HERBERT SMITH FREEHILLS

Data issues in innovation and collaborations

OPEN INNOVATION: COLLABORATE TO INNOVATE

Businesses in every sector are under pressure to innovate to stay ahead of the competition. "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.

Collaborative innovations or innovative collaborations (both descriptions apply) present opportunities to reduce costs, share risk, provide broader access to talent and ideas, and ultimately achieve greater monetary gain.

Data frequently plays a central role in this drive towards "open" innovation as there is a significant value attached to it. Data can be used to generate new products or services and revenue streams, to identify efficiencies within an organisation and reduce costs, and to inform strategic decision-making.

Unlocking the value of your data

Encouraging open innovation using data often requires a flow of information and intellectual property rights 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 whilst ensuring its future value in the context of more collaborative innovation. This involves thinking through all the legal considerations and practical steps that will allow you to adapt and have the flexibility of process to become enablers of innovation and help your organisation stay ahead of the curve.

To maximise the value of data so that it 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 it is compliant with the new data protection laws and safeguarded as far as possible against outside threats like cyber attacks, data fraud, data security breaches and shareholder activism. When sharing data assets it is also important to be mindful to avoid other potential pitfalls within competition law, ethics and criminal law.

Authors

Miriam Everett
Partner, Data & privacy
miriam.everett@hsf.com

Andrew Moir
Partner, IP, Global head of cyber & data security
andrew.moir@hsf.com

Anna McGowan
Professional Support Lawyer, Corporate
anna.mcgowan@hsf.com

Rachel Montagnon
Professional Support Consultant, IP
rachel.montagnon@hsf.com

Key contacts

Joel Smith
Partner, UK Head of IP
joel.smith@hsf.com

Rebekah Gay
Partner, IP
rebekah.gay@hsf.com

Click here for our report on client perspectives

OPEN INNOVATION: COLLABORATE TO INNOVATE

Anticipating the value in data

Knowing what data your organisation has available or accessible, assessing the type, the quantity, the quality and ensuring all data sets are properly organised in a structured way and kept up to date, where necessary, is vital before any open innovation or collaboration can occur. This can be achieved through a regular auditing process, although this can often be a challenge for organisations running multiple legacy IT systems.

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

Copyright and *sui generis* database rights can exist in collections of data, but in relation to these rights it is the structure of the compilation and the database as a whole that is protected respectively and not each individual item of data of itself, unless these data are themselves copyright works (with the required level of creative endeavour involved). Using your data to compile a database may therefore give increased protection for the data as a whole (although not individually). These rights are aimed at preventing a competitor stealing the content of your database (sui generis database rights) or protecting a particularly original structure of a database (database copyright).

A database is legally defined in the Copyright, Designs and Patents Act 1988 (CDPA) s 3A(1) 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.'

Databases can include contact management systems, document management systems, knowledge management systems, intranets, back-office inventory systems, purchase order systems, and websites, amongst others. To fall within the definition of a database there is in fact no requirement for a compilation of data to be in electronic form but in today's digital economy digitising data assets is essential to realising their maximum value.

Complex data sets can be derived from virtually every kind of digital interactions, such as internet transactions, email, mobile payments, click streams, as well as Internet of Things (IoT) devices. The possibilities are endless. These data sets can then be amalgamated and organised into larger 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 it as confidential information or trade secrets. This requires access to be limited to those within a confidentiality arrangement or who are impliedly required to keep such 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 IP Rights in data

As stated above, there are a variety of intellectual property rights that data sets can have.

Enforcement of rights in data is difficult. Not only are such rights difficult to establish but where data has been amalgamated, such as in collaborative situations, it may be difficult to establish which data comes from which party and thus show any chain of ownership. Often, the answer is to use contract law, or to define data structures so that they explicitly indicate origin.

