OPEN INNOVATION
IP, DATA AND COMPETITION ISSUES

In the second part of a two-part series on open innovation, Joel Smith, Miriam Everett, Laura Deacon, Rachel Montagnon, Jessica Welborn and Anna McGowan of Herbert Smith Freehills LLP look deeper into some specific issues that arise in the context of collaborative innovation.

This article, the second in a two-part series on open innovation, sets out some practical steps to consider when embarking on open innovation projects and examines some particular legal issues that arise in the context of collaborative innovation, including:

- Intellectual property (IP).
- Data considerations.
- Competition issues.
- Employee-inventor compensation (see box “Employee-inventor compensation”).

The first article explored the world of open collaboration, looking at patterns and trends, and models of innovation that are collaborative, both internally within organisations and externally between organisations (see feature article “Open innovation: forging innovation and collaboration”, www.practicallaw.com/w-022-2804). “Open innovation” is a term that has come to describe innovation which extends beyond the traditional research and development department of a business, and embraces a broader pool of talent and ideas within the whole business and frequently also extends to an external partnership with a third-party collaborator to assist with, and accelerate, the process.

In any collaboration, the parties will need to consider the legal issues that may arise: how the collaboration affects existing legal rights and arrangements; how the rights and obligations of the parties created under the collaboration are to be dealt with; the arrangements for exploitation of the results of the collaboration; and how the parties will operate following any termination of the collaboration.

GETTING THE IP RIGHT

The IP issues to be considered will depend on what stage a collaboration is at.

Before the collaboration

Parties should consider the issues below before entering into an open innovation venture.

Confidentiality agreements. Before any organisation decides to enter into an open innovation venture, it will undertake exploratory discussions with potential collaborators. Given the preliminary nature of these discussions, it is unlikely that there will be any appetite to involve lawyers. However, even at the initial stages, it is wise
Employee-inventor compensation

Employers will own their employees’ inventions where the employee was employed to invent and where the invention in question is one that would be reasonably expected to result from the employee carrying out their duties, or if the employee has a special duty to the company, such as company directors (section 39, Patents Act 1977) (section 39). In all other circumstances, the invention will belong to the employee. Employees may seek compensation for their loss of ownership (section 40, 1977 Act) (section 40). Employers cannot contractually exclude or diminish a claim unless a relevant collective agreement is in place. Section 40 also permits a claim by an employee who has assigned or licensed a patented invention that they own to their employer for an inadequate amount.

An employee whose employer has the right to their invention under section 39 will be entitled to compensation if they can show that an invention of theirs that has been patented is of outstanding benefit to their employer’s undertaking and it is just to grant compensation. If the patent was applied for before 1 January 2005, the relevant question is whether the patent, not the invention, was of outstanding benefit. In assessing “outstanding benefit”, regard must be had to, among other things, the size and nature of the relevant employer’s undertaking. The compensation awarded to the employee will be a “fair share” of the benefit derived from the employer from that patented invention. Unfortunately, there is limited guidance on the meaning and requirements of section 40, as there has been only a small number of cases in the 30 years since this provision was enacted. However, in October 2019, the Supreme Court considered this provision in Shank v Unilever plc and others, which was the first time that the statutory regime had been considered substantively by either the Court of Appeal or the Supreme Court ([2019] UKSC 45). The court held that:

- The employer’s undertaking is determined by analysing the commercial reality of the situation in each case from the perspective of the inventor’s employer. The court said that where, as in Shank v Unilever plc and others, the court is required to consider the extent of the benefit of Professor Shank’s patent to the Unilever group and how that compares with the benefits derived by the group from other patents for inventions arising from the research carried out by that company.

- Outstanding benefit is assessed net of costs but not net of tax. The word “outstanding” is to have its ordinary English meaning and there is no single answer as to how the size and nature of the employer’s undertaking affects the determination of whether the patented invention is of outstanding benefit to the employer’s undertaking. In Shank v Unilever plc and others, the court said that a highly material consideration was the extent of the benefit of Professor Shank’s patent to the Unilever group and how that compares with the benefits derived from other patents resulting from the work carried out at Professor Shank’s employer.

