditional notions are increasingly being challenged. IPR such as copyright in the data themselves, copyright in database structures, sui generis database rights (in countries that afford these protections), trade secrets, confidential information, and occasionally trade marks, are usually cited to support restrictions on access to and use of data but none provide a satisfactory basis for ownership of data.

When rights in data are discussed, it is crucial to step back and look at what the actual data represent. No-one would question that a photograph, a movie or a song should

not attract copyright protection, so there is no reason why the position would be any different in respect of digital data forms comprised of bits and bytes.

However, the legal position can become less clear when dealing with data that have been derived from, or generated by, other existing data. For example, if an analysis of confidential data produces aggregated statistics, a key issue is whether those statistics are confidential. If a licensee modifies data to which it has a licence, the question arises as to whether the modified data fall outside the scope of the original licence. Typically, creators of original data will want to exert legal rights over all permutations of those data throughout their lifecycle.

The question therefore arises as to the circumstances in which IPR or contractual rights can subsist in the data and this will typically depend on the nature of the data (*see box "Data and IP rights in practice"*).

RIGHTS IN DATA

Some of the key ways to protect rights in data include asserting database rights or copyright, claiming trade secrets law protection or seeking contractual protection.

Database rights

The very concept of sui generis database rights, first introduced in the EU in 1996 in the Database Directive (*96/9/EC*), was to encourage the presentation and availability of information in an accessible fashion, conceived at a time before search engines and the internet allowed this to happen far more easily (*for background, see feature article "Database right: a narrower scope of protection", www.practicallaw.com/6-201-2791*). Sui generis database rights arise in reward for the substantial investment of the maker of the database in the obtaining, verification and presentation of information. These rights were created to protect that investment and provide enforceable rights against those who, without the owner's permission, extract or reuse all or a substantial part of the contents of these databases.

However, they do not provide a right of ownership over individual items of data, as the British Horseracing Board (BHB) discovered in the European Court of Justice's (ECJ) decision in *The British Horseracing Board and others v William Hill*, when it failed to protect the content of its databases of runners and riders from use by bookies (*C-203/02*). The fact that BHB had created the data itself meant that it had not obtained and verified it and so could not rely on sui generis database rights (*see News brief "Rights in databases: success at last", www.practicallaw.com/7-520-0284*).

However, subsequently, the Court of Appeal held that the resources applied by Football Dataco resulting in a database of football match results, including details of who scored and when, and other details about each match, were invested in collecting, not creating, the data, and that the databases therefore attracted sui generis database rights (*Football Dataco Ltd and others v Stan James Plc and others [2013] EWCA Civ 27, www.practicallaw.com/3-524-3742*). This decision gives database compilers greater scope to claim database rights although this is still a difficult area in which to provide certainty.

Copyright

Copyright status can be applied in relation to the collection of data in a database or other site. For example, where the items of data being considered are copyright works, such as literary or artistic works, or the data

Data and IP rights in practice

The application of intellectual property rights to data will depend on a number of considerations and is primarily driven by the type of data in question. This is illustrated in the examples given below.

Statistics

While statistics themselves are not likely to be protected by copyright, when they are presented by way of a table, graph or chart, then copyright or database right is likely to subsist in that presentation (*see "Database rights" in the main text*). If data are released in these forms, third-party copying of the particular expression of the data; that is, in their formatted form in a table, might be prevented using copyright. However, extraction of the data from the presentation might be more difficult to prevent, unless it could be framed as an extraction from a sui generis database right-protected database.

User-generated data

Several media companies, including Disney, Fox, Myspace, Sony, Viacom and CBS, have come together to produce principles for user-generated content (UGC) services (*https://ugcprinciples.com*). The principles deal with the use to which the copyright content that is owned by these entities can be put when it is incorporated into UGC within social media venues such as Myspace. This is in classic copyright territory; ultimately, the UGC here is partial or substantial reproductions of conventional copyright works such as video or music, and can be protected as such even though it is in digital form.