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

The Database Directive (96/9/EC), implemented into the UK by the Copyright and Rights in Database Regulations 1997 (SI 1997/3032) (Database Regulations), created intellectual property rights in the contents of a database (as defined 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

As mentioned above, it is also possible for the structure of the database to attract copyright protection. For a compilation to attract copyright as a literary work consisting of a database it will only be original 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 (2) CDPA as inserted by regulation 6 of the Database Regulations). This requires the author of the database to have made free and creative choices, not formulaic ones, in order to attract database copyright, and raises

problems for databases compiled or structured without any innate creativity and calls into question whether databases created using AI or machine learning could qualify. 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. This principle has not been tested in relation to *sui generis* database rights as yet.

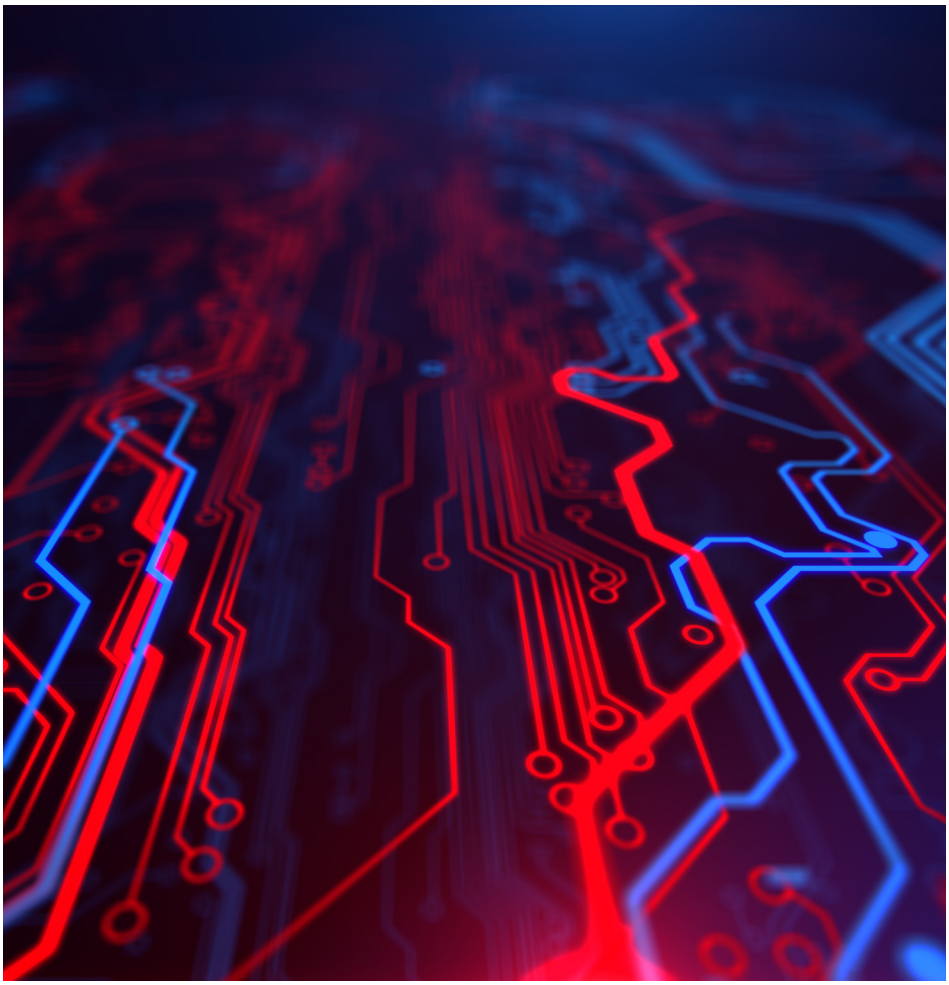
Compilations of data which do not fall within the definition of a database under Section 3A(1) of the CDPA (such as a table or graph) may be protected by copyright as literary works. The standard of originality required for copyright to apply is relatively low, but it does need to involve some demonstrable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

Generally the author or creator of a work is the first owner of copyright (whether in a database or otherwise) (section 11(1) CDPA) and similarly, the owner of a *sui generis* database right is, in the first instance, the person who created the qualifying database. 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. In order to own the copyright in it, the business must enter into an agreement with the contractor which contains an assignment of copyright.

