THE GUIDE TO **DATA AS A CRITICAL ASSET**

Editor
Mark Deem

The Guide to Data as a Critical Asset 2022

Reproduced with permission from Law Business Research Ltd
This article was first published in April 2022
For further information please contact Natalie.Hacker@lbresearch.com

Published in the United Kingdom
by Global Data Review
Law Business Research Ltd
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.globaldatareview.com

To subscribe please contact subscriptions@globaldatareview.com

ISBN: 978-1-83862-859-8

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

Preface

Data is not just a source of regulatory risk: it is a vital asset for almost every type of organisation. Artificial intelligence and other forms of sophisticated computing and automation are no longer the stuff of science fiction: the future has become the present (or, at least, the near future). None of this would be possible without data. But even 'classic' business models now rely on the use of all forms of data, and its protection – whether in a data privacy or any other sense – is more important than ever.

Whether exploited as a core part of a business model, kept confidential during the development of a new product or processed with the care required by personal data regulation, information is now a board-level concern. GDR's *The Guide to Data as a Critical Asset* takes a unique view of data. Instead of looking at it through a regulatory and risk lens, the contributors to this book – edited by Mishcon de Reya partner Mark Deem – aim to steer companies through the gathering, exploitation and protection of all types of data, whether personal or not.

Global Data Review
London
March 2022

How Best to Protect Proprietary Data in Data-Sharing Deals

Toby Bond[1]
Bird & Bird

This article focuses on the monetisation of data through data-sharing deals. As discussed elsewhere in this Guide, data is a resource that can be used to generate significant value for an organisation. Data will not always be held by the party who is best able to realise that value and, therefore, sharing data can provide another route to monetising its value. However, unlike physical resources, data can be shared with others without excluding the originating party from its use, potentially allowing the data to be monetised both directly and indirectly.[2]

Identifying which categories of data can be shared to generate value and, of these, which should be shared, is a fundamental part of any organisation's overall data strategy. It is generally not a binary question, as an organisation may be willing and able to share data in some circumstances but not others. Nor is it a static question, as decisions regarding data sharing are subject to commercial, technological and regulatory considerations that evolve over time. Understanding how a particular data-sharing deal fits into an organisation's overall data strategy is often the key to ensuring its success.

1 Toby Bond is a senior associate at Bird & Bird.

2 This does not imply that all data an organisation holds should be shared to generate value. Some categories of data deliver a key competitive edge that would be destroyed if those data were made available to competitors, customers or suppliers. Nor does it imply that all data can be shared to generate value, as some data are subject to legal restrictions that limit the circumstances in which they may be shared.

Forms of data sharing

Realising value through data sharing is not a new phenomenon. Sectors such as financial services and sports betting have many years of experience of generating value through the provision of data feeds and historic data sets and have well-developed frameworks and industry norms for data licensing. However, recent developments in data capture, storage and processing techniques have opened new streams of value that may be derived from data across a much wider range of industry sectors. As a result, data-sharing arrangements now arise in many sectors in which they have not been experienced before.

Data-sharing arrangements come in many forms. They include bilateral data licences and assignments and more complex multilateral arrangements such as data pools and exchanges, under which multiple parties contribute data and receive access to data (or analytics derived from the data) in return. Data sharing also occurs in less obvious ways. For example, by providing an SaaS[3] service, the service provider will obtain access to a customer's data. While the focus of the agreement is on the value of the service, having access to the customer's data may also provide substantial value to the service provider.

Some specific categories of data (e.g., personally identifiable information or public sector information) are subject to regulatory requirements that impose additional restrictions or obligations relating to data sharing. A survey of these regulatory requirements would require a far more expansive discussion than this article affords. Our focus here, therefore, is on general issues relating to the protection of proprietary data that may arise in any form of data-sharing deal.

Protecting proprietary data

Many data-sharing deals assume that one party 'owns' the data being shared. While this is a convenient shorthand, if taken too far it can lead to confusion.[4] This confusion arises because English law (along with many other legal systems) does not recognise that data per se is capable of being owned, in the sense of granting an 'owner' rights against third parties. In contrast, a hard drive or USB stick on which data resides are clearly forms of property, capable of being owned and protected against unlawful interference and taking. The absence of a general in rem property right that applies to all forms of data, however, does not prevent parties obtaining and exercising legal rights to control access, use and dissemination of data.

