



# The Data Economy: How does it impact my business?

MARCH 2021



# If data is the new oil, then what does that mean for my business?

First, we need to explore: 1. what is data in my business? 2. how it is legally protected?, and 3. how in my business do I derive value from it?

## WHAT IS DATA?

Data is essentially information. It can be raw data, information about customers, suppliers or other information, it may be more formal such as trade secrets or confidential information about business processes and procedures, databases, insights or forms of intellectual property such as databases or software code.

Often businesses assume data is regulated and protected in the same way as other intangible property such as intellectual property – this is generally not the case, which provides both opportunity and risk.

The task of cataloguing your data can help identify risks and opportunities of participating in the digital economy. Once data is mapped then opportunities to extract value can be explored.

Unlike physical property, which can only have one owner and be in one use at a time, data can have multiple stakeholders who contribute to its commercialisation and exploitation. This necessarily creates a complex value chain such that the legal concepts and rules conceived for traditional types of assets cannot be easily applied to data.

## HOW IT IS LEGALLY PROTECTED?

Much data is not protected unless it is subject to specific contractual provisions with the persons contributing to the data. Data that forms recognised intellectual property, such as copyright, will be subject to protection.

Some regulation also affects certain types of data. Privacy regulation, for instance, is increasingly covering the uses of “personal information” when it is merged with other data in order to provide insights. The penalties for misuse of personal information are increasing, and making it cost efficient for businesses to develop privacy

compliant data management systems to ensure they only exploit legal uses.

If you are buying or selling a business, understanding what rights come, or do not follow, data acquired is a key due diligence issue.

## HOW IN MY BUSINESS DO I DERIVE VALUE FROM IT?

If your business has collected, aggregated, analysed or transformed data, there is likely to be a market for it. If it is raw data or data that has been enhanced in some way, you may ask for a higher price. Provided that if the data set contains personal information you have the authority of the individual to use that data, your insights may be valuable to others, and able to be monetised. Think for example of the woman in West Australia who owned a hair salon. Tired of the staff not getting all of the daily tasks done in the right order – unlock the door, turn on the lights when you arrive, turn off the lights at the end of the day, lock the door behind you as you leave – she documented every daily and weekly task, and then licensed the “manual” and never actually had to work again.



# How is my **data** protected as a business asset?

Generally, it is up to you, but keeping information confidential is a start and this can be managed by contract, staff training and ensuring you have appropriate processes in place.

## WHAT ABOUT DATA SHARING?

Collaborating with other organisations is one way to get value from your data. As long as both parties have clear rights to share the data they hold this can be a way to unlock new income streams. Again you need to be wary of personal information, and if information is anonymised or de-identified, you need to be sure on this point.

Within the government sector, policy and legislation increasingly promotes the inter-departmental sharing of data to optimise efficiency and improve government services, policy and decision-making. With greater sharing of data, including personal information, government agencies must mitigate new and specific risks. Agencies must take particular care to ensure the security of data-sharing arrangements, including anonymization of datasets, and to clarify the particular data protection responsibilities as between the participating government agencies.

## WHAT ABOUT PRIVACY LAWS?

The introduction in 2018 in Europe of the General Data Protection Regulation (**GDPR**) with extraterritorial reach meant many businesses who dealt with multinationals were contractually obliged to uplift their privacy and data security compliance. That came with a cost. It also brings a competitive advantage once done to reduce transaction friction with other GDPR regulated entities and to promote consumer trust. The work done in data mapping and working through how data is used in the organisation provide insight into the possible opportunities for that data to be leveraged, in a way that manages risk.

As regulators increase restrictions on data collection and use in an effort to achieve better consumer privacy outcomes, there is a corresponding increase in regulatory interest in

giving consumers greater control of their own data through data portability.

## IS THE CDR RELEVANT TO ME?

The Consumer Data Right (**CDR**), introduced by the Australian Competition and Consumer Commission in 2020, is a pilot data portability regime designed to give consumers greater access to and portability of their own data in various markets, starting with the banking sector. The Open Banking aspect of the CDR enables consumers to conveniently port certain data accumulated by their incumbent bank to a new financial service provider. The regime is designed to reduce switching costs for consumers of banking services which will ultimately stimulate competition and promote consumer choice of service providers.





