Financial Rights
LEGAL CENTRE

Privacy practices in the general insurance industry

April 2022

Roger Clarke and Nigel Waters, Xamax Consultancy

Contents

Foreword

The collection, use and handling of data is the bread and butter of the insurance industry and, in fact at the heart of the very concept of insurance. Long before the development of a Consumer Data Right, well before the increased availability, access and use of consumer data arising out of the digital revolution, the insurance sector has *from its inception* been collecting and analysing consumer data to quantify risk in order to help consumers protect themselves from the financial consequences of misfortune.

> *If any sector should know how to handle consumer's personal data – the insurance sector should. But do they?*

This was the basic question that arose in considering the application of the Consumer Data Right to the general insurance sector.

Our report *Open Insurance: The Consumer Data Right* in Insurance identified some privacy issues that could potentially arise from the application of the Consumer Data Right to insurance and recommended that we undertake further work to identify those privacy risks that may arise. However to do so we thought it important to examine the status quo – to identify the current privacy practices of general insurers and the risks that are arise now - in order to set a benchmark upon which to examine any potential future concerns once consumer data became more easily available and portable.

The result of this examination is the fourth and final report in our series looking at the future of insurance: *Privacy Practices in General Insurance*. This report is divided into three sections – firstly, a desktop analysis of current general insurance data practices and safeguards; second, field research into the exercise of the access rights that individuals have to their own data held by insurers and the Insurance Reference Service, and finally, a consideration of the potential privacy risks that may arise in applying the CDR regime to consumer data in insurance.

The resulting findings are a cause for concern.

The report identifies a series of problems including a lack of transparency as to who it is that policyholders are sharing their data with (is it, for example, the insurance brand, the insurance group or a whole ecosystem of interrelated bodies) and the stance taken by the Insurance Reference Service that it is not responsible for complying with correction rights in respect of *My Insurance Claims Report*.

When our researchers actually assisted consumers to go through the process of obtaining their own data from both their insurers and the Insurance Reference Service, even more issues arose.

> *The quality of the data obtained was highly questionable - every My Insurance Claims Report examined included at least one error in it, be it incorrect addresses, missing claims, additional claims or missing or misleading data. The reports also featured inconsistent or misleading claims descriptions and statuses, included personal information unrelated to insurance at all, and no explanation of the terms used to assist in comprehensibility.*

> *Even the process of obtaining a My Insurance Claims Report was difficult, convoluted and confusing with consumers forced to have to 'apply' for an application form, which was in the form of a word document that was extremely difficult to read and fill in. Obtaining a report took up to 30 days. All this for the cost of $22 each.*

Obtaining information from insurers was just as opaque and difficult, with varying amounts of information provided, information provided that was inconsistent to that provided by the IRS and little in the way of assistance to explain what participants were given.

In the context of these issues, the report subsequently provides a useful analysis of the likely issues that will both carry over from current privacy practices but also new issues that are likely to arise – including concerns over CDR joint account consent rules that may exacerbate issues in family violence.

We hope that the insights collected and recommendations by Roger and Nigel assist the sector to better transition to the new world of 'Open Finance' and build strong privacy and data handling protections from the start. The application of the CDR to general insurance is a unique once-in-a-generation opportunity to improve privacy practices and data standards to improve outcomes for both insurers and consumers.

Thank you again to ECSTRA for providing the funding for Financial Rights to undertake this work - without which it would not have been undertaken. A big thank you to Xamax Consultancy and in particular Roger Clarke and Nigel Waters. Thank you again to Drew MacRae, Senior Policy and Advocacy Officer for managing the project and the Future of Insurance series, Michael Kelly for research assistance and a final thank you to Andy Lewis of Studio Shapes for the great design.

Finally – our series of Future of Insurance reports has made it clear that the CDR holds great promise to solve many of the issues long faced by consumers of general insurance. But it is important that we get it right. We ask that industry and government heed the recommendations in this report, and our previous three reports, to ensure that consumers are the real winners out of the Consumer Data Right and that the insurer consumer risk mitigation partnership is significantly improved. Without this important preparatory work, the introduction of CDR is likely to involve significant costs and deliver no meaningful benefits.

Karen Cox
Chief Executive Officer
Financial Rights Legal Centre

Executive Summary

The general insurance industry provides insurance cover for consumers in relation to their homes, home contents and motor vehicles, and for other visible and invisible assets. Insurers require the provision of a considerable amount of personal data in advance of issuing a quotation, and require that information to be comprehensive and accurate. They may decline claims if they later discover material inaccuracies in the information the consumer provided.

Consumers have an interest in disclosing sufficient and accurate information, in order to gain cover, and to ensure their claims are paid out. They also have an interest in the protection of data about themselves, and in fair dealing by the insurer.

The Financial Rights Legal Centre **(Financial Rights)** represents the interests of consumers across the financial services sectors, including in general insurance.

The Australian Government announced in November 2017 its intention to introduce a Consumer Data Right **(CDR)**. It is being rolled out sector by sector. The stated objective of the CDR is to increase the flow of personal data within sectors. This the government anticipates will generate greater competition among providers, reduce costs and lead to better service to consumers.

The CDR has been first applied with the intention of achieving “open banking”, but progress has been slow. The scheme is being extended to the energy and telecommunications sectors. The government is also now working toward what it calls “open finance”, including general insurance.

In preparation for the expansion of the CDR to "open insurance", Financial Rights commissioned a study of consumer privacy in the general insurance industry.

The study comprised three linked segments.

The first segment was an examination of the general insurance industry, with an emphasis on the current data practices and privacy safeguards of key players in the industry

The second segment complemented the desk analysis with field research, whereby the access rights of individuals were exercised to ascertain and access data held about them by their insurer. The purpose of this was to document the quality of the data held by insurers, and the practicality of the processes by which that data is accessed.

The third segment of the study considered how the implementation of CDR might affect both data quality and services to consumers. The CDR's ongoing fluidity meant it was not possible to refer to established laws and procedures. Hence it was necessary to track changes, interpret intent, and then consider how the practices might be implemented in general insurance.

A number of privacy issues of considerable concern were discovered as a result of this analysis.

The law imposes a duty on consumers “to take reasonable care not to make a misrepresentation to an insurer”. The structure of the industry, including the widespread incidence of multiple brands which have common ownership and/or backend services, causes confusion as to which organisation a consumer is actually insured with. Processes for the investigation of claims, and criteria for the refusal of claims, are areas of considerable consumer dissatisfaction. The operation of the Insurance Reference Service **(IRS)** – the existing industry scheme for sharing personal data – gives rise to

multiple concerns. Processes and criteria applying to joint accounts also give rise to a great deal of dissatisfaction, and to safety concerns.

To date, little evidence has been available regarding the quality of the data held by insurers and the industry's shared database. The sample gathered as part of this study reveals many examples of low quality, in terms of the data held both by insurers and in the shared database, and in the processes used by the industry in handling data.

Although the sample was small, the experiences were consistent. Not only is data quality low, but it appears that some industry players are in material breach of their obligations in relation to subject data access and correction rights. Every IRS report acquired during the study contained at least one error. Accessing IRS reports commonly took 4-6 days, and getting data from insurers was even slower and more arduous. This throws into serious doubt the legitimacy of the claim that consumers can ensure the accuracy of their representations to insurers by accessing data about themselves held by insurers and/or the shared industry database.

The prospects appear very limited of CDR in general insurance leading to material savings for consumers in the form of reduced premiums. If CDR is to be of value to consumers, it must drive substantial improvements in the quality of industry processes and in the quality of data handled by the industry, as well as deliver greater certainty of outcomes in relation to the handling of claims. This Report makes a series of specific recommendations, whose adoption by the general insurance industry would achieve those results, and without which CDR in general insurance is very likely to be valueless to consumers, and harmful to their interests.

1. Introduction

1.1 THE CONTEXT

The financial services industry performs many functions which consumers depend on for everyday living including transaction accounts, debit and credit card transactions, Internet banking, loans and term deposits. Consumers understand that in order to perform these functions and protect their privacy and assets at the same time, service providers need information about their customers. Interests that consumers want to protect include access to services, reasonable terms of service, reliability of service and ensuring the reasonable handling of data that is held about them.

Insurance is a category of financial service. Its purpose is to recompense consumers for losses suffered as a result of some kind of adverse event. The "general insurance" sector offers cover against a wide range of risks, particularly risks to property. The two largest segments are home and contents, and motor vehicle insurance.

For the sector to operate, insurers need to be able to manage risks that they are exposed to, such as the clustering of risks as a result of weather events. Insurers therefore seek to avoid under-quoting fees for their services. This can arise from inadvertent non-disclosure or mistaken disclosure by the consumer of information relevant to an insurer's assessment of risk. Beyond unintended misinformation, insurers must detect and deal with instances of intentional non-disclosure or misrepresentation by consumers when taking out a policy or when claims are made.

Consumers are concerned that insurers offer insurance and quote prices that are reasonable in the circumstances, process claims fairly, and handle personal data appropriately. Because of the diversity of circumstances and the substantial difference in market power between large corporations and individual consumers, insurance law, institutions, policies and practices have been developed to address consumer interests including privacy.

Several inquiries including those of Murray in 2014, Harper in 2016, Coleman in 2016, Finkel in 2017 and the Productivity Commission in 2017 recommended the establishment of a right and associated standards whereby consumers could arrange for data held by financial service-providers about them to be transferred, in a useable format, to their provider's competitors. This aimed to reduce friction in the market, such as the barriers to supplier-switching, and thereby reduce prices, by greatly simplifying the acquisition of quotations and the creation of new contractual relationships.

The Australian Government initiated reforms in 2018 which require financial services sectors to implement the Consumer Data Right **(CDR)**. The first sector to implement the reforms was transaction accounts with banks, and the term 'Open Banking', which originated in the UK, was adopted. Enabling legislation was passed by the Australian parliament in August 2019. The "open banking" project progressed slowly during 2019-21. The next sector that was designated was energy **(CDR-E)** and work is underway to introduce it in the telecommunications sector **(CDR-T)**.

The Australian Government announced in January 2022 the expansion of the CDR to some datasets in general insurance, superannuation, non-bank lending and merchant acquiring. This Report considers whether, and how, sufficient benefits for consumers can be achieved from CDR in general insurance **(hereafter CDR-GI)** to justify the high costs of design, implementation and deployment.

1.2 THE CONSUMER VOICE IN THE CONSUMER DATA RIGHT

The Financial Rights Legal Centre **(Financial Rights)** has been active in representing the interests of consumers since the CDR was introduced. Financial Rights is a community legal centre specialising in financial services in areas including consumer credit, banking, debt recovery and insurance. It provides telephone assistance, financial counselling, and legal advice and representation. Financial Rights operates the Insurance Law Service, a national, specialist consumer insurance advice service. It also operates Mob Strong Debt Help, an Aboriginal and Torres Strait Islander-led service and the Credit and Debt Legal Advice Line.

Financial Rights has undertaken extensive research and investigations to understand the potential impact of the CDR on the general insurance sector. Its report *Open Insurance: The Consumer Data Right and Insurance in 2020* (Financial Rights, 2020) examined the benefits and risks of implementing the CDR in the general insurance sector that were apparent at that stage.

The report set out important recommendations relating to:

1. Issues with the implementation of open insurance that could reduce its benefits;
2. Risks of open insurance to consumers;
3. Risks associated with the impact CDR has on insurance markets;
4. Other broader issues with the CDR.

Two key recommendations were:

> **Recommendation 4:** *consumer advocates should work with government and industry to ensure greater consideration of how historical claims data is used and provided to consumers*
>
> **Recommendation 5:** *consumer advocates undertake further work to identify privacy risks that may arise from Open Insurance and monitor privacy risks as they arise under an Open Insurance regime.*

Financial Rights is continuing its research to further assess the impact of open insurance on consumers and to identify other reforms to improve outcomes and better reflect a genuine risk mitigation partnership between insurers and consumers. This Report provides further information arising from that ongoing research.

1.3 THE PROJECT METHOD

Financial Rights commissioned Xamax Consultancy Pty Ltd, whose team comprised Roger Clarke and Nigel Waters, to conduct a literature review, field research and analysis, and to prepare a report on current privacy practices of general insurers in the handling of consumer data and the risks that could arise from the application of CDR to general insurance. The project ran during the second to fourth quarters of 2021.

A preliminary study was undertaken of the history and current state of CDR in the banking sector. The purpose of this was to provide initial insights into the potential impact of introducing the CDR to

general insurance, and to assist in identifying measures that will deliver improvements in privacy law and practice in the industry.

The expectation had been that the deployment of open banking would be well under way, and that the law, policies and practices in relation to consumers' data would be stabilising and maturing. That proved not to be the case, with considerable changes and uncertainty, both during the study period and continuing into 2022. **(See Appendix 8).**

In parallel, a baseline study was undertaken of law, terms and conditions **(T&Cs)**, and practices in the general insurance industry in relation to consumers' interests generally, with a particular focus on privacy. **(See Section 2).**

That study was supplemented by empirical research into the data held by insurers – as evidenced by the data provided to consumers on request to the IRS, and provided by insurers to their customers on request. **(See Section 3).**

The final section of the study applied the available insights into CDR to examine the potential effect of CDR applied to general insurance. This aims to identify measures that could deliver improvements in privacy law and in data practices in the industry. **(See Section 4)**.

The report then draws conclusions, and identifies a number of recommendations arising from the study. **(See Section 5)**.

Where views are expressed, they are the views of Xamax Consultancy Pty Ltd, and do not necessarily reflect the views of Financial Rights.

2. Current consumer data practices of general insurers

This section commences with a brief overview of the general insurance industry, including both insurers and shared industry schemes, and data flows within the sector. It then outlines the regulatory arrangements relating to the data handled by the industry, with a heavy emphasis on privacy aspects. An array of outstanding issues is identified.

2.1 THE GENERAL INSURANCE INDUSTRY

This section briefly summarises the nature of the industry, and the scale and structure of the market.

2.1.1 The nature of the industry

The term general insurance is loosely used in Australia to distinguish a wide range of insurance services other than "life insurance" and "health insurance".

According to the Australian Prudential Regulation Authority **(APRA)**, the general insurance industry turns over about $50 billion per annum, of which each of the business customer and consumer segments accounts for around 50% (APRA, 2021). This project was concerned exclusively with the consumer segment of the general insurance industry.

The primary segments within the general insurance industry[1] are:

- **Building-related**, including home and contents, strata title and landlord's insurance;
- **Motor vehicle-related** including comprehensive, fire and theft only, third party property-only, compulsory third party and marine insurance;
- **Income-related**, including workers compensation, sickness and accident, consumer credit, mortgage protection, and lender's mortgage protection/mortgage guarantee insurance;
- **Expense-related**, including travel, funeral, pets and extended warranty insurance.

The home and contents and motor vehicle segments are each responsible for close to half of the turnover in consumer general insurance.

This report is concerned exclusively with the home and contents and comprehensive motor vehicle market segments. These are the key insurances with which the majority of Australians engage, and are typically financially very significant. Many significant privacy issues in relation to these products. Most of these privacy issues are likely to arise in many other forms of general insurance.

2.1.2 Market structure and market share

The operation of the insurance industry lacks transparency to consumers. **(See Appendix 1)**. This directly affects consumers' understanding of who they are sharing their data with, who holds their data and who has access to it.

1 Note that Health is included in some definitions of general insurance, but is not considered here.

The industry association for the general insurance industry, the Insurance Council of Australia **(ICA)** says its members represent approximately 95% of total premium income written in the industry. Its website identifies around 57 company-members and displays around 135 brand logos.

Many of these companies have sub-entities that project an image to consumers as though they were independent organisations rather than constituent parts of a conglomerate. Consumers expect that the name and logo reflect a standalone entity, and that the data they provide to that entity is for the use of that entity only.

Companies appear to arrange their business such that the name, logo and design-style are generally not indicative of the legal entity that the consumer is dealing with, but merely an image referred to using the business term 'brand', with the data commonly being claimed to be for the use of the entire conglomerate.

There is a moderate-to-high degree of market concentration in both segments, with industry publications suggesting that:

- In home and contents, the IAG and Suncorp groups each have more than 25% of the market, and the largest four groups may account for about 65% of the business; and
- In the motor vehicle segment, IAG and Suncorp have recently experienced a decline in market share because of increased competition to approximately 15% each, with QBE and Allianz reaching 10% each. These four groups appear to be writing about 50% of the premiums, but some newcomers such as Youi appear to be gaining market share.

It is challenging to reliably identify which brands the major groups control and in the case of many brands it is challenging to identify which group they belong to. It is also challenging to identify with which organisation the contract is being written.

For example, when a consumer takes out a policy with NRMA Insurance, the contracts are written in the name of Insurance Australia Limited **(AIL)**, rather than NRMA or even the holding company IAG.

Meanwhile, policies with at least AAMI and Apia are not written with AAMI, Apia or even the holding company Suncorp, but rather in the name of AAI Limited **(AAI)**. In the second quarter of 2021, a Dun & Bradstreet page[2] for AAI Limited referred to AAI as "Doing Business As" Royal & Sun Alliance Enterprise Insurance and offered vero.com.au as AAI's web-site. In January 2022, the Dun & Bradstreet page
appeared to have been updated but still pointed to vero.com.au. Vero's "Contact Us" page says "Vero is part of the Suncorp Network", but its "About" page does not mention Suncorp.

Elsewhere on the Vero site are mentions that the name Royal & Sun Alliance resulted from a merger in 1992, and that that company changed its name to Promina in 2003. However on another page it says: "Frowm early 2003 we [Vero] ceased to be part of the Royal & Sun Alliance Group". It also states that in 2007 Promina and "Suncorp Network" merged. AAI is mentioned on Vero's website, but only in page-footers, as copyright-owner.

A scan of the market in the second quarter of 2021 identified about 45 current brands. The ICA site displays 78 brand logos of members in addition to the corporate logos of its 57 members. It appears

2 Dun & Bradstreet, https://www.dnb.com/business-directory/company-profiles.aai_limited.da9dcff5cf1cb4de2c5f15650d7b2e84.html.

that the two majors are not the only companies marketing through more than a single brand.

It would require considerable assiduousness on the part of a consumer to understand which quotations are from brands in which group, and which company they are actually contracting with, and any number of constructions could be placed on the relationships among the flotilla of legal entities. This breeds confusion among consumers.

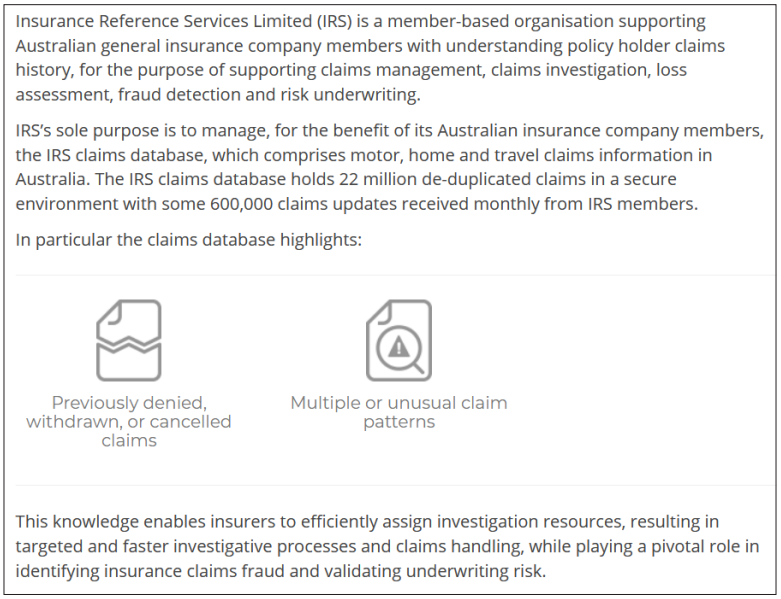
2.2 INDUSTRY-WIDE SCHEMES

Most of the larger members of the ICA are participants in at least one of two publicly-known services owned and operated by industry members on a shared basis. **(See Appendix 1).** In addition, insurers are effectively required by law to be members of a third scheme that handles complaints. **(See Section 2.4.4)**

2.2.1 The Insurance Reference Service Limited

The Insurance Reference Service Limited operates a shared insurance industry database. It was incorporated in 1989[3]. Its address is given as the premises occupied by ICA. The credit bureau and data company which styles itself as illion (hereafter Illion) has hosted and managed the IRS, on behalf of the IRS company, since late 2016[4]. Illion was formerly Dun & Bradstreet Australia. Prior to Illion, the IRS was administered by Veda (now known as Equifax) which included the service known as My Insurance Passport[5]. IRS currently describes itself as:

Figure 1. Description of the Insurance Reference Service[6]



3 ACN 003 890 613.

4 The Internet archive first records the site in March 2017. The sample report provided is dated August 2016: https://insurancereferenceservices.com.au/assets/DNBi%20IRS%20Individual%20Insurance%20Enquiry.pdf

5 http://web.archive.org/web/20160409194614/ http://www.myinsurancepassport.com.au/

6 Screenshot from https://insurancereferenceservices.com.au/, 9 June 2021

2.2.2 Insurance Fraud Bureau of Australia (IFBA)

The Insurance Fraud Bureau of Australia **(IFBA)** is not separately constituted, but has operated as part of the ICA since 2010. It is described as co-ordinating action against individuals committing insurance fraud in Australia. Details of IFBA's operations are not publicly known, nor is it known which insurers do and do not participate in information sharing initiatives under its auspices. An article in 2018 indicated that it had grown to 24 members[7].

IFBA is described by the ICA as follows:

Figure 2. Description of the Insurance Fraud Bureau of Australia[8]

Insurance Fraud Bureau of Australia

The Insurance Fraud Bureau of Australia (IFBA) is a working element of the Insurance Council of Australia established to help combat insurance fraud in all of its forms. IFBA is increasing the focus on combatting insurance fraud, working with police and other bodies to prosecute cases when identified.

What does IFBA do?

The specific mandate of IFBA is to execute information collection, sharing and analysis of insurance fraud information that facilitates insurance company action against insurance fraud, informs community decision making and law enforcement investigations activity; to reduce the incidence and impact of insurance fraud on honest policyholders.

Another page on the ICA website "Understand Insurance" further explains:

> *'[T]he IFBA receives information and allegations of insurance fraud from a variety of sources (anonymous and otherwise) and relays this information to the relevant insurer, which then takes whatever action the insurer deems appropriate. The IFBA does not undertake investigations'.*[9]

2.3 FLOWS OF PERSONAL DATA IN GENERAL INSURANCE

A visual depiction of the flows of personal data in general insurance industry business processes is in Figure 3. The purpose of this is to assist in visualising the data collecting, holding and sharing processes that occur within the industry. That in turn helps to ascertain what personal data-flows are necessary to enable services to be provided to consumers, and where items of personal data come from, go to, and are stored (Financial Rights, 2020, Section 2.2.3 and Figure 4, pp 13-14).

---

7 https://anziif.com/members-centre/the-journal-articles/volume-41/issue-1/insurance-underbelly
IFBA has at least two web-sites:
http://ifba.org.au, which redirects to the ICA's explanatory page about fraud
https://insurancecouncil.com.au/consumers/insurance-fraud/
http://www.ifbaintelligence.com/

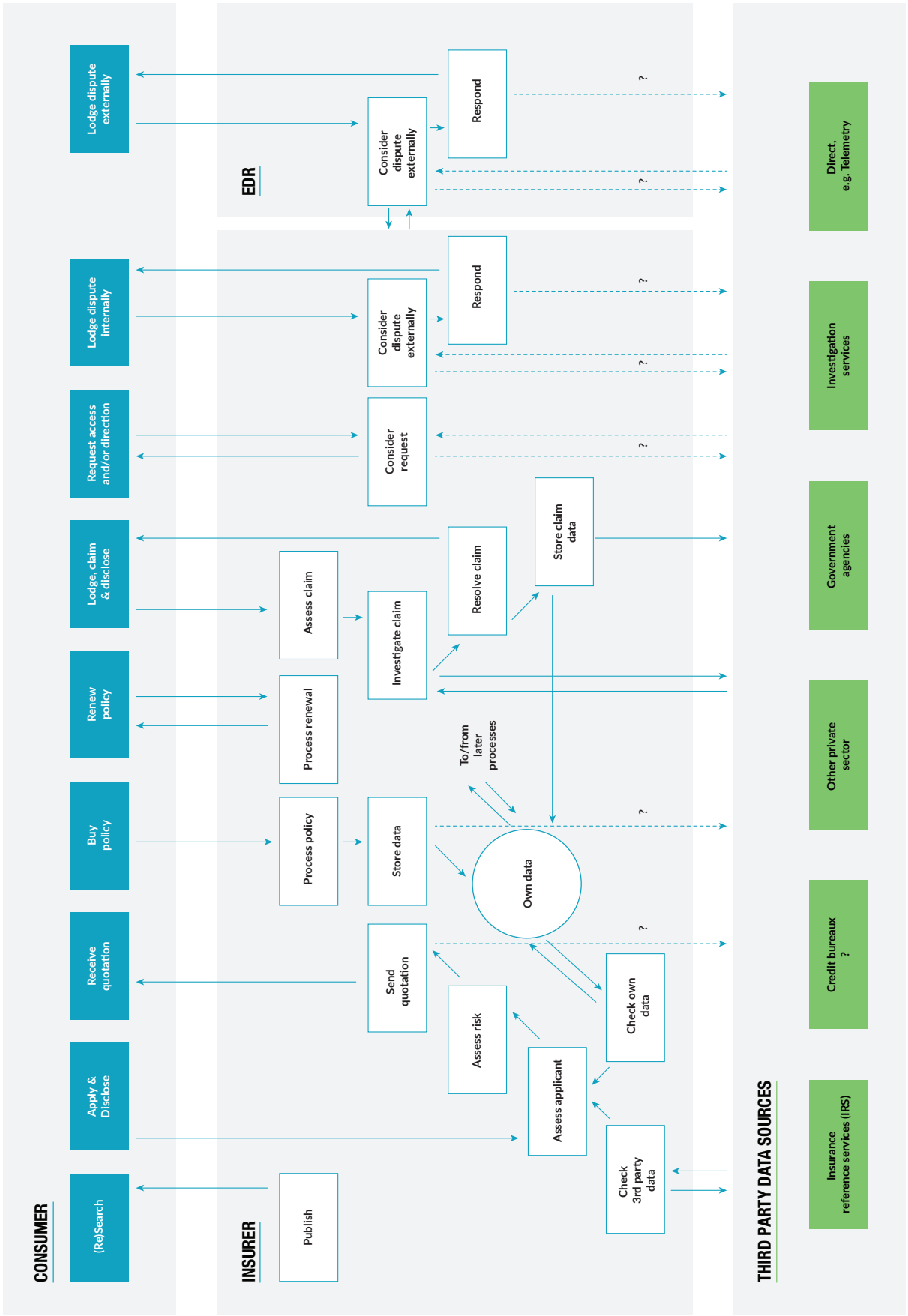
8 Insurance Council of Australia, (Accessed 9 June, 2021), https://insurancecouncil.com.au/consumers/insurance-fraud/.

9 Insurance (Accessed 13 June, 2021), https://understandinsurance.com.au/insurance-fraud.

The diagram at Figure 3 illustrates the following processes:

- The insurer publishes information, including product data, which can be accessed by consumers;
- A consumer applies to an insurer for cover, in the process disclosing a considerable amount of personal information, and providing one or more consents authorising further personal information to be acquired by the insurer from various third parties;
- The insurer acquires further data from their own data-holdings, shared industry schemes and/or third parties (involving disclosures by those parties), and uses the acquired data about the consumer and the consumer's request to assess the applicant and their risk profile. This leads to either a decline or a quotation sent to the consumer;
- The consumer may accept the quotation, in which case the insurer processes the transactions, stores data internally, and may pass the data to shared industry schemes and/or third parties;
- The consumer may lodge a claim and in the process disclose a considerable amount of additional personal information. The consumer may also provide one or more consents authorising further personal information to be acquired by the insurer from various third parties;
- The insurer acquires further data from their own data-holdings and in many cases from shared industry schemes and/or third parties (again involving disclosures by those parties), and uses the acquired data about the consumer and the consumer's claim to assess the claim, and where they judge it appropriate, to conduct an investigation. This results in a response to the consumer;
- On resolution of the claim, the insurer stores data internally, and may pass data to shared industry schemes and/or third parties;
- The consumer may submit a dispute into the insurer's internal dispute resolution process **(IDR)**. The insurer acquires further data from their own data-holdings and possibly from shared industry schemes and/or third parties, and uses the available data about the consumer and the consumer's concerns to assess the dispute, resulting in a response to the consumer;
- On completion of the dispute, the insurer stores data internally, and may pass data to shared industry schemes and/or third parties;
- The consumer may submit a dispute into the EDR process. The EDR entity acquires further data from the insurer, possibly also from their own data-holdings or from shared industry schemes and/or third parties, and uses the available data to assess the dispute, resulting in a response to the consumer and the insurer;
- On completion of the dispute resolution process, the EDR entity stores data internally, and may pass data to shared industry schemes and/or third parties; and
- At any stage, the consumer may apply for access to personal information about themselves that is held by any party, and may seek to have it corrected.

Figure 3. General insurance industry data flows



2.4 REGULATION OF PRIVACY IN INSURANCE

This section provides an overview of the regulatory environment within which the general insurance industry operates. The description:

- Commences with the regulatory basis in formal law;
- Considers supplementary industry self-regulation, and compliance and other measures by insurers; and
- Outlines complaints-handling mechanisms, at the levels of the insurer, industry bodies and regulatory agencies.

2.4.1 Privacy law

The general insurance industry has a long history of engagement with privacy, having adopted voluntary privacy principles in 1998 – three years before the *Privacy Act 1988* (the *Privacy Act*) came into effect in the private sector – in response to Guidelines issued by the then Privacy Commissioner.

Most businesses in the general insurance industry have been subject to the *Privacy Act*, since 2001.[10] Initially, the *Privacy Act* required compliance with a set of National Privacy Principles (NPPs). The insurance industry chose to develop a General Insurance Code of Practice which operated between 2002 and 2006 under the *Privacy Act*, with its own external dispute resolution and compliance committee.

Since amendments to the *Privacy Act* in 2014, the required standard has been the Australian Privacy Principles, which regulate the "life cycle" of personal information handling from collection through use and disclosure to storage and disposal. The Australian Privacy Principles also include standards for data quality and security and give individuals rights of access and correction. Table 1 reproduces the highest-level expression of the Australian Privacy Principles.

The *Insurance Contracts Act 1984* has a significant influence on what personal information is collected and processed by insurers, in particular through the duty of disclosure and related provisions of Part IV. The implications of the *Insurance Contracts Act 1984* are discussed under the relevant headings below.

Other laws that may be relevant in particular circumstances include:

- The *Disability Discrimination Act 1992* – including the partial exemption in Section 46 – and the categories of decision and of data involved. This is important since consumers frequently express concerns about insurers accessing information about various aspects of health (Australian Human Rights Commission, 2020);
- The *Corporations Act 2001* – including the obligation to act "efficiently, honestly and fairly" under Section 912A; and
- State or Territory privacy legislation, which may apply to some categories of general insurance (Insurance Council of Australia, 2016).

---

10 The legislation applies to business enterprises generally, with an exception for small businesses with less than $3 million annual turnover, and hence applies to most and probably all, insurers although not small insurance brokers for example.

Table 1: The Australian Privacy Principles[11]

APP1 - Open and transparent management of personal information: Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy

APP2 - Anonymity and pseudonymity: Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP3 - Collection of solicited personal information: Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of sensitive information

APP4 - Dealing with unsolicited personal information: Outlines how APP entities must deal with unsolicited personal information

APP5 - Notification of the collection of personal information: Outlines when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters.

APP6 - Use or disclosure of personal information: Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP7 - Direct marketing: An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP8 - Cross-border disclosure of personal information: Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP9 - Adoption, use or disclosure of government related identifiers: Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP10 - Quality of personal information: An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP11 - Security of personal information: An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP12 - Access to personal information: Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP13 - Correction of personal information: Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

2.4.2 Industry Self-Regulation

It appears that all members of the ICA may be subscribers to the General Insurance Code of Practice (the **Code**) (ICA, 2021).12

11 Privacy Act 1988 - Schedule 1 Australian Privacy Principles, http://www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/pa1988108/sch1.html

12 Insurance Council of Australia, Insurance Code of Practice (5 October, 2021) https://insurancecouncil.com.au/code-of-practice/. The ICA currently lists 47 insurers as signatories to the Code. https://insurancecouncil.com.au/code-of-practice/code-subscribers/ as at January 2022.

The current revision of that Code took full effect from 5 October 2021 and includes new standards for the investigation of insurance claims. These standards complement the relevant privacy principles. The complaint-handling provisions of the Code similarly complement the relevant provisions in the *Privacy Act*. **(See Section 2.4.4)**

2.4.3 Insurer compliance activities

Insurers' undertakings play a significant role in the protection of consumers' interests. These are generally expressed by means of:

- Privacy Policy Statements;
- Commercial terms of service;
- Product Disclosure Statements **(PDS)**; and/or
- The Code, where the insurer is a member of the ICA and a signatory to it, in which case the insurer has undertaken to comply with that Code.

Under the *Privacy Act* and Australian Privacy Principle 1.3, insurers are required to publish a privacy policy. In addition, their Terms and Conditions (often referred to as "Terms" or "T&Cs") may also include information relevant to privacy protection. Collectively these documents serve several purposes, including to:

- Satisfy the transparency and notice requirements of privacy law (including Australian Privacy Principles 1 and 5);
- Explain how the organisation seeks to comply with other requirements of privacy law (e.g. security and data quality, subject access and complaints handling); and
- Provide a basis under privacy law (including Australian Privacy Principles 6 and 7) for uses and disclosures of personal information – through a requirement for consumers to accept the Terms and Conditions and Privacy Policy as a pre-requisite for a service (in this case insurance cover).

This report presents extracts from the Privacy Policy Statements and T&Cs of one insurer. **(See Appendix 2)**. Deep analysis of the privacy policy statements and T&Cs of any insurer is very time-consuming. Hence we selected one well-known and well-established larger insurer, AAMI. Our experiences suggest that analyses of other insurers' documents would likely yield similar findings.

The analysis in this report demonstrates how difficult it is for consumers to understand who they are transacting with, what privacy-relevant protections and undertakings exist, and how likely it is that their interests will be protected. **(See Appendix 2).**

In AAMI's case, the names of multiple legal entities are evident in the documents (AAI, Suncorp, PetInsurance, Hollard, PetSure, TAL Dai-ichi). The confusion is compounded by the primary name used throughout being AAMI, which is a brand name, but is used throughout the documents as though it were the legal entity with which the consumer is entering into contract.

This sends conflicting signals to consumers. On the one hand, their data is for the purpose of a company called AAMI (but really AAI), but on the other hand their data is for the purpose of a "group" called Suncorp, presumably in order to justify the availability of that data to all or some of the

subsidiaries and brands within that group.

In order to work out what contractual T&Cs apply to the relationship with whichever legal entity or entities the consumer is dealing with, it would be necessary to pore over complex wording in up to half-a-dozen substantial and complex documents. These include at least the AAMI Privacy Policy (approximately 1,400 words) and Suncorp Group Privacy Policy (approximately 1,300 words), and AAMI's "Terms and Conditions" (over 15,000 words), as well as the Privacy Policy for the particular kind of insurance, and possibly also the relevant Product Disclosure Statement (more than 14,000 words).

Scans of the Policies and the T&Cs show that, while many of the provisions are mainstream and not greatly out of line with consumers' reasonable expectations, a number of provisions distinctly advantage the insurer, and would not be what a consumer would want.

Examples include:

- The apparent absence of any privacy-related options for consumers (i.e. opt-in or even opt-out choices for any specific uses or disclosures, including direct marketing);
- An apparent ambit claim in Term 30, seeking to allow any personal information gathered for a specific purpose to be used and disclosed for any purpose; and
- Another ambit claim purporting to authorise use and disclosure of data collected by one business by any and every business in the entire group.

2.4.4 Complaints handling

Where a consumer is dissatisfied with an aspect of their dealings with an insurer, they can raise their concerns with the insurer. Where the insurer is a member of the ICA and is a signatory to the Code, the insurer has an obligation to handle the complaint in accordance with requirements of Part 11 of the Code. The industry scheme's Code Governance Committee **(CGC)** reports annually on Code compliance and complaints.

If the consumer is not satisfied with the handling or outcome of a complaint, they can escalate the matter, or initiate a complaint about a breach of the Code, to the Australian Financial Complaints Authority **(AFCA)**.[13] The AFCA is a company limited by guarantee, comprising directors with industry expertise and consumer rights expertise, which performs an ombudsman function across the financial sector generally, acting as a non-statutory complaints-handler. It has some powers in relation to remedies, but is limited in terms of financial compensation.[14]

Under the *Privacy Act*, consumers can complain about breaches of the Australian Privacy Principles to the Office of the Australian Information Commissioner **(OAIC)**[15] which also monitors compliance through pro-active investigations or audits/inspections. AFCA also refers complaints to the OAIC that are privacy-related including alleged breaches of the Australian Privacy Principles. Many complaints involve both privacy and other issues. Those with a privacy element are processed by AFCA without formal recognition of that element. AFCA complaint statistics therefore understate the extent of privacy-related problems, including in the insurance sector.

---

13 Australian Financial Complaints Authority, https://www.afca.org.au/make-a-complaint.

14 Australian Financial Complaints Authority, https://www.afca.org.au/about-afca

15 Office of the Australian Information Commissioner, https://www.oaic.gov.au/privacy/privacy-complaints/.

The following summary provides an indication of the scale of recent complaints activities and of how limited the information is in relation to specific outcomes, the performance of individual insurers, and the discovery and rectification of systemic inadequacies:

- The most recent General Insurance Code Governance Committee Annual Report, for 2019-20, records 41,608 complaints of which the bulk were in motor retail (38%), home (32%) and travel (14%) (GICGC, 2021). 37,800 complaints were finalised during that year, with 60% found in favour of the subscriber (insurer) and 40% in favour of the consumer. As well as the complaints, Code subscribers reported 32,870 self-reported breaches, 5% up on the previous year (2018-19) but three times as many as in 2017-18, together with 112 additional 'significant breaches';
- An AFCA media release on 5 July 2021 reports 13,896 general insurance complaints received in 2020-21, but with an additional 2,115 against underwriting agencies. This compares with 19,000 general insurance complaints in 2019-20. The top grounds for general insurance complaints were claim denial (5,600 - up significantly from 3,000 in 2019-20), claim delay (3,100 - down from 3,500), claim amount (3,100 - down from 3,200) and service quality (1,200 - down from 1,400);
- AFCA introduced a new reporting tool "Data Cube" with data for 2020-21.[16] 13,805 general insurance complaints were received in the twelve-month period to 30/6/21 (20% of all complaints), 10.5% involving home insurance, 6.6% motor vehicles and 3.3% travel;
- In 2019-20, the OAIC received 2,673 complaints, of which 108 (only 4%) were classified as "insurance". This category did not make the "top ten" sectors in 2020-21. No more detailed breakdown of the issues raised in complaints is provided (OAIC 2020b, OAIC 2021).