---

3 Software as a service.

4 For example, who 'owns' a data set created through the combination of multiple other data sets? Is it jointly owned by the entities who contributed the data, or the entity who undertook the combination?

But what is data? Some use the term narrowly to refer to records of purely factual matters.[5] Others use it more expansively to refer to a much broader category of subject matter.[6] As a result, data is not a homogenous legal object and the legal rights that apply will vary depending on the nature of the data, and the circumstances in which it is created and shared. However, these rights provide the legal framework for any data-sharing transaction and understanding them is essential to ensuring effective protection.

The four legal rights provided by English law that can be used by commercial organisations to control access, use and dissemination of data in data-sharing deals are (1) rights of confidence, (2) copyright, (3) database rights and (4) contractual rights. We also discuss below the extent to which each right is harmonised across jurisdictions.

Rights of confidence

Rights of confidence arise under English law where information has the necessary quality of confidence and it is disclosed in circumstances importing an obligation of confidence on the recipient.[7] The right arises in equity and entitles the party to which the obligation of confidence is owed to prevent misuse of the information[8] through its unlawful acquisition, use or disclosure.[9]

Rights of confidence are often closely related to contractual rights as contractual terms are commonly the manner in which an equitable obligation of confidence is imposed on the intended recipient of information. However, the remedies available where an equitable right of confidence exists are generally more flexible than those

5 For example, the temperature in Trafalgar Square every day in December 2021, or the number of cups of coffee drunk during the writing of this chapter.

6 A photograph of Nelson's Column or a drawing of a cup of coffee could, for example, be referred to as 'training data' for an AI image recognition system.

7 *Coco v. A.N. Clark Engineers Ltd* [1968] F.S.R 415.

8 Protection for confidential information arises out of English common law, although the protection offered to the subset of confidential information that qualifies as a trade secret under Article 2(1) of Directive (EU) 2016/943 (the EU Trade Secrets Directive) has been partly codified by way of The Trade Secrets (Enforcement, etc.) Regulations 2018.

9 While the legal basis of a right of confidence has been the subject of debate before the English courts, the currently accepted view is that it is not a proprietary right in the information – see *Shenzhen Senior Technology Material Co Ltd v. Celgard, LLC* [2020] EWCA Civ 1293 at [58]. Instead, the right is founded in the law of equity and the public policy that parties should not breach obligations of confidence owed to others.

that arise following a breach of contract.[10] Furthermore, contractual rights may only be enforced against another contracting party whereas rights of confidence may be enforced against anyone who receives information in circumstances that give rise to an obligation of confidence. This does not require the recipient to have actual knowledge that they are under an obligation of confidence and is assessed from the viewpoint of a reasonable person in the position of the parties.[11]

While rights of confidence provide a powerful and flexible basis for the protection of data and databases in data-sharing deals, they are subject to several limitations:

- Rights of confidence cannot be enforced with respect to information in the public domain.[12]
- Enforcement will not be possible against 'innocent' recipients of the data who could not be expected to know that they were under an obligation of confidence, for instance because they were reasonably entitled to rely on reassurances from the party who supplied the data that the provision was lawful.[13]
- Rights of confidence may be subject to several public policy and public interest-based restrictions on their enforcement, including fundamental rights such as freedom of expression, the exposure of fraud or dishonest conduct, and cases involving public safety and wellbeing.

Although a limited degree of harmonisation in the protection of undisclosed information was achieved in Europe by way of Directive (EU) 2016/943 (the EU Trade Secrets Directive), the Directive only specifies the minimum protection that Member States (including the United Kingdom, prior to its departure from the Union) are required to

10 For example, both interim and final injunctions prohibiting the use or disclosure of confidential information are commonly awarded by English courts and relief may be granted in relation to goods that significantly benefit from the unlawful acquisition, use or disclosure of confidential information. See The Trade Secrets (Enforcement, etc.) Regulations 2018, Regulations 11 and 14.