- When determining what is a fair share of the benefit, regard must be had to all the circumstances with various mandatory factors specified in section 41 of the 1977 Act. The factors relevant to an invention that always belonged to the employer include: the nature of the employee’s duties; their remuneration; the effort and skill that they have devoted to making the invention; the contribution of any other person who has made the invention jointly with the employee concerned; the contribution of any other employee who is not a joint inventor of the invention; and the contribution made by the employer to the making, developing and working of the invention by the provision of advice, facilities and other assistance (section 41(4), 1977 Act).

Jonathan Turnbull is a partner, and Natasha Daniell is an associate, at Herbert Smith Freehills LLP.

to consider the implications of revealing to a third party key confidential information, such as potential avenues of investigation or the amount of work already undertaken.

While there are common law protections against misuse of certain kinds of confidential information, it is advisable to have contractual protections in the form of a confidentiality agreement or non-disclosure agreement (NDA) (see feature articles “Drafting confidentiality agreements: the DNA of an NDA”, www.practicallaw.com/9-536-5387 and “Non-disclosure agreements: key issues in international deals www.practicallaw.com/1-524-1008”).

This agreement does not need to be long or over-complicated but it should impose obligations, which are usually mutual, on the parties to maintain the confidentiality of any information and documents disclosed during preliminary discussions, and not to disclose the fact of the discussions themselves. The agreement should also provide for the return of any documents on the conclusion of discussions, if there is not going to be any collaboration.

Memorandum of understanding. If the parties agree that there is potential for an innovation project, even though substantive negotiations, further due diligence and the drafting of definitive agreements are still to take place, they may try to capture in writing the overall intention and spirit of the proposed arrangement, and some of its key terms in a memorandum of understanding (MoU) or heads of terms.

An MoU shows that the parties have serious intent and may have moral force but, in England, an MoU on its own does not legally compel the parties to conclude the deal on those terms or even at all. There is no standard content or format for an MoU. The aims of an MoU are to focus the parties’ intentions to avoid future misunderstandings and to provide a cornerstone for the steps to be taken on the way to signing a formal binding agreement.

However, the preparation of an MoU can occasionally stall the process over points of unnecessary detail which can increase the length and cost of the negotiations, and delay preparation of the definitive documents. If the parties are committed to the project, an immediate move to drafting the project agreements may be preferable.
An express term should be included that there is no intention to create legal relations or to be bound by the MoU as in some jurisdictions, a MoU can create a legally binding agreement.

Exclusivity. The parties may also consider entering into some form of exclusivity agreement pending the finalisation of the relevant agreements, so that neither party will enter into similar negotiations with a third party during the exclusivity period. This will protect the time and money spent in ultimately reaching agreement.

Contractual documents. There will never be a one-size-fits-all solution for the legal documents required to govern the relationship between the parties to an open innovation project. A staged approach is often a good idea, where the parties set realistic milestones at which they will take stock and, if the relevant target or objective is not met, agree a mechanism to deal with an appropriate way forward, such as extending the relevant deadline, exploring a different avenue or bringing the collaboration to an end.

At the outset
IP will be at the heart of any innovation project. At the start of any collaboration, the parties will need to:

- Identify the IP that each party to the collaboration will contribute, which is often known as background IP. This is important so that the parties know what they will be entitled to at the conclusion of the collaboration, whether or not it has been successful.

- Determine whether any third-party consent is required for the transfer or licensing of the IP for the purposes of the innovation project. For example, a contributing party could be a licensee that needs the consent of the IP owner to sub-license the IP for the purposes of the collaboration.

- If the parties are creating a joint venture (JV) company for the collaboration, decide whether the IP rights (IPR) to be provided by each party are to be transferred to the JV company so that the JV company owns the relevant IP or whether the parties will retain their own IP and license the JV the right to use and develop the IP.

If IP is to be transferred to a JV company, the transferor will need to bear in mind that it may lose control over the IP, which may be a concern if there is a risk that the collaboration will fail, and it may also require a licence back to be able to continue to use the IP.