Only a small proportion of insurance complaints expressly allege privacy breaches, but a significant proportion involve privacy issues or have a privacy related component – particularly data quality.

2.5 PRIVACY ISSUES IN GENERAL INSURANCE

In order to establish the necessary baseline for the study as a whole, it was important to identify the privacy issues that already arise in general insurance.

This section summarises the results of an analysis under the headings of the relevant privacy regulatory framework – the Australian Privacy Principles. The headings follow the typical stages of handling of personal information, from collection use and disclosure, storage and disposal, together with rights of access and correction, complemented by overall transparency obligations.

This section provides only a summary of the key current issues, prior to, and without reference to, any changes that may arise should an "open insurance" / CDR-GI movement eventuate. **(See Appendices 3 and 4).**

2.5.1 Open and transparent management of personal data

It is often difficult for consumers to comprehend complex T&Cs and to ascertain which entity they

16 Australian Financial Complaints Authority, https://data.afca.org.au/at-a-glance.

are transacting with. There are also problems with inappropriately inferred consent, particularly the difficulty of comprehending who it is that is collecting and using personal information. **(See Appendix A3-1).**

2.5.2 Data collection by solicitation

A substantial number of consumer concerns exist in relation to the gathering of personal data in general insurance contexts. Some of these arise from poor design of application forms, for example forms not making it clear which data collection fields are mandatory. Multiple specific concerns arise in the context of claims and their investigation. Examples include gaining access to social media and my.gov.au accounts, and uncertainty in relation to the handling of allegations of fraud on the IFBA reporting fraud page. **(See Appendix A3-3).**

2.5.3 Data use and disclosure, including for direct marketing

Concerns exist about the uses and disclosures of personal data in the general insurance industry. The concerns are particularly marked where the data is held only because of the duty of disclosure, and are exacerbated where the data is applied to marketing purposes extraneous to the relationship that the consumer considers they have with the insurer. **(See Appendix A3-6 and A3-7).**

2.5.4 Data quality

Data quality is an area in which many of the major consumer concerns in the general insurance industry arise, extending beyond privacy to effectiveness, fairness to individual consumers, and equity across categories of people. **(See Appendix A3-10)**. It has been a central focus of this assignment and is explored further. **(See Section 4)**.

2.5.5 Subject access, and data correction rights and obligations

It is vital, in an industry sector in which consumers are under an obligation to take reasonable care not to make a misrepresentation to an insurer, that these rights are supported by means of processes that are accessible, reliable and effective. **(See Appendix A3-12 and A3-13).**

2.6 PRIVACY ISSUES IN SHARED INDUSTRY SCHEMES

2.6.1 The Insurance Reference Service

This section provides only a summary of issues in relation to the IRS. **(See Appendix 5).**

2.6.1.1 The regulatory regime

The IRS has some similarity to a credit reporting database service. However, the IRS is not subject to the very detailed regulatory regime for credit reporting under the *Privacy Act* Part III, the *Privacy (Credit Reporting) Code 2014* (currently Version 2.1) and the *Privacy Regulation* (2013).

The operations of the IRS have been outsourced to a service-provider, Illion, which also operates credit reporting database services.

In respect of the conduct of credit reporting services, Illion is subject to the detailed credit reporting regulatory regime. However it is not subject to those provisions when it is performing services under contract to an industry association in the general insurance sector, except possibly if credit reporting information is accessed and used for the purposes of the IRS.

There is concern about multiple aspects of the current arrangements, as summarised below. **(See Appendix 5)**. In particular:

- It is unclear under what legal authority, and subject to what privacy protections, personal information is:
  - Disclosed by individual insurers to IRS;
  - Disclosed by IRS to IRS's service-provider, Illion;
  - Disclosed by IRS/Illion to insurers other than the insurer from which it was collected;
- It is unclear whether the service-provider is using personal information that it gains access to when performing its services to IRS for other purposes. This might be checking, or supplementing its holdings in, other shared industry databases and/or databases managed in support of its services to other clients;
- It is unclear how the provisions of the *Privacy Act* and the Australian Privacy Principles apply. This matters, because many of the customised protections afforded to consumers in relation to the industry information-sharing scheme for credit reporting are not available in the case of information-sharing in the general insurance industry.

2.6.1.2 Transparency

Understanding of the IRS is hindered by a lack of transparency. The IRS Privacy Policy[17] is ambiguous as to the purpose of IRS and hence the appropriate scope of the data it contains. There is reference to a "claims database" and most of the uses of the data by members clearly relate to "claims" but the IRS also contains details of enquiries and applications made by consumers. **(See Appendix 5-1)**. It is not clear why IRS needs to include so much data about the totality of an individual's interaction with insurers other than claims. This invites insurers to potentially draw adverse inferences from particular patterns of consumer behaviour, with the result that consumers could in effect be penalised for "shopping around" for a better insurance deal.

2.6.1.3 Data collection

There is a considerable lack of clarity concerning the practicalities of what data is provided about consumers to the IRS by insurers, to the IRS by other parties, from the IRS to insurers, and under what circumstances each category of data-flow occurs.

2.6.1.4 Data use and disclosure

There is a considerable lack of clarity about specifically which data-items are used, and in what circumstances, by (a) the IRS, (b) its service-provider Illion, (c) insurers it is disclosed to other than the insurer from which it was collected, and (d) any other parties to which it is disclosed.

Further, there is a considerable lack of clarity about specifically which data-items are disclosed by IRS, by Illion, by insurers other than the insurer from which it was collected, and by any other parties to whom it is disclosed, and under what circumstances each category of data-flow occurs.

17 https://insurancereferenceservices.com.au/privacy

2.6.1.5 Data quality

It is widely recognised that data quality issues exist, yet it is not apparent what, if any, quality assurance processes are in place. The IRS Privacy Policy fails to expressly address data quality.

2.6.1.6 Subject data access rights

The manner in which Australian Privacy Principle 12 has been implemented in relation to the IRS is of particular concern, with many process issues evident and serious inadequacies in the understandability of the data that is provided to consumers.

2.6.1.7 Subject data correction rights

Serious questions arise about the stance taken by the IRS that it is not responsible for complying with Australian Privacy Principle 13 in respect of the Insurance Claims Report part of its database, a stance that it takes on the apparently spurious grounds that it regards itself as simply a repository of that information which "belongs to" contributing insurers.

2.6.1.8 The complaints channel

The IRS Privacy Policy provides information about how to complain to IRS, and to OAIC. It does not mention that complaints can be made to the relevant insurer and to AFCA.

2.6.2 Insurance Fraud Bureau of Australia (IFBA)

IFBA receives information and allegations of insurance fraud from a variety of sources, anonymous and otherwise, and relays this information to the relevant insurer, which then takes whatever action the insurer deems appropriate.

The insurance industry is known to have sought advice in the past on privacy compliance issues raised by the informal information-sharing practices to combat insurance fraud, including the activities of IFBA. **(See section 2.2.3).**

Privacy compliance issues that may arise from information sharing for fraud control include:

- Difficulty in complying with the transparency and notification principles of privacy law when collecting fraud-related personal information;
- Difficulty in meeting the required threshold of evidence to invoke the law enforcement exceptions in use and disclosure principles;
- Quality control over suspicions and allegations of fraudulent conduct;
- Unwillingness by insurers to provide information about suspicions and allegations to the subjects of those suspicions or allegations; and
- Security over what is highly sensitive personal information.

Specific activities in relation to particular cases may need to be conducted without disclosures that could be reasonably argued to compromise an investigation and/or the potential prosecution of criminal offences or conduct of civil litigation.

On the other hand, there is justifiable concern about the operation of the IFBA without transparency in relation to its *modus operandi* and standards. There is a need to acknowledge and better protect the interests of consumers and those affected by the allegations and the subsequent actions by insurers.

3. Field research on data accessibility and quality

A project was undertaken to provide insights into:

- The processes whereby consumers can gain access to information about their previous claims; and
- The quality of the information that organisations provide to them.

This section provides background to that study, describes the method adopted and how the research was conducted, and reports the findings about the data and process quality evidenced by IRS and insurers.

3.1 BACKGROUND

Consumers have an interest in knowing what data all organisations hold about them and what is done with that data. However, the needs of consumers in the general insurance sector go much further than that.

The second Future of Insurance report on *Automating General Insurance Disclosure* published in October 2021 (Financial Rights, 2021b) explained the significant interest consumers have in obtaining accurate information concerning their insurance claims history.

Under insurance law, consumers have a duty to take reasonable care not to make a misrepresentation. This means that they must disclose to their insurer matters that are relevant to the insurer's decision to provide insurance.18 An important element of this is an obligation to disclose sufficiently comprehensive and accurate information about their prior claims against insurance policies.

When a policy is negotiated, the insurer is not obliged to check the accuracy of the information the consumer provides. The insurer is permitted to delay that check until a consumer makes a claim against a policy. In the event that, when they applied, the consumer did not (even if they could not) fulfil their disclosure obligation, they face the risk that the insurer may assert that the data provided with the application was incomplete or inaccurate, and deny the claim. The insurer might even deny a claim where the relevant information was already available to the insurer, in their own files or in the IRS database.

In response to this issue, after it was raised in the *Automating General Insurance Disclosure* report (Financial Rights, 2021b), the ICA has drawn attention to the existence of means whereby consumers can meet the reasonable care element of the legal obligation by paying a fee to access their *My Insurance Claims Report* from the IRS (Insurance News, 2021). **(See Section 1.6.1)**

18 *Insurance Contracts Act 1984*, Section 20B discussed in (Financial Rights, 2021b, pp 7-10).

Whether this is effective, however, depends on a number of factors, including:

- The extent to which data held by insurers is recorded on the IRS database;
- The comprehensiveness of such data as is held by IRS;
- The quality of such data as is held by IRS;
- The ease and speed with which IRS data can be acquired by the consumer; and
- The extent to which that data may need to be complemented by access to the data held by the consumer's previous insurer(s).

We accordingly conducted an empirical study whose purposes were to:

1. Gain meaningful insights into the quality of data in the general insurance industry, including in the IRS database and in the holdings of individual insurers, and the consistency between the data held respectively by insurers and IRS; and
2. Assess the processes by which consumers can gain access to insurance information, including the ease with which they can discover where to go and what to do, and the ease with which they can perform the necessary tasks, including the "consumer experience" and user interface factors.

The combination of these components was intended to provide baseline information about the extent to which existing systems in the general insurance industry serve consumers' needs. The study was undertaken during the second half of 2021.

3.2 RESEARCH METHOD

The approach adopted was that a sample of consumers requested access to data held by the general insurance industry about themselves. It was intended that each consumer perform five actions.

Table 2: Actions intended for each Participant

1. Access the data held by the IRS, by the participant acquiring their *My Insurance Claims Report*
2. Access the data held by the participant's current insurer(s), by them exercising their Australian Privacy Principle 12 subject access rights
3. Compare both sets of data against the participant's own records, memories and expectations
4. Compare the data held by each insurer against that held by the IRS
5. Where material errors are found, exercise their Australian Privacy Principle 13 correction rights

Three sets of participants were intended:

- **The three study-leads**
  A pilot application of the process provided initial insights into the nature of the processes, of the documents, and of the data and its quality.
  This enabled guidance to be prepared, sufficient that a project officer could provide effective support to the participants who were to perform the above set of five actions.

- **The first set of volunteers**
  These were colleagues, friends, family and acquaintances of the three study-leads. This group, as was the case with the study-leads, had only limited claims experience, but had a background in dealing with organisations. The benefit of this facet of the study was expansion of the sample of experience of process and product.
- **The second set of volunteers**
  This comprised clients of Financial Rights' Insurance Law Service **(ILS)** who had experienced difficulties with insurance claims processes. The intended benefit of this facet of the study was an appreciation of process and data quality in more problematic contexts.

The scope was limited to motor vehicle insurance (excluding compulsory third party personal insurance) and home building and/or contents insurance. This was based on these categories being the two largest market segments and the predominant forms of insurance recorded on the IRS database, as disclosed in the *My Insurance Claims Report*, and being likely to generate many more claims than other forms of insurance.

Each participant, supported by the project officer:

- requested their *My Insurance Claims Report* via the IRS; and
- requested information from their insurer or insurers directly.

The project officer:

- interviewed participants prior to them obtaining their information, to gain a picture of their understanding of their insurance claims history and their expectations of the process and the information to be provided by the IRS and their insurer;
- assisted the participant to work through the process to obtain their own information, particularly where they experienced difficulties;
- interviewed participants after they received their information, to:
  - assess the quality of the information held and record the participant's response to the information provided, including whether it reflected their understanding of their claims history; and
  - gather and analyse the insights obtained with respect to the quality of processes, key customer experience and user interface factors, and the quality of the data provided.

3.3 THE CONDUCT OF THE RESEARCH

The requests to insurers did *not* involve the straightforward exercise of well-established processes that had been anticipated. In most cases the participants encountered confusion, lengthy delays, and inadequate responses from insurers.

The delays, and the resources that had to be invested in the seemingly basic process of acquiring data, were such that both the available time and the available resources were expended, and the original plan could not be carried through to completion, in that:

- insufficient time and resources remained available to progress the final round of volunteers who had previously experienced difficulties in their dealings with general insurance industry;
- there was also no capacity to undertake the intended fifth action of exercising Australian Privacy Principle13 "data subject correction" rights in cases where material data errors were apparent.

A total of 18 participants more or less completed the first four actions, by accessing and evaluating data from the IRS and their insurers. The 18 participants comprised the 3 project-leads, 15 of the first set of volunteers, but none of the second set of volunteers. Many shortfalls arose, in all cases because of action or inaction by the IRS or the insurer.

3.4 FINDINGS RE THE IRS

The findings of the field research are outlined in this section in a series of subsections, with a substantial amount of supporting information. **(See Appendix 6, A6-1-A6-4 and A6-7).** This needs to be read in conjunction with the summary of the results of the desk review of privacy issues raised by IRS. **(See Section 2.6.1) and Appendix 5).**

3.4.1 Nature, purpose and legal basis for the IRS

The purposes, and the legal authority, for the collection, storage and disclosure of:

- insurance claims information;
- additional categories of insurance-related data, in particular enquiries and applications, and loss assessor/adjustor/investigator enquiries; and
- the extraneous data relating to bankruptcies, summons, judgments, commercial credit history, and directorships;

are unclear and opaque.

Further details are provided. **(See Appendix A6-1).**

3.4.2 Process quality

The process of obtaining a *My Insurance Claims Report* is difficult, convoluted and confusing. It involves far more steps than is justifiable for a simple request, and the information provided to guide the consumer through performing the process is poorly explained.

The steps are outlined in Table 3, and further detail is provided. **(See Appendix 6A).**

Table 3: Steps Necessary for a consumer to acquire a report from the IRS

1. Discover that:
   i) The general insurance industry operates a shared database
   ii) It is called Insurance Reference Services
   iii) A copy of the contents can be accessed by consumers, although, unlike the credit reporting scheme, for a fee, and
   iv) The relevant website is **https://insurancereferenceservices.com.au**
2. Go to insurancereferenceservices.com.au and click on Order *My Insurance Claims Report*
3. Click on <Order Now>
4. Be sent away from the IRS, without warning or explanation, to its outsourced service provider, Illion at **http://www.illion.com.au/insurance-reference-services/**
5. Provide your details (First Name, Last Name, Email Address and Contact Number) whereupon you are advised that "one of our friendly customer service representatives will be in contact with you shortly to talk through your order"
6. Wait to receive an email from irsconsumer@illion.com.au (generally within 24 hours) with an application form in a very poorly formatted Word .doc file and a request for two forms of identification
7. Fill in the form by either:
   i) Printing out the form and manually filling in the form and signing it; or
   ii) Filling in the soft copy word document by manually replacing text where required (the form is not designed to be filled in any automated way), and signing it
8. Scan two forms of identification including:
   i) Driver's licence, Passport, Birth Certificate or Proof of Age Card; and
   ii) A document issued by "an official body [sic] (such as a utility bill or a bank statement) ..."
9. Reply to the email from irsconsumer@illion.com.au including as attachments the filled-out application form and the two scanned documents
10. Wait for an email from irsconsumer@illion.com.au, including the *My Insurance Claims Report* – anywhere from 3 days to 30 days

Key issues that made the process difficult included:

- Consumers are required to "apply" for an "application" form;
- There is no acknowledgement of the request for the application form;
- The application form is a Word document, not an online form nor a fillable pdf;
- The Word document is extraordinarily difficult to complete using Word. Reasons include:
  - Boxes that need to be ticked or filled need to be cut and pasted out with the correct form of letter or numbers;
  - Filling in the Signature boxes requires cutting and pasting an image of one's signature – a completely separate and complex process to perform;
  - Inputting the credit card details is very difficult because the boxes provided are formatted in Wingding (a graphic not textual font), requiring that the font be re-set; and
  - The form is insecure, despite containing sensitive information;

- After the applicant gives up on the unusable form, they have to:
  - Have a printer available to print the form out, and fill it in manually; and then either:
    - » Have a scanner available to scan the completed form back in, and then attach the documents to an email; or
    - » Post the completed form to Illion's address in Melbourne;
- In any case, the form is very difficult to read, because it includes font sizes of 4, 5 and 6, and some are some coloured in grey;
- The form states that "Fields marked with an asterisk (*) must be filled in"; but it asks for a significant amount of detail, including the applicant's driver's licence number, current employer name and two previous addresses.
- This raises the question as to whether IRS and/or Illion may be motivated to gather additional information for inclusion in the IRS and/or other databases, on the pretext of needing it for the purpose of authenticating the applicant.

A selection of comments from participants included:

> *"Putting details onto the website and then receiving the form, then putting many of the same details into the application form and sending it back did not feel like a streamlined approach"*
>
> *"The whole process is confusing and unexpectedly clunky"*
>
> *"The type face was very small … I could not read it with my usual magnifying glass and so I got out my better magnifying glass, and I still could not read it."*

Obtaining a copy of one's own insurance claims data costs is not gratis, creating an additional procedural hurdle for every consumer, and a financial barrier for many.

No receipt was automatically offered, but where a request was made, in one case it took 69 days, a delay greatly in breach of the seven day requirement.

The time taken to obtain a *My Insurance Claim Report* was lengthy, with 24 hours just to obtain an application form, and then a further three to five days delay after a completed application was sent, and in some cases up to 30 days with multiple follow-ups necessary.

The failure to provide timely responses at the very least poses difficulties and barriers for consumers, and in some circumstances defeats the purpose of quickly and efficiently getting a couple of competitive quotations, in order to test the market.

Crucially, the nature of the process undermines the ICA's claim that consumers can satisfy their obligation to disclose sufficiently comprehensive and accurate information about prior claims simply by accessing their IRS report and using that as a basis for filling in application forms. Considerable detail about the problems with low process quality of the IRS service is provided. **(See Appendix A6-2).**

3.4.3 Data quality

Even after participants received their report, they remained unclear about the nature of the IRS service and the meaning of the data the report contains. It is seriously problematic that no explanation of the terms used is available, for example by way of a glossary. Because of the inconsistencies in the uses of terms, even experienced staff members of the ILS were unclear about the meaning of much of the IRS report content, and even worse, they were unable to interpret it.

Multiple issues that arose with data quality in the IRS reports were documented. **(See Appendix A6-3)**. These include:

- **Incorrect address details** – including the previous address being listed as the current address, and vice versa;
- **Claim descriptions were either incorrect or inconsistently described** – including one that featured two different descriptions from two different insurers for two incidents that were factually identical;
- **Claim status descriptions were incorrect or misleading** – including one that listed a claim as refused when it was withdrawn;
- **Additional claims listed** - three participants found additional claims incorrectly attributed to them;
- **Missing claims** - four participants were able to confirm omissions from the IRS report by comparing the IRS list with information obtained directly from their insurer;
- **Old claim not removed** – one participant's report included a claim that was more than 11 years old;
- **Net settlement and excess figures were missing** – for example, seven participants noted that at least one of their claims listed a "Net Settlement amount of $0" when this was not the case – as confirmed by information obtained from their insurer;
- **Third party recovery data missing** – two participants noted that their "Claims recovered from third party" incorrectly included the word "No";
- **No insurer inquiries listed** – this was despite at least one participant noting that they had made numerous enquiries searching for coverage after being denied coverage by their insurer;
- **No explanations provided for information and terms used** – no glossaries or definitions were provided
- **Confusing inclusion of the words "No record found in Illion bureau**" – with no explanation, despite the fact that the *My Insurance Claims Reports* include records and list claims;
- **Inclusion of "Other possible matches" information highly ambiguous** – with no explanation for the number 1 included in this field for two participants;
- **Inclusion of "Loss assessor/adjustor/investigator enquiry" information unclear** – with one participant listing the amount of $1 with no further explanation provided;
- **A claims count that is ambiguous** – with the two categories "Insurance claims" and "Claims with vehicle data" reading as distinct categories, whereas in reality the latter appears to be a subset of the former;

- **Inclusion of blanks in fields** – leaving the reader with no explanation as to whether this was deliberate withholding of data or absence of data in the database record;
- **No fault listed** – which raised concerns amongst participants who felt that this was relevant contextual information for their claims history.

Every *My Insurance Claims Report* accessed during the field research contained at least one error. Table 4 below lists the data errors that were identified in relation to each participant's data.

The problems are remarkable for their diversity. This applies not only to claims-related data, but also to data that, while insurance-related, is not associated with claims, viz. "insurer inquiries" and "Loss assessor/adjustor/investigator enquiry".

The IRS service evidences very poor fit to purpose, lack of clarity about data relevance, meaning, application and use, and unreliability of the processes of input, update and disclosure. In our view, it does not have the appearance of a scheme designed to serve its nominal purposes.

It appears very likely that, to the extent that insurers place any reliance on IRS, it misleads as much as it informs. In its current form, the data provided could be harmful to the interests of a proportion, and perhaps a significant proportion, of claimants against general insurance policies.

The low data quality further undermines the ICA's claim that consumers can satisfy their obligation to disclose sufficiently comprehensive and accurate information about prior claims simply by accessing their IRS report and using that as a basis for filling in application forms.

3.4.4 Data unrelated to insurance held by IRS

My Insurance Claims Reports include information that is unrelated to insurance including:

- Bankruptcies;
- Summons;
- Judgments
- Commercial credit history; and
- Directorships.

This is not disclosed in the IRS FAQ.[19] On the other hand, the IRS's Sample Report includes information on Bankruptcies, Summons and Judgments, declared as being from the "D&B Automated Court Data Feed", In many cases, this category is also incomplete or includes errors. For example, three participants found that at least one of their current or previous directorships was not listed in the report, and one participant found an error in their credit enquiry information which listed an enquiry for a loan for a substantial amount of money as $0. Further details are provided. **(See Appendix A6-4).**

Given the absence of relevance, the lack of any apparent legal basis for their inclusion, and the data's seriously low quality, we question why these categories of data exist, why the data is gathered, why it is disclosed to insurers, and why it retained in the IRS database and included in reports.

19 http://insurancereferenceservices.com.au/faq.

Table 4: Data quality inadequacies in IRS reports

Participant	Summary of Key Issue/s Identified
Participant 1	Claims type error, address error, net settlement and excess error, missing directorship
Participant 2	Incorrect address details, claim status mis-labelled as cancelled
Participant 3	Three claims missing, credit enquiry error
Participant 4	Net settlement amount and excess errors
Participant 5	Net settlement amount error, state of vehicle registration missing, third party recovery information missing
Participant 6	Directorship missing, inconsistent claims type description, other possible match listed with no explanation or details
Participant 7	Missing claim
Participant 8	Withdrawn claim listed, claim status incorrectly listed as paid
Participant 9	Enquiry listed as a claim, claim status incorrectly listed as closed
Participant 10	Net settlement amount and excess errors
Participant 11	Incorrect address details, claim status mis-labelled as closed, additional claim listed in error, net settlement amount and excess errors, other possible match listed but with obviously incorrect details
Participant 12	Two claims missing (previously included on Veda report)
Participant 13	Incorrect address details, claim status incorrectly listed as cancelled, inconsistent claims type descriptions, one claim counted as two, net settlement amount and excess errors
Participant 14	Incorrect address details, inconsistent and misleading claim type description, one claim counted as two, missing claim, net settlement amount and excess errors
Participant 15	Five claims missing, no excess listed, third party recovery information missing, the same name is listed on a policy claim multiple times

3.4.5 Failure of the IRS and Illion to fulfil their Australian Privacy Principle 13 obligations

On its "Contact" webpage,[20] the IRS denies any responsibility to amend consumer data that it holds. Specifically, it instructs the consumer to "contact your insurer who supplied the data to IRS", and

20 Insurance Reference Service, http://insurancereferenceservices.com.au/form/contact.

indicates its responsibilities relate only to "incorrect identity verification or identity matching".

On its FAQ page,[21] the IRS states that "Your Insurance Claims report will be updated within five days of the insurance provider submitting updated information". However, given the low process quality evident throughout this field research, we have little confidence in this assurance.

Further, Illion's covering email for the reports it provides to consumers says "Should you have any queries, please contact the relevant insurance company". This statement gives the reader the impression that the IRS is not subject to the Australian Privacy Principle 13 requirement that APP entities take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.

Moreover, it does not appear that there is any basis whereby either the IRS or Illion can lawfully adopt the position that it will not itself receive and appropriately handle Australian Privacy Principle 13 requests. Under *Privacy Act* Section 6.1, an "APP entity" includes an organisation, and under Section 6C, "organisation" includes "a body corporate … that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory".

Further, *Privacy Act* Section 6.1 says that an APP entity "holds" personal information *"if the entity has possession* or control of *a record that contains the personal information"* (emphasis added). A "small business operator" exception exists, but even if Illion's IRS operation fell under the financial threshold, the "APP entity" definition in Section 6(1) blocks IRS from claiming the exception, because IRS "discloses personal information about another individual for a benefit, service or advantage".

IRS and Illion each has an obligation at law under Australian Privacy Principle 13.1 to:

> *"Take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading,*
>
> *and must do that under two circumstances, where:*
>
> *(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading"; or*
>
> *(ii) the individual requests the entity to correct the information."*

Moreover, the OAIC's Guidelines are quite specific, at:

> *"13.10 Australian Privacy Principle 13 … applies to personal information that an APP entity 'holds'.* An entity 'holds' personal information 'if the entity has possession or control of a record that contains the personal information' *(Section 6(1)).*

21 Insurance Reference Service, **http://insurancereferenceservices.com.au/faq**.

> *13.11* …[where] an APP entity … has outsourced the storage of personal information to a third party …, the individual has a separate right to request correction of the information by the third party, *if the third party is an APP entity (emphases added) (Office of the Australian Information Commissioner, 2019)".*[22]

3.5 FINDINGS RE INSURERS

The findings of the field research are outlined in this section in sub-sections dealing with first process quality and then data quality **(See Appendix 6, A6-5-A7)**. This needs to be read in conjunction with the summary of the results of the desk review of privacy issues raised by insurers. **(See Section 2.5 and Appendices 3 and 4)**

3.5.1 Process quality

The approach adopted to acquiring information from insurers is outlined in Table 5. Insurers' processes were, however, inconsistent, opaque and difficult, and the work of the staff handling the request and/or the database-content was highly error-prone.

Some participants received little or no data, while others, particularly if they pressed hard and long, received a voluminous amount of information.

The information provided was generally difficult to interpret, and lacked a legend or other means of understanding what data-items are for, and what meaning their content is intended to convey.

Table 5: Generic process to acquire a report from an insurer

1. Search for the Privacy Policy of the insurer – either by searching on the home page of the insurer or via a search engine
2. Find a contact email, number or online form that appears to be the, or at least an, appropriate channel through which to communicate a request
3. Prepare and send an email to the privacy contact (or fill in the online form, or call).
   We drafted the following template to assist participants in obtaining information:
   To whom it may concern,
   I would like to request access to my information held by you in line with my right to access information under Australian Privacy Principle 12.
   Specifically I would like to request information regarding my claims history including:
   - *Any insurance claims*
   - *Any loss assessor/adjustor/investigator enquiries*

   Thank you
4. Receive an email acknowledgement
5. Await delivery of a substantive response
6. Follow up as necessary

22 Office of the Australian Information Commissioner, Australian Privacy Principle Guidelines (July, 2019), https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-13-app-13-correction-of-personal-information.

The obligation to provide subject access to data was enacted in 2000. It is perplexing that, two decades later, all eight operators in the general insurance industry that fell within the sample survey arguably failed to fulfil all the relevant legal obligations.

On the basis of the study undertaken, we do not consider that insurers are either fulfilling their obligations under Australian Privacy Principle 12, or respecting the OAIC's Guidelines in relation to that principle.

The reasons we draw this conclusion are as follows:

- If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information (Australian Privacy Principle 12.1).
- It is clear insurers hold large amounts of material on each insured, as evidenced by the provision of such material to some participants, but minimal amounts to others. This suggests that in at least some cases applicants are not being given all the information to which they are entitled;
- An organisation must respond "within a reasonable period after the request is made" (Australian Privacy Principle 12.4(a)(ii)). Some of the delays experienced by research subjects were unreasonable, at least if the information was needed to satisfy a duty of disclosure.

  Two decades after the law was enacted, it is in our opinion not credible for insurers and IRS to have not foreseen the needs for, and implemented procedures for:

  - Easy discovery of how to make an Australian Privacy Principle 12 request;
  - Convenient online application, such that consumers can quickly and easily submit their requests; and
  - Automated generation of information to fulfil the responsibility, such that review and despatch can result in prompt, simple delivery of clear information;

- If the APP entity refuses to give access to the personal information because of Australian Privacy Principle 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out reasons and mechanisms available to complain (Australian Privacy Principle 12.9).

  Multiple instances arose in which data was not provided, but the insurer's process failed to acknowledge that fact, and formally refuse access.

Beyond Australian Privacy Principle 12 itself, the OAIC Guidelines articulate what might be regarded as requirements, or at the very least the regulator's expectations:[23]

- Australian Privacy Principle 12 requires an APP entity to provide access to all of an individual's personal information that it holds (Australian Privacy Principle 12.13);
- An APP entity should endeavour to provide access in a manner that is as prompt, uncomplicated and as inexpensive as possible (Australian Privacy Principle 12.19);

---

23 Office of the Australian Information Commissioner, *Australian Privacy Principle Guidelines* (July, 2019), **https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-12-app-12-access-to-personal-information**.

- An APP entity is required by Australian Privacy Principle 1.4(d) to state in an APP Privacy Policy "how an individual may access personal information about the individual" (Australian Privacy Principle 12.20);
- An APP entity is required to ensure that any recommended procedure is flexible and facilitates rather than hinders access (Australian Privacy Principle 12.21);
- The entity must take reasonable steps to give access in a way that meets the needs of the entity and the individual (Australian Privacy Principle 12.70);
- The description of the complaint mechanisms available to an individual should explain the internal and external complaint options, and the steps that should be followed. In particular, the individual should be advised that:
  - A complaint should first be made in writing to the APP entity (Section 40(1A));
  - The entity should be given a reasonable time (usually 30 days) to respond;
  - A complaint may then be taken to a recognised external dispute resolution scheme of which the entity is a member (if any); and
  - Lastly, a complaint may be made to the Information Commissioner (Section 36) (Australian Privacy Principle 12.87).

In our view, many aspects of the guidelines do not appear to be being followed, by multiple insurers Further details are provided. **(See Appendix A6-5).**

The experience of one member of the project team, during July to October 2021, is indicative of the problems that can arise. The challenges set by both NRMA/IAG and AAMI/Suncorp would have been very likely insurmountable by most consumers, who generally lack the background, expertise and persistence required to access the information requested.

Details of the experience are provided. **(See Appendix 6B).**

Based on the experiences of the project-team and the 15 volunteers, it is clear that insurers are not handling requests in a manner that satisfies legal requirements, public expectations, and industry standards. Each insurer needs to:

- Establish an appropriate infrastructure and process for handling requests, whether or not they are formally framed as Australian Privacy Principle 12 requests;
- Train frontline staff to handle such requests;
- Train frontline staff to recognise when a request requires escalation, and where to refer it to;
- Train specialist staff to handle escalated requests;
- Establish an appropriate incident management system to ensure that all requests received are carried through an appropriate workflow and are appropriately completed; and
- Review their compliance with provisions of privacy law, from time to time.

3.5.2 Data quality

The field research also revealed major problems with the quality of data held by, used by, and disclosed by insurers. In particular:

- The information provided by insurers varied greatly but was in many cases minimal. Most participants were sent a standard pdf with basic information (for example a policy number, claim type and claim number) from their insurer or insurers.
- There was little consistency in the information that was provided. Table 6 provides some idea of the variability and low quality.
- Some participants received a voluminous amount of information that was difficult to read, understand and interpret. One participant received a 7mb pdf made up of 165 pages. Much of the information provided - in a series of screenshots - goes back to the 1990s. Another received four locked pdfs including one 7mb pdf of 147 pages.
- Importantly, half of the volunteer participants reported that they received no information at all about claims that they were aware had been made.

Further details are provided. **(See Appendix A6-6).**

The experiences of a member of the team **(see Appendix 6B)** provide additional examples of data provided to a consumer in materially inadequate form.

Data is documented that was evident in those cases in which screenshots were provided of online displays from the insurer's customer database(s). **(See Appendix 6C).**

The organisation and presentation of the data was difficult to understand, poorly formatted and structured. In our view, the data provided by insurers is not indicative of the conduct of systems analysis and design projects intended to fulfil the purposes of serving consumers' needs and achieving compliance with industry standards and the law.

In our view, it is untenable to claim that ordinary consumers could be expected to comply with their disclosure obligations by extracting claims information from each of their former insurers and providing that information to potential new insurers when seeking quotations.

Table 6: Information provided by four major insurers

	Insurer 1 (AAMI)	Insurer 2 (NRMA)[24]	Insurer 3 (RACQ)	Insurer 4 (Allianz)
Policy Holder Name	❌	❌	✅	❌
Policy Number	✅	✅	✅	✅
Cover Type/Policy Level	✅	❌	✅	✅
Risk Details/Address	✅	❌	❌	✅
Policy Inception Date	✅	❌	✅	✅
Period of Insurance	❌	❌	❌	✅
Last Policy Term	❌	❌	✅	❌
Cancellation Date	✅	❌	❌	❌
Date of Claim	✅	❌	✅	✅
Incident Date	❌	✅	❌	❌
Claim Number	✅	✅	✅	❌
Type of Claim/Incident Type	✅	✅	✅	✅
Total Payout	❌	✅	❌	❌
Claim Amount [25]	❌	❌	✅	❌
Fault	❌	❌	✅	❌
Excess	❌	❌	❌	❌
Claim Status	❌	✅	❌	❌

24 The information provided by Insurer 2 was not consistent, but rather varied considerably, from participant to participant. The information outlined above refers to the most information provided when one pdf was sent was sent to one participant, as opposed to an alternative experience of a basic email response.

25 It is not clear whether "Claim Amount" is the same as "Total Payout"

3.6 FINDINGS RE CONSISTENCY BETWEEN IRS DATA AND INSURER DATA

Where it was practicable, the examination and comparison of the information provided to participants by the IRS and participants' own insurer or insurers was also illuminating. In particular:

- Multiple participants identified claims information that was missing from or additional to that found on their *My Insurance Claims Report*. Seven participants were not provided with claims information from their insurer or insurers regarding at least one claim listed on their *My Insurance Claims Report*. Two participants identified claims in the information that they were provided by their insurer that were not in their *My Insurance Claims Report*. One participant with multiple claims found some claims reported on their IRS report, some different claims identified by their insurer, and other claims neither listed on their IRS or insurer information, all confirmed by other documents held by the participant;
- There was a lack of consistency between the claims type descriptions used in *My Insurance Claims Report* and insurer Information. For example, one participant had "Damage whilst Driven" listed for two claims on their *My Insurance Claims Report*. However the insurer listed these more precisely as "Insured Hit in Rear by Third Party" and "Insured Reversed into Third Party."

The degree of inconsistency between the two sets of records further underlines the inadequacy of the current data management arrangements in the general insurance industry and reinforces the concern among consumers that they are being subjected to industry practices that are not fit for their purpose. Further details are provided. **(See Appendix A6-7).**

3.7 SUMMARY AND CONCLUSIONS

This section has reported on field research undertaken in relation to process quality and data quality aspects of the performance of insurers and the IRS relevant to consumers. The sample was of necessity small, but considerable evidence was gathered showing that the quality is very low.

Tables 7 and 8 highlight key aspects of the problem

Table 7: IRS My Insurance Claims processes and data

Process quality issues

- The legal basis is unclear for the various aspects of data handling by IRS
- The nature of the IRS service and the report is unclear to users
- The process of obtaining a *My Insurance Claims Report* is unnecessarily difficult, convoluted and confusing
- A procedural and to some extent financial barrier exists, because obtaining one's own insurance claims data is not gratis
- The time taken to obtain a *My Insurance Claims Report* can be lengthy
- The IRS appears to refuse to receive or process Australian Privacy Principle 13 requests

Data quality issues

- No explanations are provided, making it difficult to understand report contents, and difficult to assess the possible interpretations of the information by insurers
- Every *My Insurance Claims Report* contained at least one error
- The nature of the errors in Reports was highly diverse
- Fault is not listed
- *My Insurance Claims Reports* include information that is unrelated to insurance
- Some of that extraneous information was found to be incomplete or to include errors

The Australian Privacy Principle 12 request processes operated by the two major insurance groups lack coherence, lack consistency, are not efficient and are not effective.

The industry is not providing consumers with suitable means to acquire information from their existing and prior insurers about the claims they have previously made on insurance policies.

The inadequacies of the industry's current practices are so serious that they undermine the scheme's claimed purpose. It cannot be relied upon even by such consumers as are assiduous enough to somehow find out about the IRS service and use it, on the assumption that they thereby fulfil their obligation to disclose sufficiently comprehensive and accurate information about their prior claims against insurance policies.

The effect of this is that a material proportion of consumers are paying for insurance, and depending on it for protection against financial risks, when the insurer is in a position to unjustifiably renege on what the consumer thought was a deal.

Table 8: Insurer processes and data

Process quality issues

- The process of obtaining information from insurers was opaque and difficult, and fell far short of the reasonable expectations of consumers 20 years after the subject right of access was enacted into law
- Instances of obstructionism arose that would defeat most consumers
- The information provided by insurers varied greatly but was in many cases minimal
- In multiple instances, no information was provided on claims for which the participant was in possession of documentary evidence
- On the other hand, some participants received a voluminous amount of information
- Multiple insurers appear to be non-compliant with various aspects of Australian Privacy Principle 12

Data quality issues

- The information was in general difficult to interpret, failing to fulfil the Guideline "must … give access in a way that meets the needs of … the individual" (Australian Privacy Principle 12.70)
- Some participants had sufficient information available to them that they could see omissions and errors in the claims information provided by their insurer
- There were instances of material inconsistency between the contents of the *My Insurance Claims Report* and information provided by insurers or available in consumers' own recordss

Maintaining records over a period of many years, and finding them when they are needed are likely performed well by only a small proportion of the population. Further, it is likely to be extremely difficult for time-poor, less financially literate, and disadvantaged consumers. Consumers whose claims are refused on these grounds appear likely to be among those for whom the financial consequences are the most serious. This raises questions about the fairness, equitability and appropriateness of current industry practices.