### WHAT ABOUT COMPETITION LAW?

As is slowly happening globally, the power of big data holders is being recognised and slowly regulation to ensure that power is not misused is being introduced. In Australia, there are moves by the competition and consumer regulator to regulate privacy and personal information under consumer protection laws.

### EMPLOYMENT AND WORK?

Australia's privacy laws exclude employees, but not contractors, and where workers are outsourced, issues can arise. Laws relating to surveillance also vary by state. The temptation to introduce technology to monitor and reduce costs may be appealing but may also be risky. We have seen one major case on biometrics information and given the increasing awareness of privacy and surveillance, employers are cautioned to weigh up potential short term efficiency enhancements from tracking and monitoring against reputational damage and risk of backlash. If you deal with GDPR compliant companies, they will take a dim view of relying on some very unusual Australian exceptions to privacy, and it may breach the terms of your contracts with them.

### AUTOMATION AND AI

Increasingly technology is undertaking routine tasks previously done by humans. This is a whole separate area of opportunity and risk where contractual rights need to be clearly understood

and any interaction with privacy regulated data needs to be both understood and communicated to consumers.

### INFRASTRUCTURE – “SMART” EVERYTHING

The tendency to use data and insights to reduce costs and create efficiencies as well as to increase revenue by monetising datasets is increasing. Many services can operate more efficiently with insights gleaned from smart infrastructure and opportunities abound for both service providers and for the planning and development of commercial, residential and industrial infrastructure, as well as the location of goods and services.

### DISPUTES – VALUE AND OWNERSHIP

The very nature of data, being intangible, makes it difficult to prove ownership, and many stakeholders may have many claims to the same data – some in conflict and some not. As businesses continue to rely on data for insights for revenue streams and cost reductions, all data becomes more valuable and worth arguing over, and disputes follow. In the US there have been several cases over “data scraping” where businesses “scrape” publicly available data from many websites and then aggregate, analyse and monetise – with no returns to the sites that provided the base data. We can expect these cases and others, where misuse of data provided for one reason is used for a different purpose, to increase, and for claimants to use more novel ways of establishing their claims.



# Key contacts



**Angela Flannery**  
Partner *Sydney*  
T +61 2 8083 0448  
angela.flannery  
@holdingredlich.com



**Lyn Nicholson**  
General Counsel *Sydney*  
T +61 2 8083 0463  
lyn.nicholson  
@holdingredlich.com



**Andrew Hynd**  
Partner *Brisbane*  
T +61 7 3135 0642  
andrew.hynd  
@holdingredlich.com



**Trent Taylor**  
Partner *Brisbane*  
T +61 7 3135 0668  
trent.taylor  
@holdingredlich.com



**Dan Pearce**  
General Counsel *Melbourne*  
T +61 3 9321 9840  
dan.pearce  
@holdingredlich.com



**Georgia Milne**  
Senior Associate *Sydney*  
T +61 2 8083 0423  
georgia.milne  
@holdingredlich.com





CONTACT US

**SYDNEY**

Level 65  
MLC Centre  
19 Martin Place  
Sydney NSW 2000  
GPO Box 4118  
Sydney  
NSW 2001  
T +61 2 8083 0388  
F +61 2 8083 0399

**MELBOURNE**

Level 8  
555 Bourke St  
Melbourne  
VIC 3000  
GPO Box 2154  
Melbourne  
Vic 3001  
T +61 3 9321 9999  
F +61 3 9321 9900

**BRISBANE**

Level 1  
300 Queen St  
Brisbane  
Qld 4000  
GPO Box 490  
Brisbane  
Qld 4001  
T +61 7 3135 0500  
F +61 7 3135 0599

**CAIRNS**

Level 1  
Cairns Corporate  
Tower 15 Lake St  
Cairns Qld 4870  
PO Box 4766  
Cairns  
Qld 4870  
T +61 7 4230 0400  
F +61 7 4230 0499