If IP is to be licensed to the JV company, the negotiation of licence terms can be complex and protracted. The parties should bear in mind that the JV company will have only a contractual right to use IP, rather than a proprietary interest. In addition, on termination, the JV company could lose valuable rights which it has created as part of the innovation project, based on the IP licensed to it.

The parties will need to specify the terms on which IP is to be licensed to either of the other parties in the collaboration or to the vehicle which has been created to undertake the innovation work. Matters to be dealt with include, for example, whether there will be a payment to the licensor for the use of the IP and whether there are jurisdictional limitations. The scope of the licence should be clearly defined, especially if the IP being licensed has already been licensed to third parties for different applications.

During the collaboration
The parties will need to agree which of them will own any IP created as a result of the collaboration, which is often known as foreground IP.

A common position to adopt is that each of the parties to the innovation project owns any IP, for example, inventions, designs and software, that it creates itself. This seems a relatively straightforward approach. Difficulties can arise where, due to the collaborative nature of the project, IP is jointly created or it is not possible to identify which party created which aspect of the new work. In this situation, joint ownership of IP might initially appear to offer a solution. However, rather than giving each party an un fettered right to use, develop and exploit the jointly created IP, joint ownership can be cumbersome and often restricts the activities of a co-owner.
DATA ISSUES

Businesses in every sector are under pressure to innovate to stay ahead of the competition. Collaborative innovations or innovative collaborations present opportunities to reduce costs, share risk, provide broader access to talent and ideas, and ultimately achieve greater monetary gain.

Data frequently play a central role in this drive towards open innovation as data have a significant value attached to them (see feature articles “Data assets: protecting and driving value in a digital age”, www.practicallaw.com/w-019-8276 and “Data use: protecting a critical resource”, www.practicallaw.com/w-012-5424). Data can be used to: generate new products, services and revenue streams; identify efficiencies within an organisation and reduce costs; and inform strategic decision-making.

Unlocking the value of data

Encouraging open innovation using data often requires a flow of information and IPR in and out of an organisation. The traditional rules of engagement in this context may not always apply. Engaging with external partners and sharing data assets can make a business vulnerable, its boundaries more permeable and ownership rights less certain, as well as giving rise to regulatory considerations.

Organisations therefore need to safeguard their data while ensuring their future value in the context of more collaborative innovation. This involves thinking through all the legal considerations and practical steps that will allow the organisation to adapt and have the flexibility of process to become enablers of innovation and help it to stay ahead of the curve.

To maximise the value of data so that they can be sold or licensed to third parties immediately or in the future, organisations need to prepare, collate and safeguard their data effectively from the start, as well as ensuring compliance with the data protection laws and safeguarding data as far as is possible against outside threats like cyber threats, data fraud, data security breaches and shareholder activism (see box “Shareholder activism”). When sharing data assets, it is also important to avoid potential pitfalls in competition law, ethics and criminal law (see “Competition law” below and boxes “Ethical considerations” and “Criminal liability”).

Ethical considerations

It is important for an organisation to think through any ethical issues that may be raised by what it is planning to do with data. Innovative uses of data that are not perceived to be ethical can attract adverse publicity and put an organisation at risk (see “Artificial intelligence” in the main text). The House of Lords Select Committee Report on regulating the digital environment which was published in May 2019 set out recommendations for ethical technology and urged ethical issues to be considered at the design stage of new digital services (https://publications.parliament.uk/pa/ld201719/ldselect/fdcomuni/295/295.pdf).

Anticipating the value in data

Before any open innovation or collaboration can occur, it is vital that an organisation: knows what data it has or can access; assesses the type, the quantity and the quality of the data; and ensures that all data sets are properly organised in a structured way and are kept up to date where necessary. This can be achieved through a regular auditing process, although it can often also be a challenge for organisations that run multiple legacy IT systems.

Although there is some scope for copyright protection, individual items of information or data do not generally attract IPR but it is possible that compilations of data can attract IPR which can be valued and sold or licensed.

Copyright and sui generis database rights can exist in collections of data but it is the structure of the compilation and the database as a whole that is protected, not each individual item of data, unless those individual data possess the required level of creative endeavour to be copyright works (see “Protecting II-R in data” below). For this reason, using an organisation’s data to compile a database may give increased protection for the data as a whole, although not individually. Such general database rights are aimed at preventing a competitor from stealing the content of a database, while database copyright, is aimed at protecting the particularly original structure of a database.