As a result, even the relatively careful consumer who learns about the IRS service, uses it, and relies on it, cannot be sure that their insurer will not unfairly or unjustifiably refuse claims, on the basis that the information provided at the time of application was in some way inadequate.

Even if the data in the industry-shared database were of adequate quality, consumers would still face significant difficulties, particularly those individuals:

- Who are insufficiently assiduous in their record-keeping and in their completion of applications for insurance;
- Who are not well-informed about their Australian Privacy Principle 12 rights;
- Who are unaware of the existence of IRS; or
- Who are insufficiently persistent in their pursuit of IRS and, where necessary, of current and previous insurers that are not IRS members, or that have failed to update the IRS database.

Those characteristics describe a great many people in all walks of life, but they are particularly common among disadvantaged groups, those with lower levels of financial literacy, and those with the least wealth, and hence those most in need of insurance coverage.

The current data access system operated by insurers and the industry is not fit-for-purpose.

Any insurer relying on the information obtained from the IRS is dependent on deeply flawed datasets. This has the very real potential to misrepresent the true state of each individual's affairs in the disclosure, claims, investigation or fraud identification processes. More broadly, this has potential to misrepresent the true state of affairs for risk mitigation and underwriting purposes.

4. A Consumer Data Right for general insurance

The final segment of this assignment examined the potential impacts of the CDR should it be extended to the general insurance sector. This section reports on the outcomes of that examination.

4.1 OPEN INSURANCE – PROSPECTS FOR CDR-GI

The case for a consumer data right in Australia was expressed by the Productivity Commission in 2017. Recommendation 5.1 called for a comprehensive right for consumers but did not expressly mention the insurance sector. However, it gave examples of how such a right could be of value in general insurance and entire sections of the report were devoted to the general insurance sector (Productivity Commission, 2017).

The Australian Government's initial review of CDR was confined to banking and did not mention the insurance sector (Australian Treasury, 2017). The Future Directions review of CDR in 2020 also did not expressly mention the insurance sector (other than in the context of insurance for participants in CDR-B). In fact, most consideration of competition and consumer protection in insurance, even since the CDR regime was introduced for banking, has focused on a range of other issues and proposals, including disclosure of better product information to consumers, standardised terms and products, component pricing, unfair terms, and complaints investigation practices.

At least initially, consumer groups cautiously welcomed aspects of CDR as offering, in principle, greater control to individual consumers and addressing some concerns about industry practices. The insurance industry, in contrast, has shown little enthusiasm for CDR, seeing it as disruptive and threatening to existing business models and practices.

4.2 OPEN INSURANCE – IMPLICATIONS OF CDR-GI

In 2020, Financial Rights commissioned Sapere Research to consider the implications of the CDR for the general insurance sector, including home, motor and travel insurance, building on the experience in banking:

> *"The Sapere report (Financial Rights, 2020) explores the risks and issues associated with the implementation of the CDR for the insurance sector and proposes a set of recommendations relating to:*
>
> 1. *Issues with the Open Insurance implementation that might reduce its benefits;*
> 2. *Risks that Open Insurance uses harm consumers;*
> 3. *Risks associated with the impact CDR has on insurance markets; and*
> 4. *Other broader issues with the CDR (Financial Rights, 2020)."*

This section builds on the work of Sapere, and responds in particular to the first part of Recommendation 5, that:

> *"Consumer advocates undertake further work to identify privacy risks that may arise from Open Insurance and monitor privacy risks as they arise under an Open Insurance regime."*

The mandating of data sharing would normally be seen as a clear erosion of privacy. The Australian Government has tried to "square the circle" by providing that the sharing required will only take place with the express consent of the consumers involved. It is questionable, however, whether the design of the CDR legislation, and its implementation in CDR-B through rules and standards, does in fact result in free and fully informed consent, sufficient to overcome concerns about mandatory sharing.

In January 2022, 15 months after publication of the Sapere report, and as this assignment was approaching completion, the Treasurer announced the extension of CDR to targeted datasets within general insurance (rather than the whole sector) as part of a wider "Open Finance" extension: "Open Finance will be implemented in phases involving the assessment and designation of key datasets within the … general insurance [sector] … in 2022" (Australian Treasury, 2022, p 1).

In our view, the Australian Government's decision has paid very little attention to the significant reservations that have been expressed in several submissions. In addition, the January 2022 policy statement is vague, with the only clue about the target-area being "an initial focus on consumer-specific account information, such as … product and/or attribute data for sub-categories of general insurance" (p 8). The announcement did not articulate the process whereby the government envisages that benefits to consumers would arise, beyond the assertion that "more rapid uptake and broad-based innovation … will enable … benefits for consumers by supporting frictionless switching and driving productivity gains by reducing administrative burden on SMEs" (p.10).

In order to provide a reasonably stable base for evaluation, this Report considers the state of CDR safeguards for privacy at the end of 2021 – taking into account the many changes since the original undertakings were given – and evaluates what the likely impacts of CDR in general insurance would be if the state of privacy safeguards was still much the same at that time CDR-GI is launched.

4.3 THE INTERACTION OF THE CDR PRIVACY SAFEGUARDS AND THE PRIVACY ACT

The CDR legislation introduced specific, unique CDR Privacy Safeguards[26] that according to the Explanatory Memorandum "contain more restrictive requirements on participants than those applying under the *Privacy Act*".[27]

The relationship between the CDR Privacy Safeguards and the *Privacy Act* Australian Privacy Principles is extremely complex. While most of the safeguards have the same title (and numbering) as the equivalent Australian Privacy Principles, and some of the wording is identical, there is also considerable variation, with alternative or additional wording in the safeguards.

The safeguards also need to be read in conjunction with the relevant CDR Rules in the *Competition*

---

26 This section references CDR Privacy Safeguards as per Part IVD, Division 5 of the *Competition and Consumer Act 2010*, and informed by Office of the Australian Information Commissioner, Australian *Privacy Principle Guidelines*, Version 3.0 (June 2021).

27 *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, Explanatory Memorandum, para 1.22.

and Consumer Act 2010, which in some cases impose specific requirements in addition to those in the Privacy Safeguard itself. In addition, the CDR Rules have changed since CDR commencement under the *Competition and Consumer Act 2010*, with the version current at the time of writing in force since 23 December, 2020.[28]

Furthermore, the CDR Rules themselves are supported by Consumer Data Standards and Consumer Experience **(CX)** Guidelines issued by the Data Standards Body **(DSB)**.[29]

Most of the CDR Privacy Safeguards, together with any relevant Rules and Standards, are more prescriptive than the equivalent Australian Privacy Principles, but this does not necessarily mean that they are more privacy protective. While some are clearly "consumer-centred" – for instance mandating "opt-in" consent and prohibiting a range of secondary uses – others override the normal application of the Australian Privacy Principles in pursuit of the objectives of the CDR regime, which strongly favours data sharing by businesses, with arguably weak consent conditions.

4.4 ONGOING REDUCTIONS IN CDR PRIVACY SAFEGUARDS

Government agencies have paid considerable attention to the privacy impact of the CDR Regime, beyond the inclusion of the CDR Privacy Safeguards in the Competition and Consumer Act and the relevant Rules, Standards and CX Guidelines.

Initial work was undertaken internally within Treasury, followed by an independent external Privacy Impact Assessment **(PIA)** (Maddocks 2019). A response was published by Treasury (Australian Treasury, 2019c).

Privacy implications of any extension of CDR to general insurance were a specific focus of the Sapere report to Financial Rights, of September 2020, which we summarised above.

A series of external 'Updates' to the PIA Report were published, initially for ACCC, and later for Treasury (Maddocks, 2020a, 2020b/2021a, 2021b, 2021c).

The first update (Maddocks, 2021a) made 25 recommendations, partly to address criticisms of the complexity of the CDR ecosystem. In February 2021, the ACCC published a response to the PIA Update 2, which foreshadowed some relevant changes to the Rules, but explained why it had decided not to act on many of the recommendations (ACCC, 2021). PIA Update 3 evaluated further proposed amendments to the CDR Rules, and identified additional key risks in relation to complexity and its impact on understanding and hence compliance, "trusted advisers", disclosure of CDR data outside the CDR regime, sponsored accreditation, CDR representatives and joint accounts (Maddocks, 2021b).

PIA Update 4 on 29 October 2021 (Maddocks, 2021c) was commissioned to inform version 4 of the CDR Rules, issued on 12 November 2021, which are mainly confined to the extension of the CDR scheme to the energy sector. The government response to its seven recommendations was published in November 2021 (Australian Treasury, 2021c).

---

28 Competition and Consumer (Consumer Data Right) Amendment Rules (Nos 1, 2 & 3) 2020. Subsequent amendments in the Amendment Rules (No 1) 2021 are not yet reflected in the latest Office of the Australian Information Commissioner, *Australian Privacy Principle Guidelines*, Version 3.0 (June 2021).

29 Data Standards Body, *Consumer Data Standards*, Version 1.16.0, https://consumerdatastandards.gov.au/consumer-data-standards/.

Our assessment is that agency responses to the PIA and the succession of Updates have not adequately addressed either the serious underlying privacy issues with the CDR regime or the further issues that have progressively emerged as changes have been announced. All of the PIA-related documents highlight the complexity of the CDR "ecosystem" and the importance of clear communications, including to consumers, if the scheme is to work as intended while adequately protecting consumers' privacy.

Since shortly before Treasury assumed control of the scheme in February 2021, many changes have been proposed, many of which have been found by the PIA consultants to weaken privacy protections. Relatively few of these weakened protections have been addressed or materially mitigated by subsequent amendments. The net effect has therefore been continual ratcheting-down of CDR consumer protections since late 2020.

To the extent that PIA recommendations and/or agency responses to them are relevant to our findings, we mention them in the remainder of this report.

4.5 THE POTENTIAL FOR CDR TO IMPROVE PRIVACY OUTCOMES

4.5.1 CDR disclosure and consent – a threshold issue

The CDR Privacy Safeguards are based on a "disclosure and consent" model similar to that underpinning the *Privacy Act* but more prescriptive in terms of both the information to be disclosed to consumers and the "granularity" of consent required – both for collection and for specific and distinct uses and disclosures of consumer data.

The underlying premise of the CDR disclosure and consent protections[30] is that if individuals are adequately informed about an organisation's intentions in respect of personal information/data, then they are in a position to be able to give or withhold informed consent for proposed uses and disclosures.

There has been considerable academic argument to the effect that the "disclosure and consent" model cannot be the sole basis for effective privacy protection. Consumer surveys find that people favour "in principle" being given more information and more choice over uses and disclosures of their personal information or data. However, practical experience is that few can be bothered to read privacy notices, statements or policies, and most will simply "tick a box" giving consent to almost anything if that is the simplest and easiest way of obtaining a service they desire.

Default "privacy on" settings, with individuals having to give express affirmative consent for secondary uses and disclosures (opt-in) gives far more control than "opt-out" opportunities. Most people will not take advantage of these, but even "opt-in" is subject to manipulation (or even coercion) if it is the "price" of something that the individual wants. Short term benefits will often be valued more highly than the possibility of long-term detriment, even if the individual can be made aware of privacy risks.

The limitations of the "disclosure and consent" model have been well- documented, including in a

30 The disclosure and consent model is implemented in *Privacy Act* through the interaction of Australian Privacy Principles 1, 5 and 6 (and for certain purposes Australian Privacy Principles Section 7 and 8), and in the CDR, through the same numbered Privacy Safeguards (with an additional Privacy Safeguard 10).

joint 2019 report by Australian and Dutch regulators, which characterised disclosure as "necessary" but not "sufficient" and in some cases contributing to consumer harm (ASIC and DAFM, 2019). Also, a submission by Financial Rights to Treasury in May 2021 concerning proposed changes to the joint account provisions in the CDR regime highlighted the risks of moving to an "opt-out" model based on an assumption of informed consent (Financial Rights, 2021). We discuss the joint account changes further below. **(See Section 4.7.9)**.

In the CDR context, it seems likely that the very elaborate requirements for disclosure and consent, through multiple "consumer dashboards" and referral of consumers to CDR policies (in addition to a separate privacy policy and a range of T&Cs) may be ineffective. They may achieve little practical privacy protection while acting as a barrier to the take-up of CDR both by consumers and by industry principals and intermediaries who the government expects to offer an enhanced range of services. To date, industry entities are finding that design and compliance with processes to participate in CDR are excessively onerous, and consumers are having difficulty understanding industry entities' offerings.

The conclusion we reach is not that privacy protections based on the "disclosure and consent" model are unnecessary and should be weakened or even dispensed with. The "disclosure" element is essential as a means of delivering transparency both to consumers and consumer advocacy organisations. The "consent" element is important to the minority of consumers who can cope with the complexity and whose activism plays a role in the protection of all other, less capable and/or less committed consumers.

It is necessary to recognise, however, that the "disclosure and consent" model, in complex circumstances such as CDR, is insufficient to deliver adequate privacy protections. It is essential that appropriate obligations be imposed on service-providers that complement the consent-based approach.

The CDR regime does incorporate some elements of a regulatory model to protect privacy, in the form of express prohibitions of some data practices, for example some direct marketing using CDR data. Consumer groups have also recommended prohibition of "screen scraping" as a method of data collection. As discussed in other sections of this report, however, it is not clear that the pattern and intensity of legal obligations imposed on the many organisations involved in CDR satisfies the requirement of sufficient and suitable protections complementary to disclosure and consent.

The CDR regime includes regulation of use of de-identified CDR data[31], requiring consent for some uses, such as research. This runs the risk of undermining the credibility of Privacy Safeguards. There are legitimate concerns about the possibility of re-identification, and safeguards to prevent this are appropriate. If and when CDR data can be irreversibly de-identified, privacy concerns are no longer relevant and privacy should not be misleadingly invoked to justify the use of the de-identified data. If there are good public policy reasons for regulating the use of demonstrably de-identified data, these should be articulated without unjustified invocation of privacy.

---

31 This regulation is under the CDR Rules and is separate from the Privacy Safeguards, which only apply to CDR data for which there is one or more CDR consumer, such as an individual who is identifiable). CDR consumers may be individuals, companies or partnerships, and unlike under the *Privacy Act*, where only individuals have privacy rights. The CDR Privacy Safeguards apply to all categories of CDR consumer. This report is only about privacy which relates to individuals. Thus the term CDR data refers to personal CDR data that is also personal information under the *Privacy Act*.

4.5.2 Complexity of the CDR ecosystem

The CDR regime established in Australia to date has been characterised as an "ecosystem", with an ever-increasing number and diversity of CDR players[32]. Initially included were consumers, accredited persons **(APs)**, accredited data recipients **(ADRs)**, data holders **(DHs)** and designated gateways **(DGs)**[33]. In addition, and as the regime has evolved, there is a range of further roles, including "secondary user", "CDR representative", "trusted advisor", " insight recipient", "enclave provider", "affiliate", "sponsor" and "associate". We note that the CDR rules for the energy sector, issued in November 2021, introduce a further concept of peer-to-peer **(P2P)** data sharing, involving two sub-categories of primary and secondary DHs. PIA update 4 expressly warned of the importance of considering the implications of this if any future extension involves multiple secondary DHs.

A further indication of the complexity is that there are now five separate categories of consent in the CDR Rules relating to consent for collection, use, disclosure, direct marketing and de-identification.

While a CDR consumer might not need to understand all of these complexities in the CDR ecosystem, the detailed disclosure/consent requirements mean that some at least need to be explained. It is legitimate to ask the question whether it is practical and realistic to expect CDR consumers to understand the complex ecosystem which they will be invited to join, to the extent that would be necessary for them to make informed decisions. It seems doubtful that many consumers will be at all interested in the machinery underlying any new services such as supplier comparison or switching sites. If they desire these services, there is a significant risk they will just accept whatever T&Cs, including privacy policies, are imposed.

The insurance industry itself has acknowledged, in a wider context than just privacy, the limitations of a "disclosure and consent" model of regulation. In 2015, a report to the ICA Board made many of the same points as we have done above (ICA, 2015).

4.6 CDR AND THE LIMITATIONS OF THE "DISCLOSURE AND CONSENT" MODEL

If the same rules and Privacy Safeguards as are in place for "open banking" **(CDR-B)** are applied to CDR-GI, they will compound the existing problem with the "disclosure and consent" model, except in a few cases where they may be beneficial.

One feature of the CDR regime that may be considered at least a mitigant in relation to reliance on "disclosure and consent" is that consents, for collection, use and disclosure of CDR data are expressly time-limited. The default is 12 months, after which the relevant CDR participants are required to confirm with the CDR consumer their continued consent. Furthermore, the rules expressly provide for withdrawal of some consent, whereas this is left ambiguous in the Australian Privacy Principles.

However, the effectiveness of these additional safeguards depends at least in part on a CDR consumer's ability to fully understand and navigate the complexity of the CDR processes, and the

---

32 The term "CDR participant" cannot be used as it has a defined meaning – including only Data Holders and Accredited Data Recipients. Similarly, CDR entity has a defined meaning – including DHs, ASRs and DGs.

33 As at 25 January 2022, 72 organisations are accredited as CDR Data Holders (with 30 additional "brands"), but only 26 as ADRs. The Office of the Australian Information Commissioner, *CDR Privacy Safeguard Guidelines*, Version 3.0 (June, 2021), state "there are currently no designated gateways", A.37 Note.

varied and potentially inconsistent interpretations and implementations of the Data Standards, and the diversity of user interfaces and experiences they are likely to lead to.

Changes to the CDR Rules in September 2021 in relation to joint accounts in banking (CDR-B) reversed the previous requirement for "opt-in" consent from both/all joint account holders, replacing it (from July 2022) with a default sharing model with only an "opt-out" opportunity. We discuss the merits of this in relation to joint accounts later in this report, but this significant change has wide implications.

4.7 THE IMPACT OF THE CDR ON PRIVACY ISSUES IN GENERAL INSURANCE

This report outlines the privacy issues that arise in general insurance under the headings of the relevant current privacy regulatory framework, which is the *Privacy Act*, including the Australian Privacy Principles that currently apply to businesses other than small business enterprises, and very probably to all insurers. **(See Section 2).**

In this section, we report on our review of the CDR regime including the Privacy Safeguards and related rules, which may in future be applied to an even wider range of businesses, large and small, operating in and around general insurance. For convenience, we have assumed that the current CDR Privacy Safeguards and related Rules would apply to general insurance without change.

This section contains brief summaries. Detailed assessments are provided. **(See Appendix 7).**

4.7.1 Open and transparent management of personal information

There is a risk that the very detailed compliance requirements of the CDR, overlaid on the continuing Australian Privacy Principle 1 requirements, would increase complexity, which could overwhelm consumers and ultimately undermine the objective of meaningful consensual participation. (**See: Appendix A7-1)**. This is particularly the case given our findings reported above that insurers' privacy policies are already difficult to find, read and engage with. **(See Section 4).**

4.7.2 Collection of personal information

The CDR Privacy Safeguards are in theory more privacy protective than the Australian Privacy Principles, but the CDR rules are even more prescriptive than the equivalent "content of notice" requirements of Australian Privacy Principle 5, and in our view the complexity would overwhelm consumers and insurers alike. **(See Appendix A7-2).**

In any extension of the CDR regime to general insurance, care should be taken to ensure insurers are not able to obtain more personal information than is required for the provision of the requested services, or in the case of claims assessment or investigation, more than is required for the specific claim.[34] Both the specification of "required consumer data" and the provisions for broad "consents" could facilitate "fishing expeditions" that collect too much information. **(See Appendix A7-6)**.

34 Contrary to *General Insurance Code of Practice*, Section 67.

4.7.3 Collection of solicited personal information

Privacy Safeguard 3 is more restrictive and seemingly more privacy protective than Australian Privacy Principle 3. However, it could give rise to abuse of the consent provisions, for example, to justify and automate insurers' continual updating of CDR data from a third party source.

Privacy Safeguard 3 also lacks an explicit "fair collection" requirement, which may encourage unfair practices, for example in the context of claims investigation. In addition, extraneous data may find its way into insurance records. As noted **(see Section 3)**, this is an existing practice in IRS reports, which include irrelevant data about a consumers' finances. This is inappropriate because it exacerbates the risks of unfair discrimination. **(See Appendix A7-4).**

4.7.4 Use and disclosure

The CDR regime as currently implemented substitutes Privacy Safeguards 6 and 7 for Australian Privacy Principles 6 and 7. The Privacy Safeguards are more specific than the Australian Privacy Principles, but also less extensive in their coverage. In addition, the effects of Privacy Safeguards are highly dependent on the definitions of key terms. An example is "required consumer data". This is vaguely described in the CDR rules and hence dependent on articulation in Data Standards issued by the DSB. The outcomes could accordingly be improvements to and/or serious reductions in consumer data privacy.

The CDR regime also features a designed-in loophole in the form of "voluntary consumer data", which in CDR-B appears to be undefined, and uncontrolled. Moreover, the consent arrangements under CDR are complex and provide many opportunities for the abuse of anything that can be represented to be "voluntary consumer data".

Particularly in view of the continual ratcheting-down of consumer protections evident since late 2020 **(see Section 4.4)**, consumer groups are understandably concerned about the likelihood that the CDR in practice could further weaken already inadequate protections in relation to the use and disclosure of CDR data.

4.7.5 Direct marketing

Australian Privacy Principle 7 is not primarily a privacy protection principle, but rather an authorisation mechanism for direct marketing, with some modest privacy protections built into it.

Privacy Safeguard 7, which replaces Australian Privacy Principle 7 for CDR data improves the weak protections of Australian Privacy Principle, for example it applies to offers for the renewal of existing goods or services, not just new ones. However, insurers could be expected to want to use CDR data for direct marketing of "related products" such as home contents as related to building insurance, or even motor vehicle cover bundled with home and contents. Anti-hawking rules[35] and restrictions on deferred sales processes for unsolicited sales[36] are also relevant.

It will be unclear for some time as to whether the CDR would improve privacy protections in relation

35 Australian Securities and Investments Commission, RG 38 The Hawking Prohibition (Reissued 23 September, 2021), https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-38-the-hawking-prohibition/.

36 Australian Securities and Investments Commission, RG 275 The Deferred Sales Model for Add-On Insurance (Reissued 28 July, 2021), https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-275-the-deferred-sales-model-for-add-on-insurance/.

to direct marketing in general insurance, or whether the positives will prove illusory or be withdrawn, and/or complexities will be utilised to circumvent these protections. **(See Appendix A7-7).**

4.7.6 Additional use and disclosure controls

Australian Privacy Principle 8 addresses a subset of disclosure provisions relating to data transferred to other jurisdictions, whether by or within the APP entity or to or by a contractor. Such cross-border transfers are subject to additional safeguards.

In the CDR regime as currently implemented for banking, Privacy Safeguard 8 replaces Australian Privacy Principle 8.

Many Australian insurance companies are part of a large multinational group and the implications of Privacy Safeguard 8 will depend on the extent to which insurers currently or prospectively give access to their customer data to their overseas parent or associated companies, whether just for administrative or IT processes or for more substantive purposes. Also, most reinsurers are international not Australian entities. Further knowledge of industry practices would be necessary to assess these implications. **(See Appendix A7-8).**

Australian Privacy Principle 9 places some restrictions on the adoption, use and disclosure of government related identifiers.

In the CDR regime as currently implemented for banking, Privacy Safeguard 9 applies to all ADRs, and is in effect a more restrictive version of Australian Privacy Principle 9, limiting the adoption, use and disclosure of government related identifiers.

In the insurance context, Privacy Safeguard 9 is most likely to affect the use and disclosure of driver licence numbers. Insurers would need to ensure that their use of licence numbers in motor vehicle insurance complies with the narrower conditions of Privacy Safeguard 9 rather than those of the more permissive Australian Privacy Principle 9. Another potential area of application would be in the use of government-issued numbers in the criminal justice system, to the extent that insurers need to keep records of criminal histories. **(See Appendix A7-9).**

4.7.7 Data quality

In the CDR regime as currently implemented for banking, Privacy Safeguard 11 imposes some of the data quality obligations from Australian Privacy Principle 10 on DHs via Privacy Safeguard 11(1) and on ADRs as in Privacy Safeguard 11(2), but they are greatly weakened because they only apply to the disclosure of CDR data, and not to *collection or use*.

Given the low quality of personal data in the general insurance industry, as confirmed by the findings of the empirical research reported **(see Section 3)**, and ASIC's recent focus on data quality issues in the insurance sector (ASIC, 2021), the relative weakness of Privacy Safeguard 11 will be of great consequence if and when CDR is extended to the general insurance sector.

A key element in addressing data quality problems is through the standardisation of terms and definitions. This seems to be one area in which the explicit role of data standards in the CDR-B regime is already yielding significant benefits, and could also be a part of a CDR-GI regime. **(See Appendix A7-10).**

4.7.8 Security, retention and deletion of data

Privacy Safeguard 12 replaces Australian Privacy Principle 11 in respect of CDR data, listing the same security risks. However, instead of being limited to a general requirement to take reasonable steps to protect the personal information, detailed steps are specified in the CDR Rules. The Rules are subject to ongoing change.[37]

The relevant provisions are in Schedule 2 to the Rules, including procedural aspects and named technical safeguards.[38] For example, malware protections are required, including "anti-malware anti-virus [solutions], Web and email content filtering, and Application whitelisting". The requirements are conventional, and the Schedule is considerably more informative than the OAIC's still-vague guidance. However the Schedule is also highly prescriptive and inflexible and likely to be ignored, as quickly-dated, technologically-specific provisions generally are.

There is a strong tendency for security, retention and deletion practices not only to ignore obviously-ineffectual provisions, but also to be circumvented and subverted by organisations in order to achieve what those organisations see as the key objectives – commonly an effective system that serves its own organisational objectives. Hence, while there is a prospect of improved data security, the risk exists that privacy protections may actually be reduced under CDR. **(See Appendix 7-11)**.

4.7.9 Joint accounts

The privacy protections specified in the CDR scheme have been progressively and significantly reduced. The changes that have been made to the provisions relating to joint accounts can have potentially serious consequences where joint insurance policyholders become estranged, or intra-family disputes arise. In addition to financial abuse, the possibility exists of verbal and physical abuse, and psychological abuse, particularly if children are involved, should the victim's otherwise-unknown location be disclosed to the abuser. **(See Appendix A7-12).**

4.7.10 Subject access

This is another area in which policy changes have greatly diminished vital privacy protective features of the original scheme. The right to obtain your own CDR data was a fundamental objective of the CDR legislation and rules, and included in CDR-B Rules.[39] However, in September 2021 the feature was deferred indefinitely in the banking context. It will also not apply to the energy sector.

Because of ambiguity about the application of Australian Privacy Principle 12 to CDR data, the CDR scheme now facilitates third party access to shared data, with no apparent balancing right for CDR consumers to directly access and control their own CDR data.

The field research conducted in this assignment delivered important information about the poor process quality and poor data quality prevalent in the industry. That research would have been severely hampered, and quite possibly precluded, if the subject access right had already been undermined by the imposition of CDR. Further, if this deficiency in CDR-B and CDR-E is carried over into CDR-GI, the legal underpinnings are undermined for insurance consumers' access to reliable information that they can use in applications for insurance.

---

37 Competition and Consumer (Consumer Data Right) Rules 2020 (Current version), https://www.legislation.gov.au/Series/F2020L00094.

38 Ibid, pp 133-143.

39 CDR-B Rules, 3.4(3).

If the quality and consistency of data held by insurers were considerably improved, a range of consumer benefits could be achieved. These include more readily obtaining disclosure information for the purpose of preparing quotations, obtaining one's insurance history gratis (rather than paying the IRS $22), more readily identifying errors in information held by insurers and more readily updating information. However, this would require a significant program of data standards setting amongst insurers to improve data quality. **(See Appendix A7-13).**

4.7.11 Correction of personal information

Privacy Safeguard 13 is substituted for Australian Privacy Principle 13 in respect of correction rights and obligations. It is, however, a more limited provision. For example, it lacks a general obligation to make corrections irrespective of how the DH becomes aware of a data quality problem. There is also no provision that enables an individual to challenge a refusal. The poor quality of data revealed by the field research reinforces the importance of and need for strong and effective correction provisions. **(See Section 3)**. In short, CDR would take privacy protection backwards in this area. **(See Appendix A7-14).**

4.7.12 Outsourcing

At first sight, the application of CDR Rules and Privacy Safeguards relating to outsourcing may provide some improvement over the unsatisfactory and ambiguous current situation with the Australian Privacy Principles. However, the prevalence of outsourcing in the general insurance sector – including widespread use in claims investigation and assessment – makes it all the more important that privacy protection for CDR data handled by third party contractors is adequately addressed. **(See Appendix A7-15).**

4.7.13 Sharing of CDR data outside the "protected" CDR regime

Original design undertakings for the CDR have also been withdrawn in relation to the authorisation of some CDR data to be shared with parties who are subject to the CDR regulatory regime. This appears likely to have serious consequences for consumers.

Given the highly networked nature of the general insurance sector and the significant overlap of many participants into other industry sectors and segments, this is a major weakness from a consumer perspective.

If the CDR regime is extended to general insurance, the position of insurance brokers would be an important issue. It is not clear if they would fall under the definition of "trusted adviser" under the CDR Rules. If they did not fall under that definition, this would leave a major gap in privacy protection, as flagged in the PIA Update 2 (Maddocks, 2021a). **(See Appendix A7-16).**

4.7.14 Complaints and enforcement

Under the CDR, responsibilities for complaint-handling, monitoring and enforcement are split across several agencies, but with much of the effort falling on the OAIC. The OAIC is perceived by many advocates and members of the public to operate in a slow and bureaucratic manner, and it is chronically under-resourced. Moreover, it is continually loaded up with additional responsibilities without commensurate increases in resources. More resources are needed to enable the OAIC to undertake these activities in addition to its current operations. **(See Appendix A7-17).**

4.8 CONCLUSIONS

This analysis of CDR safeguards, and their potential impacts if CDR is implemented in the general insurance industry, has been based on the assumption that CDR safeguards when CDR-GI is launched would be those prevailing for CDR generally at the end of 2021. There are some potential, modest improvements in comparison with the present state under the Australian Privacy Principles. However, CDR also embodies multiple, potentially serious reductions in consumer safeguards.

Moreover, there are considerable uncertainties about the availability, effectiveness and longevity of the CDR consumer safeguards as they stand at the end of 2021. Multiple privacy safeguards that were integral to the original design have been withdrawn, despite the concerns expressed by privacy advocates, and the independent advice of the government's PIA consultant. The scale of the reductions has been such that even the safeguards that remain appear to be fragile. It is critical that the interests of consumers are reflected in modifications to the system.

If and when CDR is imposed on the consumer segment of general insurance, the proposition that consumers would benefit from it is unsupported by current evidence, unless there are fundamental changes to current systems and practices. There is great diversity in consumers' contexts and in the risk assessment applied by insurers. Only limited efficiencies appear to be available. On the other hand, considerable additional costs will be involved in achieving the levels of data and process quality essential to the effective operation of the general insurance industry.

On the basis of the field research reported **(see Section 3)**, it is clear that data management in the general insurance industry is of low quality, and that business processes supporting consumer access to data about themselves also require considerable improvement.

The industry has failed to create an environment within which consumers can easily gain access to comprehensive information about their claims history, despite the industry's claim that IRS reports can be used to fulfil their legal obligation to disclose sufficiently comprehensive and accurate information about their prior claims against insurance policies.

The only feasible payback for consumers from CDR-GI is quality of data and processes, sufficient that they receive accurately-assessed quotations and do not suffer unfair rejections of claims.

To attract support by consumers and their advocates, we contend that any CDR-GI scheme needs to involve:

- Wholesale redesign of claims information management; and
- Convenient and inexpensive access by consumers to the data held about them, and in particular to data about claims held about them.

Addressing the quality problems is an urgent priority given the Australian Government's announcement of adjustments to "open finance" in January 2022. Particular emphasis needs to be placed on:

- Agreed objectives for open insurance that are not based on unrealistic notions of substantial reductions in premiums, but instead focus on achieving necessary improvements in commonality of terminology and definitions, and in data and process quality;

- Negotiation and promulgation of data standards for claims datasets;
- A plan for transition to those standards;
- Early commencement of implementation;
- A requirement for compliance by all industry participants with reasonable quality standards firstly for the data, but also for associated business processes; and
- Enforcement of compliance with the obligations of insurers and any shared schemes, with privacy law generally, and in particular with Australian Privacy Principle 12 and Australian Privacy Principle 13.

Without such action, CDR-GI would, in our view, compound the problems of current consumer experiences and lead to an increase in the circulation of, and reliance upon, low-quality data across the industry.

A further concern **(see Section 4.7.10 and Appendix A7-13)** is that CDR no longer appears to include any means whereby consumers can exercise their subject access rights. The scheme is designed to enable the trafficking of personal data by insurers and third parties, without consumers being able to see the data that is being trafficked.

This deficiency is exacerbated by the fact that the consent element in the CDR is capable of being further compromised.

To serve consumers' interests and ensure respect for their rights against insurers, CDR-GI needs to be designed to be solely consent-based and to incorporate effective means to gain access to the data that is and/or is to be trafficked.

The final Recommendations section of this Report identifies a considerable number of further conditions that need to be satisfied. Without these measures, any benefit to consumers of the CDR-GI would be undermined.

5. Conclusions and recommendations

This report has used a combination of desk-analysis and field research to:

- Obtain an overview of current data collection and handling practices of general insurers;
- Collate and detail known privacy issues in the general insurance sector including in individual insurers and shared industry schemes such as the IRS;
- Assess the quality of consumer data in the general insurance sector;
- Examine the quality of processes whereby consumers can gain access to their personal data and in particular their historical claims data; and
- Identify the risks that are likely to arise from the extension of the CDR to the general insurance sector.

Consumers have an obligation to disclose sufficiently comprehensive and accurate information about their prior insurance claims. However, the ability of consumers to act upon their obligation is compromised by poor industry processes and data quality.

This section provides a series of recommendations for actions that emerge from the study.

In this section, a reference to "an insurance industry entity" encompasses insurers, associations of insurers, industry-wide schemes such as IRS and IFBA, specialist service-providers in the industry, and outsourced service providers handling consumer data.

5.1 RECOMMENDATIONS RE GENERAL INSURANCE DATA PRACTICES AND PRIVACY

Recommendation 1

Each insurance industry entity should act to reduce the confusion caused to consumers by the use of distinct **brand names, group names and contracting-entity names**, and email-traffic coming from and going to email addresses in different domains. **(See Section 2.1 and Appendices 1, 2, A3-1 and 6B).**

Recommendation 2

Each insurer should reduce the confusion caused to consumers by **multiple, long documents** (including privacy policies, T&Cs, product disclosure statements and codes). Parts of these are relevant to consumers' interests. On the other hand, most contain large volumes of complex and turgid prose; none of them are easy to navigate around; and none of them appear to offer straight answers to what the consumer sees as straightforward questions. **(See Appendices 2 and A3-1).**

Recommendation 3

Each insurer should address consumer concerns about:

- **Bundled consent**, particularly for those uses and disclosures of personal information not likely to be contemplated by the consumer;

- **"Take it or leave it"** consent whereby the insurer seeks to impose non-negotiable terms. **(See Sections 2.5 and Appendices 2, A3-1, A3-3, A3-5, A3-6 and A5-2)**;
- Inadequate application of the **data minimisation principle** to prevent the collection and holding of personal data that is irrelevant or not contemplated by the consumer. **(See Sections 2.5, 2.6.1, 3.4.4, 3.5.2 and Appendices 2, A 3-3, A 3-6, A 3-7, A3-8, A3-11, 4, A6-1 and A6-4)**; and
- The risk of **unfair discrimination** against individuals, and inequitable discrimination against categories of individuals, that arises from extraneous data being available to decision-makers. **(See Sections 2.5, 3.4.1, 4.7.3 and Appendices A3-3, A6-1 and A7-4)**.

The Australian Government should introduce regulations, standards or laws as part of the CDR to address these concerns.

Recommendation 4

Each insurance industry entity should implement measures to greatly improve the **quality of processes** in relation to consumer data access requests, which are currently falling far short of the requirements of Australian Privacy Principle 12 **(See Sections 3.4.2, 3.4.5, 3.5.1, 3.7, 4.7.10, 4.7.11 and Appendices A3-13, A5-8, A6-2, A6-5 and A7-14)**.

Recommendation 5

Insurance industry entities – in collaboration with the Australian government including Data 61, Australian Prudential Regulation Authority, OAIC and Australian Securities and Investments Commission **(ASIC)** – should:

- Develop a program to establish **data standards**;
- Implement that program; and
- Transition to those data standards;

in order to:

- Significantly raise the quality standards of insurers' data holdings, most crucially in relation to prior claims. **(See Sections 2.5, 2.6.1, 2.6.2, 3.4.3, 2.4.4, 3.5.2, 3.7, 4.7.10 and 4.7.11 and Appendices A3-10, A3-13, A5-5, A6-3, A6-6, A6-7, A7-10 and A7-14)**;
- Overcome the inconsistencies in both the content and the descriptions of that content provided to consumers, by individual insurers and by the IRS, and between different insurers. **(See Section 3.6 and Appendix A6-7)**; and
- Improve business processes that give rise to low data quality, such that the data currently provided to the IRS, and provided directly to consumers, is of sufficient quality to ensure that consumers exercising reasonable care have no reason to fear unfair rejection of claims.

Recommendation 6

Insurance industry entities should:

- Clarify the **legal basis for all aspects of IRS/Illion operations**. (**See Sections 2.6.1, 3.4.1 and Appendices A3-14 and A6-1)**; with particular reference to:
  - The IRS providing insurers with access to non-insurance data. **(See Section 3.4.1 and Appendix A6-1 and A6-4)**; and
  - Any ability of the IRS and/or its outsourced service provider to utilise data acquired from insurers or insurance consumers for any purpose other than the declared, justifiable and lawful purposes associated with general insurance. **(See Sections 2.6.1, 3.4.4 and Appendices A3-3(4), A3-6 and A6-1)**.

Recommendation 7

Each insurance industry entity should address the difficulties confronting consumers in achieving **appropriate understanding of data** provided to them, by providing support and education to assist consumers. **(See Sections 2.6.1, 3.5.1 and 3.5.2 and Appendix 6B)**.

Recommendation 8

Insurance industry entities should provide a workable mechanism for consumers to obtain a reliable claims history from the IRS and/or insurers, in order to greatly reduce the risk of **unfair claim refusals** based on low quality data.

Recommendation 9

Each insurer, and the IRS and its outsourced service-provider, should:

- implement business processes that are compliant with Australian Privacy Principle 13 for **self-initiated data correction**; and
- provide **subject correction arrangements** that are compliant with Australian Privacy Principle 13.

Recommendation 10

The Australian Government should regulate **industry-wide reporting of general insurance claims**, in the same manner that a sui generis scheme has applied to credit reporting since the early 1990s.