11 *The Racing Partnership Limited v. Sports Information Services Limited* [2020] EWCA Civ 1300 at [70].

12 In other words, information that has a sufficient degree of accessibility such that it would be unjust to require the party against whom a duty of confidence is alleged to treat it as confidential.

13 See, for example, *The Racing Partnership Limited v. Sports Information Services Limited* [2020] EWCA Civ 1300, in which the majority of the Court of Appeal held that there was no breach of confidence by a recipient of horse racing data because they had been entitled to rely on an express contractual warranty that the supplier had all necessary rights from third parties to provide the information and that the recipient's use of the data would not breach any third-party rights.

provide. International harmonisation is also limited to Article 39 of TRIPS,[14] which requires World Trade Organization members to ensure the protection of certain categories of undisclosed information against acquisition, use or disclosure contrary to honest commercial practices. The circumstances in which data and databases can be protected as undisclosed information and the protection that arises can vary significantly, therefore, between jurisdictions and local advice is recommended whenever relying on this form of protection in a data-sharing deal.

Copyright

Copyright can potentially protect both data and databases. Where copyright arises, the owner is provided with a powerful right to prohibit further dealings with the data or database, including the creation of copies and communicating the data or database to the public. Although copyright is a national right, the creation or publication of a copyright work in one country will generally give rise to a copyright in most other countries.[15]

However, copyright will only arise when the work is original[16] or if a sound recording or film has not been copied from an earlier sound recording or film:[17]

- Data (other than sound recordings or films) will only qualify for protection by copyright in relation to subject matter that is original in the sense that it is its author's own intellectual creation.[18] This requires a reflection of the author's personality where the author is able to express his or her creative abilities in the production of the work by making free and creative choices.[19] The existence of technical constraints on the possible forms of expression is a factor that can reduce the scope for originality,[20] such that the more restricted the choices, the less likely it is that the product will be the intellectual creation (or the expression of the intellectual creation) of the person who produced it.[21]

14 The Agreement on Trade-Related Aspects of Intellectual Property Rights.
15 By operation of The Berne Convention for the Protection of Literary and Artistic Works and other international treaties.
16 Copyright, Designs and Patents Act 1988, Section 1(1).
17 ibid., Section 1(2).
18 *Infopaq International A/S* (Case C-5/08), at [37]).
19 *Painer* (Case C-145/10), at [88]–[89].
20 *Bezpečnostní softwarová asociace* (Case C-393/09).
21 *SAS Institute Inc v. World Programme Ltd* [2013] EWCA Civ 1482, at [31].

- A database may be protected by copyright as an original literary work when it is an author's intellectual creation by reason of the selection or arrangement of its contents.[22] As with copyright in data, copyright in a database will not arise if the selection or arrangement of the contents is entirely dictated by technical function, such that the author has no freedom to express creativity.

The requirement for originality prevents copyright applying to all data and databases. When individual data is captured to provide a record of objective facts, there is little scope for each datum to reflect an author's intellectual creation. Data capture through automated processes is therefore unlikely to qualify for copyright protection. The selection and arrangement of data in many databases will also be dictated solely by technical function, limiting the application of database copyright.

Copyright is partially harmonised through several international agreements[23] and at the EU level through various directives.[24] The United Kingdom continues to implement the EU copyright directives in its national law.[25]

Database rights

A database right arises in the United Kingdom when a substantial investment is made in obtaining, verifying or presenting the contents of the database.[26] 'Verification' means ensuring the reliability of data and monitoring its accuracy and covers checking, correcting, maintaining and updating the contents of a database.[27] 'Presenting' covers the structuring and organisation of the data and making it accessible to users (including the creation of indexes, thesauruses, etc.). An investment in 'obtaining' data refers to the resources used to seek out existing independent materials and collect them in the

22 Copyright, Designs and Patents Act 1988, Section 3A.

23 Including The Berne Convention for the Protection of Literary and Artistic Works and the World Intellectual Property Organization Copyright Treaty.