For the purposes of internal innovation by employees, the CDPA and the Database 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). It is important not to be caught out in the case of temporary or self-employed agency staff: check the individual's contract, as if they are working as a consultant, they will also need to sign an assignment as with a third party contractor.

Monetising your data assets

Commercially, database owners will often choose to exploit their database assets via 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 which allows for use of an organisation's data should provide adequate protection for IPRs in the data. It is also possible to apply a model where access to a database is solely via an API (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.



Asserting contractual rights over data

Although it may be possible for compilations of data to be protected via intellectual property rights as described above, the protections are often patchy and inflexible for organisations wishing to assert quasi-ownership rights over data in their possession. The natural consequence of this is that companies often seek to assert contractual rights over data or otherwise negotiate commercial arrangements quite apart from any IP protection they may be able to take advantage of.

However, when considering the monetisation of data, a key element of this process is considering whether the data is also 'personal data' for privacy purposes, and then having a legitimate basis in place (such as the consent of the data subjects) to use the data as desired. Thus a well thought through data governance and privacy policy is key to creating data sets which have the potential for monetisation.

Data governance and privacy

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 it is combined with other information that you hold as an organisation or otherwise have access to, the person can be identified, then the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA) must be complied with.

The importance of data protection impact assessments

A Data Protection Impact Assessment (DPIA) will need to be carried out before any new venture or collaboration is embarked upon involving new technologies and where the relevant data sets contain personal data. Article 35 (1) of the GDPR stipulates:

"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."

Article 35 (3) highlights that a DPIA will be essential in all circumstances where:

(a) there is "a 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)

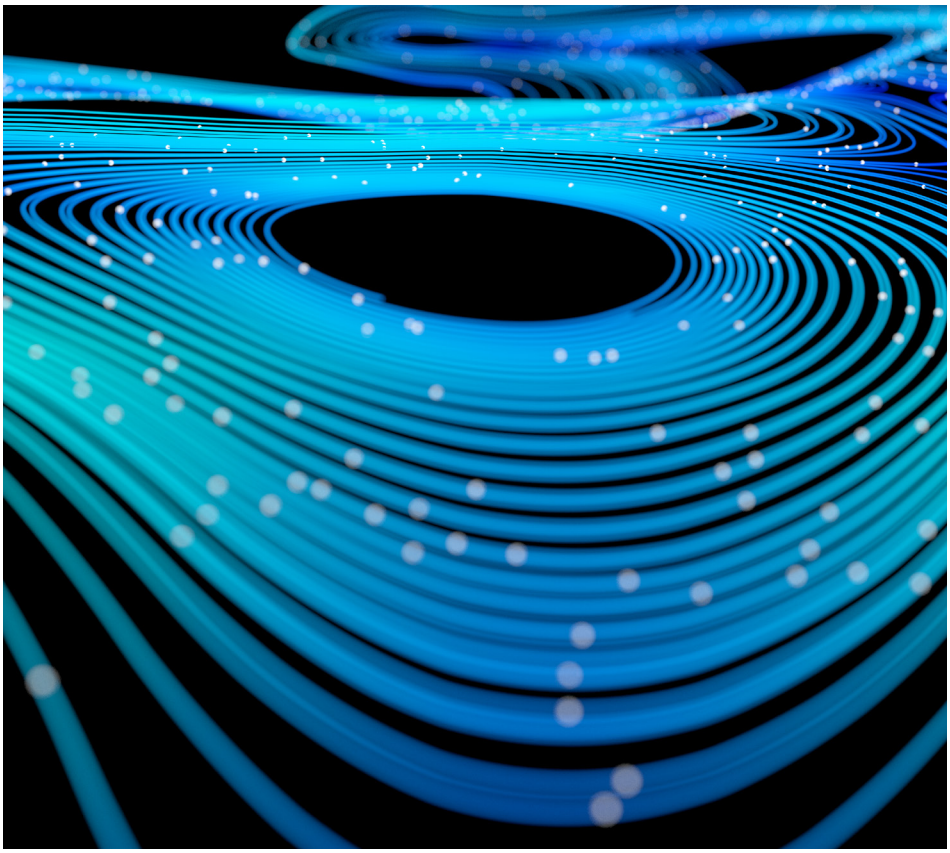
(b) processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences; or