The scope of the regulatory regime should address the need for:

- Assurance of much higher quality and consistency of data;
- Assurance that consumers are not unfairly disadvantaged by reliance on poor quality reports;
- Requirement that reports be available gratis to consumers at least four times per annum – as credit reports are. **(See Appendices A3-12, A5-7 and A6-2);**
- Specification of what, if any, non-insurance data is permitted to be included or excluded. **(See Section 3.4.1 and Appendices A6-1 and A6-4)**;

- Assurance that reports:
  - Are in plain English; and
  - Are accompanied by glossaries and contextual information to assist consumer comprehension. **(See Section 2.6.1 and Appendices A3-3(4), A6-2 and A6-3)**;
- Requirements that business processes deliver reports in a sufficiently timely manner and a sufficiently useful format to support the purpose of claims data quality assurance;
- Stipulation that an entity providing an insurance report cannot refuse to accept and process a correction request as required by Australian Privacy Principle 13. **(See Sections 2.6.1, 3.4.4 and Appendices A5-8 and A5-9)**; and
- Assurance that:
  - Consumers may rely on insurance claims data provided by insurance industry entities for the purposes of disclosure; and
  - Insurance industry entities are precluded from denying claims on the basis of errors in such insurance reports.

Recommendation 11

Insurance industry entities should improve the **visibility of the availability of insurance claims history reports** to consumers for disclosure purposes. **(See Appendix A6-2).**

5.2 RECOMMENDATIONS IN RELATION TO CDR

Recommendation 12

Insurance industry entities including the ICA, the IRS and regulators should **work with consumer groups** to address the concerns raised in this report.

This could be facilitated by the establishment of a working-party in relation to CDR-GI, with a view to establishing a common position in relation to:

- CDR-GI's expected costs, benefits and risks;
- The objectives of CDR-GI; and
- The sequence of actions needed to achieve benefits from CDR-GI.

Recommendation 13

Consumer groups should maintain a **watching brief on CDR developments** in CDR-B, CDR-E and CDR-T, in order to sustain an up-to-date assessment of consumer impacts of CDR-GI.

Recommendation 14

The CDR DSB/Data 61 should work closely with insurance industry entities and consumer groups to establish **consistent data standards** for datasets, in coordination with the process referred to in Recommendation 5.

Recommendation 15

The Australian Government should conceive and articulate CDR-GI so as to assist consumers and insurance industry entities in relation to:

- The exercise of, and compliance with, Australian Privacy Principle 12 **subject access rights and obligations**; and
- The exercise of, and compliance with, Australian Privacy Principle 13 data **quality obligations and subject data correction rights**.

Recommendation 16

The Australian Government should reconsider the current CDR Rules regarding:

- Joint accounts **(See Section 4.7.9)**;
- Subject access rights **(See Section 4.7.10)**;
- Correction of personal information **(See Section 4.7.11)**;
- Outsourcing **(See Section 4.7.12)**; and
- Trusted advisors **(See Section 4.7.13)**;

with particular focus on the potential consumer harms that may arise, and unique circumstances in the general insurance context.

6. References

Australian Bankers Association, *Open Banking* (Undated), viewed April 2021, **https://www.ausbanking.org.au/policy/the-future/open-banking/**.

Australian Competition and Consumer Commission, *Consumer Data Right* (CDR): Project Overview (Undated), viewed 19 April 2021, **https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0**.

Australian Competition and Consumer Commission, *Consumer Data Right: Rules Outline* (December, 2018), **https://www.accc.gov.au/system/files/CDR-Rules-Outline-corrected-version-Jan-2019.pdf**.

Australian Competition and Consumer Commission, *Media Release: Consumer Data Right Rules amended to include intermediaries* (1 October, 2020), **https://www.accc.gov.au/media-release/consumer-data-right-rules-amended-to-include-intermediaries**.

Australian Competition and Consumer Commission, *Consumer Data Right Rules – Update 2 to Privacy Impact Assessment – Agency response* (February 2021), **https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/accc-makes-amendments-to-the-consumer-data-right-rules/privacy-impact-assessment-and-acccs-response-to-privacy-impact-assessment**.

Australian Financial Complaints Authority, *AAI Limited Case No. 705394* (13 August, 2020), **https://service02.afca.org.au/CaseFiles/FOSSIC/705394.pdf**.

Australian Financial Complaints Authority, *Annual Review for 2019-20* (2020), **https://www.afca.org.au/media/1057/download**.

Consumer Data Right, *Consumer Data Right: ACCC/OAIC Compliance and Enforcement Policy for the Consumer Data Right* (May, 2020a), **https://www.accc.gov.au/system/files/CDR%20-%20CE%20-%20Joint%20ACCC%20and%20OAIC%20compliance%20and%20enforcement%20policy%20-%208%20May%202020.pdf**.

Consumer Data Right, *Consumer Data Right: Become an Accredited Data Recipient* (Undated), **https://www.cdr.gov.au/for-providers/become-accredited-data-recipient**.

Consumer Data Right, *Consumer Data Right: Phasing* (December, 2020b), **https://www.accc.gov.au/system/files/20-64FAC_CDR_Phasing_D07.pdf** and **https://www.cdr.gov.au/sites/default/files/2021-01/CDR%20phasing%20table%20-%20January%202021.pdf**

Australian Human Rights Commission, *Guidelines for Providers of Insurance and Superannuation Under the Disability Discrimination Act 1992 (Cth)* (November, 2016), **https://humanrights.gov.au/sites/default/files/AHRC_DDA_Guidelines_Insurance_Superannuation2016.pdf**.

Australian Law Reform Commission, "Privacy: Executive Summary" in *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)* (August, 2008), **https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/**

Australian Prudential Regulation Authority, *Quarterly General Insurance Statistics* (25 November, 2021), **https://www.apra.gov.au/quarterly-general-insurance-statistics**.

Australian Securities and Investments Commission (ASIC) and the Dutch Authority for the Financial Markets (AFM), *Disclosure: Why it Shouldn't Be the Default (REP 632)* (October, 2019), **https://download.asic.gov.au/media/5303322/rep632-published-14-october-2019.pdf**.

Australian Securities and Investments Commission, *Speech by Deputy Chair Karen Chester at the 2021 Annual Industry Forum of the Insurance Council of Australia* (13 October, 2021), **https://asic.gov.au/about-asic/news-centre/speeches/general-insurers-from-trust-deficit-to-trust-dividend/**.

Australian Treasury, *Review into Open Banking in Australia - Final Report* (23 December, 2017), **https://treasury.gov.au/consultation/c2018-t247313**.

Australian Treasury, *Consumer Data Right Rules Outline* (December, 2018), **https://www.accc.gov.au/system/files/CDR-Rules-Outline-corrected-version-Jan-2019.pdf**.

Australian Treasury, *Disclosure in General Insurance: Improving Consumer Understanding* (January 2019a), **https://treasury.gov.au/consultation/c2019-t354736**.

Australian Treasury, *Consumer Data Right: Overview* (September, 2019b), **https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf** .

Australian Treasury, *Privacy Impact Assessment – Response to Recommendations*, (December 2019c), **https://treasury.gov.au/publication/p2019-41016**.

Australian Treasury, *Submission on Measures Relating to the Consumer Data Right, Supplementary Submission 166.1 to the Senate Select Committee on Financial Technology and Regulatory Technology* (2020a), **https://www.aph.gov.au/DocumentStore.ashx?id=4da83cbd-90fe-40fd-bab8-0641da12bfad&subId=680576**.

Australian Treasury, *Inquiry into Future Directions for the Consumer Data Right - Final Report* (23 December, 2020b), **https://treasury.gov.au/publication/inquiry-future-directions-consumer-data-right-final-report**.

Australian Treasury, *DSB Opt-out Joint Account Data Sharing Model: CDR Rules and Standards Design Paper* (30 April, 2021a), **https://treasury.gov.au/sites/default/files/2021-04/c2021-168954-cdr_design_paper_joint_accounts.pdf**.

Australian Treasury, *Privacy Impact Assessment – Agency Response* (November, 2021b) **https://treasury.gov.au/sites/default/files/2021-11/p2021-223520-agency-response.pdf**.

Australian Treasury, *Government Response to the Inquiry into Future Directions for the Consumer Data Right* (14 December, 2021c), **https://treasury.gov.au/sites/default/files/2021-12/p2021-225462.pdf**.

Australian Treasury, *Consumer Data Right: Strategic Assessment: Outcomes* (January 2022), at **https://treasury.gov.au/sites/default/files/2022-01/p2022-242997-outcomes-report_0.pdf**.

Colin Biggers and Paisley, *Privacy Lessons for Insurers* (21 June, 2014), **https://www.cbp.com.au/insights/insights/2014/june/privacy-lessons-for-insurers**.

Competition and Markets Authority, *Open Banking: Background to Open Banking* (Undated), **https://www.openbanking.org.uk/wp-content/uploads/What-Is-Open-Banking-Guide.pdf**.

Competition and Markets Authority, *Retail Banking Market Investigation* (26 February, 2016), https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk.

Data Standards Body, *Consumer Data Standards, Version 1.16.0*, https://consumerdatastandards.gov.au/consumer-data-standards/.

Data Standards Body, *Consumer Experience Guidelines* (17 July 2020), https://consumerdatastandards.gov.au/consumer-data-standards/

Data Standards Body, *CX Guidelines – Consumer Dashboards* (5 August 2021), https://www.notion.so/Dashboards-e7c2aadc4677412b84f282272db9719e

European Commission, *European Parliament Adopts European Commission Proposal to Create Safer and More Innovative European Payments* (8 October, 2015), https://ec.europa.eu/commission/presscorner/detail/en/IP_15_5792.

Financial Rights Legal Centre, *Submission to Australian Treasury on Implementation of an Economy-Wide Consumer Data Right - Strategic Assessment* (September, 2021a), https://financialrights.org.au/wp-content/uploads/2021/09/210903_CDRStratAssess_FINAL.pdf.

Financial Rights Legal Centre, *Automating General Insurance Disclosure* (October, 2021b), https://financialrights.org.au/wp-content/uploads/2021/10/AutomatingDisclosure_report_FINAL.pdf.

Financial Rights Legal Centre, *Guilty Until Proven Innocent: Insurance Investigations in Australia* (March, 2016), https://financialrights.org.au/wp-content/uploads/2016/03/Guilty-until-proven-innocent.pdf.

Financial Rights Legal Centre, *Open Insurance – The Consumer Data Right and Insurance* (22 September, 2020), https://financialrights.org.au/wp-content/uploads/2020/12/Open-insurance-final-report.pdf.

Financial Rights Legal Centre, *Submission to Australian Treasury Opt-out Joint Account Data Sharing Model* (26 May, 2021), https://financialrights.org.au/wp-content/uploads/2021/05/210526_TreasuryCDROptoutModel_FINAL.pdf.

Fintecsystems, *The History of Open Banking* (20 March, 2019), https://knowledge.fintecsystems.com/en/blog/the-history-of-open-banking.

General Insurance Code Governance Committee, *Annual Industry Data and Compliance Report 2019-20* (March, 2021), https://insurancecode.org.au/app/uploads/2021/03/CGC_2019-20_Annual-Report_Final-Version.pdf.

Insurance Council of Australia, *ACCC Digital Platforms Inquiry: Preliminary Report* (February 2019), https://www.accc.gov.au/system/files/Insurance%20Council%20of%20Australia%20%28February%202019%29.PDF

Insurance Council of Australia, *Draft Australian Privacy Principles Guidelines* (20 September, 2013), https://insurancecouncil.com.au/wp-content/uploads/resources/Submissions/2013/2013_09/2013_09_Privacy%20Commissioner_ICA%20response%20to%20Draft%20APP%20Guidelines%201-5.pdf

Insurance Council of Australia, *General Insurance Code of Practice* (5 October, 2021) https://insurancecouncil.com.au/code-of-practice/.

Insurance Council of Australia, *Productivity Commission Inquiry into Data Availability and Use Submission* (29 July, 2016), https://insurancecouncil.com.au/wp-content/uploads/resources/Submissions/2016/2016_07/2016_07_Submission_PC_Data%20Access%20and%20Use.pdf.

Insurance Council of Australia, *Review of the General Insurance Code of Practice: Interim Report* (November, 2017), http://www.codeofpracticereview.com.au/assets/interim%20report/02112017_Interim_report.pdf.

Insurance Council of Australia, *Review of the Privacy Act 1988 (Cth) Issues Paper Submission*, (December, 2020), https://insurancecouncil.com.au/wp-content/uploads/resources/Submissions/2020/2020_12/2020_12_Privacy%20Act%20Issues%20Paper%20Submission.pdf.

Insurance Council of Australia, *Too long, Didn't Read: Enhancing General Insurance Disclosure* (October, 2015), https://web.archive.org/web/20160318225855/https://www.insurancecouncil.com.au/assets/Effective%20Disclosure%20report.pdf.

Insurance News, *Consumer Group Seeks Disclosure Oversight Solution (11 October, 2021)*, https://www.insurancenews.com.au/local/consumer-group-seeks-disclosure-oversight-solution.

Insurance News, *Cyber Attack Impacts Insurance House (14 June, 2019)*, https://www.insurancenews.com.au/daily/cyber-attack-impacts-insurance-house.

Insurance Reference Service, *DNBi: Individual Insurance Enquiry (27 August, 2016)*, https://insurancereferenceservices.com.au/assets/DNBi%20IRS%20Individual%20Insurance%20Enquiry.pdf.

Maddocks, *Analysis of the Consumer Data Right Regime Privacy Impact Assessment (PIA) Report to the Department of the Treasury* (November, 2019) https://treasury.gov.au/sites/default/files/2019-12/p2019-41016_PIA_final.pdf.

Maddocks, *Australian Competition and Consumer Commission: Consumer Data Right Regime, Update 1 to Privacy Impact Assessment* (4 September, 2020a), https://www.accc.gov.au/system/files/CDR%20Accredited%20Intermediary%20Rules%20–%20Update%201%20to%20Privacy%20Impact%20Assessment.pdf.

Maddocks, *Australian Competition and Consumer Commission: Consumer Data Right Regime, Update 2 to Privacy Impact Assessment* (29 September, 2020b, but finalised on 8 February 2021a), https://www.accc.gov.au/system/files/CDR%20v2%20Rules%20–%20Update%202%20to%20Privacy%20Impact%20Assessment.pdf.

Maddocks, *Update 3 to the Privacy Impact Assessment – For the ACCC* (September, 2021b) https://treasury.gov.au/sites/default/files/2021-10/p2021-213006-pia-maddocks.pdf

Maddocks, *Update 4 to the Privacy Impact Assessment – for the Department of the Treasury* (October, 2021c), https://treasury.gov.au/sites/default/files/2021-11/p2021-223520-update-4.pdf.

Malbon, Professor Justin, and Oppewal, Professor Harmen, *(In)effective Disclosure: An Experimental Study of Consumers Purchasing Home Contents Insurance* (Monash Business School and Monash Faculty of Law, research report of a study commissioned by Financial Rights Legal Centre) (2018), https://financialrights.org.au/wp-content/uploads/2018/09/InEffectiveDisclosure-final_embargoed-until-17-Sep.pdf.

Manthorpe, Rowland, "To Change How You Use Money, Open Banking Must Break Banks" in *Wired United Kingdom* (16 October, 2017), https://www.wired.co.uk/article/psd2-future-of-banking.

Manthorpe, Rowland, "What is Open Banking and PSD2? WIRED explains" in *Wired United Kingdom* (17 April, 2018), https://www.wired.co.uk/article/open-banking-cma-psd2-explained.

Martin, Mina, "Youi and Blue Zebra Confirm New Underwriting Relationship" in *Insurance Business Australia* (27 February, 2020), https://www.insurancebusinessmag.com/au/news/breaking-news/youi-and-blue-zebra-confirm-new-underwriting-relationship-215002.aspx.

Office of the Australian Information Commissioner, *Annual Report 2019-20* (November, 2020), https://www.transparency.gov.au/annual-reports/office-australian-information-commissioner/reporting-year/2019-20-11.

Office of the Australian Information Commissioner, *Australian Privacy Principle Guidelines* (July, 2019), https://www.oaic.gov.au/__data/assets/pdf_file/0009/1125/app-guidelines-july-2019.pdf.

Office of the Australian Information Commissioner, *CDR Privacy Safeguard Guidelines*, *Version 2.0* (July, 2020), https://www.oaic.gov.au/assets/consumer-data-right/cdr-privacy-safeguard-guidelines-v2.0-july-2020.pdf.

Office of the Australian Information Commissioner, *CDR Privacy Safeguard Guidelines*, *Version 3.0* (June, 2021), https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines.

Office of the Australian Information Commissioner, *CDR Regulatory Action Policy* (June, 2020), https://www.oaic.gov.au/consumer-data-right/cdr-regulatory-action-policy/.

Office of the Australian Information Commissioner, *Consumer Data Right Complaints*, (24 August, 2021) https://www.oaic.gov.au/updates/videos/cdr-complaints.

Office of the Australian Information Commissioner, *Third-party Access to Credit Reports* (2021), https://www.oaic.gov.au/privacy/credit-reporting/third-party-access-to-credit-reports.

Productivity Commission, *Data Availability and Use (Report No. 82)* (31 March 2017), https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf.

Select Committee on Australia as a Technology and Financial Centre, *Final Report* (October, 2021), https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/AusTechFinCentre/Final_report.

Select Committee on Financial Technology and Regulatory Technology, *Interim Report* (September, 2020) https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/FinancialRegulatoryTech/Interim_Report.

Senate Economics References Committee, *Australia's General Insurance Industry: Sapping Consumers of the Will to Compare* (August, 2017), https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Generalinsurance/Report.

LEGISLATION

Australian Securities and Investments Commission Act 2001, https://www.legislation.gov.au/Details/C2021C00281

Competition and Consumer Act 2010, http://www5.austlii.edu.au/au/legis/cth/consol_act/caca2010265/

Competition and Consumer (Consumer Data Right) Rules 2020 (Current version), https://www.legislation.gov.au/Series/F2020L00094.

Corporations Act 2001, http://www5.austlii.edu.au/au/legis/cth/consol_act/ca2001172/

Disability Discrimination Act 1992, http://www5.austlii.edu.au/au/legis/cth/consol_act/dda1992264/

Do Not Call Register Act 2006, http://classic.austlii.edu.au/au/legis/cth/consol_act/dncra2006201/

Data Standards Body, Consumer Data Standards, Version 1.16.0, https://consumerdatastandards.gov.au/consumer-data-standards/

Insurance Contracts Act 1984, http://classic.austlii.edu.au/au/legis/cth/consol_act/ica1984220/.

Privacy Act 1988, http://www5.austlii.edu.au/au/legis/cth/consol_act/pa1988108/

Privacy Act 1988 - Schedule 1 Australian Privacy Principles, http://www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/pa1988108/sch1.html.

Spam Act 2003, http://classic.austlii.edu.au/au/legis/cth/consol_act/sa200366/

Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth), http://classic.austlii.edu.au/au/legis/cth/num_act/tladra2019450/sch1.html

Appendix 1: The general insurance market

This Appendix identifies sources accessed in the development of a brief outline of the nature and structure of the consumer segment of the general insurance industry in Australia.

OUTLINE OF THE GENERAL INSURANCE INDUSTRY

See Section 2.2, pp.10-16, of the "Open Insurance Report" of 22 September, 2020 (Financial Rights, 2020).

MARKET SIZE

https://www.apra.gov.au/quarterly-general-insurance-statistics

LISTS OF MARKET PLAYERS

https://insurancecouncil.com.au/industry-members/members-and-member-brands/

The IAG Group

https://www.iag.com.au/about-us/who-we-are
https://www.iag.com.au/coles-insurance

In mid-2021, the site listed seven brands: NRMA Insurance, CGU, SGIO, SGIC, Swann Insurance, WFI and Poncho Insurance. Recently lapsed brands in the IAG stable appeared to be Lumleys and Buzz Insurance.

In the case of at least NRMA Insurance, contracts with consumers are written in the name of Insurance Australia Limited (AIL), rather than NRMA or IAG.

At least two further brands appear to be within the IAG Group:

- The IAG page declares that "[IAL] is the underwriter of general insurance products under the Coles Insurance brand"; and
- RACV's page-footer declares that "RACV Motor Insurance is issued by Insurance Manufacturers of Australia Pty Limited", which is owned 70% by IAG and 30% by RACV.

The Suncorp Group

https://www.suncorpgroup.com.au/about/brands
https://www.suncorpgroup.com.au/uploads/FINAL%20-%20Companies%20and%20Brand%20122016.pdf
https://www.suncorpgroup.com.au/uploads/Companies-and-Brand-28-Nov-19.pdf
https://www.vero.com.au
https://www.vero.com.au/content/dam/suncorp/

In mid-2021, the site listed 8 brands AAMI, Apia, GIO, Bingle, CIL, Terri Scheer, Shannons, Vero and "Essentials by AAI". Other sources suggest Suncorp controls at least four more brands: InsureMyRide, Tyndall Insurance and Just Car (all of which appear to be no longer operating), but also MTA Insurance, which declares on its homepage that it "is the distributor of certain insurance products issued by AAI Limited" and that "Suncorp acquired MTAI in 2014".

https://www.mtai.com.au/faq_remediation/
https://www.abr.business.gov.au/AbnHistory/View/64001698228

APRA's Register of General Insurers lists about 80 names, but this appears to encompass both the business and consumer segments, to include reinsurers, and to exclude brands:
https://www.apra.gov.au/register-of-general-insurance

ICA's "Find an Insurer" service identifies:

- 62 'Building' insurer-members, athttps://www.findaninsurer.com.au/category/132;
- 69 motor vehicle insurer-members, at https://www.findaninsurer.com.au/category/33 .

Other Players

Other Players identified by Wikipedia, at https://en.wikipedia.org/wiki/Insurance_in_Australia#General_insurers, are:

- Allianz Australia, which has brands including Club Marine and Hunter Premium Funding
- Auto and General, which has brands including Budget Direct, Australia Post and Virgin Money, and underwrites home and car insurance from 1Cover.
- Its "Find a PDS" page also discloses the brands Aussie, Best Buy Insurance, Cashback Car Insurance, Catch Insurance, Maxxia Insurance, Ozicare Insurance, QANTAS Insurance and Retirease Insurance
  https://www.autogeneral.com.au/customers/find-pds
- Hollard Insurance markets its policies through brands including Real Insurance and Guardian, and through agents such as Woolworths and Australian Seniors Insurance. On its Insurance Partners page Hollard also identifies Kogan Insurance, and nine seemingly different Pet Insurance brands
  https://www.hollard.com.au/insurance-partners/retail-brands-and-partners.aspx
  (However, Hollard and PetInsurance are linked to from AAMI's site; so it is unclear what the relationship is between AAMI/Suncorp/AAI and Hollard/PetInsurance)

The following 25 motor vehicle insurers – variously insurance companies and brands – were sampled by Financial Rights during a recent research project:

- AAMI, Allianz, ANZ, Bingle, Budget Direct, BUPA, CGU, Coles, Comminsure, GIO, Guild, NRMA, Progressive, QBE, RAC, RACQ, RACT, Real Insurance, St George, Suncorp, Toyota Insurance, Virgin Money, Westpac, Woolworths, and Youi.

An early-2021 Choice survey considered these 34 car insurers:

- AAMI, Allianz ANZ, Bank of Melbourne, BankSA, Bankwest, Bingle, Budget Direct, Catch, CGU, Coles, Comminsure, GIO, Huddle, ING, Kogan, NAB, NRMA, QBE, RAA, RAC, RACQ, RACT, RACV, Real, SGIC, SGIO, StGeorge, Suncorp, TIO, Virgin Money, Westpac, Woolworths, Youi.

In mid-2021, comparethemarket compared only 12 motor vehicle insurers: /**https://www.comparethemarket.com.au/car-insurance/**

- 1st for Women, Budget Direct, Huddle, Ozicare Insurance, Retirease, Virgin Money, Woolworths, PD Insurance, Eric, Carpeesh, Stella, ING

and only 6 home and contents insurers:**https://www.comparethemarket.com.au/home-contents-insurance/**

- ING, Budget Direct, CHU, Huddle, Woolworths, Virgin Money

iSelect.com.au compared across an even smaller sub-set of the industry – 8 and 3 respectively **https://www.iselect.com.au/partners/**

Canstar lists about 50, a mix of corporation-names and brand-names:**https://www.canstar.com.au/providers/life-insurance/**

Appendix 2: The Privacy Policy and Terms of AAMI

A2-1 BACKGROUND

Relevant law and regulation in relation to privacy in the general insurance industry are complemented by each insurer's:

- Privacy Policy. This is a document required by Australian Privacy Principle 1.3, and required to be clearly expressed and up-to-date; and
- Any aspects of the commercial terms and conditions that apply to the insurer's services, and that are relevant to privacy matters.

In order to provide general insight into the relationship between these documents including their accessibility and comprehensibility by consumers, the documents of large, well-known insurer AAMI were selected and assessed.

A2-2 AAMI'S PRIVACY POLICY

We commenced by locating the company's Privacy Policy. The company has a readily-accessible homepage at aami.com.au. The page is very busy and long. The word "privacy" exists in two places:

- In a clickable link "Privacy statement" within the car insurance block (but not within the home and contents block beneath it); and
- In another clickable link, "Online Terms and Privacy", in the footer.

Both link to **https://www.aami.com.au/privacy.html**.

Figure A5-1 is a screenshot of the first half of the roughly 2 x A4-page display, the remainder being common footers of limited relevance to this part of the analysis. The image was captured on 17 January, 2022. No material difference was detected between this and screenshots taken in June 2021.

The page evidences the complexity of information about privacy and related terms available to the public from the website of a major insurer. The page contains no fewer than 20 clickable links, including three group privacy policies and 12 product-specific privacy statements.

Most of the links are to pages on the aami.com.au site. The exceptions are:

- The first link from:

  "Read our Group Privacy Policy – Suncorp Group Privacy Policy (including list of countries)" leaves the aami.com.au site, and goes to: **https://www.suncorpgroup.com.au/about/corporate-governance/privacy-policy**

  Nothing on these pages explains to the consumer which organisation their contract is with, nor the extent to which, or circumstances in which, the Suncorp Policy applies.
- The last four links in the "Pet Insurance" block also leave aami.com.au and direct consumers to various pages on the **https://www.petinsurance.com.au/** site.

No explanation is provided about the commercial relationship between AAMI and PetInsurance, nor between the consumer and AAMI.

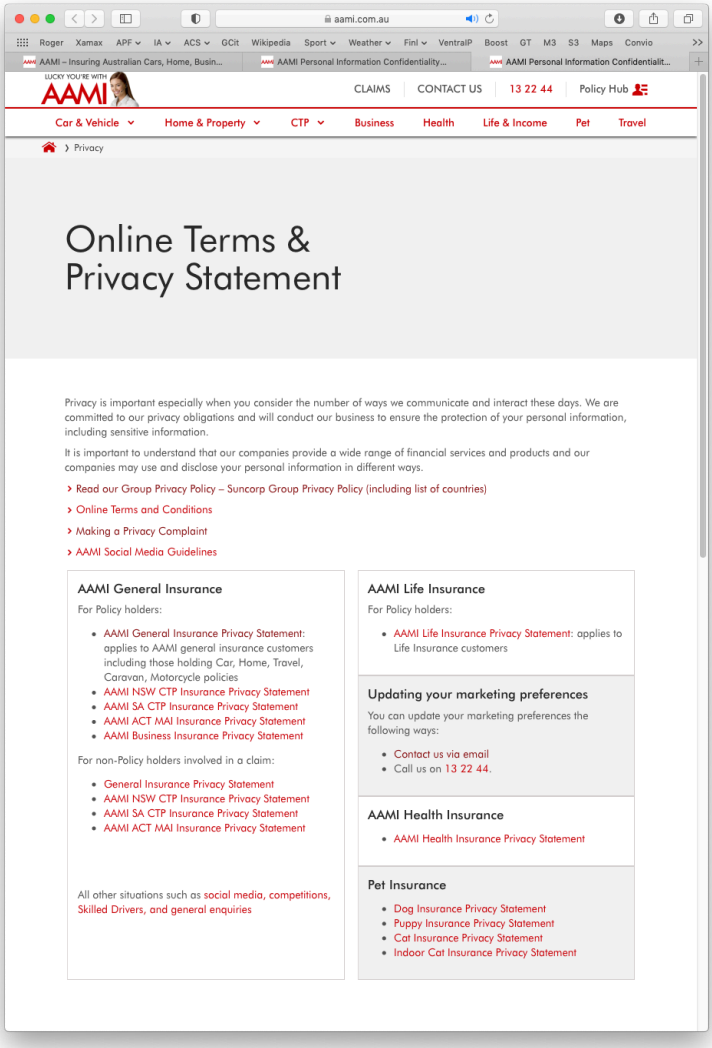
Moreover, the title page of the .pdf documents states:

"Petinsurance.com.au insurance is issued by:
The Hollard Insurance Company Pty Ltd (Hollard) ...
Pet Insurance Pty Ltd is an Authorised Representative of PetSure (AR No. 1234944).
Petinsurance.com.au is arranged and administered through:
PetSure (Australia) Pty Ltd (PetSure) ABN 95 075 949 923 ..."

The first link in the first block "AAMI General Insurance Privacy Statement" links to a .pdf document: AAMI General Insurance Privacy Statement.

This speaks as AAMI. Further confusion arises from the statement that "AAI Limited trading as AAMI is the insurer and issuer of your insurance product, and is a member of the Suncorp Group, which we'll refer to simply as "the Group". It is entirely unclear which organisation or organisations are party to the consumer contract, which organisation(s) will deliver the service, and which will possess, use and disclose the personal data arising from the relationship(s).

Figure A5-1: AAMI Privacy Page[40]



40 AAMI, Privacy Page, https://www.aami.com.au/privacy.html.

A2-3 AAMI'S TERMS AND CONDITIONS

The second link on the page to "Online Terms and Conditions".[41]

As is the case with many other insurers, some of the information available relates specifically to online interactions, while other information is more generally about any interaction including by phone, post or face to face. The distinction is not always clear.

The "Terms and Conditions" in AAMI's case are clearly labelled as "On-line". It is not clear whether there are other terms and conditions that apply to any insurance contract entered into. These may only be visible at some point in an application and acceptance process, hopefully before a consumer is expected to commit themselves.

The "Terms and Conditions" are actually those of AAI Limited, trading as AAMI. Because the company/brand/group documents use AAMI as the brand in most communications, this Appendix continues to use "AAMI" even when the reference is to the legal entity AAI Limited.

The AAMI "Online Terms and Conditions" current version dated 1 October, 2021 replaced an earlier version dated March 2019. The size of the document increased from more than 14,000 words to more than 15,500 words across 34 sections. It starts by introducing two further complexities:

- AAMI Life Insurance and Income Protection products are provided by separate entities which are part of the TAL Dai-ichi group of companies **(TAL)**. TAL companies are not part of the Suncorp Group.

  The "Online Terms and Conditions" state that: "TAL is responsible for the content on and output from the [Life Insurance] webpages". Those pages are however branded as AAMI, without any immediate recognition that users would now be dealing with TAL; and
- A distinction between different "Online Sites" or media/channels, for example the AAMI "main site", "mobile site", "social media site" and "AAMI app" to which different terms and conditions (and different provisions of the privacy policies) may apply.

There are 52 occurrences of the word "privacy", and 47 of the expression "personal information".

Term 27 states that use of an Online Site constitutes acceptance of the relevant Terms together with relevant provisions of the Suncorp Privacy Policy and of applicable AAMI Privacy Statements.

There are 13 separate specific references to "consent" in the "Online Terms and Conditions". Only some of these are privacy related. Of those, most seem reasonable to those familiar with business structures and activities, even though some are clearly designed primarily to protect AAMI. It is unlikely that all of them would be within the reasonable expectations of consumers, e.g. consent for *any* AAMI use of social media content submitted by users for *any* purpose (terms 12 & 30.2.5). However, there is no reference in the "Online Terms and Conditions" to any privacy-related options for consumers, for example opt-out or opt-in choices for any specific uses or disclosures, including direct marketing. This level of detail is left to the various AAMI Privacy Statements.

The most significant privacy-related term is term 30 - Personal information submitted to an Online Site. This term mostly summarises, and overlaps with, treatment of the same issues in the various Suncorp Group and AAMI privacy policies and statements.

---

41 AAMI, Online Terms and Conditions, https://www.aami.com.au/privacy/online-terms-and-conditions.html

Most significantly, term 30.2.1 states that in relation to any personal information submitted "via" an Online Site "... you consent to that personal information being collected by AAMI and used and disclosed for any purpose permitted by these "Online Terms and Conditions", and otherwise as permitted by relevant privacy laws in Australia" – giving AAMI authority for the broadest possible range of uses and disclosures.

Subsequent terms refer to product-specific Privacy Statements for further detail on how AAMI processes personal information from potential or actual customers (30.2.3) and from other individuals such as witnesses (30.2.4).

Other terms explain AAMI's compliance with other Australian Privacy Principles such as security (Australian Privacy Principle 11), rights of access (Australian Privacy Principle 12) and direct collection (Australian Privacy Principle 3.6), as well as contributing to compliance with the transparency and notice principles (Australian Privacy Principles 1 and 5).

In a section of the "Online Terms and Conditions" dealing specifically with recruitment, a commitment is given that when engaging or employing third part contractors or vendors "... [AAMI] will take reasonable steps to prohibit these parties from using your personal information except for the purposes for which it was supplied" (30.4.7). It is not clear why the T&Cs do not extend this commitment to all outsourcing circumstances.

A2-4 THE VARIOUS SPECIFIC PRIVACY POLICIES AND STATEMENTS

The Suncorp Group Privacy Policy

Both the privacy page on AAMI's website (Figure A5-1) and their "Online Terms and Conditions" make reference to the Suncorp Group Privacy Policy.[42]

That policy provides "... general information about how the companies/brands in Suncorp manage your personal information as required by relevant Privacy laws". This therefore constitutes an overview of the privacy practices of all businesses within the Suncorp Group, using the terms "we", "us" and "our" generically, although not expressly defining them.

The policy defers to the various company and product specific privacy statements, and to T&Cs, for specific detail:

> *"The Privacy Statement will give you specific information about how we will manage the personal information for the particular product or service and/or the particular company/brand."*

The policy also refers and links to Suncorp T&C, which are similar but not identical to the AAMI "Online Terms and Conditions". The Suncorp T&C include a further 13,000 words across 38 sections.

In the event of any inconsistency between the Suncorp privacy policy and T&C and the AAMI Privacy Statements and "Online Terms and Conditions", it is unclear whether those of AAMI would prevail since AII, trading as AAMI, is the legal entity with whom an individual will be communicating, or those of Suncorp, given that AAI/AAMI is a member of that group.

---

42 Suncorp Group, *Privacy Policy*, **https://www.suncorp.com.au/about-us/legal/privacy.html**.

The statement that "parties to whom we may disclose your personal information to and collect personal information from" lists 24 separate categories of "disclosee" and six sub-categories of contractors. It is possible that the length of this list may partly reflect the fact that it relates to the whole Suncorp Group.

One significant clause in the Suncorp Privacy Policy addresses information sharing within the Group:

> *"Collection, use and disclosure of personal information between companies in Suncorp*
>
> *We will share your personal information with all companies that form a part of Suncorp. If one Suncorp company collects your personal information, other Suncorp companies may use and disclose your personal information for the purposes described in the "Collection of personal information" section in relation to any products and services they may provide to you. Other companies in Suncorp may also use your personal information for the purposes of providing products and services to other customers (but we will not disclose your personal information to any other customer without your consent)."*

The AAMI General Insurance Privacy Statement

We have reviewed in detail a representative Privacy Statement. However, the other 14 AAMI Privacy Statements appear very similar. The document we selected [43] is undated, but the filename suggests this version dates from May 2019.

As with the "Online Terms and Conditions", this is actually the privacy policy of the legal entity AAI Ltd, trading as AAMI. Under the *Privacy Act*, the APP entity will also be AAI Limited.

The Privacy Statement is relatively brief at six pages, and unlike the "Online Terms and Conditions" is written in a "plain English" style.

Under a heading "How we handle your personal information" the Privacy Statement lists several categories of people, organisations and sources that "...We may disclose your personal information to and/or collect your personal information from". It states:

> *"We will use and disclose your personal information for the purposes we collected it as well as purposes that are related, where you would reasonably expect us to." (emphasis added)*

Most of these categories are likely within individuals' reasonable expectation of uses and disclosures. They appear to be either associated with the service or transaction, or reasonable business practices, for example statistical analysis or research.

---

43 The document selected is at **https://www.aami.com.au/aami/documents/aami/privacy/aami-privacy-statement-general-insurance-23052019.pdf**, viewed on 11 Jun 2021

An area in which the assertion of reasonable expectation might be challenged and where at least some individuals may be expected to have concerns, is in relation to disclosure and use by associated businesses, and in particular use for marketing of other products or services.

The privacy statement states:

> *"We also provide your personal information to other related companies in the Group, and they may disclose or use your personal information for the purposes described in 'Why do we collect personal information?' in relation to products and services they may provide to you …".*

It also states, under a separate heading: "Your personal information and our marketing practices":

> *"Every now and then, we and any related companies that use the AAMI brand might let you know – including via mail, SMS, email, telephone or online – about news, special offers, products and services that you might be interested in. We will engage in marketing unless you tell us otherwise. You can contact us to update your marketing preferences at any time."*

Appendix 3: Privacy issues in general insurance

This Appendix supports Section 2.5 by providing further detail about privacy issues that arise in relation to data practices in the general insurance industry. The sections correspond with the Australian Privacy Principles. The term "APP entities" includes larger general insurance businesses and Australian Government agencies.

A3-1 AUSTRALIAN PRIVACY PRINCIPLE 1 – OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

This ensures that APP entities manage "personal information" in an open and transparent way. This includes having a clearly expressed and up-to-date APP privacy policy.

It is a requirement under Australian Privacy Principle 1 for APP entities to have a clear and up to date privacy policy. OAIC guidance permits a layered approach to the communication of privacy information. Larger organisations may have short privacy notices where personal information is collected, for example on forms, which link to longer statements or full policies which should be readily accessible, typically online.

The privacy notices, statements and policies of insurers vary in quality.

Communicating complex information clearly and accurately remains challenging as a report by Financial Rights revealed in 2018 (Malbon and Oppewal, 2018). There has been considerable academic argument to the effect that most consumers do not even read, let alone understand privacy-related material, but typically just "accept" privacy settings as a condition of service. This incidentally gives insurers the opportunity to claim inferred consent for the practices described in the detailed text.

It is often difficult for consumers to ascertain which organisation is collecting and using their personal information. Services are often "branded" in that they are provided under a brand-name which often does not correspond to the legal entity behind the brand. Confusion is compounded by corporate structures in which related entities are grouped. There is the further complication of intermediaries such as agents or brokers, and of re-insurance whereby another party takes on all or part of the risk initially accepted by an insurer. These are well- established industry practices, but the relationships are not well understood by consumers.

For example, as discussed **(see Section 2.1.2 and Appendix A2-4)**, Suncorp Financial Services Group offers insurance through a legal entity AAI Limited which is marketed under various brands such as GIO, AAMI and Vero. Even where these corporate relationships are explained in the fine print, different consumers may well have different perceptions of which organisation it is they are dealing with and entrusting with their personal information.