24 Directive 2001/29/EC (on the harmonisation of certain aspects of copyright and related rights in the information society), Directive 2006/116/EC (on the term of protection of copyright and certain related rights) and Directive 2009/24/EC (on the legal protection of computer programs).

25 Except for Directive (EU) 2019/790 (on copyright and related rights in the Digital Single Market), which the United Kingdom chose not to implement as the transposition date fell after the end of the transition period under the EU–UK Withdrawal Agreement. This Directive provided exceptions to copyright for the purposes of text and data mining, that have not been replicated in UK law to date.

26 The Copyright and Rights in Databases Regulations 1997, Section 13(1).

27 *Fixtures Marketing I* (Case C-338/02), at [27].

database. It does include the resources used for the creation of materials that make up the contents of a database. [28] As a result, an investment in creating new subjective information is unlikely to give rise to a database right protection, whereas investment in capturing pre-existing objective information can give rise to such protection.[29] When a qualifying investment arises, the maker of the database is afforded an intellectual priority right that can be licensed and assigned, and enforced to prevent third parties from extracting or reutilising all, or a substantial part, of the database without consent.

The maker of a database is the person who takes the initiative in and assumes the risk of obtaining, verifying or presenting the contents. However, for a database right to arise in the United Kingdom in relation to a database created before 1 January 2020, the maker of the database must be either a national or habitual resident of a Member State of the European Economic Area (EEA) or a company (1) formed in accordance with the laws of an EEA Member State and (2) having its central administration or principal place of business in an EEA Member State, or a registered office in an EEA Member State with a genuine link and continuing link to the economy of an EEA Member State. For databases created after 1 January 2020, references to a EEA Member State are replaced with the United Kingdom (i.e., makers based in the EEA will no longer obtain protection for their databases in the United Kingdom, and vice versa).

Database rights are harmonised in the European Union by way of the Database Directive,[30] which continues to be implemented in UK national law.[31] An equivalent right has not been implemented outside the European Union, although other jurisdictions may offer similar forms of protection through a broader application of their copyright law or through laws relating to unfair competition.

Contractual rights

Contracts can be used to define the scope of a permission granted under another right, such as a copyright or database right[32] or to impose (and define the scope of) an obligation of confidence on the recipient. Contracts can also be used to impose direct obligations on a party in receipt of data or a database regarding access, use and

28 *The British Horseracing Board Limited v. William Hill Organisation Limited* (Case C-203/02).

29 *British Sky Broadcasting Group Plc v. Digital Satellite Warranty Cover Ltd* [2011] EWHC 2662 (Ch) at [21] and *Football Dataco Ltd v. Sportradar GmbH* [2013] EWCA Civ 27.

30 Directive 96/9/EC (on the legal protection of databases).

31 The Copyright and Rights in Databases Regulations 1997.

32 The contract defines the scope of the permission granted to the data recipient to undertake acts in relation to data or a database that would otherwise infringe that copyright or database right.

dissemination. If the data or database is protected by an intellectual property (IP) right or an obligation of confidence, these contractual rights exist in addition to the underlying legal right.[33] However, contractual obligations regarding access, use and dissemination of data can be imposed on a recipient even when the data is not subject to an IP right.[34] In these circumstances, a contractual obligation restricting access, use or dissemination of data or a database is a negative covenant for consideration that the court will enforce 'provided only that the covenant itself cannot be attacked for obscurity, illegality or on public policy grounds such as that it is in restraint of trade'.[35] Subject to the limitations on contractual terms discussed below, contractual restrictions are therefore commonly imposed in relation to data that is in the public domain and cannot be made the subject of an obligation of confidence.

The flexibility of contractual rights to protect data irrespective of any underlying legal rights and to impose fine-grained controls on the access, use and dissemination of that data makes them a crucial tool in any data-sharing deal. However, contractual rights are subject to two key limitations:

- They are rights *in personam* and can only be enforced against specific persons.[36]
- The remedies available for breach of contract are generally more limited than those available for infringement of an IP right or a breach of confidence.[37]

Other than some limited areas (e.g., prohibitions on anticompetitive agreements), contract law is not harmonised between different jurisdictions and local advice under the governing law of the contract is recommended.