A database is defined as “a collection of independent works, data or other materials which are arranged in a systematic or methodical way and are individually accessible by electronic or other means” (section 3A(I), Copyright, Designs and Patents Act 1988) (CDPA) (section 3A(I)).

Databases can include customer management systems, document management systems, knowledge management systems, intranets, back-office inventory systems, purchase order systems and websites, among others. There is no requirement for a compilation of data to be in electronic form but, in the modern digital economy, digitising data assets is essential to maximising their value.

Complex data sets can be derived from virtually every kind of digital interaction, such as internet transactions, email, mobile payments, click streams, as well as internet of things devices. The possibilities are endless. These data sets can be amalgamated and organised into large data sets that can be analysed to reveal useful information about users’ preferences, to learn more about a particular market, find trends in a market or to make predictions about future behaviour.

Another way to keep control of data is to treat them as confidential information or trade secrets (see feature article “Trade secret protection: guarding against a global threat”, www.practicallaw.com/5-637-7032). This requires access to be limited to those within a confidentiality arrangement or who are impliedly required to keep the information confidential. This form of protection has its limitations since, once the confidentiality arrangements are breached, it is very difficult to recapture the data and re impose confidentiality, although injunctions can be used to prevent further dissemination.

Protecting IPR in data

Enforcement of rights in data is difficult. Not only are these rights difficult to establish but where data have been amalga mated. Such as in collaborative situations, it may be difficult to establish which data comes from which party and the chain of ownership. The answer often is to use contract law for the enforcement of rights in data or to define data structures so that they explicitly indicate origin.
Criminal liability

It is important in any data innovation or collaboration to avoid unwittingly committing a cybercrime under the criminal law (see feature article “Cyber risk and directors’ liabilities: an international perspective”, www.practicallaw.com/2-635-5748). The Computer Misuse Act 1990 has a wider scope than many organisations are aware of. A potential data-harvesting activity may be unlawful so checks need to be made to avoid criminal liability and the resulting damage to reputation. An example of this might be scraping information or data from third-party websites to populate a database using automated bots.

The use of a contractual licence for collaborations allows for all terms of the sharing of data to be addressed. For example, if an organisation holds valuable copyright material, it can specify that using, copying or doing anything else with it, except as set out in the contract, will be a fundamental breach of contract which entitles it to a claim. The terms of this liability can be negotiated; an organisation may wish to stipulate unlimited liability for breach of the IP clause or another limit of liability may be agreed.

The Database Directive (96/9/EC), implemented in the UK by the Copyright and Rights in Database Regulations 1997 (SI 1997/3032) (1997 Regulations), created IPR in the contents of a database (see “Anticipating the value in data” above). The contents are protected under a sui generis database right where there has been a substantial investment in the obtaining, verifying and presentation of data, and can be enforced against those extracting data from the database in large chunks or repeated small amounts.

It is also possible for the structure of the database to attract copyright protection (see “Anticipating the value in data” above). A compilation will attract copyright as a literary work consisting of a database only if “by reason of the selection or arrangement of the contents of the database the database constitutes the author’s own intellectual creation” (section 3A(1), CDPA). This requires the author of the database to have made free and creative choices, not formulaic ones.

It raises problems for databases compiled or structured without any innate creativity and calls into question whether databases created using artificial intelligence (AI) or machine learning could qualify (see feature article “Artificial intelligence: navigating the IP challenges”, www.practicallaw.com/w-015-2044). UK copyright law provides a solution to this problem: where a computer has generated something, then the person who made the arrangement for the computer to do this is the owner of the copyright in the created work (section 9(3), CDPA). This principle has not been tested in relation to sui generis database rights.

Compilations of data that do not fall within the definition of a database under section 3A(1), such as a table or graph, may be protected by copyright as literary works. The standard of originality required for copyright to apply is relatively low but it does need to involve some demonstrable skill and labour.