A3-2 AUSTRALIAN PRIVACY PRINCIPLE 2 – ANONYMITY AND PSEUDONYMITY

Australian Privacy Principles 2, 3 and 5 regulate the collection of personal information/data.

Australian Privacy Principle 2 requires APP entities to give individuals a qualified option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

Australian Privacy Principle 2 has limited relevance to the issues of privacy for most general insurance customers as there are few circumstances in which insurers would need to hold information from or about an individual customer but could reasonably offer anonymity or a pseudonymous option:

> *"It will generally be impracticable for insurers to provide their services or products to customers unless they are able to gather essentially personal information to ascertain and price for risk." (ICA, 2020).*

One important exception is the receipt of accusations of fraud, if a person reporting does not wish to be identified. Another exception is general enquiries about products and services, particularly where there is no need to be able to make contact at a later stage and continue a conversation.

A3-3 AUSTRALIAN PRIVACY PRINCIPLE 3 - COLLECTION OF SOLICITED PERSONAL INFORMATION

Australian Privacy Principle 3 outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of sensitive information

Australian Privacy Principle 3 is an important safeguard. In 3.2, it requires private sector APP entities collecting personal information to only collect information reasonably necessary for one or more of the organisation's functions or activities.

Australian Privacy Principle 3 does not generally require consent for collection, but consent is a basis for the collection of sensitive information.

Further limitations in Australian Privacy Principle 3.3 and 3.4 apply to the collection of "sensitive information" as defined in the *Privacy Act*. While financial information is not included in the definition of "sensitive information", two other categories involved in the collection of some insurance information are included. These are "criminal record" which may be relevant in motor and home building and contents insurance and "health information" which may be relevant in travel insurance, and, in respect of some conditions, for example such as epilepsy and sight-impairment, in motor insurance.

Collection of sensitive information can be based on either consent (provided it is reasonably necessary) or a range of exceptions.

Australian Privacy Principle 3.5 also regulates the means of collection of personal information, requiring that collection must be by lawful and fair means. This will be relevant to surveillance practices in claims and fraud investigation.

Australian Privacy Principle 3.6 and 3.7 require that solicited personal information should be collected by private sector organisations directly from the individual concerned, unless it is unreasonable or impracticable to do so. This is relevant to the common practice of obtaining some personal information from third party databases, discussed below.

A3-3.1 Collection issues in enquiry/application for cover

Some data collection forms fail to make clear which data items must be disclosed or which may only need to be disclosed under particular circumstances. Many forms use an asterisk or other symbol to indicate mandatory fields. This is not an appropriate design feature, because various fields require completion only under particular circumstances. Moreover, in the case of online forms, consumers may find there is no other way to continue with an application without entering something in fields that are not justifiably mandatory. Consumers may gain the wrongful impression that their obligations at law extend to answering all questions, or doing so at levels of detail that are unjustified.

Online application processes often preclude the submission of an incomplete form and often even preclude temporarily storing an incomplete form and returning to complete it later. Moreover, it is often impractical for a person completing a form to find the answers to some questions in real time. There is also the common problem of not knowing how long an application process will take and finding it necessary to abort the process due to lack of time. Both problems may contribute to the provision of inaccurate information if consumers either make a guess or enter what information they think might be required without verifying it.

Unlike many business relationships, where an insurer's decisions about what information to request, and a consumer's decisions about what information to provide, are based on a combination of practical and commercial considerations, insurance contracts are subject to statutory disclosure obligations under a "duty to take reasonable care not to make a misrepresentation to an insurer" in the *Insurance Contracts Act 1984* (Part IV). This duty is enforceable from 1 October 2021 and replaces the former "duty of disclosure" which had come under criticism during the Financial Services Royal Commission.

Another collection issue specific to motor vehicle insurance relates to automated and often unseen data collection. This occurs with telematics such as vehicle auto-reporting of engine condition to manufacturers, or location to hire-car companies.

Routine collection by insurers of personal information from third party databases is discussed further below.

A3-3.2 Consent for collection

Other than for the narrowly-defined category of "sensitive" information, there is no express or implied requirement for consent for the collection of personal information. In most circumstances, where information is being collected directly from an individual, their consent could reasonably be inferred from their willingness to provide the information, although this assumes awareness and understanding on part of the consumer. These issues are discussed under Australian Privacy Principle 5 further below.

In relation to consent, ICA stated in their 2020 submission to the *Privacy Act* Review:

> *"A written [consent] notification requirement would limit the ability for insurers to provide quotes to prospective customers who contact general insurers by telephone, as written notice would first need to be provided prior to information collection. This would delay the provision of the quote, and potentially insurance cover in time-critical situations."*

There are many practical ways in which consent can be achieved. For example, in voice conversations, a record can be expressly made by the insurance company's employee or agent to the effect that a request for consent was made and a verbal consent was given. Forms can contain a brief explanation, a pointer to more detailed information, and an adjacent tick-box to signify agreement. In the case of relatively lengthy forms, this is most reasonably done early in the process, rather than confronting the consumer with a demand only after they have invested considerable time and effort.

A3-3.3 Collection issues in claims investigations

The generic problems noted in the case of applications apply to claims forms as well.

Specific issues and concerns raised with us in interviews by Financial Rights and other consumer groups include:

- Investigator asking for my.gov.au details and password;
- Investigator asking for social media passwords;
- Investigators asking seemingly inappropriate and irrelevant questions about people's private lives;
- Contacting colleagues, family and friends revealing an investigation;
- Collection and storage of sensitive data, proxies for sensitive data, and discriminatory practices such as asking particular kinds of questions of people only of particular ethnic backgrounds;
- Potentially inappropriate use of flags for claims investigation purposes, use of proxies for sensitive information (Financial Rights Legal Centre, 2016);
- Unreasonable requests for information; and
- Demand for overly broad consents to obtain information from third parties.

The issues noted above are all in the data privacy arena. Further issues arise in relation to behavioural privacy, including:

- Covert Surveillance. This is used less in general insurance and more in health and income protection insurance. However there are new rules in the General Insurance Code covering surveillance
- Overt Surveillance. Where used, this may be less to gather information than to put pressure on the claimant

> *In one matter, the insurer's standard claim form asked the insured to agree that the insurance company "may disclose to anybody any information about you". The insured did not sign the claim form and instead wrote to the Privacy Commissioner.*
>
> *On investigation, and not surprisingly, the Privacy Commissioner agreed that the terms of the claim form were very broad. He did not take further action because the insurance company provided evidence that its practice was not to rely on the broad consent given in the standard claim form, but to rely on later more specific authority and because it also agreed to amend the claim form to remove the broad form of consent (Colin Biggers and Paisley, 2014).*

A3-3.4 Collection issues with third party databases

Insurers routinely obtain personal information about their clients from third party databases, including, but not limited to:

- The IRS **(See sections 2 and 3)**;
- The electoral roll;
- Registers of Births, Deaths and Marriages;
- Bankruptcy records; and
- Court judgments

There are other databases which may be seen by insurers to be useful to verify information provided by applicants or clients, but to which they currently do not have access. These include:

- Driver licence records, including infringements;
- Criminal records;
- Credit reporting databases, operated by commercial organisations but tightly regulated by a specific regime under the Privacy Act (Part IIIA):

> ***Who isn't allowed access***
>
> *"Neither a real estate agent, landlord, employer, foreign credit provider, foreign credit reporting body or insurance company (other than mortgage insurer and trade insurer) are allowed to access your credit report.*
>
> *Your consumer credit report also includes a log of who has accessed it. A credit provider or other third party isn't generally able to view this information." (OAIC, 2021).*

The distinction between available and prohibited databases is complicated by the way in which the large commercial database operators organise and maintain records. Often a basic index of identifying particulars, for example names, date of birth, driver licence no, addresses, other contact details, is held separately. Links are made only as required to more detailed information such as insurance applications, contracts and claims in the case of the IRS or to make up a consumer credit information in the case of the large credit reporting bodies, of which there are three currently operating in Australia –Equifax (formerly Veda), Illion (formerly Dun & Bradstreet) and Experian.

The relationships are further complicated in the case of the IRS which is operated on behalf of its insurer members by Illion. It is unclear whether Illion checks any personal information about customers of insurers against any of the data-holdings that form part of its credit reporting business. **(See Sections 2.2.2 and 2.6.1)**.

Governments have allowed progressively greater access for the private sector to some official databases over the past few decades, including the electoral roll and registers of births, deaths and marriages, particularly for the purposes of identity authentication. This has increasingly been made an obligation for such activities as the opening of accounts in telecommunications and to comply

with financial services laws such as anti-money laundering. The Australian Government now operates a Document Verification Service, as part of a wider suite of identity matching services:

> *"The Document Verification Service (DVS) is a national secure online system, which enables authorised entities to electronically verify Evidence of Identity documents issued by a range of Australian, State and Territory government agencies.*
>
> *The Document Verification Service (DVS) checks whether the biographic information on your identity document matches the original record. The result will simply be 'yes' or 'no'. The DVS does not check facial images.*
>
> *The DVS makes it harder for people to use fake identity documents.*
>
> *The DVS has been operational since 2009. Both the public and private sector use the DVS."*[44]

The Department of Home Affairs privacy notice for the Identity matching service only offers this general explanation:

> *"Use of the Identity Matching Services must be reasonable, necessary and proportionate to a user's functions or activities, and organisations must ensure their use complies with all relevant privacy and other laws.*
>
> *Approved government and private sector organisations in Australia and New Zealand can access the DVS."*[45]

Private sector users gain access through a Gateway Service Provider **(GSP)**.[46] The criteria for business use is set out in an "Access Policy and Guidelines". This includes examples of purposes likely to meet a "reasonable necessity" test. Insurers seem likely to qualify under a provision relating to "entering into a binding legal contract involving significant financial or other liabilities".

There does not appear to be a readily accessible list of approved private sector users of the DVS. However, we understand that the three credit reporting bodies have access. Equifax is a GSP and in the case of Illion this access is presumably also used for the IRS, and therefore by or on behalf of its insurer members.

A3-3.5 Wider access by insurers to third party databases

There is an active debate as to whether permitting insurers access to further third party databases is in the interests of consumers (Financial Rights, October 2021). Automated access to such databases may improve the quality of the information used by insurers and avoid some of the many instances where insurance claims are refused on the basis that incomplete or inaccurate information has been provided by an insured party.

---

44 Australian Government, *Identity Matching Services - What Are They?* **https://www.idmatch.gov.au/our-services**.

45 Australian Government, *Identity Matching Services Help You to Prove You Are Who You Say You Are*, **https://www.idmatch.gov.au/for-individuals**.

46 Australian Government, *Become a Document Verification Service Business User* states that 19 are currently fully operational with a further four approved but not active, **https://www.idmatch.gov.au/for-organisations/business-user**.

However, routine automated access to third party databases, even if it were ostensibly conditional on informed consent, is in apparent conflict with the spirit of Australian Privacy Principle 3.6(b) – which requires direct collection where reasonable and practicable, and with the underlying objective of the *Privacy Act* to give individuals as much control as possible over their own personal information.[47]

A3-3.6 Collection from third parties necessarily involves disclosure

Compliance with Privacy Principles when collecting personal information from third parties relates not only to the collection principles embodied in Australian Privacy Principles 2 and 3 but also necessarily involves Australian Privacy Principle 6 relating to limitations on use and disclosure. This is because in order to collect information about an individual from a third party, an insurer must first disclose information it already holds, usually at least a name, in order to make the request.

Insurers would typically be able to rely on one or both of two exceptions; consent in Australian Privacy Principle 6.1(a) and/or "related purpose within reasonable expectation" in Australian Privacy Principle 6.2(a). This in turn would be based on notice given to individuals and/or acceptance of T&Cs. This is analysed in the section relating to transparency in Australian Privacy Principle 1 and notice in Australian Privacy Principle 5.

A3-3.7 Collection issues in anonymous allegations of fraud

Without making test calls or sending test emails concerning allegations directly to insurers, it is not possible to ascertain how insurers respond to an attempt to make an anonymous allegation of insurance fraud.

The insurance industry operates a public fraud reporting facility whereby anyone can report a suspicion of insurance fraud. The ICA website states that "IFBA provides a business hours service for community members to report suspected insurance fraud" but notes "We will shortly be launching a new portal for reporting fraud, in the meantime, to report suspected fraud, please email IFBA".[48] The link provided opens an email to **IFBAcoordinator@insurancecouncil.com.au**, with the subject line "reporting suspected insurance fraud via ICA website".

1. Persons reporting fraud are invited to give the following information:
2. Your name;
3. Your preferred email address;
4. Your contact number;
5. The full name of the person(s) that you believe may be committing insurance fraud; and
6. Description of the suspected fraud.

Additional details if known:

1. The date of birth of the person(s) you believe may be committing insurance fraud;
2. The full address of the location where you believe the fraud occurred; and
3. Date of incident, if known.

---

47 http://www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/pa1988108/sch1.html

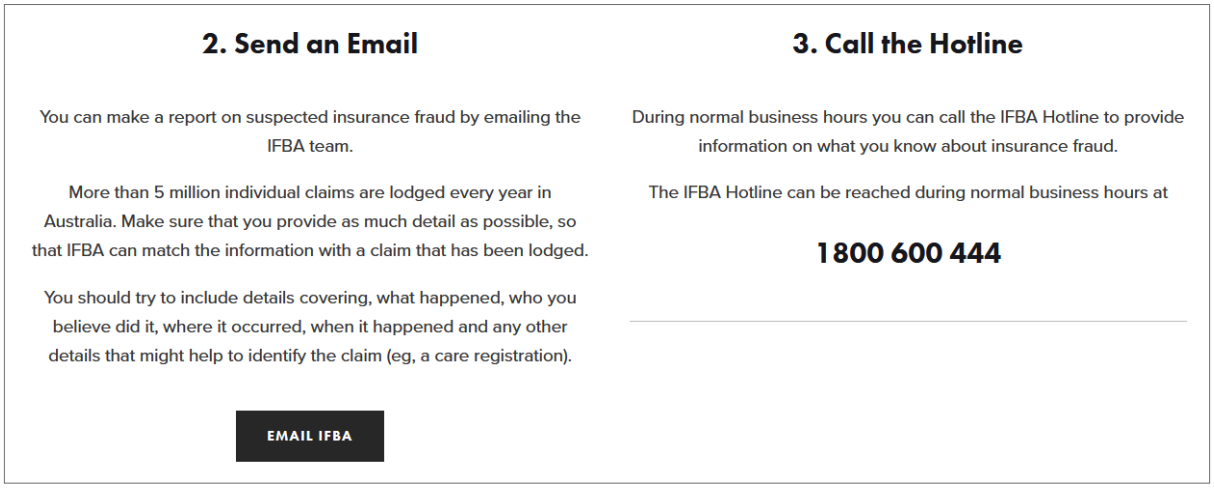
48 Insurance Council of Australia, *Insurance Fraud*, https://insurancecouncil.com.au/consumers/insurance-fraud/.

Obviously, following these instructions does not assure the person making the report of anonymity, but they could presumably use a pseudonym and non-personal email address, and either a false or no phone number, if they wished to protect their identity.

The ICA webpage appears to be out of date, as the new portal it foreshadows is now available.[49] However, only one of the two "Report fraud" links on this worked when tested on 25 July, 2021, opening on a page which gives three options.

The first option "Submit a secure form" did not work in either Firefox or Chrome browsers.

The other two options are:



2. Send an Email

You can make a report on suspected insurance fraud by emailing the IFBA team.

More than 5 million individual claims are lodged every year in Australia. Make sure that you provide as much detail as possible, so that IFBA can match the information with a claim that has been lodged.

You should try to include details covering, what happened, who you believe did it, where it occurred, when it happened and any other details that might help to identify the claim (eg, a care registration).

EMAIL IFBA

3. Call the Hotline

During normal business hours you can call the IFBA Hotline to provide information on what you know about insurance fraud.

The IFBA Hotline can be reached during normal business hours at

1800 600 444

Neither of these options canvass the option of anonymous or pseudonymous reporting, but neither do they rule it out. A trial call to the Hotline would be needed to ascertain how IFBA would respond to an attempted anomymous report.

Specific collection issues relating to the IRS are addressed in this report **(section 2.6.1)**.

A3-4 AUSTRALIAN PRIVACY PRINCIPLE 4 - DEALING WITH UNSOLICITED PERSONAL INFORMATION

Australian Privacy Principle 4 outlines how APP entities must deal with unsolicited personal information.

The meaning of unsolicited has never been clarified.

In its 2013 submission to the OAIC on draft Australian Privacy Principle Guidelines, the ICA offered one view, giving as an example of solicited information:

> *"Information provided to a 'fraud hotline' that is designed to capture 'tip-offs' from the public*
>
> *"A number of Insurance Council members operate 'hotlines'. However, despite having a hotline service available, individuals may instead make contact with an insurer through other means such as by anonymous email or mail. This information*

49 Insurance Fraud Bureau of Australia, *Insurance Fraud*, http://www.ifbaintelligence.com

> *would need to be treated as unsolicited when it is not substantially different to the information 'solicited' via the fraud hotline.*
>
> *"The Insurance Council submits that it would be reasonable to treat all information provided on fraud as 'solicited'. This would be on the basis that the insurer in general invites fraud tipoffs. There would need to be acknowledgement that it would be reasonable in such situations not to provide a privacy notification (under APP 5) because for example, the identity of the person providing the information is unknown or to avoid alert the potential fraudster that they are being investigated." (ICA, 2013).*[50]

Australian Privacy Principle 4.1 requires entities receiving unsolicited personal Information to firstly determine if the data could have been collected if it had solicited it. If it could not, then Australian Privacy Principle 4.3 requires that the information collected "inadvertently" be destroyed. All of the other relevant safeguards must be applied to any unsolicited personal information that does not need to be destroyed as per Australian Privacy Principle 4.4.

There may be practical issues in making the judgement required by Australian Privacy Principle 4.1. It would be reasonable to expect insurers to put in place processes to ensure any unsolicited information is assessed within a reasonable timeframe.

In its 2013 submission to the OAIC on draft Australian Privacy Principle Guidelines, the ICA asserted that:

> *"Reasonable time [for dealing with unsolicited information] is necessary for entities to properly consider the range of information received. For example, an insurer may receive police reports containing information from and about several witnesses yet may not be in a position to know whether the information is needed until sometime in the future." (ICA, 2013).*[51]

A3-5 AUSTRALIAN PRIVACY PRINCIPLE 5 - NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION

Australian Privacy Principle 5 outlines when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters.

Australian Privacy Principle 5 complements Australian Privacy Principle 1 by requiring insurers to take reasonable steps to make individuals aware of specific matters relating to the handling of their personal information. This is generally implemented by means of notices to individuals on forms or when otherwise collecting information from them. More detail is often provided in longer privacy statements or policies which are also the means of satisfying Australian Privacy Principle 1. Successive Privacy and Information Commissioners have endorsed such a 'layered' approach to awareness

---

50 Insurance Council of Australia, *Draft Australian Privacy Principles Guidelines* (20 September, 2013), https://insurancecouncil.com.au/wp-content/uploads/resources/Submissions/2013/2013_09/2013_09_Privacy%20Commissioner_ICA%20response%20to%20Draft%20APP%20Guidelines%201-5.pdf.

51 ibid

obligations, rather than requiring individuals to be overloaded with privacy information at every point of collection.

The ICA submission to the current Review of the *Privacy Act* (ICA 2020) states:

> *"Insurance Council members are concerned about the implications of introducing a requirement for an express notice to be given when collecting personal information. Information collection by insurers is limited to that provided by a consumer expressly so that insurers may deliver products or services to them. The purpose of information collection in insurance is not for large scale aggregation purposes by advertisers. The current framework allows insurers to collect, use and disclose information where it is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.*
>
> *Insurance Council members believe that there are already a number of appropriate, written notifications to consumers when collecting information to provide insurance products. Introduction of a specific 'notice of collection' may have the opposite impact intended. Given that consumers already receive many disclosures and notices regarding insurance, providing additional ones may result in confusion and/or refusal to properly read and understand the information supplied.*
>
> *... it would be impractical for insurers to always notify particular third parties, such as witnesses of motor vehicle claims, that their personal information may be needed and collected via the policyholder. In fact, Insurance Council members submit that not only should the information be able to be used to establish, exercise or defend a legal or equitable claims, this right may need to be strengthened to make it clear that the information can also be used to obtain legal advice about the event."*

Despite this, the level of detail provided in privacy notices, statements and policies, pursuant to Australian Privacy Principle 5, has direct implications for compliance with the use and disclosure limitation principle in Australian Privacy Principle 6, in that it will be a factor in determining whether an individual has given informed consent to particular uses and disclosures:

> *In the case F v Insurance Company [2007] PrivCmrA 8, the complainant objected to Insurer disclosing information about them and their claim to an employee of a deceased policy-holder's employer. The Commissioner found insufficient explanation in the collection notice, and as a result, no basis for disclosure (See Appendix 4).*[52]

A special case is data generated or assigned by the data-holder. An insurer, like any other organisation, may supplement personal information collected from an individual or from a third party with information it generates itself, for example scores, or assigns, such as vulnerability or hardship flags. In some cases such data may be inferred or derived from other personal information that has

---

52 Colin Biggers and Paisley, "Overly broad consents to use and share information" in *Privacy Lessons for Insurers* (21 June, 2014), **https://www.cbp.com.au/insights/insights/2014/june/privacy-lessons-for-insurers**.

been collected externally. An example of this in an insurance context is a suspicion or imputation of fraudulent intent.

Because such information is not "collected", it escapes the range of privacy obligations that apply to collection under the Australian Privacy Principles discussed above.

Most of the other privacy obligations relating to such matters as data quality, security and other attributes do apply to inferred or derived personal information.

A3-6 AUSTRALIAN PRIVACY PRINCIPLE 6 - USE OR DISCLOSURE OF PERSONAL INFORMATION

Australian Privacy Principle 6 outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

The distinction between use and disclosure in privacy law is not always clear. The OAIC has published guidance on the issue, informed by case law (OAIC, 2019). The guidance is in line with mainstream interpretations of the terms:

- "Uses" means the data remains within the entity's effective control [over-simplified]; and
- "Discloses" means making accessible to others outside the entity and releases the subsequent handling of the information from its effective control, including shares, publishes, enables access, reveals, and displays openly.

However, since Australian Privacy Principle 6 applies mostly the same rules and limits to both use and disclosure, the distinction is not in practice of much consequence for compliance.

Primary purpose

There will usually be a package of uses and disclosures directly associated with the 'primary purpose' for which personal information has been collected. How broadly or narrowly this primary purpose is defined affects the nature of those uses and disclosures. The organisation may perceive its primary purpose differently from the way it is seen by the consumer. While the information provided in advance, pursuant to Australian Privacy Principles 1 and 5, may help to align these different perspectives, and may provide a benchmark in any assessment of compliance with Australian Privacy Principle 6, it will often be necessary to also apply a supposedly objective "reasonable expectation" test to ascertain what the primary purpose is:

> *In an Own Motion Investigation (OMI) v Insurance Company [2010] PrivCmrA1, the Commissioner found that the wording of the privacy notice, and by inference, of consent sought – 'disclosure to anybody …' was too broad. While the Insurer claimed it would not have relied on such a broad consent, it accepted the finding and changed the wording in its privacy notice/consent.* **(See Appendix 4)**.

This finding suggests that an organisation cannot unreasonably just assert too broad a primary purpose.

Secondary use and disclosure

The term "secondary purpose" refers to a purpose that is not a primary purpose but for which exceptional approval exists in the *Privacy Act*. The currently-approved categories of exceptions are (paraphrased):

- Consent;
- The individual would reasonably expect the secondary use or disclosure (and the secondary purpose is related to the primary purpose, or, for sensitive information, directly related);
- Required or authorised by or under law;
- A permitted general situation exists (*Privacy Act*, Section 16a);
- A permitted health situation exists;
- Reasonably necessary for law enforcement; and
- Biometric information or biometric templates to an enforcement body in conformance with guidelines.

The first three may be applicable in a number of circumstances within general insurance, while the other four are specialised exceptions. While these will not routinely apply in insurance, one of the permitted general situations is "investigation of unlawful activity or serious misconduct". This is relevant in insurance fraud investigation, and if and when law enforcement agencies become involved, the "reasonably necessary for ..." exception may also provide a basis for use and disclosure.

If an insurer seeks to rely on consent as the basis for a secondary use or disclosure then a generic set of issues arise in relation to whether the consent has been fully informed and freely given, express or implied or merely assumed or inferred by the collector. While we are not aware of any insurance-specific cases on this point, general case law on consent, both within privacy jurisdiction and in wider jurisprudence will be relevant.

There have been some insurance-specific cases addressing the second exception – "related and within reasonable expectations":

> *In the case "IQ" and NRMA Insurance, Insurance Australia Limited [2016] AICmr 36, the Information Commissioner made a formal Determination about secondary use. The Commissioner found that a disclosure of details of the complainant's car insurance to their close but estranged relatives was a breach of NPP 2 (the use and disclosure limitation principle in force at the time of the disclosure). The Determination rejected the Insurer's argument that the disclosure was a "related secondary purpose" and "within reasonable expectations". This was based on the shortcomings in the Insurer's then privacy policy, although interestingly the Commissioner found that the Insurer's new APP policy (the APPs having replaced the NPPs in 2014) might have established the disclosure as a permissible secondary use*
>
> *In the case I v Insurance Company [2009] PrivCmrA 11, the complainant objected to disclosure by the Insurer of the complainant's criticism of a repairer to the repairer.*

The Privacy Commissioner found that while disclosure of an entire letter breached the use and disclosure limitation principle, disclosure of some information contained in the letter would have been an acceptable related secondary purpose within reasonable expectations

In the case "WG" and Australian Super Pty Ltd (Privacy) [2020] AICmr 64, the Information Commissioner made a formal Determination that disclosure to two law firms that had previously represented the complainant was not a 'related secondary purpose… "within reasonable expectations". This conclusion led directly from the Insurer's failure to accurately record the complainant's express revocation of authority for the law firms. **(See Appendix 4)**.[53]

A3-7 AUSTRALIAN PRIVACY PRINCIPLE 7 - DIRECT MARKETING

Australian Privacy Principle 7 states that an organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

Use or disclosure for the purpose of direct marketing is precluded unless an exception applies. The approved exceptions are very broad and even include (counter-intuitively) where:

- The individual would *not* reasonably expect the use or disclosure; and
- The personal information has been collected from a third party such as a data list provider.

However this is subject to the easily-satisfied condition that seeking consent is impracticable, and subject to provision of an obligatory opt-out facility.

There are many circumstances in which consumers object to the use of personal data for direct marketing, particularly for products and services extraneous to the relationship that the consumer considers they have with the insurer. The concern is heightened by the fact that some of the data is only held because of the duty of disclosure under the *Insurance Contracts Act*.

However, insurers, like most other businesses, can generally justify marketing communications about a wide range of goods and services to existing customers on the basis of exceptions in Australian Privacy Principle 7. They will also typically mention direct marketing, sometimes obliquely, in their privacy policies or statements and in T&Cs.

The Spam Act 2003 and the *Do Not Call Register Act 2006* also regulate direct marketing by email and by phone respectively, but both contain exemptions for marketing to existing customers, so offer no further relief.

53 See also the case "IR" and NRMA Insurance, Insurance Australia Limited [2016] AICmr 37, discussed in relation to security of joint accounts, **Appendix 4**.

A3-8 AUSTRALIAN PRIVACY PRINCIPLE 8 - CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION

Australian Privacy Principle 8 outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

Australian Privacy Principle 8 seeks to protect the personal information of Australian consumers when it is transferred overseas, to jurisdictions which have differing levels of privacy protection in their own laws.

In 2008, the ALRC commented:

> *"It is now commonplace for major companies in Australia dealing with great volumes of personal information—including banks, insurance companies, credit card companies and others – to conduct their 'back office' processing of data overseas (often in Asia)." (ALRC, 2008, p 23).*

Outsourcing of a range of functions may involve cross-border disclosure of personal information, as may the routine internal processes of multinational businesses, including some insurers.

Most large private sector organisations now seek to satisfy the requirements of Australian Privacy Principle 8 by giving appropriate notice in their privacy policies or T&Cs. Insurers appear to be no exception. **(See Appendix 2)**. Given the ease of achieving compliance with such a weak consumer protection, we are not aware of any insurance-related cases that have raised Australian Privacy Principle 8 compliance issues.

A3-9 AUSTRALIAN PRIVACY PRINCIPLE 9 - ADOPTION, USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

Australian Privacy Principle 9 outlines the limited circumstances in which an organisation may adopt a government-related identifier of an individual as its own identifier, or use or disclose a government-related identifier of an individual.

Government-related identifiers means identifiers assigned by federal, state or territory governments. Australian Privacy Principle 9 allows for the use and disclosure of government-related identifiers to verify identity *for the purposes of an organisation's activities or functions* as per Australian Privacy Principle 9.2(a). This appears to cover the common use by insurers of driver licence numbers as evidence of identity (EoI) and *for investigation of unlawful activity or serious misconduct* in accordance with Australian Privacy Principle 9.2(d) and *Privacy Act* s.16, which appears to cover insurance fraud investigation. There are also other permitted uses or disclosures which might be relevant in some cases.

We are not aware of misuse of government identifiers being raised as a significant privacy issue either in complaints or more generally in the insurance sector.

A3-10 AUSTRALIAN PRIVACY PRINCIPLE 10 - QUALITY OF PERSONAL INFORMATION

Australian Privacy Principle 10 states that an APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

Reasonable steps are required to be taken in relation to each of collection, use and disclosure.

Quality issues, and how "reasonableness" is to be gauged, are major concerns in every industry sector.

The only data quality criteria listed in Australian Privacy Principle 10 are "accurate, complete and up-to-date". However, the related obligation under Australian Privacy Principle 13 (see below) requires correction to ensure that information is "accurate, up-to-date, complete, relevant and not misleading". The omission of "relevant" and "not misleading" from Australian Privacy Principle 10 has been identified as a significant weakness in the *Privacy Act* regime.

In general insurance, issues arise in relation to:

- The quality of data acquired from third parties generally;
- The quality of data provided by insurance companies into industry databases;
- The quality of data acquired by insurance companies from industry databases; and
- The quality of data gathered by insurance companies in claims investigations.

Some issues arise because of the behaviour of a consumer, for example:

> *In the case P v Insurer [2010] PrivCmrA 19, the insurer accepted the need to remove the complainant as an insured party on a policy which had not covered them since a separation 10 years previously, but where the policy holder had failed to notify the Insurer of the separation* **(See Appendix 4)**.

Many data quality issues arise from a simple failure to follow procedures and to use mechanisms already built into systems, for example:

> *In the case I and Insurance Company [2011] AICmrCN 3, the Insurer's staff used inaccurate descriptors for enquiries, and failed to use a reference number field in the Insurance Reference Service (IRS) which made it difficult to locate all enquiries relating to the same individual and led to multiple entries. The Insurer apologised to the complainant and improved staff training* **(See Appendix 4)**.
>
> *In the case "WG" and Australian Super Pty Ltd (Privacy) [2020] AICmr 64, already cited above in relation to APP6, the Information Commissioner determined both data quality and data security breaches, leading to an unauthorised disclosure, despite the complainant not having raised quality or security issues. The findings were based on the Insurer's failure to accurately record revocation of authority* **(See Appendix 4).**

Data quality issues relating to third party databases are also discussed in section of this report on the IRS. The use of any third party database as a source of personal information greatly increases the importance of subject access and correction rights. See under Australian Privacy Principles 12 and 13 below, as there is not the same real-time opportunity for an individual to ensure quality data as when information is collected directly from them.

A3-11 AUSTRALIAN PRIVACY PRINCIPLE 11 - SECURITY, RETENTION AND DELETION OF PERSONAL INFORMATION

Australian Privacy Principle 11 states that an APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

Security issues, and how "reasonableness" is to be gauged are major concerns in every industry, including in the general insurance industry. The issues include:

- The effectiveness of access control, to limit access to sensitive data;
- The security of information in transit;
- The security of information passed to third parties, including where it is sensitive, such as the value of property, vacant premises for example in the case of travel insurance;
- Inadequate control over the behaviour of third parties;
- sending information to the wrong party;[54]
- The security of information in storage, with the incidence of data being extracted by hackers from organisations across all industry sectors making clear that safeguards are generally inadequate. An example has arisen in relation to a brokerage insurance house; and[55]
- Failure to delete data when its purpose has expired.

Joint accounts

We address the issue of joint accounts here because security concerns are particularly significant, although other Australian Privacy Principles are also relevant.

In general insurance, the contract is normally with the owner(s) of the insured property, such as a house, vehicle or household goods. Where the property is jointly owned, the contract is often with the owners, as joint insured parties.

Where more than one individual is covered, some customer information may be person-specific. This applies, for example, to contact details, in all categories of insurance. For home building and contents insurance, the account information will be common, but for vehicle insurance it will also

54 Australian Financial Complaints Authority, *AAI Limited Case No. 705394* (13 August, 2020), https://service02.afca.org.au/CaseFiles/FOSSIC/705394.pdf.

55 Insurance News, *Cyber Attack Impacts Insurance House* (14 June, 2019), https://www.insurancenews.com.au/daily/cyber-attack-impacts-insurance-house.

include driving history information specific to the individuals covered. For travel insurance, cover will either be the same for all insured parties such as the members of a family or vary between them, as in where there are pre-existing health conditions.

Privacy issues arise when different individuals covered by the same policy are estranged, separated or divorced. In such cases, contact details may be very sensitive, and disclosure of details especially those indicating physical location, may be at best unwelcome and at worst dangerous.

There is also the potential for one insured party to change or cancel the cover, and perhaps seek a partial refund of premiums, without the knowledge and/or consent of another party.

While any jointly-insured party who has become estranged from their partner can in theory address these risks by contacting the insurer and requesting changes to policies and to data-holdings and their handling, this is in practice often difficult and time-consuming. It is also unlikely to be top-of-mind for people in such circumstances. It is therefore incumbent on insurers to anticipate the privacy risks that arise and take steps to address them. A number of cases have involved these issues:

> *In the case I v Insurance Company [2007] PrivCmrA 11, the Privacy Commissioner found a breach of security when the complainant's new address was disclosed to an estranged partner. The complainant had requested separation of a joint account but the Insurer's systems had failed to eliminate a link.*
>
> *In the case IR and NRMA Insurance, Insurance Australia Limited [2016] AICmr 37, the Information Commissioner made a formal Determination about a joint account privacy issue. The Commissioner found that the Insurer's practice of listing all other policies (including those which were held jointly) on certificates of insurance was unnecessary and a breach of APP 6 in respect of complainant's personal information. The Insurer argued that inclusion in certificates was a "related secondary purpose" within "reasonable expectations", informed by PDS and privacy policy (and also a contributor to compliance with data quality). The Commissioner ruled that while some information might pass these tests, the level of detail about unrelated assets did not. The Commissioner also found, on balance, that the format and content of the certificates led to a breach of APP 11, the security principle. An apology and system change was required, along with a small compensation payment* **(See Appendix 4)**.

It should be noted that the fact of an unauthorised disclosure does not automatically mean that there has been a security breach:

> *In the case IQ and NRMA Insurance, Insurance Australia Limited [2016] AICmr 36, already cited above under APP 6, the Information Commissioner made a formal Determination that there had been no breach of security, despite finding that there had been a disclosure of personal information in breach of the use and disclosure limitation principle* **(See Appendix 4)**.

A3-12 AUSTRALIAN PRIVACY PRINCIPLE 12 - ACCESS TO PERSONAL INFORMATION – OBTAINING DATA ABOUT YOURSELF

Australian Privacy Principle 12 outlines an APP entity's obligations when an individual requests access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

Individual consumers have a right of access to data about themselves under the *Privacy Act*. Australian Privacy Principle 12 requires all APP entities to give individuals access to any personal information they hold, subject to a range of exemptions. Individuals cannot be charged for requesting such data, or for being told that it is held. However, private sector APP entities can charge a reasonable fee for actually providing the data.

Part 12 of the General Insurance Code of Practice also deals with "Your access to information". It goes beyond the minimum requirements of Australian Privacy Principle 12 by committing subscribers to giving access free of charge, generally within 30 days. This is a vital mechanism, particularly in an industry sector in which consumers are under an obligation to take reasonable care not to make a misrepresentation to an insurer.

There were 3,555 self-reported breaches of the equivalent Section 14 in the 2014 version of General Insurance Code in 2019-20 representing 11% of total self-reported breaches (GICGC, 2021)[56]. Of these, 99% were breaches of Section 14.1 concerning a failure to abide by privacy laws. However, 80% were self-reported by one (unnamed) insurer, which had also accounted for most Section 14.1 breaches the previous year. The CGC report fails to explain the nature of these breaches, although it hints that they may have related to security, by referencing the obligation to also report "data breaches" to the OAIC (CGC, report p 34).

Australian Privacy Principle 12.3 and General Insurance Code clause 163 provide for some personal information to be withheld on various grounds, including privacy of third parties and prejudice to legal proceedings or law enforcement action.

> *In the case of C v Insurance company [2006] PrivCmrA 3, the Privacy Commissioner found that the Insurer had reasonable grounds for withholding some documents (third party privacy and commercial sensitivity) but that others could be released with redaction* **(See Appendix 4)**.

"Forced" subject access – potential to undermine Privacy Safeguards

We are aware of longstanding public concerns that there is a risk of abuse by organisations of individuals' right of access to personal information about themselves. Individuals may be required by an organisation to apply for access and then provide the information received to the organisation, as a condition of service. In some cases, an organisation may even require individuals to have the results of a request sent directly to the organisation, or even to appoint the organisation as an authorised representative or agent in order to gain direct access to information (referred to as 'diverted' subject access).

---

56 General Insurance Code Governance Committee, *Annual Industry Data and Compliance Report 2019-20* (March, 2021), p 27, https://insurancecode.org.au/app/uploads/2021/03/CGC_2019-20_Annual-Report_Final-Version.pdf.

Organisations might justify these practices where they seek information that may be adverse to an individual's interests such as criminal history or where they fear an individual may not give honest answers to legitimate questions. To justify re-routing the response to subject access requests directly to the organisation, it may be argued that the individual may omit or alter adverse third party information if they are allowed to receive and forward it.

In some cases "diverted" subject access may be an acceptable convenience for the individual. In other such cases, however, societal interests have led to the establishment of formal mechanisms such as working with children checks. These are generally underpinned by legislation, with safeguards against inappropriate use.

We are not aware of any evidence of forced or diverted subject access in the general insurance sector in Australia. Insurers commonly seek to verify information provided by individuals in other ways, for example by checking third party databases as discussed above. **(See Sections 2.2 and 3.4)**.

A3-13 AUSTRALIAN PRIVACY PRINCIPLE 13 - CORRECTION OF PERSONAL INFORMATION

Australian Privacy Principle 13 outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

More specifically, Australian Privacy Principle 13 requires APP entities to:

> *"Take reasonable steps to correct personal information [they] hold, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held."*

This obligation applies whenever the APP entity becomes aware of incorrect data, whether or not the individual has requested correction or has previously applied for access. In this respect, Australian Privacy Principle 13 complements Australian Privacy Principle 10 which addresses data quality more generally. It has already been noted in discussion of Australian Privacy Principle 10 that it does not include the "relevant" and "not misleading" criteria. However the inclusion of these criteria in Australian Privacy Principle 13 effectively adds them into the Australian Privacy Principle 10 standards whenever and however they become aware of errors.