---

33 For example, acting outside the scope of a contractual licence to a database protected by a database right would give rise to a claim for both IP infringement and breach of contract.

34 See *Atheraces & Anor v. British Horse Racing Board* [2007] EWCA Civ 38, at [153], in which the Court of Appeal agreed with the High Court's conclusion that the British Horse Racing Board was entitled to charge for use of its data irrespective of whether it had any IP rights in that data.

35 *Attorney General v. Barker* [1990] 3 All E.R. 257, at 259.

36 Once the data 'escapes' beyond the control of the contracting parties, the data supplier may have a breach of contract claim against the data recipient if it is responsible for the 'escape', but will not have a breach of contract claim against third parties who receive the data. Tortious claims for procuring breach of contract or unlawful means conspiracy, however, may be available if the third party has played an unlawful part in securing access to the data.

37 For example, damages for breach of contract are generally limited to placing the claimant in the same position had the contract been performed and equitable remedies such as injunctions are less commonly awarded in breach of contract claims than in IP infringement and breach of confidence cases.

Four dimensions of control in data-sharing deals

Whatever form a data-sharing deal takes, there are four 'dimensions' of control that a party sharing data can use to protect their interests:

- Who can access the data?
- What data can they access?
- How can they access the data?
- What can they use the data for?

Decisions regarding each dimension of control will ultimately be informed by a range of commercial, legal and technical factors, including the value and sensitivity of the data, the benefit each party hopes to realise through the arrangement, the legal rights that protect the data and the technical infrastructure that will facilitate the sharing. Decisions regarding control should also be informed by any overall data strategy of the organisation sharing the data.

Who can access the data?

A starting point for any data-sharing arrangement is to establish limits on how far the data can be shared. Most data-sharing arrangements restrict access to members of certain groups, such as the employees and professional advisers of an organisation. Access may be made subject to certain legal conditions (e.g., a request for access that is approved by the data provider or an agreement to certain terms of use). It may also be subject to technical restrictions. Controls on who can access data should consider both the original data supplied to the data recipient and any materials created based on that data (e.g., the results of analysis of the data by the data recipient).

What data can they access?

Modifying data to remove or reduce its sensitivity is one dimension of control that a data provider can exercise to protect its interests. This modification can take the form of removing specific data fields from a data set, aggregating data or providing insights based on the data rather than the actual data. In some circumstances, controlling the nature of the data that can be accessed can facilitate a data-sharing transaction that would otherwise not be possible for legal or commercial reasons.

How can they access the data?

The method by which data is accessed can be an important factor in its protection. The least protected form of access is direct transfer, where the entirety of the data set is available for the recipient to download onto its own systems as direct control over the

data is lost once a copy of the data set leaves the data supplier's systems. More protection is offered by hosting the data set on the data supplier's systems and exposing it to the data recipient over the internet via an API.[38] This approach does not require the full data set to be provided to the recipient and allows access to be dynamically removed or altered. Further protection can be afforded by providing a more limited interface to the data (such as a web interface allowing a limited range of user-defined queries) or by only permitting the data user to access the data in a secure environment hosted by the data provider, such that the data always remains under the data provider's direct control.

What can they use the data for?

Data can often be reused for many purposes, some of which will be more acceptable to the data provider than others. Controls on the purpose for which data can be used are therefore important in ensuring that the data-sharing arrangement provides value to the data provider, while avoiding potential harm. Controls on use can be defined in positive terms, with a list of permitted uses and all other uses being prohibited, or in negative terms, with any use allowed unless it falls within a prohibited category. A commonly prohibited category of use is the creation of products or services that would compete with the business of the data provider.

Key contractual terms to implement controls

Contractual terms that control the legal rights of a data recipient to access, use and disseminate data received as part of a data-sharing deal are commonly found in clauses dealing with IP, confidential information, data licences and data protection. Practical restrictions on access, use and dissemination of data may also be found in other clauses, such as conditions for accessing a service and obligations on termination. Issues that commonly arise when drafting and negotiating data-sharing agreements include the following:

- *Conflicting clauses*: As the issues of data access, use and dissemination can arise in more than one place in a data-sharing agreement, it is not uncommon for inconsistencies to arise between different clauses. For example, data may be included in the definitions of confidential information and IP, such that the IP and confidential information clauses conflict with a data licence clause.