Generally, the author or creator of a work is the first owner of copyright, whether in a database or otherwise, and similarly, the owner of sui generis database right is, in the first instance, the person who created the qualifying database (section 11(1), CDPA). This is important when considering monetising the asset by innovation or collaboration in cases where the business has commissioned a third-party contractor to create the database. The contractor must assign copyright to the business in order for the business to own the copyright.

For the purposes of internal innovation by employees, the CDPA and the 1997 Regulations give an employer automatic ownership of copyright and database rights in works created by its employees in certain circumstances, subject to any agreement to the contrary (section 11(2), CDPA). In the case of temporary or self-employed agency staff, it is important to check the individual’s contract as, if they are working as a consultant, they will need to assign the copyright.

Monetising data assets
Database owners will often choose to exploit their database assets through a licence, rather than a one-off sale, to enable them to maximise the financial potential of the database which can be reproduced under licence an infinite number of times without degrading the original and accessed by many users at the same time. Any licence that allows for the use of an organisation’s data should provide adequate protection for IPR in the data. It is also possible to provide access to a database solely through an application programming interface to enable it to be used effectively but without the need to provide a copy of the full database to a third party.

Contractual rights
Although it may be possible for compilations of data to be protected by IPR as described above, the protections are often patchy and inflexible for organisations wishing to assert quasi-ownership rights over data in their possession. Companies therefore often seek to assert contractual rights over data or otherwise negotiate commercial arrangements separately from any IP protection that they may be able to take advantage of.

Data governance and privacy
When considering the monetisation of data, a key issue is whether the data are also personal data for privacy purposes. If they are, the organisation must have a legitimate basis, such as the consent of the data subjects, to use the data as desired. A well-thought through data governance and privacy policy is therefore key to creating data sets which have the potential for monetisation.

Data privacy is a prime consideration from a regulatory and compliance perspective in any new innovative or collaborative venture involving data.

It is important first to consider whether a data set contains personal data. The definition of personal data is broad. The raw data might not be personal data but if, when combined with other information that an organisation holds or otherwise has access to, the person can be identified, then the General Data Protection Regulation (679/2016/EU) (GDPR) and the Data Protection Act 2018 (DPA 2018) must be complied with (see feature article “GDPR one year on: taking stock”, www.practicallaw.com/w-020-0982).

Data protection impact assessments
A data protection impact assessment (DPIA) will need to be carried out before any new venture or collaboration is embarked on involving new technologies and where the relevant data sets contain personal data (Article 35(1), GDPR).
A DPIA will be essential where there is:

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person. This includes AI decision-making (see feature article “AI and data protection: balancing tensions”, www.practicallaw.com/w-020-9713).

- Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences.

- Systematic monitoring of a publicly accessible area on a large scale, which would include CCTV and any use of facial recognition technology in a public space (Article 35(3), GDPR).

The format that the DPIA should take is left to the individual organisation but the document will become an important part of the company's audit trail should its activities ever be challenged. It is also invaluable in order to focus minds on possible privacy risks associated with planned activities, in order to try and mitigate these risks to an acceptable level.

Data retention

Under the GDPR and the DPA 2018, personal data must not be held for any longer than is necessary. Also, only the minimum data that is required should be collected and retained. This can create a conflict when thinking about the potential value of data as there is often a commercial incentive to collect as much data as possible and to keep that data for as long as possible because they might be valuable at some point, or another way to use and monetise the data may be found in the future.

However, this can offend the data minimisation and retention principles, as well as making it more difficult to find a legitimate basis on which to collect and process data. Finding the right balance to strike is therefore crucial. It is important to keep in mind these legal compliance requirements in data innovation or collaboration projects, and to remember that although it may be tempting to retain vast amounts of data for a given project for as long as possible, this may not be legally compliant. Conducting a DPIA at the outset of any innovation or collaboration project as well as considering

Competition law considerations

The European Commission recognises innovation as a parameter of competition and so, as a basic principle, companies are encouraged to innovate in competition with other players in the market (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:201:011:0001:0072:EN:PDF; www.practicallaw.com/0-504-5550). This has become particularly relevant for innovation-driven industries, such as the pharmaceutical and digital sectors, where research and development (R&D) activities are an important driver of competition.