Australian Privacy Principle 13 also effectively provides individuals with a right to request correction, and they cannot be charged for exercising that right. As with the right of access under Australian Privacy Principle 12, there are exceptions. In many cases where correction requests can be declined, the APP entity is required to give reasons and, on request, to associate a statement of challenge with the information alleged to be incorrect, and to do so free of charge.

Insurers, like any other entity, aree required to process requests for correction of personal information in accordance with the rules in Australian Privacy Principle 13.

We are not aware of any insurance-specific cases relating to correction issues, other than those that arise in relation to the IRS.

Data deletion

There is no express right to deletion of personal information under Australian Privacy Principle 13, but there is nothing to stop an individual from requesting deletion of some or all of the information held by an APP entity as part of a request for correction. Any such request will need to be considered on its merits against the quality standards in the *Privacy Act*.

The issue of a right of deletion, sometimes known as a "right to be forgotten", has arisen for many years in debates about privacy law reform. It was raised both in the Final report of the ACCC's Digital Platforms Inquiry of June 2019 and in the Attorney-General Department's *Privacy Act* Review Discussion Paper of October 2020.

The ICA commented on a right to erase in its submission to the ACCC Inquiry (ICA, 2019):

> *"The ACCC has recommended enabling consumers to require erasure of their personal information. However, data collected by insurers in the course of underwriting insurance products and paying out claims becomes actuarial data which is essential to the pricing of future applications for insurance. Enabling consumers to delete data collected about them will have a detrimental impact to the sustainability of the industry. In addition, insurers often retain personal data after a customer no longer has a current policy with them in order to continue servicing potential long tail claims."*

There is one reported case involving correction:

> *In the case of D v Insurance Company [2007] PrivCmrA 6, a complainant objected to inaccurate and irrelevant information about them being recorded on the insurer's files relating to a third party (a relative of the customer). The insurer had previously declined to act on request for removal from the relative, and had offered only some changes to the records. After the Commissioner's intervention, further information was removed.* **(See Appendix 4)**.

Whether or not a right of erasure emerges from the current *Privacy Act* Review, there will now be cases in which deletion of some personal information is an appropriate action to ensure compliance with Australian Privacy Principle 13.

A3-14 OUTSOURCING

A set of issues related to handling of data by third party service providers cut across a number of Australian Privacy Principles. These include how to ensure that the same standards apply and that all obligations of the client are appropriately passed on to the contractor.

The operation of the IRS is contracted by the ICA, on behalf of its members, to the data analytics business Illion (previously known as Dun & Bradstreet Australia. **(See Sections 2.2 and 2.6 and Appendix 4).**

We are not aware of any reported evidence of insurance-specific outsourcing issues, whether involving individual insurers contractors or the IRS. On the other hand, such activities are seldom

transparent to consumers, and hence unlikely to be raised by consumers who are unaware of them. An exception is the outsourcing of IRS to Illion, discussed separately.

A3-15 COMPLAINTS, ENFORCEMENT AND OUTCOMES

Current privacy regulations are addressed elsewhere. **(See Section 2.4)**. Presently, all privacy complaints relating to Australian Privacy Principles are assessed only against the Australian Privacy Principles in the *Privacy Act*, with OAIC as the relevant external dispute resolution body. Privacy elements of complaints that escalate from insurers' internal complaint handling processes, including complaints relating to the access to information provisions in Part 12 of the Insurance Code of Practice, would generally be referred initially to AFCA, but then forwarded to OAIC, if they involve an Australian Privacy Principle.

The OAIC is also responsible for pro-actively monitoring and enforcing compliance by APP entities in insurance with *Privacy Act* obligations – including the Australian Privacy Principles and Data Breach requirements. This responsibility is distinct from and additional to the handling of complaints from specific individuals. Overall monitoring of compliance with the Insurance Code of Practice including Part 12 is undertaken by the independent CGC but this body does not have a role in relation to individual cases.

Complaints may be upheld, or the investigation may find either no breach, or insufficient evidence:

> *In the case O v Insurance Company [2007] PrivCmrA 17, the Privacy Commissioner found no breach of either the collection or data quality principles, and no evidence that disclosure was from an Investigation report – there being a plausible alternative source.* **(See Appendix 4)**.

Remedies for established breaches of privacy principles range from apologies and changes to policies and practices, through to compensation. Some cases (see Appendix 4) involved compensation, although as is generally the case in enforcement of privacy law in Australia, the amounts involved are modest. In the only four cases where compensation was reported, the amounts ranged from $1250 to $4500, although in another case the undisclosed amount was described as "substantial".

Appendix 4: Privacy and insurance case studies – Summarised

This Appendix provides summaries of case notes and cases from the Privacy Commissioner up until 2010 and Information Commissioner from 2010 which involve insurance companies and the application of general privacy principles. Of the 14 cases, only the last three were formal Section 52 determinations.

Some other cases involving insurance companies relate to specialised privacy regimes including tax file numbers and credit reporting, or are indirectly insurance-related, for example complaints against law firms representing insurers in litigation. These have not been included in this list.

In some but not all of the case notes, the Commissioner offers an opinion about whether a Australian Privacy Principle (or a National Privacy Principle prior to 2014) was breached, whereas all formal determinations do so.

DENIAL OF ACCESS: C V INSURANCE COMPANY [2006] PRIVCMRA 3

Complainant objected to insurer withholding some documents in response to a subject access request under National Privacy Principle 6. Commissioner found reasonable grounds for withholding some documents relating to third party privacy and commercial sensitivity but that others could be released with redaction.

Outcome: Some additional disclosure

DISCLOSURE, ACCURACY AND SECURITY: D V INSURANCE COMPANY [2007] PRIVCMRA 6

Complainant objected to inaccurate and irrelevant information about them being recorded on the insurer's files relating to a third party. The only connection was that a relative of the complainant was managing the third party's affairs. Insurer had previously declined to act on request for removal from the relative. Insurer had offered an apology, some changes to records and $750 – complainant dissatisfied.

Outcome: Complainant accepted further changes, staff training and $1250

COLLECTION AND DISCLOSURE: F V INSURANCE COMPANY [2007] PRIVCMRA 8

Complainant objected to insurer disclosing information about them and their claim to an employee of a deceased policy-holder's employer. Commissioner found breaches of Information Privacy Principles 1 and 2 – insufficient explanation in collection notice, and no basis for disclosure.

Outcome: Unspecified conciliation – "agreed resolution".

SECURITY: I V INSURANCE COMPANY [2007] PRIVCMRA 11

Complainant had had joint account or policy and sought to have details separated when estranged. Objected to release of new address to estranged partner. Insurer accepted systems failure – had set up new account but failed to eliminate a link. Commissioner found breach of security under National Privacy Principle 4.

Outcome: Apology and substantial compensation.

COLLECTION, DISCLOSURE AND ACCURACY: O V INSURANCE COMPANY [2007] PRIVCMRA 17

Complainant had made a workers compensation claim against employer which insurer had investigated. Complainant objected to information from investigator's report about a work colleague having been disclosed to the employer. Commissioner found no breach of collection principle National Privacy Principle 1 or inaccuracy National Privacy Principle 3 and no evidence that disclosure was from investigation report – plausible alternative source, so no disclosure breach National Privacy Principle 2 either.

Outcome: No further action

DISCLOSURE: E V INSURANCE COMPANY [2008] PRIVCMRA 5

Complainant objected to disclosure of their contact information to a third party involved in a motor vehicle insurance claim. Insurer accepted disclosure was inappropriate and paid compensation.

Outcome: Apology and compensation

DISCLOSURE: I V INSURANCE COMPANY [2009] PRIVCMRA 11

Complainant had made a claim on home buildings policy - objected to disclosure by Insurer of complainant's criticism of repairer to the repairer, who had come back to the complainant. Commissioner found disclosure of entire letter breached National Privacy Principle 2 – although disclosure of some information would have been an acceptable related secondary purpose within reasonable expectations.

Outcome: Apology and staff training

DISCLOSURE: OWN MOTION INVESTIGATION (OMI) V INSURANCE COMPANY [2010] PRIVCMRA 1

OMI, but issue raised by an insurance company customer – objecting to "breadth" of wording in privacy notice, and by inference, of consent sought – "disclosure to anybody …". Insurer claimed would not have relied on such a broad consent, but accepted that it was too broad.

Outcome: change of wording in privacy notice/consent

DISCLOSURE: E V INSURANCE COMPANY [2011] PRIVCMRA 5

Complainant objected to insurer disclosing information about a claim on a motor vehicle policy to a member of the family, while attempting to ascertain the identity of the driver involved in an accident. Commissioner found breach of National Privacy Principle 2.

Outcome: Apology

ACCURACY & CORRECTION: P V INSURER [2010] PRIVCMRA 19

Complainant requested insurer remove claims shown on her file. Claims related to a policy taken out from her former partner, who had failed to remove the complainant as an insured party on the policy after their separation 10 years ago.

Outcome: Insurer accepted and removed listings, to comply with National Privacy Principle 6.5

ACCURACY: I AND INSURANCE COMPANY [2011] AICMRCN 3

In conduct of a loss assessment fraud investigation where the category of insurance is unknown, the insurer's staff used inaccurate descriptors for enquiries and failed to use reference number field in the IRS which made it difficult to locate all enquiries relating to the same individual and led to multiple entries.

Outcome: Apology and staff training – accepted by complainant - discontinued

DISCLOSURE AND SECURITY: 'IQ' AND NRMA INSURANCE, INSURANCE AUSTRALIA LIMITED [2016] AICMR 36

NRMA customer objected to unauthorised disclosure of details of his car insurance to his possibly estranged wife and daughter. Exposed assumption by NRMA that a close relative with knowledge of an insurance contract and assertion of financial interest was authorised to discuss it – assumption compounded by fact that they did have another joint policy and that wife was named as a driver on the other one.

NRMA claimed no breach of use/disclosure principle National Privacy Principle 2 because "related secondary purpose" and "within reasonable expectations". Commissioner dismissed – privacy policy at the time unhelpful to NRMA – new one for Australian Privacy Principles might have excused them. Breach of National Privacy Principle 2 found.

NRMA provided evidence of policy and training that constituted 'reasonable' security measures. No breach of National Privacy Principle 4 was found.

Note finding that an unauthorised disclosure does not necessarily mean there was a security breach

Outcome: Conciliation failed. Commissioner made Determination requiring apology, training and $2000 comp.

DISCLOSURE AND SECURITY: "IR" AND NRMA INSURANCE, INSURANCE AUSTRALIA LIMITED [2016] AICMR 37

NRMA customer complained about disclosure of information about other policies held, in some cases jointly with husband, on certificate of insurance for a joint home insurance policy held jointly with a third party.

Commissioner found NRMA practice of listing all other policies on certificates of insurance was unnecessary and a breach of Australian Privacy Principle 6 in respect of complainant's personal information but not of husband's personal information as he was not identified on the certificate.

NRMA argued certificate content was a "related secondary purpose" within "reasonable expectations", informed by PDS and privacy policy (and also a contributor to compliance with data quality). Commissioner found that while some information might pass these tests, the level of detail about unrelated assets did not.

Commissioner also found, on balance, that the format and content of the certificates led to a breach of Australian Privacy Principle 11, the security principle.

Outcome: Conciliation failed. Commissioner made Determination requiring apology, systems change, and $3000 compensation.

DISCLOSURE, QUALITY AND SECURITY: "WG" AND AUSTRALIAN SUPER PTY LTD (PRIVACY) [2020] AICMR 64

AusSuper member complained about unauthorised disclosure of personal information by AusSuper to a contracted insurance assessor, and to two law firms that had previously represented the complainant in relation to an income protection insurance claim. AusSuper had failed to properly record and honour the complainant's revocation of authority for the law firms.

Commissioner found breach of Australian Privacy Principle 6 in relation to disclosure concerning the two law firms, but no breach in relation to the administrator, which was a related secondary purpose within reasonable expectation, informed by the PDS and privacy policy.

Commissioner also found breach of Australian Privacy Principle 10.2 relating to data quality and breach of Australian Privacy Principle 11.1 relating to Security.

Outcome: Commissioner made Determination requiring apology, training, audits and $4500 compensation.

Appendix 5: Privacy Issues in Relation to IRS

This Appendix supports Section 2.6, by providing a further level of detail about the privacy issues that have already arisen in relation to data practices in the general insurance industry, which are specific to the shared industry database. The empirical research reported **(see Section 3 and Appendix 6)**, based on a sample of requests for IRS data, raises significant additional concerns about IRS compliance with some of the Australian Privacy Principles.

A5-1 TRANSPARENCY

We assume that the IRS seeks to meet the transparency requirements of Australian Privacy Principle 1 through its privacy policy, FAQs and T&Cs.[57]

Understanding of the IRS is hindered by the same complexities and lack of transparency about brands and ownership as is the case with the industry more generally. For example:

- IAG is a member of the IRS in its own name, and in the names of four of its brands CGU, SGIO, SGIC and NRMA Insurance, but not Swann Insurance, WFI and Poncho Insurance;
- Suncorp is a member of IRS, but none of its brands appear in the IRS's list.

It is unclear whether brands, either of the two majors that are not mentioned as IRS members, or of other corporations that operate through multiple brands, such as Allianz, Auto & General and Hollard, gain access to IRS data through their holding companies' memberships.

Of the IRS's 19 members:

- 12 are also member-companies of ICA;
- 6 appear to be brands of member-companies of ICA, including Pd (Progressive Direct) and Blue Zebra (was Zurich, now Youi);[58]
- At least one is not an ICA member (Huddle – a brand name of Open Insurance);
- Of ICA's 57 member-companies, encompassing 135 brands:
  - 12 of the 57 companies are members of the IRS;
  - 16-30 of 135 brands are members of the IRS; and
  - Around 80% of ICA companies and brands are not members of IRS. This is a head-count only and does not take into account market-share.

The IRS privacy policy is somewhat ambiguous as to the purpose of the IRS. There is reference to a "claims database" and most of the uses of the data by members clearly relates to claims. But it is clear from other parts of the policy, FAQs and T&Cs that the IRS also contains details of enquiries and applications made by consumers. It is not clear why the IRS includes so much data about the totality of an individual's interaction with insurers.

---

57 Insurance Reference Service, https://insurancereferenceservices.com.au/.

58 Mina Martin, "Youi and Blue Zebra Confirm New Underwriting Relationship" in *Insurance Business Australia* (27 February, 2020), https://www.insurancebusinessmag.com/au/news/breaking-news/youi-and-blue-zebra-confirm-new-underwriting-relationship-215002.aspx.

Concern has been expressed by consumer groups that adverse inferences may be drawn from particular patterns of contact and that consumers could in effect be penalised for shopping around" for a better insurance deal. **(See Section 3)**.

A5-2 DATA COLLECTION

Assessment of IRS privacy compliance necessarily involves both the IRS itself and the member insurers, given that the operation of the IRS involves a two way exchange of information.

Collection issues arise in relation to collection by insurers *from* the IRS; to collection by insurers *for* the IRS; to collection by the IRS from insurers; and to collection by the IRS directly from individuals.

Collection of personal information by insurers FROM the IRS

The insurance industry justifies collection of information from third party databases including the IRS on the basis that it needs to verify information provided by consumers and to ensure that any additional relevant information is taken into consideration in their assessment of applications for and claims under insurance policies.

Compliance with the collection principles when collecting from the IRS is a matter for each individual insurer. The corollary of their collection is disclosure by the IRS – see under Use and Disclosure below.

Collection of personal Information by insurers FOR the IRS

We understand that in order to become a member of the IRS, insurers need to supply at least three years of their policy holders' claims history. It is not clear if they also have to commit to providing enquiries data for at least the same period.

The IRS keeps enquiries data for five years, and claims data for 10 years. It appears from the IRS FAQ that older data is meant to be automatically deleted by the IRS when it reaches these ages.

It is not clear if some information is routinely collected from individuals by insurers exclusively in order to populate the IRS – that is, where the information might not be necessary for the immediate purposes of the insurer. Requesting additional information just for the IRS could be challenged on the basis that it may not comply with Australian Privacy Principle 3.1 in that it is not "reasonably necessary".

It is not clear if the IRS claims data includes any information about alleged fraud or fraud investigations, or whether such information is only exchanged between insurers under the separate IFBA schemes. The Sample Report from the IRS includes information on bankruptcies, summons and judgments, declared as being from the "D&B Automated Court Data Feed".[59]

59 Insurance Reference Service, *DNBi: Individual Insurance Enquiry* (27 August, 2016), https://insurancereferenceservices.com.au/assets/DNBi%20IRS%20Individual%20Insurance%20Enquiry.pdf.

Collection of personal information by IRS from insurers

The justification for the IRS's collection of information from insurer members is that it is needed for the corollary purpose of insurers using the IRS. That is, for the provision of the service to insurers to authenticate information provided by consumers, and to ensure that any relevant information not already held by an insurer is taken into consideration in their assessment of an applications for, or a claims under, an insurance policy.

Collection is clearly "reasonably necessary" for the purpose of providing the shared database resource, and therefore satisfies Australian Privacy Principle 3.2 for personal information that is not "sensitive", as defined in the *Privacy Act*.

The IRS Privacy Policy confirms that it holds some "sensitive" information, and states that where this is collected directly from an individual, it is collected with the individual's consent thereby satisfying Australian Privacy Principle 3.3(a)(ii).

However, the Privacy Policy also states that sensitive information is collected:

> *"From IRS members or from third parties in connection with processing and dealing with information received from the public to help combat insurance fraud."*

If the qualification in this statement only applies to the collection from third parties, then the collection from insurers is presumably based on an assumption that member insurers have obtained the consent of individuals for disclosure of any sensitive information to the IRS. Whether this assumption is correct for all insurers would be a question of fact to be determined in the event of a complaint.

The collection from third parties appears to rely on the exception provided by Australian Privacy Principle 3.4(b) in conjunction with Section 16A for "taking appropriate action in relation to suspected unlawful activity or serious misconduct". However, this is not likely to provide a basis for routine collection of sensitive information by IRS from insurers – it would have to be triggered by active investigation of particular cases. **(See Section 2.6).**

Collection of personal information by IRS from individuals

IRS only collects information directly from individuals when they make enquiries, request their *My Insurance Report* or challenge the quality of the data. **(See Sections 2.2 and 3.4).**

A5-3 USE AND DISCLOSURE

The use and disclosure by the IRS of the personal information in the database, as explained in its Privacy Policy, appear to comply with Australian Privacy Principle 6, being either in accordance with the primary purpose of collection, or meeting the criteria for one of the exceptions in Australian Privacy Principle 6.

The IRS seeks to control the use and disclosure of IRS data by member insurers through its "Terms of Use" and a "Member Deed". While only the Terms of Use are publicly available, its list of "authorised purposes" together with an explanation given of the Member Deed in the Privacy Policy suggests that between them they help to ensure compliance by members and by the IRS itself with the Australian Privacy Principles, with no obvious areas of concern other than those which arise from the general limitations of the *Privacy Act* regime.

A5-4 DATA QUALITY

In 2017, the ICA acknowledged that the IRS had data quality issues (ICA, 2017, p 43):

> *"A number of insurers have advised that they do not have easy access to this data and that access to consumer information through a third party insurance report service can be ambiguous. For example, withdrawn claims may be shown as declined, which could lead to an insurer believing a customer may have failed to disclose a previously declined claim. Insurers have also noted that it could be costly to have to generate an external insurance report for every sale."*

The IRS Privacy Policy does not expressly address data quality.

A5-5 SECURITY

The IRS Privacy Policy includes a generic outline of its security measures. The IRS can be expected to face the same range of security challenges as any other large shared database. We are not aware of any specific problems or cases involving security of the IRS.

A5-6 OUTSOURCING AND OFFSHORE PROCESSING

The operation of the IRS is described as "externally hosted" – in practice, contracted out by the ICA, on behalf of the IRS members, to a service provider, currently the data business Illion.

The IRS Privacy Policy does not indicate that the operation of the IRS itself involves any routine cross-border disclosure but does advise that the processes of its insurer members may involve offshore access to the IRS.

We are not aware of any specific issues relating to the IRS and either outsourcing or cross-border disclosure.

A5-7 SUBJECT DATA ACCESS RIGHTS

The application of Australian Privacy Principle 12 to the IRS is of particular interest. The contracted service provider for the IRS, Illion provides "subject" access to the shared industry database through a service *My Insurance Claims Report*.[60]

Despite its name, this report includes not only an individual consumer's claims history over the past 10 years, but also records of any insurance cover enquiries they have made to contributing insurers over the past 5 years, whether or not a claim was ever made.

The IRS charges a fee of $22 for a "Claims Report". No opportunity is provided to confirm whether or not there are any relevant records prior to paying the fee. In addition, the IRS appears to use information provided when making an application for access to update its records. Hence, where no record previously existed, an application may well enable the IRS to create a new record. This

60 Insurance Reference Service, *About*, http://insurancereferenceservices.com.au/about

appeared to have occurred in the case of one of the research leads.

The website gives the impression that it is not possible to just order a 'Claims Report' online – the website invites you to provide contact details so that a "… customer service representative [can] … talk you through your order". This arguably creates a barrier which may deter some individuals from pursuing their right of access, particularly if they are seeking a claims report in the context of a dispute.

In practice, submitting contact details does not result in personal contact – instead you receive an email, as follows:

Hi,

Thank you for your request.

In order for illion to provide you with a copy of your Insurance Claims Information, we will require you to first complete an application form.

Our application process will also require us to complete identify verification so we will also require 2 forms of identification.

Please complete the attached form and return with it the following:

- A copy of Driver's license OR Passport OR Birth Certificate OR Proof of Age Card
- A copy of a document issued by an official body (such as a utility or bank statement)

Kindest Regards,

illion
Formerly Dun & Bradstreet

illion Public Access Centre on behalf of IRS
479 St Kilda Rd
Melbourne VIC 3004
Phone 1300 734 806
Fax 03 9828 3118

An application form accompanies the email. A sample appears below (as copied-in .docx).

The form is problematic in several ways. If filling in the form digitally:

1. The form is provided to a consumer as a Word document. It is not a fillable PDS;
2. The form states that "Fields marked with an asterisk (*) must be filled in" and asks, without explanation, for a significant amount of detail beyond what is strictly required. For example:
    a. Driver's licence number;
    b. Middle name;
    c. Any other first names you have used;
    d. Any other surnames you have used;
    e. Current employer name;

f. Contact information beyond "At least one number is required to assist us with processing your request";

g. Two previous addresses; and

h. At this address since.

3. The form is largely unreadable at 100% size with some words at 4, 5 and 6 point font. Adding to this many field where information is required to be provided have their font colour set at light grey, adding to reading difficulties;

4. Ticking boxes was not an option since the boxes were in fact Wingding boxes – which had to be erased and replaced;

5. Filling in the suburb box was set at 4 point and has to be changed manually;

6. Filling in the Signature boxes is difficult because the consumer needs to paste an image (which is easier in PDS forms) in a word .doc the image has to fit in the one line room space provided meaning signatures are tiny;

7. Inputting credit card details is also difficult since the boxes provided for the numbers are again in wingdings font and have to be replaced and the font re-set to another font to ensure that it is in numeral form. The problems with the form outlined above seem designed to require the customer to print it out and fill in manually, scan it and send it. This may be a significant hurdle for consumers without easy access to a printer.

The IRS, as an APP entity, is only required to respond to subject access requests "within a reasonable period" as per Australian Privacy Principle 12.4(a)(ii). In practice, it can respond much more quickly, and in two of the test cases conducted as part of the empirical research, it did so within five days.

The *My Insurance Claims Report* is sent by email from "Illion DIRECT". A typical report obtained in June 2021 comprises five pages, respectively:

- Individual insurance enquiry plus – report summary;
- Insurance history (listing claims and enquiries, but not policies held);
- Public record information;
- Business relationships;
- Appendix – Information sources.

My Insurance Claims report

Australia

Cost: The cost of this report is $22.00 (Inclusive of GST) and will be processed within five days of having received your fully completed request .

Fields marked with an asterisk (*) must be filled in.

First Name*				Salutation*	☐Mr ☐Mrs ☐Miss ☐Ms
Middle Name				Date of birth*	DD / MM / YY
Surname*				Gender*	Male ☐ ☐
Any other First Names you have used				Driver Licence No	
Any other Surnames you have used					
Current Employer Name					
Contact Information* (At least one number is required to assist us with processing your request)	Work		Home		Mobile	
	Email*				
Current Residential Address *	Unit No.	Street No*	Street Name*		
	Suburb*		State*		At this address since	MM / YY
1st Previous Residential Address	Unit No.	Street No.	Street Name		
	Suburb		State		At this address since	MM / YY
second Previous Residential Address	Unit No.	Street No.	Street Name		
	Suburb		State		At this address since	MM / YY

In addition to completing the form, you will need to provide the following documents to verify your identity:

1.) A copy of your Driver's Licence or Passport or Birth Certificate or Proof of Age card AND
2.) A copy of a document issued by an official body (such as a utility bill or bank statement) which includes your name and address

Please confirm the following:

- ☐ I confirm that I am requesting a copy of my own insurance claim report and the details supplied to identify me are true and correct
- ☐ I have completed all mandatory fields
- ☐ I have attached my identification documentation
- ☐ I have signed the application form

Signature		**Date**	DD / MM / YY
Office use only	consumer Reference No	— — — — — — — — — — — — — — — —	

I authorise illion to charge my credit card for the amount of $22 (Inclusive of GST)

Cardholder's Signature	

PRIVACY STATEMENT

illion Australia Pty Ltd – ABN 95 006 399 677 only collects personal information about the individual to whom this letter has been addressed (you) for the purpose of supplying the Insurance Claim report. For more information on how IRS collects, holds, uses and discloses personal information, please go to: http://insurancereferenceservices.com.au/privacy.

illion Public Access Centre - PO Box 7405 St Kilda Rd, Melbourne, VIC 3004
Tel 1300 734 806 - Fax 03 9828 3188 - Email isconsumer@illion.com.au
illion Australia Pty Ltd – DUNS 75 340 7170 | ABN 95 006 399 677 | ACN 006 399 677

PAYMENT DETAILS

Charge my MasterCard Visa Amex

Credit Card no	☐☐☐☐–☐☐☐☐–☐☐☐☐–		
Cardholder Name		Expiry Date	MM / YY
		CCV	

A5-8 SUBJECT DATA CORRECTION RIGHTS

The insurance industry recognises there have been some significant data quality issues with the IRS, and the ICA are currently engaged in a data improvement program for the IRS.

The IRS accepts responsibility for the "Personal Details" part of the IRS database.

However, the IRS takes the view that it is not responsible for complying with Australian Privacy Principle 13 in respect of the Insurance Claims Report part of its database because it regards itself as simply a repository of that information which belongs to contributing insurers. If an individual requests correction of IRS data, usually after having received their *My Insurance Claims Report*, they are told to contact the insurer that provided the data to IRS. The text of the FAQ on the IRS website is as follows:

> *"Inaccurate Insurance Claims Report*
>
> *If an insurance claim or insurance enquiry on your My Insurance Claims Report is inaccurate, please contact the insurance company listed and request them to update their records. Your Insurance Claims Report will be updated within five days of the insurance provider submitting updated information.*
>
> *IRS does not make any representation or warranty as to the information provided by IRS members and which is used to generate Insurance Claims Reports."*[61]

Also, in answer to another FAQ:

> *"Should you find any errors on your My Insurance Claims Report, you can request an amendment and get it rectified before it impacts any of your claims. If the error relates to insurance claims information please contact your insurer who supplied the data to IRS, as the error needs to be rectified at source. If the error relates to incorrect identity verification please contact IRS@insurancecouncil.com.au."*

The covering email received with a *My Insurance Claims Report* also states: "Should you have any queries, please contact the relevant insurance company". Furthermore, the Terms of Use include a waiver statement that:

> *"IRS does not make any representation or warranty as to the information provided by IRS members and which is used to generate Insurance Claims Reports."*

IRS could in our view be challenged about their position on the correction of claims data. Given that there must be a possibility of errors resulting from processing by IRS, they should accept that they might sometimes be responsible for correction. Not all data quality issues in a third party database will necessarily stem directly from the quality of the input data.

---

61 Insurance Reference Service, *FAQ*, **http://insurancereferenceservices.com.au/faq**.

It would sometimes be appropriate for the IRS to play an active part in resolving any challenge to the quality of claims data, liaising as necessary with the insurer that contributed the data. Consumers should not have to deal only with the insurer, when the IRS may be partly or wholly responsible for the problem.

A5-9 COMPLAINTS ABOUT THE IRS

The IRS Privacy Policy includes contact details for internal complaints and for external complaints to the OAIC. It is not clear why there is no reference to the alternative external dispute resolution route of referral to AFCA, which would be the normal route for escalation of privacy complaints against member insurers.

The text of the FAQ on the IRS website states:

> **"Personal details**
>
> *If your Personal Details are not accurate please contact IRS@insurancecouncil.com.au. Further verification documents may be required. If further verification of the supporting documentation is not required, we will amend the entry within 5 working days and forward you a copy of your amended My Insurance Claims Report. If verification is required, please allow us 30 days to respond to you. Please note that your address history on your My Insurance Claims Report is not a chronological list of addresses you have lived at. Addresses and your employer's name are added to your My Insurance Claims Report by insurers in conjunction with an insurance enquiry or claim you have made with them. Neither IRS nor illion add addresses or current employer information to the IRS database or My Insurance Claims Reports."*[62]

Whether this interpretation and approach by the IRS complies with its obligations under Australian Privacy Principle 13 is questionable, not least because there is obvious potential for data to become altered either in transmission between insurers and the IRS or while held by IRS, separately from the source data held by an insurer.

62 Insurance Reference Service, *FAQ*, **http://insurancereferenceservices.com.au/faq**.

Appendix 6: Details of the field research

This Appendix provides detailed information in support of the summary of the field research. (**See Section 3)**.

A6-1 NATURE, PURPOSE AND LEGAL BASIS FOR IRS

The IRS does not itself perform the functions, but contracts the entire operation out to Illion, which previously traded as Dun & Bradstreet in Australia. It has long operated a commercial credit reporting business. The outsourced activities appear to encompass the gathering of data from insurer members, maintenance of the database, provision of access to the database contents by insurer members, and the provision of a report from the database to consumers on request.

The IRS states that its sole purpose is to:

> *"Manage, for the benefit of its Australian insurance company members, the IRS claims database, which comprises motor, home and travel claims information in Australia"* [63]

It does so to support:

> *"Claims management, claims investigation, loss assessment, fraud detection and risk underwriting.*
>
> *This knowledge enables insurers to efficiently assign investigation resources, resulting in targeted and faster investigative processes and claims handling, while playing a pivotal role in identifying insurance claims fraud and validating underwriting risk."* [64]

The IRS also offers a service to consumers as:

> *"My Insurance Claims Report ... based upon the aggregated home and motor claims records of the IRS home and motor claims database."*

Elsewhere, the site also mentions "insurance enquiries (last 5 years)" and indicates that insurance claims information relates to the past 10 years.

Illion projects the document to both insurers and consumers as being an "Insurance Claims Report".

On the other hand, the IRS/Illion also collects, stores, and discloses in its reports, much more than claims information, including details of enquiries and applications made by consumers, and data from other sources entirely.

---

63 Insurance Reference Service, **https://insurancereferenceservices.com.au/**.

64 Insurance Reference Service, **https://insurancereferenceservices.com.au/**

No explanation is provided by the IRS/Illion of the legal authorities for the disclosure of information by insurers, for the collection of information by the IRS, and for the disclosure of information by the IRS to other insurers. The information flows include claims information, insurance enquiries, and enquiries from loss assessors, adjustors and investigators. We identified a handful of PDS's that explicitly referenced the disclosure.

Further, it is not clear what purpose, and under what authority, the IRS/Illion includes within the database, and/or within disclosures, extraneous information on other matters, including:

- Bankruptcies;
- Summons;
- Judgments;
- Commercial credit history; and
- Directorships.

It is particularly concerning that credit-reporting data may be disclosed to insurers.

Beyond that, it is not clear whether Illion uses or discloses any data received from insurers for any purposes additional to the operations it performs under contract with IRS, or absorbs any of that information into the other databases it operates.

A6-2 IRS PROCESS QUALITY

The process of obtaining a *My Insurance Claims Report* is difficult, convoluted and confusing.

It involves a large number of steps described. **(See Appendix 6A and Table 3).**

Participants described the process as unnecessarily multi-stepped, clumsy and inconvenient:

> *Participant 2: "Putting details onto the website and then receiving the form, then putting many of the same details into the application form and sending it back did not feel like a streamlined approach."*
>
> *Participant 7: "The whole process is confusing and unexpectedly clunky."*
>
> *Participant 8: "Formatting of the application form was an issue."*
>
> *Participant 9: "the need to apply for an application form should not be a necessary step … the setup of the process was amateurish. And that the persons responsible for creating the process through the website and putting together the application form clearly did not know what they were doing" … it was ridiculous I don't understand why they made a report which was so obscure and so needlessly complex for consumers to obtain."*
>
> *Participant 11: "The type face was very small … I could not read it with my usual magnifying glass and so I got out my better magnifying glass, and I still could not read it."*

> *Participant 12: "It is baffling that they do not simply have a single secure online form … the information I put into the form was much the same as the information IRS initially required from me to apply for access to that application form. They [the IRS service] could have copied and pasted this information themselves."*

Obtaining one's own insurance claims data is not gratis

Unlike a credit report where a consumer is entitled to four free credit reports a year, obtaining your data from the IRS is not gratis. A fee of $22 is levied.

This is an additional procedural hurdle for most people, and a financial barrier for many.

The provision of credit card details is not via a secure system. A consumer needs to fill in a word document with their credit card number and other details:

> *Participant 12: "This is not a good look for a company that handles personal information and accepts payments through unsecured email exchanges. I felt uncomfortable providing my credit card details to them in this unsecure way."*

The time taken to obtain a *My Insurance Claim Report* is lengthy

The process for obtaining the report was far from timely. It generally took 24 hours just to obtain an application form, and then a further three to five days to obtain the report once a completed application was sent. However this was not a uniform experience. Some participants had to make multiple requests and wait up to 30 days for the report.

One participant endured numerous emails back and forth after payment details were rejected. Another participant received an unjustifiable demand for a mobile phone number.

These aspects were construed by some participants as obstacles intended to dissuade applicants.

In response to the *Automating General Insurance Disclosure* report (Financial Rights, 2021b) seeking more streamlined ways for consumers to automatically share their insurance disclosure information, the ICA said: "individual policy holders can also access a personal claims report via the Insurance Reference Services (IRS) website for a service fee" (IN 2021). While this may be true, what it does not reveal is that consumers must often wait between three and 30 days to fill in the disclosure question when asked at quote time, that is, if they are aware of the service in the first place. The failure to provide timely responses is problematic for consumers and in many circumstances defeats the purpose of quickly and efficiently accessing a couple of competitive quotations, in order to test the market.

No receipt was automatically provided

When a receipt was requested – as per the right to request a receipt for anything under $75 – the receipt was provided 69 days later – not the seven days as required.

A6-3 IRS DATA QUALITY

The IRS FAQ[65] includes this entry:

> *"Understanding My Insurance Claims Report*
>
> *My Insurance Claims Report can contain the following information:*
>
> - *Personal details such as name, residential address, date of birth, driver's licence number*
> - *Enquiries made by during the past five years including enquiries where cover applied but not taken out. The report records each enquiry by insurance companies, not actual insurance policies taken out*
> - *Enquires [sic] made by third party agents of insurers during the course of a claims process*
> - *Details of claims submitted to IRS member insurers – whether or not they eventuated in a payment, and may include withdrawn and denied claims."*

No further information is provided about interpreting the contents of the IRS reports.

Every *My Insurance Claims Report* accessed included at least one error with respect to the data provided, as shown in Table 4. The errors identified included a large variety of missing information, imprecisions and obscurities, listed below. Most participants were fatigued by the delays and effort involved in the process. Financial Rights does not have the authority to discuss these problems with the ICA, IRS or Illion on behalf of participants. Therefore it may be that some of what appear to be errors in the IRS database and/or report are capable of explanation. As detailed below, however, it appears unlikely in respect of most of the problems.

A6-3.1 Incorrect address details

Six of the 15 participants identified incorrect home address details. For example, the previous address was listed as the current address and vice versa while others included different forms of the same address – just with the Lot number included.

A6-3.2 Claim type descriptions were either incorrect or inconsistently described

One participant's claim was misrepresented as a collision, when their car was in a carport that collapsed under the weight of a falling tree during a weather event.

Others noted a difference between the claim type description on their *My Insurance Claims Report* and the description in the information their insurer provided such as "storm" versus "Storm/Flood/Earthquake" and "Third Party Hit in Rear by Insured" versus "collision".

Participant 14 had two different descriptions from two different insurers for two incidents that were

65 Insurance Reference Service, *FAQ*, **http://insurancereferenceservices.com.au/faq**.

factually identical. One described the claim type as "insured hit in rear by third party" the other as "damage whilst driving" – the latter description potentially being materially misleading given the lack of information regarding fault.

A6-3.3 Claim status descriptions incorrect or misleading

Five of the participants raised concerns with respect to the way the claims status was framed. Participant 2 noted that a claim listed as cancelled when it was in fact refused. Participant 8 included a claim listed as paid when in fact it was withdrawn. Participant 13 had a claim listed as "cancelled" when the insurer had in fact originally accepted the claim against the wrong policy and had to transfer it to the correct policy.

The absence of reasons for refusals puts consumers at risk of a refusal being misconstrued, for example, partial rather than full, exclusion clause rather than non-disclosure.

A6-3.4 Additional claims listed

Three participants found additional claims incorrectly attributed to them on their *My Insurance Claims Report*. As above:

- Participant 13 had a claim listed as "cancelled" when their insurer had in fact originally accepted the claim against the wrong policy and had to transfer it to the correct policy. This administrative error was listed as an additional claim;
- A similar administrative error led to an additional claim listed for the participant 14; and
- Participant 9 asserted that a claim listed in their *My Insurance Claims Report* was not a claim at all – merely an enquiry made. The information obtained from their insurer confirmed that no claim was in fact made.

Two further participants were surprised to find their withdrawn claims listed as closed – not withdrawn.

A6-3.5 Missing claims

Five participants identified one or more claims that were missing from their *My Insurance Claims Report*. One participant found five claims were missing. Four participants confirmed omissions from the IRS report by comparing the IRS list with information obtained directly with their insurer to the *My Insurance Claims Report*. One participant held material confirming the discrepancy but was unable to obtain the information directly from their insurer.

A6-3.6 Old claims not removed

The report received by one of the team-leaders included a claim that should have been removed by the end of August 2020, but was still being displayed 11 years and 12 days after the "Date of Loss".

A6-3.7 Net settlement and excess figures were missing

Seven participants noted that at least one of their claims listed a net settlement amount of $0 when this was not the case – as confirmed by information obtained by their insurer. Similarly six participants noted that at least one of their claims listed "no" with respect to the field "Excess paid" when this was not the case.