(c) there is 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).

The format that the DPIA should take is left to the individual organisation but the document will then 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 such risks to an acceptable level.

Data retention

Under the GDPR and the Data Protection Act 2018 personal data must not be held for any longer than is necessary. Also, only the minimum required data 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 it might be valuable at some point, or another way to utilise and monetise the data may be found in the future. However, this can contravene the data minimisation and retention principles, as well as making it more difficult to find a legitimate basis upon which to collect and process it. 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 just because you are tempted to retain vast amounts of data for a given project for as long as possible does not mean you will be legally compliant if you do so. Conducting a DPIA at the outset of any innovation or collaboration project as described above will encourage setting reasonable and legally compliant retention periods, as well as considering the legal basis for processing the types and quantities of data kept for a given project. These requirements should also be in any Data Sharing Agreement with a third party collaborator.



Data sharing agreements

In July 2019, the ICO published its draft updated data sharing code of practice (the "Draft Code") for public consultation which ended on 9 September 2019. The Draft Code reflects changes introduced by the GDPR (and the Data Protection Act 2018) in relation to data processing requirements for transfers of personal data, including:

- transparency;
- the lawful bases for processing;
- the accountability principle; and
- the need to document processing activities.

The Draft Code also contains useful practical guidance and good practice recommendations. The final code is expected to be published imminently following the end of the consultation period. To the extent an organisation shares any personal data with third party controllers, the final version of the code will apply to such transfers of data. It is therefore important to monitor the development of the Draft Code.

Organisations may therefore be wise to carry out a review of their current data sharing arrangements with third parties against the Draft Code, and determine whether further actions (for example, revisions to data sharing arrangements) are required to ensure compliance with the best practice contemplated in the Draft Code.

As mentioned above, the Draft Code encourages organisations who are sharing data sets (eg 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 is to happen to the data at each stage; and
- set standards.

Specific obligations should also include requiring the immediate notice of any data breaches as well as auditing rights over data centres.

In all cases of collaboration, even one-off, you should require the third-party collaborator to sign a Data Security and Confidentiality Agreement to protect your data.

Information and cyber security

Organisations need to ensure that security and technology appropriate to the risk is utilised to keep their data sets secure in compliance with Article 25 of the GDPR and as incorporated into UK law by the Data Protection Act 2018. Installing the appropriate level of data security and security by design from the very beginning of any project when you are building products, rather than trying to retro fit will ensure that any risks associated with holding the data are minimised which in turn will reduce potential liability in the longer term.

Data security breaches can be very damaging to an organisation's public image and reputation (not to mention the loss of profit that can be caused by the level of fines that can be imposed by the Regulator) and can therefore 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.

Increasingly, when contracting for services, organisations are looking for the assurance of Information Security Standards (like ISO27001 or SOC 2) within contracts involving use or processing of their IP or data. To obtain certification your 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.

Where you are agreeing contract terms with a third party innovator or collaborator where you will be sharing valuable data, it is worth considering whether you should protect your own interests by requesting that the third party sign an Information Security Agreement stipulating required standards and best practices and containing appropriate warranty and liability clauses. Such types of agreements are increasingly annexed to contracts where there is inherent risk to one party's intellectual property or personal data.