While open innovation is likely to be viewed positively by competition authorities, as it may ultimately result in market efficiencies and benefit consumers, it can also conflict with the principle that companies should compete to innovate, in particular, when that collaboration involves competitors.

Innovative collaboration with a competitor should be mindful of the prohibition on anti-competitive agreements or concerted practices (see Briefing “Intellectual property rights and competition law: a balancing act”, www.practicallaw.com/3-605-4047).

This means, for example, that the collaboration should not lead to a loss of competition on prices, output, product quality, product variety or innovation, nor should it give rise to any unlawful sharing of commercially sensitive information between competitors.

To mitigate these risks, before engaging in any collaboration with an actual or potential competitor, some safeguards should be implemented. Depending on the specific circumstances, these could include, for example: identifying delineated teams involved in the project; limiting any information exchange on a need-to-know basis; ensuring that the scope of the co-operation arrangement does not go beyond what is necessary for the innovative purpose; and providing guidance and training to the teams involved to assist in achieving these aims.

In addition, since not every project is ultimately taken forward, it is important to agree the parties' rights and obligations in the event that the project is abandoned, for example, destroying confidential information received from the other party and considering the parties' rights to develop projects on their own. As regards the latter point, any exclusivity or non-compete obligations should be reviewed closely.

Where open innovation could lead to a restriction of EU competition law, some general exemptions may allow, in certain circumstances, innovation-related agreements not to be found in breach. For example, R&D agreements may fall within the block exemption in Regulation 1217/2010 and specialisation agreements may fall within the block exemption in Regulation 1218/2010. This is on the basis that these agreements are more likely to promote technical and economic progress if the parties contribute complementary skills, assets or activities.

Competition authorities may also recognise, on a case-by-case basis, the benefits arising from certain co-operation on the basis that certain restrictions of competition can give rise to efficiencies and consumer benefits which could not be achieved without that restriction (Article 101(3), Treaty on the Functioning of the European Union).

At each stage of a collaborative initiative, it is important to determine a legal framework which takes potential competition law challenges into account. This should allow stakeholders to define the red lines, and to structure their projects to ensure more legal certainty and greater protection.

Susan Black is a partner, and Clemente Barraud is an associate, at Herbert Smith Freehills LLP.
and legally compliant retention periods (see “Data protection impact assessments” above). These requirements should also be included in any data sharing agreement with a third-party collaborator.

Data sharing agreements

In July 2019, the Information Commissioner’s Office consulted on its draft updated data sharing code of practice (the code) (https://ico.org.uk/media/261b361/data-sharing-code-for-public-consultation.pdf). The code reflects changes introduced by the GDPR and the DPA 2018 in relation to data processing requirements for transfers of personal data, including:

- Transparency.
- The lawful bases for processing.
- The accountability principle.
- The need to document processing activities.

The code also contains useful practical guidance and good practice recommendations. At the time of writing, the code is expected to be finalised imminently. It is important to monitor the development of the code as, to the extent that an organisation shares any personal data with third-party controllers, the code will apply to those transfers of data.

Organisations may therefore wish to carry out a review of their current data sharing arrangements with third parties to determine whether any steps are required to ensure compliance with the best practice contemplated in the code.

The code encourages organisations that are sharing data sets, for example, joint collaborations between parties, to enter into an appropriate data sharing agreement in order to document some of the important compliance obligations on both parties.

For example, the data sharing agreement should:

- Help all the parties to be clear about their respective roles.
- Set out the purpose of the data sharing.
- Cover what are to happen to the data at each stage.
- Set standards.

Specific obligations should also include requirements to notify any data breaches immediately and to grant auditing rights over data centres.

In all cases of collaboration, even if it is a one-off, an organisation should require the third-party collaborator to sign a data security and confidentiality agreement to protect its data.

Cyber security

Organisations need to ensure that security and technology appropriate to the risk is used to keep their data sets secure in compliance with Article 25 of the GDPR and as incorporated into UK law by the DPA 2018 (see feature article “Cyber security: top ten tips for businesses”, www.practicallaw.com/3-621-9152).