A6-3.8 Third party recovery missing

Two participants noted that their "Claims recovered from third party" incorrectly included the word "No". It was their understanding that these were claims that recovered from third parties and the "No" raises significant ambiguities that could be misleading. Some entries were clearly incomplete data, particularly in the vital area of claims.

A6-3.9 No insurer inquiries listed

No insurer inquiries were listed on any participant *My Insurance Claims Report*. It was noted by one participant that they had made numerous enquiries searching for coverage after being denied coverage by their insurer. The researchers have however seen insurance enquiries listed on other *My Insurance Claims Reports* not a part of this study. These list the date the enquiry was made, a reference number, the insurer, insurance type, the reason (quotation, new business, claim), the amount and the relationship.

A6-3.10 No explanations are provided for information and terms used

No glossary or definitions of terms is provided for any of the terms used in the report, nor are explanations for the information included.

A6-3.11 "No record found in Illion bureau"

Seven out of the 15 *My Insurance Claims Reports* obtained included a label – highlighted in red on the front page – stating:

> *"No record found in Illion bureau"*

It is not clear what the label refers to or what is meant to be conveyed. No explanation is provided despite the fact that the *My Insurance Claims Reports* include records and list claims. The entry is highly ambiguous and can potentially be read as implying some fault by, or risk associated with, the person concerned.

A6-3.12 "Other possible matches"

It is not clear what "Other possible matches" means.

Participant 11 had a number "1" in this field on the front page and found their own name and details listed in "Other possible matches" except with their birthdate incorrectly listed as "1 January 1900". No explanation was provided as to what the relevance of this information was, whether the participant needed to do anything about this, nor any information as to steps they could take to correct the information.

Participant 6 also had a number "1" in this field, however there was no further information included in the report. No further information or explanation is provided in the report to assist the participant's comprehension of this listing. The participant indicated that it was "incredibly odd" to include this reference in the summary without providing any further information about it later in the report.

A6-3.13 "Loss assessor/ adjustor/ investigator enquiry"

Participant 14 noted that there was one "Loss assessor/adjustor/investigator enquiry" listed relating

to a compulsory third party claim for the amount of $1. Participant 14 was "completely gob-smacked by that one" and "has absolutely no idea what this is". Participant 14 said: "When I saw it I said: "What the hell!" and "What kind of claim or enquiry would the entry be for? I don't know".

A6-3.14 Claims count

The presentation of the claims history count on the front page of the *My Insurance Claims Report* is not clear where it lists "Insurance claims" and "Claims with vehicle data". The two categories read as distinct, whereas in reality the latter appears to be a subset of the former.

A6-3.15 Relationship

Claims histories include a "relationship" field which either includes the word "Claimant or Driver", or is left blank. It is not clear from the context what these refer to. For example, whether it is the recipient's relationship to the policy or something else. It is not clear when the claimant or driver is used what the significant of this is – especially since these are more often than not left blank.

A6-3.16 Claim type

A large array of claim type descriptors are used in *My Insurance Claims Reports*. Some terms seem standardised and general although in some cases may be too general. For example "collision", "damage whilst driven", "flood" and "natural hazard". The term "Other" was used to describe six claims across the participant pool.

Other terms used become very specific and raise a question as to whether there is standardisation of terms at all. For example, it is not clear what the difference is between "Damage whilst Anchored Moored or Parked" and "Vehicle Damaged Whilst Parked", or "Impact Or Damage By Object Vehicle Or Person" and "Insured Hit in Rear by Third Party."

Of concern is the description "At fault" for one claim which seems like it belongs in a separate fault category rather than being used as a description of the claim type.

Finally, it is important to repeat that there is no glossary or dictionary of terms to assist policyholders to understand the information that they are being provided.

A6-3.17 Blanks

Almost every claim listed amongst the participants had fields that were left blank. No explanation is provided as to whether the information in that field was left deliberately blank, the information was irrelevant or non-applicable, no data was held for that data-item, or data exists in the database but was intentionally omitted from the report. This is made even more confusing since the phrase "unknown" is used at times. For example, Participant 5 noted that "Registration State" was listed as "unknown" when they felt the insurer would clearly hold this information.

A6-3.18 No fault listed

Some participants noted with concern that "fault" is not listed as a field on the *My Insurance Claims Report*. A number of participants felt that fault was relevant information that provided important context for their claims history. One participant noted that: "Otherwise it is misleading". This misleading impression is exacerbated by the lack of information included in the net settlement section. One participant found the lack of this information "troubling" because it was unclear

whether it has had or may in the future have any effect on his insurance premiums. This is particularly given the information is out there and can presumably be made available to insurers, including insurers other than the one from whom that data was acquired.

As noted above one claim listed "At fault" as a "claim type". By contrast, five participants received information regarding fault directly from their insurer.

A6-4 MY INSURANCE CLAIM REPORT CONTENT UNRELATED TO INSURANCE

The *My Insurance Claims Report* includes information that does not seem related to one's insurance history or insurance needs. The document includes:

- Public Record information including:
  - Bankruptcy information;
  - Summonses; and
  - Judgments.
- Commercial Credit History including:
  - Defaults;
  - Serious credit infringement notices;
  - Credit enquiries; and
  - Authorised agent enquiries.
- Business relationships including:
  - Current and previous directorships.

Most of this information seems irrelevant to disclosure requirements in obtaining insurance. Many participants were perplexed by the inclusion of some information:

> *Participant 3: "Credit enquiries are irrelevant."*
>
> *Participant 6: "Information contained in the report should at least be relevant to insurance claims and these sections in the report ought to be complete. Information that was not relevant to insurance claims should not appear in the report at all."*
>
> *Participant 14: "I was surprised to see credit information in the report. I'm not sure exactly what it was there for."*

Some information unrelated to insurance was found to be incomplete or included errors. For example, three participants found that at least one of their current or previous directorships was not listed in the report. Two participants found that one of their directorships did not include a cease date, despite having ceased many years ago.

Participant 3 found an error in their credit enquiry information which listed an enquiry for a loan for a substantial amount of money as $0.

Most *My Insurance Claims Reports* had no or minimal information in these additional non-insurance information sections. The lack of comprehensive information in these additional non-insurance related sections raised concerns with some participants.

Participant 14 noted that during the relevant period they had entered into a home loan and they had made credit enquiries in connection with it, yet nothing appeared in the *My Insurance Claims Report* about these enquiries. Participant 14 said that having space for this information with nothing listed there – "created an assumption that there was nothing". Participant 14 said it created the assumption that they had not made credit enquiries.

Participant 6 category noted that categories of information that were not relevant to insurance should not even be listed since they may create a misleading impression when left blank.

A6-5 INSURER PROCESS QUALITY

As summarised **(see Section 2.4)**, insurers have process quality obligations under privacy law, the General Insurance Code and their own undertakings to their customers.

The 15 participants held claims with eight different insurers. All eight insurers are current members of the IRS service: AAMI, Allianz, Auto & General, Comminsure, GIO, NRMA, QBE, RACQ.

The process of obtaining information from insurers was opaque and difficult

The obligation to respond appropriately to requests for access to personal information has existed for two decades. It would therefore be reasonable to expect that well-articulated procedures are applied by trained and experienced staff and operating smoothly.

Instead, the sample studied in this project had to be far smaller than originally envisaged, because the processes encountered at four major industry members66 were:

- extremely opaque, inconvenient and slow;
- in many cases, failed to satisfy the consumer's needs; and
- in multiple cases, arguably in breach of the law.

A number of participants were forced to email going back and forth with their insurer, with the correspondence extending over days or weeks, to obtain the information. Some felt forced to, or preferred to, call instead. This inevitably costs a consumer a considerable amount of time, including waiting-time, and often lengthy explanations concerning the background of the request to each new call-centre staff-member who answers their call.

Participant 3 was not provided with a response to their initial request and had to send a number of emails and a complaint to the insurer to obtain the requested information.

Participant 4 sent the request in mid-August and received a final response in mid-November. After their initial email bounced back, the participant re-sent the email from a different email address on or around 22 October, 2021. A confirmation email was received 9 days after this indicating that the

66 AAMI, NRMA, RACQ and Allianz

response would take 1-30 days to respond. It took 15 days. Discounting the bounce-backs and initial difficulties, the enquiry took a total of 19 days.

Participant 5 noted there was no dedicated privacy email address. Two emails arrived in response, the second email causing them to expect more information to come … which never arrived.

Participant 14 experienced very difficult processes for a variety of reasons. Participant 14 received a number of calls from the insurer requesting permission to contact their partner to seek their partner's permission to share the information with them. Some calls cut out before they were concluded. The Participant 14's partner experienced the same problem. The partner received a number of calls that would cut out before permission was given. The exchange of calls "went on for days".

Participant 14 also sought clarity with respect to a "loss assessor/adjustor/investigator" listing. Participant 14 received an email with a phone number to call for "equiries [sic]" Upon telephoning this number to seek more information regarding a reference to $1 noted on their *My Insurance Claims Report*, Participant 14 found that the number in fact belonged to an unrelated insurer. They subsequently made a complaint to the insurer but at time of preparation of this document had not received a response – nor an acknowledgement that the insurer received the complaint.

Participant 12 received 3 emails, all seemingly from a different department within the insurer brand and group. Each email seemed "incoherent" and essentially directed Participant 12 to ask another department. When Participant 12 received a concluding email all they received was a statement that: "We have reviewed the profile and confirm there is [sic] no current claims on your profile." This was incorrect. Two claims made with the insurer were never identified or provided. This is confirmed by an older *My Insurance Claims Report* obtained in 2015 which does list these claims. Participant 12 felt their request was being "bounced around" and then in the end she never received an accurate or at least satisfactory reply.

Participant 12 also observed that while the web form was easy enough to use, it did not seem to be fit for purpose. That is, the webpages were difficult to navigate to arrive at the form. The insurer's privacy policy directed people to use the enquiry form through their "privacy policy" and "privacy-security page" and then "contact us" page. Then once one arrives at the form, the form itself, in its drop down list, did not have "privacy" or "information access" option for them to choose. Participant 13 was confused about whether they were in the right place to make a privacy access request.

Participant 13 received from their insurer "nothing" just an "email saying there were 5 claims" and had to send a detailed follow up requesting further information. The participant said the process was complicated by the insurer providing a deficient first response which meant they had to request that their enquiry be chased up.

A6-6 INSURER DATA QUALITY

Insurers have obligations in relation to data quality arising from privacy law, the General Insurance Code, and their own undertakings to their customers.

As summarised in the following table, the information provided by insurers varied greatly but was in many cases minimal.

Information provided by four major insurers

	Insurer 1 (AAMI)	Insurer 2 (NRMA[67])	Insurer 3 (RACQ)	Insurer 4 (Allianz)
Policy Holder Name	❌	❌	✅	❌
Policy Number	✅	✅	✅	✅
Cover Type/Policy Level	✅	❌	✅	✅
Risk Details/Address	❌	❌	❌	✅
Policy Inception Date	✅	❌	✅	✅
Period of Insurance	❌	❌	❌	✅
Last Policy Term	❌	❌	✅	❌
Cancellation Date	✅	❌	❌	❌
Date of Claim	✅	❌	✅	✅
Incident Date	❌	✅	❌	❌
Claim Number	✅	✅	✅	❌
Type of Claim/Incident Type	✅	✅	✅	✅
Total Payout	❌	✅	❌	❌
Claim Amount[68]	❌	❌	✅	❌
Fault	❌	❌	✅	❌
Excess	❌	❌	❌	❌
Claim Status	❌	✅	❌	❌

67 Note that the information provided by Insurer 2 was not consistent and varied considerably from participant to participant. The information outlined above refers to the most information provided when one pdf was sent was sent to one participant, as opposed to a basic email response.

68 It is not clear whether "Claim Amount" is the same as "Total Payout".

The information provided by some insurers lacked detail and listed basic data only. It was often impossible to assess the quality of the data held by the insurer. Most participants were sent a standard pdf with basic information from their insurer or insurers. There was however little consistency in what information was provided. Some participants were sent an email outlining basic information or telling them that they held no information at all. The table below provides some idea of the variability and low quality.

One insurer provided an email response detailing in discursive form the various dates of claims, the claim types, the claim numbers and the amount paid. One noted that the insurer had recovered the repair cost.

Some participants received a voluminous amount of information that was difficult to read

Three participants, two with the same insurer were sent a large amount of information.

Participant 4 received a 7mb pdf made up of 165 pages. Much of the information provided - in a series of screenshots - goes back to the 1990s. Many of the screenshots involve historic material – while further information on calls made, actions taken and conversations held during a claim made in 2020 claim are included in another near-indecipherable format for 72 pages.

Participant 14 received 4 locked pdfs including one 7mb pdf of 147 pages. The information is largely made up of policy documents and payment details pages, with some information on claims notes and file notes of conversations held in screen shot form.

Participant 15 received a series of computer screenshots from one insurer. It was unclear why this were provided and how it related to the information requested because the covering letter offered no explanation. Another insurer provided various documents comprising 13 different pdfs and no explanation or commentary relating to them. Most were copies of policy renewal documents.

The experiences of a member of the team **(see Appendix 6B)** provide additional examples of data provided to a consumer in materially inadequate form.

Documents data-items that were evident in those cases in which screenshots were provided of online displays from the insurer's customer database(s). **(See Appendix 6C).**

A6-7 CONSISTENCY BETWEEN IRS AND INSURER INFORMATION

A crucial indicator of data quality is consistency between data provided by the IRS and data in the records of insurers. This matters not least because discrepancies are likely to work to the disadvantage of consumers, because data delivered in neat form from a computer-based system will tend to be more highly regarded by employees than that provided directly by consumers. Differences are likely to create doubt about the consumer's reliability and/or honesty.

Some participants identified claims information that was missing from, or additional to, that found on their *My Insurance Claims Report*

Seven participants were not provided with claims information from their insurer (or insurers, in one case – Participant 15) regarding at least one claim listed on their *My Insurance Claims Report*.

Participant 7 did not receive claims information on a claim that was also not listed on their *My Insurance Claims Report*.

Two participants identified claims in the information that they were provided by their insurer that were not in their *My Insurance Claims Report*:

Participant 5 was provided information on three claims not on their *My Insurance Claims Report*. Two claims were – according to the participant - in fact claims made under another person's policy about another (albeit related) person's property;

- Participant 13 was provided with the prior insurance claims the participant disclosed to the insurer. These however had incorrect details regarding the motor vehicle involved.

Participant 5 was provided with claims information from their insurer that was outside of the 10 year scope of the *My Insurance Claims Report*.

Participant 15 had eight claims in total over the past 10 years. Four were listed on their IRS form. They were provided with information on two of these claims. The participant was provided with information on another claim not listed on their IRS form. A further four claims were not listed on the *My Insurance Claims Report* nor included in the material provided under the information request to the insurer. Participant 15 confirmed there were another four claims with one of their insurers because with an older email showing that the insurer provided a list of those claims. The participant expressed the view that the response sent by the insurer did not "bear any relationship to the information request."

Further, as reported in earlier sections:

- Participant 9 asserted that a claim listed in their *My Insurance Claims Report* was not a claim at all – merely an enquiry made. The information obtained from their insurer confirmed that no claim was in fact made;
- Four participants were able to confirm omissions from the IRS report by comparing the IRS list with information obtained directly with their insurer to the *My Insurance Claims Report*. One participant held material confirming the discrepancy but was unable to obtain the information directly from their insurer; and
- Seven participants noted that at least one of their claims listed a "Net Settlement amount of $0" when this was not the case – as confirmed by information obtained by their insurer.

Lack of consistency between the claims type descriptions used in My Insurance Claims Report and insurer information

In addition to consistency in claims types descriptors listed in *My Insurance Claims Reports* **(See Section 3.6)**, there was further inconsistency between the description of a claim used in the IRS to that used by the original insurer.

For example Participant 6 included the claim type description "Damage whilst Driven" for two claims. However the insurer listed these more precisely as:

- Insured Hit in Rear by Third Party; and
- Insured Reversed into Third Party.

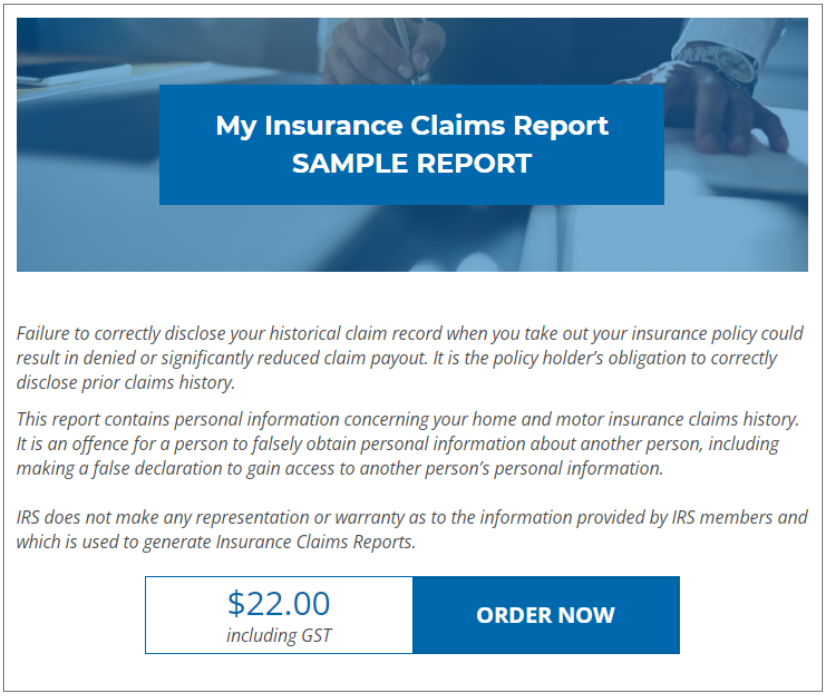
Participant 13 had a claim listed on their *My Insurance Claims Report* as "Impact Or Damage By Object Vehicle Or Person" but was listed merely as "collision" by the insurer information.

Appendix 6A - Steps required to obtain a My Insurance Claims Report

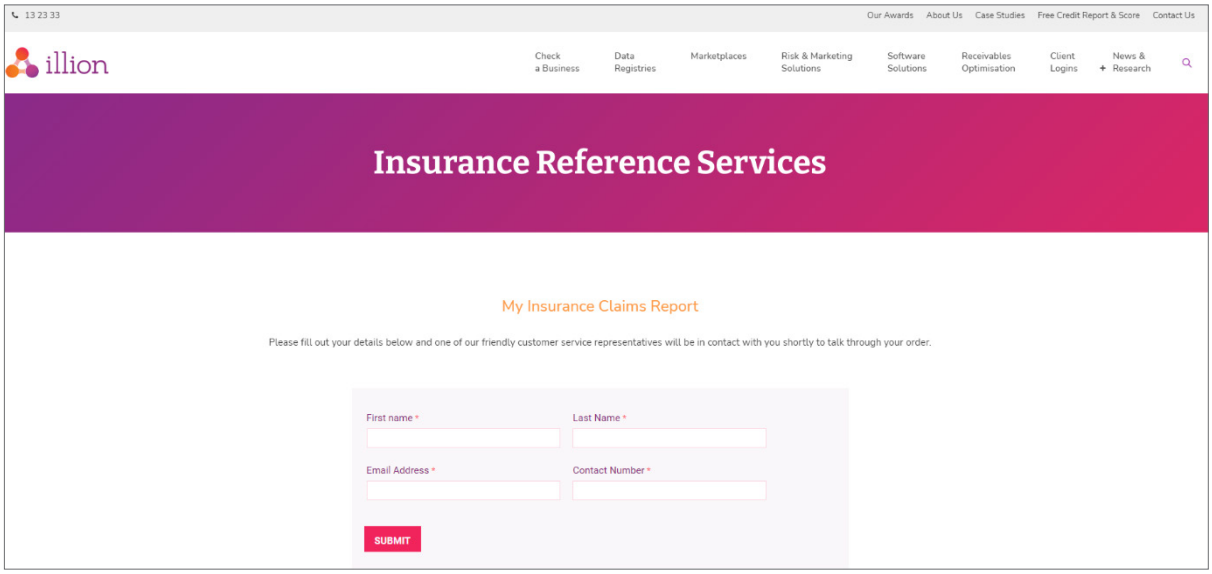
This Appendix provides a description of the process that consumer must go through to access to a report from the IRS. It includes screenshots of relevant displays and forms.

1. Go to the insurancereferenceservices.com.au and click on Order *My Insurance Claims Report*.

2. Click on Order Now and be taken to www.illion.com.au/insurance-reference-services/



3. Provide your details (first Name, last name, email address and contact number) whereupon "one of our friendly customer service representatives will be in contact with you shortly to talk through your order"



4. Wait to receive an email from **irsconsumer@illion.com.au** (generally within 24 hours) with an application form in Word .doc form and a request for two forms of identification

irsconsumer <irsconsumer@illion.com.au>
to me

Hi,

Thank you for providing us with your completed application form.

Your identification has now been verified and your application for a copy of your Insurance Claim Report has now been processed.

Your reference is **IRS202106290404**

Please refer to the attached claim report.

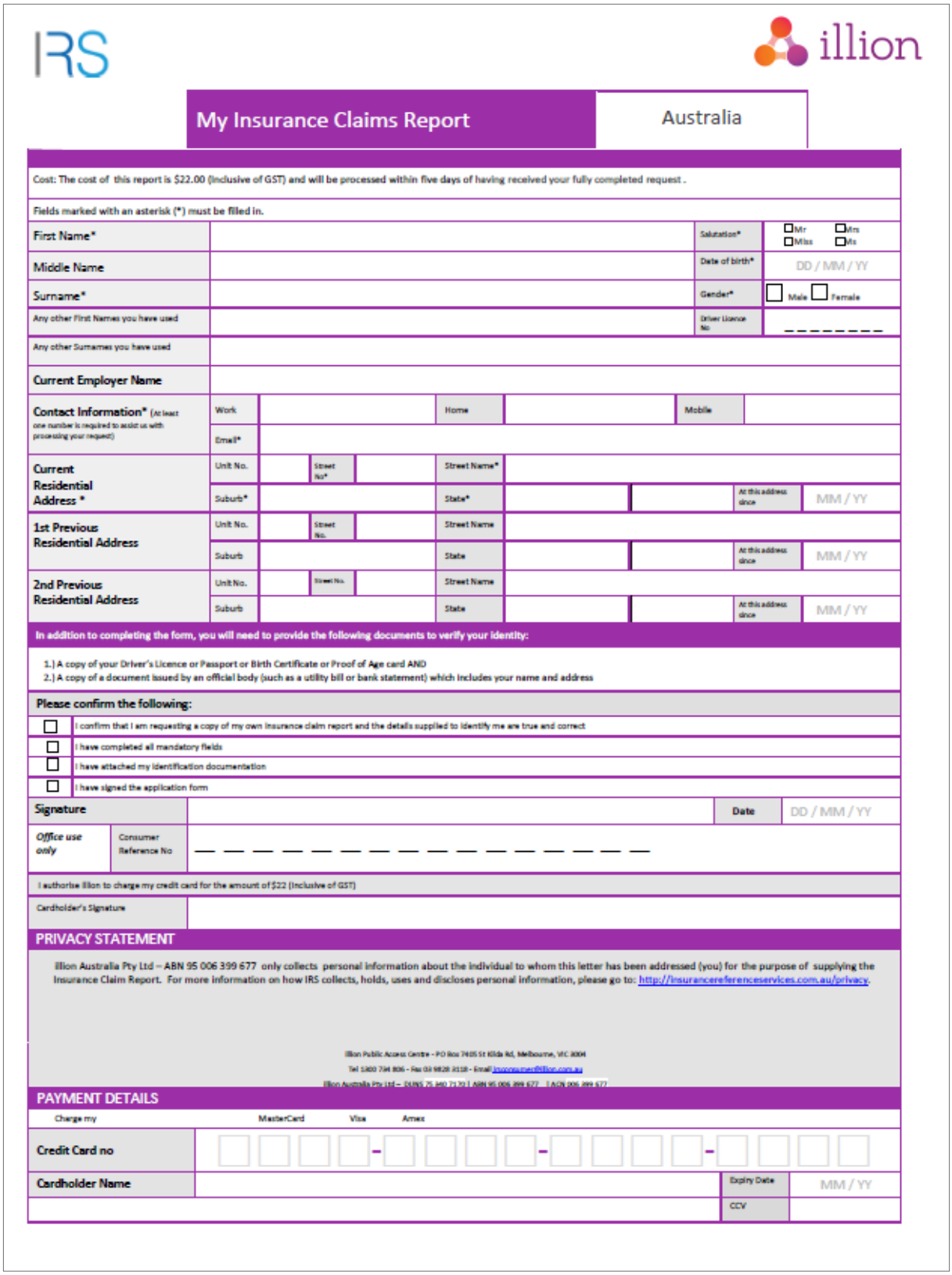
Should you have any queries, please contact the relevant insurance company.

Kindest Regards,

illion
Formerly Dun & Bradstreet

illion Public Access Centre on behalf of IRS
479 St Kilda Rd
Melbourne VIC 3004
Phone 1300 734 806
Fax 03 9828 3118

5. Fill in the form by either printing out the form and manually filling in the form or filling the soft copy word document by manually replacing text where required (the form is not designed to be filled in any automated way). Sign the form



IRS illion

My Insurance Claims Report | Australia

Cost: The cost of this report is $22.00 (Inclusive of GST) and will be processed within five days of having received your fully completed request .

Fields marked with an asterisk (*) must be filled in.

First Name*			Salutation*	☐Mr ☐Mrs ☐Miss ☐Ms	
Middle Name			Date of birth*	DD / MM / YY	
Surname*			Gender*	☐ Male ☐ Female	
Any other First Names you have used			Driver Licence No	_ _ _ _ _ _ _ _	
Any other Surnames you have used					
Current Employer Name					
Contact Information* (At least one number is required to assist us with processing your request)	Work		Home		Mobile	
	Email*				
Current Residential Address *	Unit No.		Street No*		Street Name*	
	Suburb*		State*		At this address since	MM / YY
1st Previous Residential Address	Unit No.		Street No.		Street Name	
	Suburb		State		At this address since	MM / YY
2nd Previous Residential Address	Unit No.		Street No.		Street Name	
	Suburb		State		At this address since	MM / YY

In addition to completing the form, you will need to provide the following documents to verify your identity:

1.) A copy of your Driver's Licence or Passport or Birth Certificate or Proof of Age card AND
2.) A copy of a document issued by an official body (such as a utility bill or bank statement) which includes your name and address

Please confirm the following:

- ☐ I confirm that I am requesting a copy of my own insurance claim report and the details supplied to identify me are true and correct
- ☐ I have completed all mandatory fields
- ☐ I have attached my identification documentation
- ☐ I have signed the application form

Signature		Date	DD / MM / YY
Office use only	Consumer Reference No	_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	

I authorise Illion to charge my credit card for the amount of $22 (Inclusive of GST)

Cardholder's Signature	

PRIVACY STATEMENT

Illion Australia Pty Ltd – ABN 95 006 399 677 only collects personal information about the individual to whom this letter has been addressed (you) for the purpose of supplying the Insurance Claim Report. For more information on how IRS collects, holds, uses and discloses personal information, please go to: http://insurancereferenceservices.com.au/privacy.

Illion Public Access Centre - PO Box 7405 St Kilda Rd, Melbourne, VIC 3004
Tel 1800 734 806 - Fax 03 9828 3118 - Email insurance@illion.com.au
Illion Australia Pty Ltd – DUNS 75 440 7170 | ABN 95 006 399 677 | ACN 006 399 677

PAYMENT DETAILS

Charge my MasterCard Visa Amex

Credit Card no	☐☐☐☐-☐☐☐☐-☐☐☐☐-☐☐☐☐		
Cardholder Name		Expiry Date	MM / YY
		CCV	

6. Scan two forms of identification including:
    - A copy of Driver's license OR Passport OR Birth Certificate OR Proof of Age Card; and
    - A copy of a document issued by an official body (such as a utility or bank statement)
7. Reply to the email from **irsconsumer@illion.com.au** including as attachments the filled-out application form and the two scanned documents
8. Receive an acknowledgement:

irsconsumer <irsconsumer@illion.com.au>
to me

Hi,

Thank you for providing us with your completed application form.

Your identification has now been verified and your application for a copy of your Insurance Claim Report has now been processed.

Your reference is **IRS202106290404**

Please refer to the attached claim report.

Should you have any queries, please contact the relevant insurance company.

Kindest Regards,

illion
Formerly Dun & Bradstreet

illion Public Access Centre on behalf of IRS
479 St Kilda Rd
Melbourne VIC 3004
Phone 1300 734 806
Fax 03 9828 3118

9. Wait for an email from **irsconsumer@illion.com.au**, including the *My Insurance Claims Report* – anywhere from 3 days to 30 days.

   A copy of the cover sheet of the Sample *My Insurance Claims Report* is below[69]:

69 Insurance Reference Service, DNBi: Individual Insurance Enquiry (27 August, 2016), https://insurancereferenceservices.com.au/assets/DNBi%20IRS%20Individual%20Insurance%20Enquiry.pdf.

DNBi

Individual insurance enquiry

Date: 27 August 2016

Report summary

Personal details

Name	John Doe
Date of birth	10 Feb 1950
Gender	Male
Driver's licence number	12345678
Address	1 Right Street Melbourne VIC 3000 Australia
First reported date	27 Aug 2016
Previous address	10 Right Street Melbourne VIC 3000 Australia
First reported date	27 Aug 2016

Insurance history

Insurance claims	2
Insurance enquiries	1
Loss assesor/ adjustor/ investigator enquiries	1

Public record information

Bankruptcies	1
Summons	2
Judgments	1

Commercial Credit history

Defaults	1
Serious credit infringement notices	1
Credit enquiries	1
Authorised agent enquiries	3

Business relationships

Current directorships	2
Previous directorships	2

Appendix 6B - Experience of a team member

This Appendix records the experiences of one of the team members while endeavouring to exercise their Australian Privacy Principle 12 subject access rights with two of the largest general insurers.

LAUNCH

- The team member has many years of policies, of several relevant kinds, with both NRMA and AAMI
- In early-mid July 2021, searches failed to locate on either NRMA's or AAMI's site the expected webpages with clear and simple instructions on the making of an Access Request, for example, using a web-form or with a link to an application form in pdf format
- A check of another provider, Youi, similarly found no simple, single-step means of applying

NRMA

- The only avenue for sending a message appeared to be via its complaint web-form
- I received an auto-generated copy of my message, from <do-not-reply@nrma.com.au>
- I received a response within half-business-day, but from an IAG rather than an NRMA email-address: Customer.Relations@iag.com.au
- It answered my question (1): "Where do I go to request access to my personal information?" by providing an attached pdf form
- It did not respond to my question (2): "How is one meant to use NRMA's web-site to answer question (1)?"
  It remains unclear why a link was unavailable with instructions and a link to download the form directly
- The form required (* = "mandatory") the following "details of the personal information that you would like to access":
  - Policy/Insurance type (e.g. home, car)
  - Policy number
  - Claim number

  It is unclear whether such information can reasonably be "mandatory".
- I submitted my request in mid-August
- A short succession of interactions occurred, as the "Specialist, Customer Relations" sought to "confirm exactly what information that you are after". I tried to explain that "I'm trying to request access to the personal information that you hold about me" meant what it said. This culminated in my clarifications that:

1. *I don't want a summary.*
   I want the data, and not just some categories.
   I'm interested in what you have available about me.
   Many companies add information into the record.
   Many companies collect information from additional sources.
   I'm interested in all of that as well.

2. *However, call recordings *is* pushing it a bit.*
   *Would you please provide me with all of the data *except* call recordings.*

   If there are easy formats and difficult formats, please let me know.
   I can handle a lot of different digital formats on my desktop.

- 5 days later, I received a 2-page boilerplate letter about what NRMA would not do
- I replied, asking for confirmation that my data was coming
- I had no reply after 14 days, so I enquired again
- There was a further attempt to reduce the scope of the request
- I denied that in an email of the same day
- The matter was promptly escalated: "sent your email to our Policy support team to review and respond", with an internal staff thread saying "I don't envy you this one, M. … Is Mr Clarke still on about his privacy access. Still do not really understand what he is actually wanting"
- 2 days letter I received from DI.Policy.Support@iag.com.au a list of 12 policy-numbers and (presumably) a null/empty list of claims (plus my NRMA Roadside membership number, which was irrelevant to the matter)
- 3 days later, I explained that: "your response is inadequate, and very seriously so"

  - *I've extracted below the key parts of the thread.*
  - *My request is, and always has been, unequivocally for access to all of my personal data.*
  - *You've already acknowledged that you hold a range of relevant data. But you've failed to provide it to me.*
  - *You have an obligation at law to do so.*
  - *Would you please now do one of two things:*

    1. *Provide me with the data I have requested (or advise the date by which you will provide it); OR*
    2. *Confirm that you are refusing to provide it to me.*

- 1 day later, I received an email sating "You can login to your online account which will enable you to access all your personal data"

- After a delay of 10 days, I responded:

> - *It seems that my Request has been passed to the wrong place.*
> - *I'm not asking for whatever you display in an online account.*
> - *(And in any case, that requires a mobile phone, and I don't use one).*
> - *Please assign this to your specialists in Australian Privacy Principle12 requests.*
> - *Please copy me in on the transfer across to the right person, so that I know who I'm talking to.*
> - *I repeat, yet again, my request: …*

- I heard nothing more for 30 days, so I followed up
- I heard nothing more

Summary of my dealings with NRMA/IAG

The exchange with NRMA/IAG reflects a failure of organisational processes, including two or more occurrences in which the enquiry was altogether lost. It also reveals multiple potential breaches of the *Privacy Act*.

AAMI

- I found the apparently-appropriate avenue for sending a message to AAMI: privacyaccessrequests@aami.com.au
- I emailed an enquiry to it on 11 Jul 21
- A reply was received one business-day later, but from aami@aami.com.au, signed by an "Assisted Digital Specialist". But it said only that:
- "Your email has been forwarded to the relevant team to assist with your enquiry".
- This suggests that, contrary to the expectation, there is no purpose-specific email-address.
- No contact-point or other information was provided about who was handling the matter
- Having heard nothing further 36 days later, I re-sent to the same address
- That received a prompt apology, saying they had "forwarded another request", to the originally-used email-address
- The same day, I wrote, again, to the nominally specialist address: privacyaccessrequests@aami.com.au
- This resulted in a response from IDR@aami.com.au (IDR AAMI), but with a signature block saying that the person was from Suncorp, referring to my "complaint", and saying that "a Customer Relations Specialist … will contact you within the next 10 business days"

- I replied immediately, saying:

> - *... I didn't make a complaint - although the way things are going, it's looking like I might indeed have to escalate the matter.*
> - *If you read my email, rather than just passing it on, you'd see that I'm actually asking for appropriate handling of my now-40-days-old request for simple answers to simple questions: ...*
>
> 1. *Would you please advise how I request access?*
> 2. *Do you not have an online form that I can use??*

- A couple of exchanges occurred with the person the matter was referred to, at a suncorp.com.au address
- After a further 14 days, to 15 September 2021, I received a phone call from the Group Leader apologising and saying that the message had *again* been sent to the original (and apparently correct) email address. However, the email address appears to be inoperative
- There is no evidence of any further email correspondence
- On 7 October, 2021 after a further 22 days, and a total of 88 days after the original request, I received in the physical post a covering letter with 14 printed screenshots, seemingly of a legacy system (VT100 or similar VDU-display), some headed "Customer Contact Summary", "Policy Header Enquiry", "Client Enquiry", "Motor Vehicle Enquiry".

Summary of My Dealings with AAMI/Suncorp

The process took great persistence to prevent the request being lost.

It took 88 days before any information was provided.

A considerable amount of personal data was eventually provided, as requested.

However, it is in a form which may be convenient to the insurer, but is not convenient to the consumer.

No guidance was provided on how to understand and interpret the screenshots.

No clarification was provided about what was, and what was not, being provided.

Some data-item descriptors are clear, however some are unclear to a consumer, and their meaning is open to interpretation.

Appendix 6C - Data-items evident in screenshots

When screenshots were provided of the customer databases, participants were shown all or part of the following:

1. **Customer contacts** page made up of basic customer information including name and address, phone etc. It also includes "Risk Profile indicators" although it is not clear what the abbreviated letters used mean such as CV, BT, TR etc.
2. **Policy header** enquiry includes information with respect to elements of the policy including:
    a. Inception date
    b. Loyalty date
    c. Previous policies (Prev Pol)
    d. Payment details (Direct Debit BSB etc)
    e. Payment frequency/Instalment Frequency (Instal Freq)
    f. The type of discount offered (Discount Group)
    g. Where they obtained the business (Bus Source)
3. **Client enquiry page** centres on the personal details of the insured including:
    a. Name (Surname, Given Name, Initials)
    b. Birth Date
    c. Sex
    d. Occupation (It is listed as Unknown here)
    e. Licence
    f. ABN number
    g. GST Exemption status
    h. Number of policies and claims (Pol./Clms 1 0)
    i. Email
4. **Motor vehicle enquiry** page includes significant underwriting information such as:
    a. Vehicle details
    b. Where the vehicle is parked (Parked)
    c. Any modifications to the car (Access/Mods)
    d. Pre-existing damage
    e. The number of kilometres driven annually (Yearly Kilometres)
    f. Whether it is used for business purposes (Vehicle Use)
    g. Whether there is financing on the car (N)

h. The market value

i. The sum insured

j. A range of the amounts that the property is covered for (Amy Covered Range)

k. Other

It is unclear what the section relating to Item No. Class, Sub Class, Status, Reason etc means. It is also unclear what fields these are:

a. Lurn

b. FBA

c. SDR

d. Nvic

e. ITC Percentage

5. **Household items** enquiry page includes significant underwriting information such as:

a. Occupied As

b. Dwelling Type

c. Wall Const

d. Roof Const

e. Year Built

f. Door Locks

g. Window Locks

h. Alarm

i. Restrict Access

j. Old Insd DOB

k. Senior Cardholder

l. Bld Condition

m. Under Reno/Const

n. Used for business

o. Unoccupied

p. Storeys

q. Const Standards

r. Land Slope

s. Bld Size

t. Bedrooms

u. Bedroom Size

v. Bathrooms

w. Ducted AC/Heat

x. Granny Flat

y. Pool

z. Tennis Crt

aa. Verandah/Deck

ab. Granny Shed

ac. Garage/Carport

ad. Water Tanks

6. **Policy item list** - a summary page with the sum insured and for the first time the premium paid.

7. **Policy messages inquiry** pages detail incoming contacts from the policyholder and details:

   a. The date and time of the contact

   b. The first name of the customer service representative involved in the communication

   c. A free form field detailing what the contact involved and steps take.

Appendix 7: Potential Impact of CDR-GI on Current Privacy Protections

This Appendix provides detailed information in support of Section 4.7.

A7-1 OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION/DATA

Australian Privacy Principle 1 requires that personal information be managed in an open and transparent way.

Could CDR-GI improve the openness and transparency of personal data management by insurers?