However, there is also an issue about the ownership and use of original content generated independently by users and, similarly, data produced from devices. This may be the copyright of the user that created it if it is creative enough to qualify for copyright but, even as such, it may be licensed to the site owner or product manufacturer through terms of use or purchase. In most cases, the simple data produced by the user, much of which the user will be unaware of, will not have copyright protection.

The increasing use of the internet of things to generate data on the functionality of products or the location of the user also produces an enormous amount of data which could be accessed and stored by the product provider and is not necessarily personal data. Nevertheless, individuals may feel that when data are accumulated and analysed, and this leads to personal targeted advertising, including advertising based on location, this is quite a personal use of their data and one over which they might reasonably be allowed to have some control or visibility.

Competition law issues

The increasing accumulation of data by organisations presents various competition law challenges, not least because traditional competition analysis tools often, though by no means exclusively, focus on price. As a result, these established analytical methods are harder to apply if the value of the product is intangible and difficult to locate. Rather, the value of data as an asset can depend on a variety of factors including: the owner's processing ability; the development of analytical algorithms and machine learning; the availability of services founded on the data; and the degree to which the data can be replicated.

Access to data. One type of abuse of dominance where increased regulatory intervention is possible is where access to a particular data set is essential to enable competition in a downstream or adjacent market. In certain circumstances, big data sets may be difficult to replicate and could act to reinforce barriers to entry. Under traditional competition law analysis, the threshold for forcing access to an "essential facility" is high.

However, there is starting to be increased oversight of these kinds of data accumulation. The European Commission (the Commission) is due to publish a recommendation on access to connected vehicle data, while other regulators have already issued warnings in relation to group company data sharing arrangements, for example, the Belgian Competition Authority's decision against the National Lottery, *Stanleybet ea v National Lottery* (*www.belgiancompetition.be/sites/default/files/content/download/files/20150923_press_release_15_abc.pdf*). Tech companies, in particular, should be conscious of possible regulator involvement in this vein and the possible effect on the value of previously unshared data.

Data sharing. Even sharing data sets may not be without risk. Exclusive licensing arrangements and other data sharing agreements may raise competition concerns where they foreclose competitors who are not permitted similar access. Alternatively, dominance may arise where a company has specific systems capable of extracting additional value from the data, even if the data set is shared.

To give one international example of how regulators are dealing with this issue, the Australian Competition and Consumer Commission will soon start overseeing a consumer data right scheme. The scheme is designed to give consumers greater ability to obtain their customer data and facilitate their transfer to other companies, allowing for more competitive pricing and product offerings. The scheme is being rolled out progressively by industry, starting with banking, then moving onto energy and likely telecommunications.

Consumer choice. The increasing availability and commercialisation of data may further lead to data-related anti-competitive behaviour where parties discriminate on the basis of data analysis. Of particular interest here are voice-commanded digital assistants, which could act as gatekeepers for consumers accessing digital content. Some responses to a recent Commission consultation flagged concerns that these platforms harvest consumer data and produce single answers to consumer queries, rather than a series of alternatives, and that this presents an opportunity for exclusive deals favouring the tech company's own products and services without the context of other available options (*http://ec.europa.eu/competition/information/digitisation_2018/media_en.html*).

Merger control. Data, whether in the context of large or essential data sets, or data processing systems, is also a hot topic in merger control. The increasingly close link between a company's market power, its data collection processes, and the characteristics of those data is likely to lead to high levels of scrutiny from competition regulators in the future. Where a merger relies on the value of substantive data sets to be acquired, competition controls will not be the only issue to bear in mind (*see "Corporate transactions" in the main text*).

Privacy. In addition, an overlap between competition and data privacy regulation is starting to develop. Historically, competition regulators have viewed data protection as the exclusive jurisdiction of the privacy regulators. However, the recent decision (*B6-22/16*) of the German competition regulator with respect to Facebook has highlighted the potential increased overlap between competition and privacy regulation (*www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf*).

are in a particular format, there may be copyright protection.

The UK's traditional approach to copyright is that copyright in the data themselves will arise where there has been skill and effort involved in the creation of the items of data. The approach taken by the ECJ in relation to copyright provisions in EU directives such as the Information Society Directive (*2001/29/EC*) is to recognise copyright where the data are the author's own intellectual creation (*Painer v Standard VerlagsGmbH and others C145/10*). This is arguably a higher standard than the UK common law, where the criteria for copyright to exist is for the author to have made free and creative choices when creating the work.