Installing the appropriate level of data security and security by design from the very beginning of any project to build a product, rather than trying to retrofit will ensure that any risks associated with holding the data are minimised which in turn will reduce potential liability in the longer term (see feature article “Data protection: privacy by (re)design”, www.practicallaw.com/w-018-6087).

Data security breaches can be very damaging to an organisation’s public image and reputation, not to mention the loss of profit caused by any fines imposed by the ICO. These can have a knock-on, damaging effect on perceived data asset value. Data security and cyber security more generally is also becoming a significant area for due diligence in corporate transactions; a company can be significantly devalued if its cyber and data security is lacking. It is important therefore not to overlook the data security aspects.

Increasingly, when contracting for services, organisations look for the assurance of Information Security Standards, such as ISO27001 or SOC 2, in contracts involving the use or processing of their IP or data. To obtain certification, an organisation’s information security systems and processes are checked annually by an independent auditor and certified as being of the required standard. While certification is sometimes seen as a rubber stamp for an organisation’s security, it does not follow that it is compliant from a GDPR or other regulatory perspective.

It is worth considering whether, where an organisation is agreeing contract terms with a third-party innovator or collaborator where it will be sharing valuable data, it should protect its interests by requesting that the third party sign an information security agreement. This will stipulate required standards and best practices, and contain appropriate warranty and liability clauses. These agreements are increasingly frequently annexed to contracts where there is an inherent risk to one party’s IP or personal data.

Artificial intelligence

The GDPR gives individuals the right to be informed when decisions are made using profiling, to appeal and to have the decision re-examined. The Centre for Data Ethics and Innovation has been set up to provide ethical and innovative deployment of AI and is specifically looking at the potential for bias in decisions made using algorithms. It has published an interim report and its final report was expected in December 2019 but at the time of writing has not yet been published (https://assets.publishing.
government/uploads/system/uploads/attachment_data/file/819168/ Interim_report_-_review_into_algorithmic_ bias.pdf). Increasing concern is given to the deployment of AI and it is therefore recommended that during a DPIA, which must be carried out in any project where AI is to be deployed in decision-making affecting individuals, the potential for bias in the decision-making process is studied and any biases are removed (see feature article “Algorithms, apps and AI: the next frontier in discrimination law”, www.practicallaw.com/w-013-8054).

The ICO has outlined the key elements that organisations should focus on when carrying out a DPIA for AI systems (https://ico.org.uk/about-the-ico/news-and-events/news- and-blogs/2019/10/data-protection-impact-assessments-and-ai/). These include the need to make clear: how and why AI is going to be used to process the data, including how they will be collected, stored and used; the volume, variety and sensitivity of the data: the nature of the data controller’s relationship with data subjects; and the intended outcomes for individuals, wider society and the data controller. The ICO highlights the importance of involving data protection officers and other information governance professionals from the earliest stages in AI projects.
The ICO has published its first draft framework and guidance on explaining decisions made with AI (https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-and-the-turing-consultation-on-explaining-ai-decisions-guidance/). It gives practical guidance rather than being a statutory code of practice under the DPA 2018 and provides an explanation of AI, what an AI-assisted decision is, the steps that organisations need to take to provide explanations of their AI decisions, an overview of the roles that will be involved in providing these explanations, and a checklist of the policies and procedures that organisations will require.

**COMPETITION LAW**

Data sharing agreements should be monitored from a competition law perspective (see box “Competition law considerations”). For example, in some circumstances, exclusive licensing arrangements can raise competition concerns where they foreclose third-party access to a specific product or service.

In the context of any proposed collaboration, it is also important for companies to monitor their market power in respect of the data that they have access to or what value they can extract from those data. For example, a company could be viewed as having a dominant position on a relevant market where it has specific systems capable of extracting additional value from the data, even if those data are not shared.

Competition regulators are increasingly looking at competitive dynamics in the digital sector and are scrutinising the close link between market power, data collection and characteristics of data being collected.

*Joel Smith and Miriam Everett are partners, Laura Deacon is of Counsel, Rachel Montagnon is a professional support consultant, Jessica Welbom is a senior associate, and Anna McGowan is a professional support lawyer, at Herbert Smith Freehills LLP.*