38 Application programming interfaces allow software programs to communicate with one another.

- *Unclear purpose limitation*: Purpose limitations are key in controlling the use of data under a data-sharing agreement and may give rise to a dispute if they are not sufficiently clear. Although general definitions such as 'for the purposes of this agreement' or 'in the ordinary course of business' may be appropriate in some data-sharing agreements, parties may arrive at different understandings of the extent of the permission granted, resulting in the potential for future conflict.
- *Status of derived data*: If a data recipient is permitted to process the data it has received, or combine it with other data, a data-sharing agreement should address the ownership of any new IP rights that may arise and whether the data recipient is permitted to disseminate this 'derived data' to others. In some circumstances, the derived data may embody IP rights or confidential information contained in the original data and dealings with the derived data without the permission of the rights holder would be a breach of those rights. In others, the derived data is not subject to earlier rights and the data recipient will be free to use and disseminate the data unless expressly prohibited from doing so by the contract. In either case, the parties to a data-sharing agreement should consider what is permitted in respect of derived data. A common approach is to draw a distinction between derived data that can be reverse engineered to obtain the original data and derived data that cannot.
- *Status of metadata*: In addition to data that is directly shared through a data-sharing arrangement, interactions between the contracting parties may give rise to new data (e.g., metadata regarding the use of a service by a customer). Data-sharing agreements should address the ability of each party to the agreement to access, use and disseminate this metadata.
- *Audit rights*: To ensure compliance with the terms of a data-sharing agreement, the data supplier may impose the right to audit the data recipient's use of the data. Audit rights will commonly include record-keeping requirements along with rights to access records and systems to ensure compliance.
- *Post-termination obligations*: Data-sharing agreements will commonly have a defined term or the possibility of termination under certain circumstances (e.g., a material breach of the terms or the insolvency or change of control of the parties). The agreement should address how the termination of the agreement affects the parties' respective rights to access, use and disseminate data, derived data and metadata. For example, the data provider may want the data recipient to delete all copies of the data following termination. Special consideration is required where the data has been used to train an artificial intelligence system, and the training data set needs to be retained for regulatory or technical reasons.

Limits on contractual terms in data-sharing agreements

Although freedom of contract is a basic principle of English common law, other principles exist that can prohibit certain contractual terms in data-sharing agreements. The most relevant in the context of business to business data-sharing agreements are likely to be the following.

Restraint of trade

Under English common law, covenants in restraint of trade are prima facie unenforceable unless (1) there is a valid interest that the party imposing the restraint of trade seeks to protect, (2) the restraint is no wider than is reasonable to protect that interest and (3) it is not contrary to the public interest.[39] The doctrine can potentially be engaged in the context of data-sharing agreements by way of terms that prohibit a party from carrying out trade with parties identified in the data, or from engaging with certain parties while they remain in possession of the data.[40] It is also generally considered that an obligation of confidence that remains in force once the information has entered the public domain through no fault of the recipient could engage the doctrine.

Competition law

Section 3(1) of the UK Competition Act 1998 prohibits agreements between undertakings that may affect trade within the United Kingdom and have as their object or effect the prevention, restriction or distortion of competition within the United Kingdom (referred to as the 'Chapter I prohibition'). An infringing agreement is invalid, although if the infringing provision can be severed, the rest of the agreement will remain in force. Data-sharing agreements can potentially engage the Chapter I prohibition. For example, an exclusive licence to data could restrict competition, particularly if the data set cannot easily be replicated, and the exclusivity granted under the licence is perpetual or for a substantial number of years. Section 9 of the Competition Act provides a general exception to the Chapter I prohibition. A safe harbour also exists for some data-sharing agreements by a set of block exemptions,

39 For a recent summary of the principles and main authorities from which the doctrine arises, see *Harcus Sinclair LLP v. Your Lawyers Ltd* [2021] UKSC 32.