There could also be grounds under copyright law to protect against the copying of the structure of the database which might be protected by copyright. The Database Directive provides for copyright to be recognised in databases. This was implemented in the UK in the Copyright and Rights in Databases Regulations 1997 (*SI 1997/3032*) under which a database will be capable of protection by copyright only if, by reason of the selection or arrangement of its contents, it is the author's own intellectual creation.

In the *Football Dataco* cases that dealt with copyright in databases, which preceded those on database rights, the ECJ confirmed that copyright in a database is determined by the selection and arrangement of the data in it, not the creation of the data themselves, which might or might not attract

copyright (*Football Dataco v Brittens Pools [2010] EWHC 841 (Ch), www.practicallaw.com/4-502-3495; Football Dataco v Yahoo [2010] EWCA Civ 1380; Football Dataco v Yahoo [2012] EWCA Civ 1696; and Football Dataco v Yahoo C-604/10*; *see News brief "Football Dataco: implications for copyright subsistence", www.practicallaw.com/7-518-6424*). These cases involved football fixture lists that were ultimately held by the Court of Appeal not to attract copyright despites the complexities of the process by which they were put together. The effect is that there needs to be original input from the creator of the database to attract copyright; simply following a set of rules is not enough.

Trade secrets

Trade secrets law, especially in its recently harmonised form across the EU in the Trade Secrets Directive (*2016/943/EU*), or the law of confidential information, is one way to protect specific items of data (*see Briefing "Trade Secrets Directive: the need for harmonisation", www.practicallaw.com/5-633-8644 and Opinion "Trade Secrets Directive in practice: business as usual?", www.practicallaw.com/w-014-5083*). However, this form of protection is not available for published data. Once made public with the permission of the data controller or creator, individual data would not be confidential nor attract trade secret protection. If made public without consent, while there could be recourse to breach of confidence or infringing use of trade secrets, the information could no longer be protected against third-party use.

Clear restrictions are a key part of creating the environment in which trade secrets may be recognised. The Trade Secrets Directive's new harmonised regime, as implemented in the UK under the Trade Secrets (Enforcement etc) Regulations 2018 (*SI 2018/597*), depends much more on the steps taken to keep information secret, rather than the notion that the information itself is of its very nature confidential, as was the case under the old common law on confidential information (*www.practicallaw.com/w-015-3958*).

IP limitations

As a legal toolkit, IPR can certainly offer a helpful means of protecting valuable data (*see box "Data and IP rights in practice"*). However, due to the challenges of asserting ownership and the subsistence of IPR in many types of data, contractual protection often provides the best source of protection and the most efficient to clarify between parties who owns, or has rights over, what data and which data may be used for what purpose. Data owners therefore most often seek to rely on a contractual right when protecting their data assets or attempting to restrict their use.

Contractual rights

Perhaps the most reliable way to articulate and enforce rights in and over data is therefore by contract law. From non-disclosure agreements and data licences, to collaboration arrangements and user terms and conditions, contracts can play a powerful role in extracting, exploiting and protecting value in data (*see feature article, "Drafting confidentiality agreements: the DNA of an NDA", www.practicallaw.com/9-536-5387*). It is also important to remember that obtaining consent from individuals can give rise to a contractual relationship. Key issues and best practice considerations relating to commercial data contracts are beyond the scope of this article, but should form a central part of any organisation's data commercialisation strategy.

For example, in relation to contractual rights over data which are likely to evolve over time, there is often a tension between the data creators, disclosers or licensors, which will not want to lose control over their original work, and data users, recipients or licensees, which will want flexibility to use the outputs of data processing, modification or analysis without restriction. This tension will generally be resolved by commercial negotiation, although parties will sometimes seek to agree co-ownership models, which can be challenging to enforce and administer in practice.