Ethical considerations

It is also important to think through any ethical issues that may be raised by what you are planning to do with data. Innovative uses of data that are not perceived to be ethical can attract adverse publicity and put your organisation at risk. The House of Lords Select Committee Report on regulating the digital environment which was published in May 2019 sets out recommendations for Ethical Technology and urges for ethical issues to be considered at the design stage of new digital services.

Considerations in the use of artificial Intelligence (AI)

The GDPR gives individuals the right to be informed when decisions are made using profiling and to appeal and to have an individual re-examine the decision. 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. They have published an Interim Report and their final report is expected in December 2019. Increasing concern is given to the deployment of AI and it is therefore recommended that during the DPIA (which must be carried out in any project where AI is to be deployed in decision-making affecting individuals), studies are made of the potential for bias in the decision-making process and that these biases are removed.

The latest update in the ICO's AI Auditing Blog following their Call for Input on developing the ICO Auditing Framework for AI published on 28 October 2019, outlines the key elements that organisations should focus on when carrying out a Data Protection Impact Assessment (DPIA) for AI systems. which includes the need to make clear how and why AI is going to be used to process the data including how it 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 as well as the intended outcomes for individuals or wider society and for the data controller. One very important point that the ICO highlights is the need for data protection officers and other information governance professionals to be involved from the earliest stages in AI projects.

The ICO's' first draft framework and guidance Explaining Decisions made with AI was published on 2 December 2019 in conjunction with the Alan Turing Institute (The Turing) in response to the Government's AI Sector Deal. The draft guidance is out for consultation until January 24 2020. It is a practical guidance rather than a statutory code of practice under the Data Protection Act 2018 and provides an explanation of AI, what an AI-assisted decision is, the steps 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 policies and procedures organisations will require.

Avoiding criminal liability

It is important in any data innovation or collaboration to avoid unwittingly committing a cybercrime under the crime laws. 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.

Averting competition law Issues

Exclusive licensing arrangements and other data sharing agreements may raise competition concerns where they foreclose competitors who are not permitted similar access. Dominance may also arise where a company has specific systems capable of extracting additional value from the data, even if that data is not shared.

It is important for companies to consider their market power in the context of any proposed collaboration as the European Commission is looking to increase the burden of proof on dominant companies required. This would be a risk, for example, where a merger relies on substantive data sets being acquired. Competition regulators are

increasingly looking to 'unlock' competition in the digital market and are scrutinising the close link between market power, data collection and characteristics of data being collected.

Reducing the risk of shareholder activism

It is important to be aware of how your data innovation and collaboration activities might be viewed by shareholders.

Organisations need to mitigate the risk of being targeted by shareholder activism. This can be achieved, for example, by monitoring the shareholder base, holding proactive discussions with key investors, maintaining good standards of governance, preparing for all eventualities at shareholder meetings, using publicity positively and maintaining good investor relations, monitoring shareholder activity, voting patterns, understanding possible tools that shareholders may have, anticipating lines of attack, reviewing existing structural defences and staying up to date with legal and regulatory developments.

Conclusion

There is currently significant movement by the World Trade Organisation, the European Commission, and government and regulatory bodies worldwide towards greater regulation of data across the board; whether by competition law, data protection law, company law or criminal law as we have highlighted here. This creates a broad patchwork of laws, impending legislation and threatened legislation all seeking to deal with the use and ownership of data, which organisations are already (or soon will be) required to navigate.

It is therefore essential when looking to maximise the opportunities for innovation and collaboration that the use of data is thoroughly considered. Collaborators need to recognise the value that the data created by a collaboration may have and provide for the future mutual or independent uses which parties accept. Effective monetisation of that data will depend on its correct collation, fulfillment of privacy requirements and the necessary assignments and contractual arrangements being in place to allow the uses which give data value. The regulatory framework also needs to be considered from the outset and given appropriate consideration throughout.

Previous editions in our Open innovation: Collaborate to innovate series

Issue 1

Getting the IP right in collaborations

For a full list of our global offices visit **HERBERTSMITHFREEHILLS.COM**