40 See, for example, *Jones v. Ricoh UK Ltd* [2010] EWHC 1743 (Ch), in which an obligation not to deal with certain parties while in possession of confidential information was said to be likely to engage the doctrine.

such as the Technology Transfer Block Exemption (TTBE).[41] To benefit from the TTBE, the raw data provided under the licence would need to qualify as know-how under the TTBE:

> *a package of practical information, resulting from experience and testing, which is (i) secret, that is to say, not generally known or easily accessible, (ii) substantial, that is to say, significant and useful for the production of the contract products, and (iii) identified, that is to say, described in a sufficiently comprehensive manner so as to make it possible to verify that it fulfils the criteria of secrecy and substantiality*

To benefit from the TTBE, an agreement should also not contain any of the hard-core restrictions listed under Article 4 of the Technology Transfer Block Exemption Regulation and the parties' market shares must be below the relevant thresholds set out therein.

A strategy for protecting data in data-sharing deals

Drawing together the strands discussed above, a successful strategy for protecting proprietary data in data-sharing deals will include the following steps.

- Which legal rights apply? Assess the legal rights that can be used to control access, use and dissemination of the particular data set that will be shared. These rights will depend on the nature of the data, the circumstance in which the data has been generated or collected and the way in which the data will be shared. They can also vary between different jurisdictions. Understanding the legal rights that can be used to protect the data will inform the subsequent steps in the strategy.
- Decide how to apply each of the four dimensions of control over data sharing. Form a clear view about who can access the data, what data they can access, how they access data and what they can use the data for. Decisions regarding each issue should be considered as early as possible in a data-sharing deal. Successful data sharing is most likely to happen where control issues have been considered in advance of engaging with potential data-sharing partners and are informed by the organisation's data strategy.

41 Commission Regulation (EU) No. 316/2014 retained in UK law as a result of Section 3 of the European Union (Withdrawal) Act 2018 and the Competition (Amendment etc.) (EU Exit) Regulations 2019.

- Implement decisions regarding control through technical measures and contractual arrangements that reflect the legal rights in the data. Decisions regarding control of data are implemented through technical and legal means. Contracts should reflect the underlying legal rights in the data and implement decisions regarding the four dimensions of control. Clauses dealing with use limitations, the status of derived data and metadata, audit rights and post-termination obligations will often be key points of control. Contractual terms will also need to be drafted with an eye to restrictions on contractual terms, including the restraint of trade doctrine and competition law.

TOBY BOND
Bird & Bird

Toby Bond is an intellectual property (IP) solicitor in Bird & Bird's London office specialising in high-tech patent, trade secrets and copyright litigation and the practical application of IP rights to data and artificial intelligence systems. He is a member of the International Association for the Protection of Intellectual Property (AIPPI) Standing Committee on Digital Economy and a member of council for AIPPI UK. Toby is also the co-author of the UK chapter of Thompson Reuters' *Trade Secrets Throughout the World* and the author of the UK chapter of Kluwer's *Law of Raw Data*. He is a tutor in patent law for the University of Oxford's postgraduate diploma in intellectual property law and practice and was named one of Global Data Review's '40 under 40' data lawyers in 2021.

Bird & Bird

Bird & Bird is an international law firm with a focus on helping organisations being changed by technology and the digital world. With more than 1,400 lawyers in 30 offices across Europe, Africa, the Middle East, Asia-Pacific and North America, we're ready to help you wherever you are in the world.

12 New Fetter Lane
London, EC4A 1JP
United Kingdom
Tel: +44 20 7415 6000
www.twobirds.com

Toby Bond
toby.bond@twobirds.com

Data is not just a source of regulatory risk: it is a vital asset for almost every type of organisation. Whether exploited as a core part of a business model, kept confidential during the development of a new product or processed with the care required by personal data regulation, information is now a board-level concern. GDR's *The Guide to Data as a Critical Asset*, edited by Mishcon de Reya partner Mark Deem, offers a unique approach to data that helps steer companies through their gathering, exploitation and protection of all types of data – whether personal or not – and looks at data as an asset class that is increasingly important across all industries.

Visit globaldatareview.com
Follow @GDR_alerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-859-8