Due diligence questionnaires

Due diligence questionnaires will invariably become more detailed and focused in the context of data commercialisation. Buyers should, as a minimum, consider:

- What data have been collected.
- When and how the data were collected.
- Whether the data include personal data. If so, further checks should be carried out for data protection compliance.
- Whether any other jurisdictional or industry sector data laws are relevant. If so, further compliance checks should be carried out.
- Whether any third parties have rights in the data.
- What intellectual property rights subsist in the data, who owns them and whether they can be transferred.
- Whether there are limitations, such as contractual rights or consent restrictions on reliance, modification or disclosure, which would affect the buyer's intended ongoing use of the data.
- If relying on software tools to analyse or derive value from data, who owns the right in these software tools.

DATA GOVERNANCE

The legal considerations of data commercialisation are not straightforward. As organisations set out to establish or refine a data commercialisation model, it is the role of their legal advisers to ensure that a multitude of regulatory and contractual angles and risks are adequately covered. As a starting point, it is helpful for data lawyers to consider the three preliminary key issues discussed below.

Lawfulness

Despite the potential value of data and the way in which technology has enhanced, and often simplified, the capability of exploiting them for varying commercial

purposes, organisations need to be aware of the compliance burdens around the use and exploitation of data, some of which are onerous.

Data privacy considerations are often first on the list from a regulatory perspective. To the extent that the applicable data sets contain identifiable personal information, including anonymised data where there is a risk of re-identification, data privacy laws will bite. In the EU (and beyond), this will trigger the application of the GDPR or equivalent laws (*see box "Personal data and the GDPR"*). Similar privacy laws have started to proliferate throughout the world, each with slightly different requirements, so organisations will need to navigate these laws carefully.

Aside from privacy, organisations will also need to assess the legality of their proposed data commercialisation activities under all local jurisdictional or sector-specific laws which may be relevant.

For example, organisations should be aware of the increasing risk of competition law ramifications relating to data commercialisation activities (*see box "Competition law issues"*). Increasing numbers of jurisdictions, including China, Indonesia, Russia and Vietnam, have also enacted data localisation requirements. If data are considered critical from a state or national security perspective, or if platforms containing data are considered to be important state infrastructure, there may be requirements that these data must be stored within the home jurisdiction and cannot be stored or transferred overseas. Specific data laws vary both across different jurisdictions and industry sectors.

As data processing techniques become more sophisticated in an online and connected world, organisations should also pay attention to potential cyber crimes which could taint data or render their sale illegal under proceeds of crime laws. In the UK, for example, the Computer Misuse Act 1990 has a far wider scope than many organisations realise, and can potentially render many data activities unlawful.

Protection

As explained above, IPR may afford some protection to an organisation's data assets, but often do not afford the protection for data, particularly unstructured data, that organisations may be seeking. For data which are to be disclosed to third parties, contractual protections are generally more reliable (*see "Rights in data" above*). For data that is intended to stay within an organisation's walls, robust data hygiene, and confidentiality policies and procedures will be essential.

Other legal consequences

The fast-moving world of data can lead to unpredictable and sometimes unintended consequences. Innovative uses of data may not always be perceived as ethical, and can attract significant adverse publicity and class actions.

Organisations should also consider how data commercialisation activities might affect shareholder activism risks and, more generally, future transactions (*see feature article "Shareholder activism: coping with the rising tide", www.practicallaw.com/6-550-4785 and "Corporate transactions" below*).

With proactive planning and robust ongoing data governance, organisations can establish clearly-mapped data flows and processing methods that are capable of supporting highly profitable use cases. However, given that data are so pervasive, the commercialisation of data currently requires consideration of a patchwork of applicable data-related and associated laws and regulations; this is increasingly evident in corporate transactions.

CORPORATE TRANSACTIONS

In any mergers and acquisitions (M&A) deal, the seller should have certainty as

Related information

This article is at practicallaw.com/w-019-8276

Other links from uk.practicallaw.com/

Topics

Confidentiality	topic/7-103-1304
Copyright	topic/0-103-1270
Databases	topic/6-103-1272
Data protection: general	topic/1-616-6550
Information technology	topic/5-103-2074
Technology: data protection	topic/8-616-6207
Transactions: data protection	topic/5-616-6195

Practice notes

Data Protection Act 2018: overview	w-014-5998
Data protection in corporate transactions (GDPR and DPA 2018) (UK)	w-014-9200
Legal aspects of managing big data	1-581-1225
Overview of copyright	9-107-3741
Overview of EU General Data Protection Regulation	w-007-9580
Overview of rights in databases	4-107-4762
Protecting confidential information: overview	8-384-4456

Previous articles

Data protection in M&A: under lock and key (2018)	w-017-6243
Data use: protecting a critical resource (2018)	w-012-5424
Trade secret protection: guarding against a global threat (2017)	5-637-7032
Trade secret protection: the regimes in key jurisdictions (2017)	0-639-0286
General Data Protection Regulation: a game-changer (2016)	2-632-5285
Big data: protecting rights and extracting value (2015)	1-595-7246
The law of confidence: where are we now? (2014)	2-556-5238
Drafting confidentiality agreements: the DNA of an NDA (2013)	9-536-5387
Database right: a narrower scope of protection (2005)	6-201-2791

For subscription enquiries to Practical Law web materials please call +44 0345 600 9355

to the assets being sold and its right to sell them. In turn, the buyer needs to be certain of title to the purchased assets and its ability to use them for the intended purposes. Where a deal turns on the value of the underlying data or the potential value of commercialisation of those data, the parties must undertake considered valuations, thorough due diligence and identification of IPR, and must agree an appropriate assessment and allocation of risk to ensure that this value can be realised.

Seller issues

Before a sale, the seller should carry out a data-mapping and audit exercise, often involving data scientists, to confirm what data it has the right to access or receive, the characteristics of those data and the associated obligations and restrictions on their use and disclosure. Care needs to be taken in assessing data, or creating common "data lakes" (that is, consolidated repositories of raw data) before closing, including due to potential competition concerns.

Importantly, the seller should investigate whether it has the ability to sell its interest in the data, noting any encumbrances or other restrictions, and whether it needs to retain rights over those data in the future. If personal data is within the scope of the transaction, the seller will need to consider whether it has complied with applicable data protection legislation throughout its time as data controller, particularly at the point of collection and in relation to the existing and planned uses of those data (*see feature article "Data protection in M&A: under lock and key", www.practicallaw.com/w-017-6243*).

Buyer issues

For the buyer, the immediate issues are: how to conduct effective due diligence on a company whose core assets are intangible and often undefined; and how to value data. It is unlikely that the buyer will be granted unfettered access to data until after the sale, so the buyer is dealing with a degree of uncertainty. Some indication can be given by evaluating the relevant market, considering the availability of the types of data in question and understanding how fundamental the data is to the business being bought. A valuable data set is likely to have unique characteristics. Careful and thorough questioning will be critical to assessing whether the buyer will be able to realise the value in the relevant data, including being able to use the data as intended after closing (*see box "Due diligence questionnaires"*).

Issues for both parties

Both the seller and the buyer in an M&A deal will need to consider carefully the representations, warranties and indemnities that they are prepared to give with respect to the acquisition of data, as well as related conditions precedent and post-acquisition planning. The seller will wish to avoid risk relating to the buyer's future use of the data. On the other hand, the buyer will want protections to ensure that it is not buying a worthless asset and that the data are both useful and usable. Throughout the process, lawyers need to deliver a practical assessment of the risks, in order to protect the parties and ensure legal and regulatory compliance.

Similarly, when entering into joint ventures and collaboration agreements, the parties need to be clear as to the allocation of rights and responsibilities over data contributed, used, generated and shared in the course of the planned activities, for example by establishing data protocols.

Edward du Boulay is a senior associate, Miriam Everett is head of Data Protection and Privacy, Kyriakos Fountoukakos and Andrew Moir are partners, and Rachel Montagnon is a professional support consultant, at Herbert Smith Freehills LLP. *The authors would like to thank their colleagues Hannah Brown, Peggy Chow, David Coulling, Mark Robinson, Peter Rowland, Joel Smith, Manish Soni and Kaman Tsoi for their contributions.*