In the CDR regime as currently implemented for banking, Privacy Safeguard 1 is a more specific and prescriptive version of the equivalent Australian Privacy Principle 1 but operates concurrently with Australian Privacy Principle 1[70]. DHs, ADRs and DGs are all required to take reasonable steps to ensure compliance with the CDR regime including Privacy Safeguard 1(2)), and to maintain a policy about their management of CDR data, with the specific content requirements varying between the three categories of CDR entity as per Privacy Safeguard 1(3-6).

The requirement for a CDR Policy is in addition to the obligation on most CDR entities under the *Privacy Act* to maintain and publish a privacy policy. The OAIC advice is that while they can extend their Australian Privacy Principle practices and procedures to CDR data that in itself will not be sufficient. OAIC also recommends a specific CDR data management plan and also sets out an entire four-point approach to compliance with Privacy Safeguard 1, even before giving further guidance on a CDR Privacy Policy.

While the additional requirements of Privacy Safeguard 1 appear beneficial, there is a risk that the very detailed bureaucratic approach to compliance could add to the complexity that may overwhelm CDR consumers and undermine the objective of meaningful consensual participation. Given that insurers' privacy policies are difficult to find, read and engage with. **(See Section 3)**, it appears unlikely the requirements of the CDR will necessarily improve the situation.

A7-2 COLLECTION OF PERSONAL INFORMATION/DATA – HOW MUCH AND WHERE FROM?

Australian Privacy Principles 2-5 in the currently applicable privacy regime

Australian Privacy Principle 2 provides that individuals must have the option of dealing anonymously or by pseudonym with an organisation. Australian Privacy Principles 3 and 4 are concerned with the collection of solicited and unsolicited personal information. Australian Privacy Principle 5 stipulates a requirement for notification of data collection.

---

70 Office of the Australian Information Commissioner, *CDR Privacy Safeguard Guidelines, Version 3.0* (June, 2021), A35, **https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines**.

How would CDR-GI affect the privacy issues around collection of personal information?

In the CDR regime as currently implemented for banking, Privacy Safeguards 2 to 5 cover the same ground as Australian Privacy Principles 2 to 5, but with some significant differences. The overall effect - specifically of Privacy Safeguard 1, 5 and 10) is the same. Requirements on different types of CDR participants to make more information about their data handling practices available both publicly as per Privacy Safeguard 1 and directly to consumers as per Privacy Safeguard 5 and Privacy Safeguard 10, over and above their existing obligations under the Australian Privacy Principles. At least in respect of direct notice when collecting CDR data under Privacy Safeguard 5 and when or before disclosing it as per Privacy Safeguard 10, the CDR Rules are even more prescriptive than the equivalent "content of notice" requirements of Australian Privacy Principle 5 which also covers the matters separately addressed in Privacy Safeguard 10.

This could result in consumers being overwhelmed with detailed privacy information, from multiple organisations, most will probably never read it and or find it very difficult to fully understand.

The CDR Privacy Safeguards are in theory more privacy protective than the Australian Privacy Principles in that collection of CDR data by accredited persons, whether directly or through a DG, is only allowed in response to a specific "valid request" from a consumer as per Privacy Safeguard 3(1)[71] which should convey informed consent for collection and use of CDR data.

A7-3 ANONYMITY AND PSEUDONYMITY

Australian Privacy Principle 2 in the currently applicable privacy regime

Privacy Safeguard 2 replicates the Australian Privacy Principle 2 requirement to give consumers the option of not identifying themselves. This may be illusory in the CDR-GI context since it is difficult to envisage circumstances in which it would be practicable to allow a consumer to use a pseudonym when dealing with them in relation to CDR data. Privacy Safeguard 2 appears to recognise this by including an apparent "override" of the safeguard by the CDR Rules Privacy Safeguard 2(3), reflecting an exemption in Rule 7.3.

A7-4 COLLECTION OF SOLICITED PERSONAL INFORMATION

Australian Privacy Principle 3 in the currently applicable privacy regime

Privacy Safeguard 3 is a more prescriptive version of Australian Privacy Principle 3, and defers to the relevant CDR Rules, one of which is a data minimisation principle, imposing a strict test of relevance and proportionality in Rule 1.8. Privacy Safeguard 3 also requires express consent. Consent only remains valid for a maximum of 12 months after which it must be renewed. The CDR Rules prescribe the processes for obtaining consent[72]. This must also have regard to the CX Guidelines. All

---

71 For convenience and ease of understanding, we refer to the sub-sections of Division 5, Subdivision B of the *Competition and Consumer Act 2010* by substituting the number of the Safeguard for the section number. For example, Section 56ED(1) becomes Privacy Safeguard 1(1), and in this instance, Privacy Safeguard 3(1) is technically Section 56EF(1).

72 *Competition and Consumer (Consumer Data Right) Rules 2020* (Current version), Division 4.3, https://www.legislation.gov.au/Series/F2020L00094. Note that the requirements for consent in relation to joint accounts have arguably proved too onerous, and hindered take up of CDR-B. In response, Australian Treasury issued a consultation paper in May 2021 which includes a proposal to modify the consent requirements for joint accounts (See Section 3).

these conditions make Privacy Safeguard 3, on paper, a much more privacy protective control than Australian Privacy Principle 3.

However, this re-assurance needs to be reviewed in light of the significant weaknesses of the "disclosure and consent" model explained. **(See Section 4.5.1).**

The assumption of consent for collection, which remains valid for 12 months, should be qualified by a condition that it applies only where there is a valid reason for the insurance data to be held by the recipient **(ADR)** which obtains the consent. Some of this data, such as previous claims history and driving history is potentially prejudicial if used out of context, and as the data is increasingly obtained indirectly – for other good reasons, there is a risk that a 12 month consent could be used to justify continual updating of CDR data from a third party source. This was highlighted by the findings of the *Automating General Insurance Disclosure* report (Financial Rights, 2021b). The CDR data collected under a "consent" where a consumer seeks a quote should only be held for the period during which the offer of cover remains open, or, if cover is taken out, for the period of that cover. The related issue of data retention is discussed below. **(See Section 4.7.8).**

There is no equivalent CDR Privacy Safeguard to Australian Privacy Principle 3.5, which requires collection of solicited personal information by lawful and fair means, and favours direct collection from the individual. This gap presumably reflects the very prescriptive rules for the collection of CDR data, and the fact that the CDR regime is expressly designed to facilitate indirect collection and sharing of data. However, the lack of an explicit "fair collection" requirement for CDR data can be seen as a loss of privacy protection, allowing potentially unfair practices, particularly in the context of claims investigation to occur. One obvious area of potential unfairness, including discrimination, arises from the presence in insurance data (at least in the IRS database) of apparently irrelevant data about consumers finances such as banking and credit data. This is found in the empirical study The growing use of automated disclosure again increases the risk of unfair use, including by routinely taking into account irrelevant financial and other potentially prejudicial data (Financial Rights, 2021b).

A7-5 DEALING WITH UNSOLICITED PERSONAL INFORMATION

Australian Privacy Principle 4 in the currently applicable privacy regime

Privacy Safeguard 4 replicates Australian Privacy Principle 4.3, requiring destruction of any CDR data collected "unsolicited" such as inadvertently as per Privacy Safeguard 4(1). But there is no equivalent in Privacy Safeguard 4 to two other requirements of Australian Privacy Principle 4 – determining if the data could have been collected if it had solicited it as per Australian Privacy Principle 4.1), and applying all of the other relevant safeguards to any unsolicited CDR data that does not need to be destroyed as per Australian Privacy Principle 4.3. The reason for this omission is not clear, but can be regarded as lessening privacy protection for CDR data.

Note: The CDR data expressly includes directly or indirectly derived CDR data, with "derived" not defined but having its ordinary meaning. This means that the CDR Rules and Privacy Safeguards do regulate the collection of what we have described in the discussion of the Australian Privacy Principles **(see Section 2)** as inferred information, patching a gap in the *Privacy Act* coverage.

A7-6 USE AND DISCLOSURE

Australian Privacy Principle 6 in the currently applicable privacy regime

Australian Privacy Principle 6 stipulates requirements in relation to the use and disclosure of personal information.

Would CDR-GI increase or reduce the incidence of secondary uses and disclosures?

In the CDR regime as currently implemented for banking, Privacy Safeguards 6 and 7 are substituted for Australian Privacy Principles 6 and 7.

Australian Privacy Principle 6 provides for a wide range of potential primary and secondary uses, whereas the Privacy Safeguards address a much more limited set of circumstances, given the focused purpose of the CDR – to allow the access to and sharing of CDR data.

Privacy Safeguard 6 only allows uses and disclosures that are required or authorised by the CDR Rules, and those required or authorised by or under any other Australian law or court or tribunal order. In the latter case, the same requirement to make a note applies under the equivalent Australian Privacy Principle 6.

It is therefore necessary to review the relevant CDR Rules requiring or authorising use and disclosure of CDR data, and any associated CX Standards, to ascertain if Privacy Safeguard 6 provides the same, more or less privacy protection than Australian Privacy Principle 6.

A key feature of the CDR regime is mandatory data sharing. Once a valid consumer data request is received from an AP, a DH is required[73] to disclose the "required consumer data" to that AP, which on receipt of the data becomes an ADR.

"Required consumer data" for the banking sector (CDR-B) is specified in the CDR Rules at Schedule 3, Clause 3.2 and an equivalent set of specified data is expected for a CDR-GI regime. "Required consumer data" for CDR-B comprises customer data, account data and transaction data as well as product specific data which is not personal. A more detailed description is included in Data Standards issued by the DSB.

"Required consumer data" in a CDR-GI context might include insurance-related data as currently shared in the IRS, such as:

- Policyholder data;
- Policy/product data;
- Disclosure data – required personal information for underwriting purposes disclosed in the process of obtaining the data; and
- Claims history.

It might also extend to insurance enquiries, if sufficient relevance were demonstrated to justify its inclusion.

---

73 There are specified grounds for refusal to disclose, including where the DH "considers this to be necessary to prevent physical or financial harm or abuse" as per *Competition and Consumer (Consumer Data Right) Rules 2020* (Current version), Rule 3.5(1)(a).

Given the major data quality issues with the IRS outlined **(see Section 3)**, it would be important to carefully review what constitutes "required consumer data" in any CDR-GI regime.

In CDR-B, there is also "voluntary consumer data" which is any other data. However, it is not clear in what circumstances this can be requested or disclosed. For example, what role it plays in CDR. Until more detail is provided, the implications of this for CDR-GI cannot be ascertained.

The Rules initially included an obligation that APs "not use CDR data beyond what is reasonably needed in order to provide the requested goods or services" as part of a data minimisation principle in Rule 1.8(b). This provided enhanced privacy protection compared with the relevant parts of Australian Privacy Principle 3. However, this principle was weakened by a 2020 amendment of the Rules and the addition of "...or fulfil the other purpose", being "any other purpose consented to by the CDR consumer"[74].

Although the condition of additional consent may appear to provide a sufficient safeguard, it is subject to all the weaknesses of the "disclosure and consent" model discussed **(see Section 4.5.1)**, including the problem of bundled consent for multiple purposes.

It should be noted there are now five separate categories of consent in the CDR Rules – consent for collection, use, disclosure, direct marketing and de-identification.[75] Many of the recommendations of PIA Update 2 (Maddocks, 2021a) related to the complexity of the consent options in the CDR regime, but the ACCC's response (ACCC, 2021) effectively rejected any simplification.

In any extension of the CDR regime to general insurance, care should be taken to ensure insurers are not able to obtain more personal information than was strictly required for the provision of the services requested, or in the case of claims assessment or investigation, more than was strictly required for the specific claim.[76] Both the specification of "required consumer data" and the provisions for broad "consents" could facilitate fishing expeditions that lead to the collection of too much information.

The Rules expressly prohibit the use of CDR data to identify (or compile insights or build profiles about) third party individuals, unless it is necessary for the provision of a service to the primary CDR consumer in accordance with Rule 7.5(2), and prevent this prohibition being overridden by consent as per Rule 4.12. This appears to be a strong safeguard, although it is not clear in what circumstances an ADR might wish to use CDR data in this way.

A7-7 DIRECT MARKETING

Australian Privacy Principle 7 in the currently applicable privacy regime.

Australian Privacy Principle 7 authorises a range of direct marketing purposes to which personal information can be put.

Privacy Safeguard 7 applies differently to ADRs and DGs. ADRs may use or disclose CDR data for direct marketing only where it is required or authorised by the CDR Rules as per Privacy Safeguard 7(1). DGs (of which there are none yet in CDR-B) may only disclose CDR data for direct marketing

74 *Competition and Consumer (Consumer Data Right) Amendment Rules No 3, 2020* - Schedule 1, Clause 12.

75 *Competition and Consumer (Consumer Data Right) Rules 2020* (Current version), Rule 1.10A.

76 Insurance Council of Australia, *Insurance General Code of Practice* (5 October, 2021), Section 67, https://insurancecouncil.com.au/code-of-practice/.

if that is required by the Rules, but may use or disclose for direct marketing where it is authorised by the Rules as per Privacy Safeguard 7(2). Rule changes in 2020 confirmed that ADRs can disclose CDR data to other APs, and to outsourced service providers for the purposes of direct marketing where this is otherwise permitted.

By comparison with Australian Privacy Principle 7, Privacy Safeguard 7 appears more restrictive. For example, there is no allowance of direct marketing simply on the basis that it would be "reasonably expected" as in Australian Privacy Principle 7.2(b), or where obtaining consent is "impracticable" as in Australian Privacy Principle 7.3(b). Privacy Safeguard 7 appears to require clearer notice of intended direct marketing as well as express consent. Privacy Safeguard 7 also applies to offers for the renewal of existing goods or services, not just new ones. Also, Rule changes in 2020 applied the data minimisation principle in Rule 1.8 to the use of CDR data for direct marketing – there is no such restriction under Australian Privacy Principle 7.

It would be necessary to review the detailed CDR Rules relating to direct marketing, and any associated CX Standards, to ascertain the extent to which Privacy Safeguard 7 provides the same, more or less privacy protection than Australian Privacy Principle 7.

Insurers could be expected to wish to use CDR data for direct marketing of what they see as "related products" such as home contents as related to building insurance, or motor vehicle cover bundled with home and contents. Consideration would need to be given to the relationship of the Privacy Safeguard 7 restrictions to anti-hawking rules[77] and restrictions on deferred sales processes for unsolicited sales.[78] Consent for direct marketing under a CDR-GI regime should not be used to get around the ASIC rules.

A7-8 CROSS-BORDER DISCLOSURE

Australian Privacy Principle 8 in the currently applicable privacy regime

Australian Privacy Principle 8 addresses a subset of disclosure provisions relating to data transferred to other jurisdictions, whether by or within the APP entity or to or by a contractor. Cross-border transfers are subject to additional safeguards.

Would CDR-GI raise any special issues in relation to cross-border disclosure?

In the CDR regime as currently implemented for banking, Privacy Safeguard 8 replaces Australian Privacy Principle 8. An ADR can make a cross-border disclosure to another "accredited person" under the CDR regime, or to other overseas entities where the ADR either:

- Has taken reasonable steps to ensure the recipient does not breach the Privacy Safeguards and that the recipient remains accountable – which we consider is unlikely if they are not an AP; or
- Reasonably believes that the recipient is subject to a law or binding scheme that provides similar protections to the CDR Privacy Safeguards, and can be enforced by a CDR consumer.[79]

---

77 Australian Securities and Investments Commission, *RG 38 The Hawking Prohibition* (Reissued 23 September, 2021), https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-38-the-hawking-prohibition/.

78 Australian Securities and Investments Commission, *RG 275 The Deferred Sales Model for Add-On Insurance* (Reissued 28 July, 2021), https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-275-the-deferred-sales-model-for-add-on-insurance/.

79 Office of the Australian Information Commissioner, *CDR Privacy Safeguard Guidelines, Version 3.0* (June, 2021), https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines, Section 8, including flowchart at 8.19.

Privacy Safeguard 8 also provides a "fallback" protection that in certain circumstances, acts or omissions by the overseas "new recipient" are taken to also be acts or omissions of the disclosing ADR. This is equivalent to the effect of Section 16C of the *Privacy Act*.

On the face of it, Privacy Safeguard 8 appears stricter than Australian Privacy Principle 8, which has a range of exceptions, including the ability for an individual to consent to disclosures that do not meet the normal standard of protection as per Australian Privacy Principle 8.2(b). However, Privacy Safeguard 8 contains an exception for cross-border disclosures which meet conditions specified in the CDR Rules as per Privacy Safeguard 1(f). Therefore, it would be necessary to review any detailed CDR Rules relating to cross-border disclosures, and any associated CX Standards, to ascertain if Privacy Safeguard 8 provides the same, more or less privacy protection than Australian Privacy Principle 8.

An additional complication is that the acts or omissions which breach the Privacy Safeguards, including Privacy Safeguard 8, that take place overseas, are only subject to the safeguards in limited circumstances, including only where an Australian person may suffer disadvantage as in Section 56AO(3) of the *Competition and Consumer Act 2010*. This "harm" test is not included in the *Privacy Act*, and the CDR privacy regime is therefore less protective at least in those narrow circumstances.

Many Australian insurance companies are part of a large multinational groups. The implications of Privacy Safeguard 8 depend on the extent to which insurers currently or prospectively give access to their customer data to their overseas parent or associated companies, and whether just for administrative or IT processes or for more substantive purposes. Also, most reinsurers are international not Australian entities. Further knowledge of industry practices would be necessary to assess these implications.

A7-9 GOVERNMENT RELATED IDENTIFIERS

Australian Privacy Principle 9 in the currently applicable privacy regime

Australian Privacy Principle 9 places some restrictions on the adoption, use and disclosure of government related identifiers.

Would CDR-GI raise any special issues in relation to the use of Government Identifiers?

In the CDR regime as currently implemented for banking, Privacy Safeguard 9 applies to all ADRs, and is in effect a more restrictive version of Australian Privacy Principle 9, limiting the adoption, use and disclosure of government related identifiers[80]. While Privacy Safeguard 9 does not include a range of "exceptions" that appear in Australian Privacy Principle 9.2, it does provide for exceptions in the CDR Rules as well as in other laws, regulations and court and tribunal orders. Therefore, it would be necessary to review any detailed CDR Rules relating to government related identifiers, and any associated CX Standards, to ascertain if Privacy Safeguard 9 provides the same, more or less privacy protection than Australian Privacy Principle 9.

In the insurance context, Privacy Safeguard 9 is most likely to affect the use and disclosure of driver licence numbers. Insurers would need to ensure that their use of licence numbers in motor vehicle

80 This means identifiers assigned by either the federal, state or territory governments.

insurance complies with the apparently narrower conditions of Privacy Safeguard 9 rather than those of the more permissive Australian Privacy Principle 9. Another potential area of application would be in the use of government issued numbers in the criminal justice system, to the extent that insurers need to keep records of criminal histories.

A7-10 DATA QUALITY

Australian Privacy Principle 10 in the currently applicable privacy regime.

Australian Privacy Principle 10 establishes some requirements designed to ensure that personal information is accurate, up-to-date and complete.

Would CDR-GI increase or decrease problems of data quality?

In the CDR regime as currently implemented for banking, Privacy Safeguard 11 imposes some of the data quality obligations from Australian Privacy Principle 10 on DHs as per PS11(1) and on ADRs as in Privacy Safeguard 11(2), but they only apply to the *disclosure* of CDR data, and not to *collection or use*. The quality obligation when disclosing also excludes the Australian Privacy Principle 10.2 requirement for the data to be "relevant". Like Australian Privacy Principle 10, Privacy Safeguard 11 does not include '"not misleading" as a data quality criterion in contrast to the correction obligation under Australian Privacy Principle 13 and Privacy Safeguard 13. Privacy Safeguard 11 also only applies to CDR data when it is being used under the CDR Rules. CDR data may for instance be disclosed under one of the exceptions in Australian Privacy Principle 6, in which case the overlapping quality obligations of Privacy Safeguard 11 do not apply.

Overall, Privacy Safeguard 11 appears to impose fewer data quality obligations than Australian Privacy Principle 10 to CDR data when it is being disclosed under the CDR Rules.

ASIC has recently drawn attention to data quality issues in the insurance sector, suggesting "investing in data, systems and processes" as one of three key actions required to address a current "trust-deficit".[81] Given the low quality of personal data in the general insurance industry, as confirmed by the findings of the empirical research outlined **(See Section 3)**, the relative weakness of Privacy Safeguard 11 would be a matter of great consequence in the event that CDR were to be extended to the general insurance sector.

One obvious way of addressing data quality problems is through the use of standard terms and definitions. This seems to be one area is which the explicit role of data standards in the CDR-B regime is already yielding significant benefits, and could also do so as part of a CDR-GI regime.

The full extent of data quality and correction obligations involves consideration of both Privacy Safeguard 11 and Privacy Safeguard 13.

The meaning of Privacy Safeguard 11(5) is unclear, and the OAIC CDR Privacy Safeguard Guidelines do not assist.

---

81 Australian Securities and Investments Commission, *Speech by Deputy Chair Karen Chester at the 2021 Annual Industry Forum of the Insurance Council of Australia* (13 October, 2021), https://asic.gov.au/about-asic/news-centre/speeches/general-insurers-from-trust-deficit-to-trust-dividend/.

A7-11 SECURITY, RETENTION AND DELETION OF DATA

Australian Privacy Principle 11 in the currently applicable privacy regime

Australian Privacy Principle 11 requires that reasonable steps be taken to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Would CDR-GI change the range and nature of data security concerns?

In the CDR regime as currently implemented for banking, Privacy Safeguard 12 replaces Australian Privacy Principle 11 for ADRs and DGs. The listed security risks are the same, but instead of a general requirement to take reasonable steps to protect the personal information, in this case CDR data, detailed steps are specified in the CDR Rules. Therefore, it would be necessary to review the detailed CDR Rules relating to security of CDR data, and any associated CX Standards, to ascertain if Privacy Safeguard 12 provides the same, more or less privacy protection than Australian Privacy Principle 11.1.

Privacy Safeguard 12(2) is a customised version of Australian Privacy Principle 11.2 requiring all CDR entities including DHs, ADRs, and DGs to take steps to destroy or de-identify redundant CDR data. However, instead of unspecified reasonable steps, the obligation is to take "the steps specified in the CDR Rules". Rule changes in 2020 provided further requirements. It would be necessary to review the detailed CDR Rules relating to redundant data, and any associated CX Standards, to ascertain if Privacy Safeguard 12(2) provides the same, more or less privacy protection than Australian Privacy Principle 11.2.

The definition of "redundant" is clearly critical in terms of its implications for what data is held and for how long. We have already discussed this above under the "Collection of solicited personal information" heading. In any CDR-GI regime, care is needed to ensure industry practices do not permit the justification of permanent routine retention of sensitive insurance related data where it is not strictly necessary in relation to a specific insurance contract.

A7-12 JOINT ACCOUNTS

Would CDR-GI compound, or help to address, the privacy issues arising from joint accounts?

Joint accounts is an issue that has been given extensive consideration in the open banking context (CDR-B). An initial requirement for express consent by both joint account holders to CDR data sharing was regarded by the industry as creating friction that hindered consumer take-up.

Despite strong opposition from consumer groups, amendments were made to the CDR Rules in September 2021 providing "... for joint accounts to be in scope for data sharing under the CDR by default (a pre-approval setting) ..."[82] and requiring joint account holders to opt-out if they object. A joint account holder will be notified when another joint account holder gives consent. These changes take effect on 1 July, 2022.

---

82 *Competition and Consumer (Consumer Data Right) Amendment Rules* (No. 1) 2021.

Despite the requirement for notification, this change is a major reversal of the consent basis of the original CDR scheme. The interests of ADRs have been placed ahead of the privacy interests of CDR consumers who are joint account holders.

Consumer groups fear these changes will heighten the risk of financial abuse in family dispute situations, where insurance is jointly held.

A7-13 SUBJECT ACCESS – OBTAINING DATA ABOUT YOURSELF

Australian Privacy Principle 12 in the currently applicable privacy regime

Australian Privacy Principle 12 requires an organisation that holds personal information about an individual to give the individual access to that information on request.

How might CDR-GI affect the rights and obligations relating to subject access

In the CDR regime as currently implemented for banking, there is no Privacy Safeguard equivalent to the subject access right under Australian Privacy Principle 12. Instead, the ability to obtain your own CDR data is supposed to be a fundamental objective of the CDR legislation and Rules. While this right is included in CDR-B Rules 3.4(3), the commencement of the obligation to set up a "direct request service" to allow a consumer to request some or all of their own CDR data was deferred until 1 November, 2021. However, in September 2021 this deadline was removed and the "direct request" aspect of the regime is now deferred indefinitely "... to allow a future consultation process".[83]

This delay in progressing the "subject access" right in CDR-B appears partly due to legitimate fears that "forced" and/or "diverted" subject access could be used to circumvent the CDR consumer safeguards – including but not exclusively the Privacy Safeguards. A question remain as to why organisations would submit to the complex and onerous requirements of a CDR regime to obtain CDR data to offer a service if they can obtain the same information by asking or requiring the consumer to request it under "subject access" and then supply it to the organisation, without some or all of the CDR Rules and Privacy Safeguards applying.

Notwithstanding these concerns, the indefinite deferral of the direct consumer request provisions leaves a gaping hole in the CDR scheme. The entire scheme now facilitates third party access to shared data, with no apparent balancing right for CDR consumers to directly access and control their own CDR data. The guidance on the relationship of the CDR Privacy Safeguards and the Australian Privacy Principles is ambiguous about the application of Australian Privacy Principle 12 to CDR data. We cannot be confident that there is any subject access right in respect of such data, at least when it is held by APs and ADRs (OAIC 2021, Table at A.27, and paragraph A.33).

In an insurance context, a range of benefits from the confirmation of a right for consumers of subject access" to CDR data have been identified (Financial Rights, 2021b, p 32):

- More easily obtain the information general insurers hold on you and the extent to which your personal information may be shared with other insurance companies, loss assessors, claims agents and insurance reference bureaus;

83 Ibid, Schedule 5, Items 1 and 2, Amending Rules 6.4(3) and 6.6.

- Obtain your information for free rather than paying $22 to the IRS to access the My Insurance Report for the same information;
- More readily identify incorrect information held by insurers;
- Potentially more easily correct any incorrect information held by insurers;
- Identify disclosure information that is missing and update it as appropriate;
- Greater knowledge and control over the information held;
- Increased transparency and confidence in insurance sector information handling; and
- Use the information in a manual rather than automatic way for disclosure purposes with comparison services or another insurer for better quoting and switching.

We note that in its response to the PIA update 4, the Australian Government expressly rejected the need for consideration of "direct to consumer requests" in the energy sector (Australian Treasury, 2021c).

A7-14 CORRECTION OF PERSONAL INFORMATION/DATA

Australian Privacy Principle 13 in the currently applicable privacy regime

Australian Privacy Principle 13 requires an organisation to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading. This is both where an individual requests correction and where the organisation otherwise becomes aware that personal information it holds is incorrect.

How might CDR-GI affect the rights and obligations concerning correction?

In the CDR regime as currently implemented for banking, Privacy Safeguard 13 is substituted for Australian Privacy Principle 13 in respect of correction rights and obligations. It is however a more customised and limited provision. Privacy Safeguard 13(1) requires DHs and Privacy Safeguard 13(2) requires ADRs to respond to specific requests for correction from a CDR consumer. There is no equivalent in Privacy Safeguard 13 to the more general obligation on APP entities under Australian Privacy Principle 11 to make corrections *however* they become aware of data quality problems. This gap is partly filled by Privacy Safeguard 11. There is no equivalent to the provisions of Australian Privacy Principle 13.3 and 13.4 that allow an individual to challenge a refusal to correct. Privacy Safeguard 13 does not appear to allow for refusal to correct.

Overall, the correction rights and obligations under Privacy Safeguard 13, when combined with Privacy Safeguard 11(3) and (4) are broadly equivalent to those under Australian Privacy Principle 13, but arguably with some deficiencies.

The empirical study reported **(see Section 3)** was originally intended to include "testing" of correction rights following the exercise of access rights, but this proved impractical in the timeframe available. However, the poor quality of data revealed by the study reinforces the importance of and need for strong and effective correction provisions.

A7-15 OUTSOURCING

In the current application of privacy law to general insurance, there are multiple issues that relate to the handling of data by third party service providers, which cut across a number of Australian Privacy Principles. These include how to ensure that the same standards apply, and that all obligations of the client are appropriately passed on to the contractor.

Would CDR-GI raise any special issues in relation to outsourcing?

The short answer is yes – outsourcing has been a major topic in CDR-B.

The CDR Rules do at least confirm that any provision of CDR data by an ADR to an outsourced service provider will generally be a disclosure. This contrasts with the confusing situation under the *Privacy Act* where in some circumstances the release of personal information to an outsourced service provider is treated as a "use" (OAIC, 2021). The Rules also require that consumers are expressly notified about any outsourcing.[84] Both the principal (client) and the service provider have to be APs subject to the Privacy Safeguards, although Rules amendments in 2020 allow many of the obligations to remain with the principal, even where the service provider is collecting CDR data directly from consumers.

At first sight, the application of CDR Rules and Privacy Safeguards relating to outsourcing may provide some improvement to the unsatisfactory and ambiguous current situation. However, the prevalence of outsourcing in the general insurance sector – including widespread use in claims investigation and assessment – makes it all the more important that privacy protection for CDR data handled by third party contractors is adequately addressed.

A7-16 SHARING OF CDR DATA OUTSIDE OF THE "PROTECTED" CDR REGIME

A concerning development has been the introduction of provisions for some CDR data to be shared with parties who are not accredited under the CDR regime and are not therefore subject to the CDR Rules or CDR Privacy Safeguards. The PIA Update 2 (Maddocks, 2021a) raised some major concerns which were largely dismissed by the ACCC in its response (ACCC 2021).

These changes were effected by amendments to the CDR Rules in 2021 relating to "CDR insights" and "Trusted Advisers".[85] The Australian Government has given assurances that "insights" are only a very limited subset of CDR data. It is in the interests of CDR consumers that this is more easily shared and that "Trusted Advisers" can only be members of professions which are regulated.

If the CDR regime is extended to general insurance, the position of insurance brokers would be an important issue. It is not clear if they would fall under the definition of "Trusted Adviser" under the CDR Rules – if so this would potentially leave a major gap in privacy protection, as flagged in the PIA Update 2 (Maddocks, 2021a).

A7-17 COMPLAINTS AND ENFORCEMENT

84 *Competition and Consumer (Consumer Data Right) Rules 2020* (Current version), Rule 4.11(3)(f).

85 *Competition and Consumer (Consumer Data Right) Amendment Rules* (No. 1) 2021, Schedule 3.

Attention was drawn to the overlapping roles of the OAIC in relation to *Privacy Act* compliance and AFCA in relation to general insurance Code of Practice breaches (See Section 2). At present, all privacy complaints relating to an Australian Privacy Principle are assessed only against the Australian Privacy Principles in the *Privacy Act*, with OAIC as the relevant external dispute resolution body. The OAIC separately accepts CDR privacy complaints, currently only for CDR-B and assesses them against the CDR Privacy Safeguards[86]. OAIC is also solely responsible for pro-actively[87] monitoring and enforcing compliance by APP entities in insurance with *Privacy Act* obligations – including the Australian Privacy Principles and Data Breach requirements.

In relation to pro-active monitoring and enforcement of the CDR Privacy Safeguards, OAIC shares responsibility with the ACCC, again currently only for CDR-B.

It is not clear how well the OAIC will manage in practice to handle complaints that may involve both CDR data and other personal information – given that CDR-B is only gradually being implemented, there is little practical experience available for assessment.

How might CDR-GI affect privacy complaints and enforcement?

If the current CDR-B regime is extended unchanged to the insurance sector, OAIC would be responsible for both privacy complaint handling and monitoring and enforcement of the CDR Privacy Safeguards as well as the overlapping Australian Privacy Principles as discussed.

The OAIC is chronically under-resourced. Moreover, it has been continually loaded with additional responsibilities without commensurate increases in resources. The agency is likely to be further over-burdened should complaints arising from CDR implementation in multiple sectors be added to its workload.

The ACCC also has a strategic enforcement role where there are repeated or serious breaches of the CDR Rules. The OAIC and the ACCC have a joint Compliance and Enforcement Policy.

Because of OAIC's responsibility for both privacy regimes, the Australian Privacy Principles and mostly, for the CDR Privacy Safeguards, the introduction of CDR-GI would be unlikely to make any significant difference. There may possibly be different outcomes resulting from the relatively minor differences between the CDR Privacy Safeguards and the Australian Privacy Principles.

If responsibility for the CDR Privacy Safeguards was transferred from OAIC to another regulator such as the ACCC which had a different approach to complaint handling or enforcement of compliance, outcomes for consumers might be different.

---

86 Office of the Australian Information Commissioner, *Consumer Data Right Complaints*, (24 August, 2021) **https://www.oaic.gov.au/updates/videos/cdr-complaints**.

87 For example, without a complaint from a specific individual.

Appendix 8: CDR Backgrounder

A8-1 INTRODUCTION

The notion of "Open Insurance" derives from the Australian Government initiative generically referred to as a "Consumer Data Right" **(CDR)**. CDR commenced in financial services, as "open banking" **(CDR-B)**. Some progress has been made in relation to energy **(CDR-E)**, and multiple mentions have been made of it being applicable to telecommunications **(CDR-T)**. This project is concerned with the possibility of the CDR being introduced in general insurance **(CDR-GI)**.

This document was prepared early, as a Backgrounder to assist in the conduct of the project.

The document briefly reviews the history of the "open consumer data" notion. It identifies its key features, based on a brisk assessment of its most advanced form, CDR-B, with an eye to detecting aspects that appear likely to be of greatest relevance to CDR-GI, should it eventuate.

A8-2 ORIGINS OF CDR

Various threads of "open banking" can be detected at an early stage (for example, Fintecsystems, 2019). A direct stimulus for CDR in Australia was the EU Payment Services Directive (PSD2 – EC 2015). PSD2 included new rules aimed at "opening the EU payment market for companies offering consumer or business-oriented payment services based on the access to information about the payment account".

The United Kingdom used PSD2 to spur what they termed "open banking". This was envisaged as making it "easier for consumers to compare the details of current accounts and other banking services, as well as providing information about ATMs and branches", and giving "consumers including small businesses the ability to share their banking information securely with other banks, building societies and regulated companies". The motivation was that "older and larger banks do not have to compete hard enough for customers' business, and smaller and newer banks find it difficult to grow. This means that many people are paying more than they should and are not benefiting from new services. To tackle these problems [CMA is] requiring banks to implement Open Banking by early 2018 …" (CMA 2016, Media Release and slides 5-6) (Manthorpe, 2017, 2018).

In Australia, the groundwork had already been laid. "The Murray [2014], Harper [2016], Coleman [2016], and Finkel inquiries all recommended that Australia develop a right and standards for consumers to access and transfer their information in a useable format" (Australian Treasury, 2019, p 8). These recommendations were sector specific. At the end of the first quarter of 2017, a Productivity Commission report on "Data Availability and Use" (Productivity Commission, 2017) took the economic arguments further and proposed their generic application. The Productivity Commission's view of privacy issues is evident in its statement that:

> *"Despite claims of a few privacy advocate groups, this Inquiry has not been presented with evidence to suggest widespread concern about the provision of personal information to governments." (p 11)*

A8-3 CDR-B IN AUSTRALIA 2017-2020

The initiative began in July 2017, with the Treasurer asking his Department for a report on an open banking model for Australia, completed in December (Australian Treasury, 2017). The Australian Government agreed to the recommendations on 9 May, 2018. An accessible summary, current at December 2018, is in Treasury (2018). This covers the general obligations, the relevant parties, data-sets, accreditation, the register, Privacy Safeguards and functions of the DSB.

CDR legislation was passed by the Australian Parliament in August 2019. The term Consumer Data Right refers to core enabling features of open banking – and of applications in further sectors later (Australian Treasury 2019). The Australian Bankers Association stated that:

> *"Open banking gives you the ability to share your banking data with third parties that have been accredited by the ACCC. This will allow you to get better-suited banking products and switch products or banks more easily" (ABA, 2021).*

However, the proposition was not completely dominated by economic considerations, primarily because consumer concerns were anticipated. The following statement is in Treasury (Australian Treasury, 2019, p 5):

> *"Privacy and security are core features of the consumer Data Right. To protect the privacy of consumers, privacy protections will be strengthened and tailored to adequately reflect the needs of the consumer Data Right and each sector.*
>
> *These privacy protections will include:*
>
> - *Requirements that data can only be transferred under the consumer Data Right at the direction of the consumer*
> - *Requirements for greater transparency and choice so that consumers control how their information will be used*
> - *The mandatory accreditation of data recipients*
> - *Obligations regarding deletion or de-identification of data*
> - *The introduction of transfer, security and data standards via a newly created Data Standards Body (initially hosted by Data61)*
> - *Extension of Privacy Act 1988 protections to bind all accredited data recipients, including small to medium sized enterprises*
> - *A strong role for the OAIC in advising on and enforcing privacy protections*
> - *A range of avenues for consumers to seek meaningful remedies for breaches, including external dispute resolution and direct rights of action."*

Privacy Impact Assessment **(PIA)** reports were provided by (Maddocks 2019, 2020a, 2020b, totalling more than 350 pages). They drew to the attention of both the Australian Treasury and ACCC the need not only for a great many specific safeguards, but also for repeated reevaluations and upgrades of safeguards to reflect the rapid change that CDR-B has been and continues to be undergoing.

They also emphasised the complexity of the legislative framework, and the likelihood that all participants will have difficulties understanding their rights and obligations. Although some of the recommendations have subsequently been addressed, others have not been, resulting in significant risks confronting consumers, despite the high sensitivity of much of the data.

A8-4 STATUS OF CDR-B IN AUSTRALIA IN 1Q 2021

Consumer data sharing in CDR-B was intended to become operational in three phases. For the "big four" banks, the deadlines were scheduled for mid-2020, late 2020 and early 2021 respectively, with deadlines for the other approximately 100 Authorised Deposit-Taking Institutions **(ADIs)** each about a year later (CDR 2020b) – see Figure A8-1:

- Phase 1 –All mainstream transaction and deposit accounts
- Phase 2 – Loan-related accounts
- Phase 3 – Remaining categories of consumer accounts

At launch on 1 July 2020, it was intended that customers of the big four banks could request transmission of a copy of their transaction account, deposit account, credit card and debit card data to an ADR. This term is defined to mean a financial services provider – specifically an unrestricted ADI – that has satisfied the CDR registration requirements. See (CDR, 2020b).

In practice, however, ADRs have been slow to emerge. Industry participants are understood to lay much of the blame on the restrictive rules that arise from the consumer safeguards. These exist because they were deemed necessary in order to earn consumer trust. Demonstrated compliance with the substantial regulatory regime provides assurance to potential consumer users of CDR that the initiative was intended to serve their interests, is of benefit to them, and is worth the effort required.

Another key factor underlying the implementation delays is the sheer complexity of the undertaking. A substantial raft of technology needed to be conceived, designed, negotiated among stakeholders, coded, tested, piloted and launched. The suggestion has also been made that agile neo-banks and FinTechs see better prospects elsewhere.

During late 2020 and early 2021, changes were made to the scheme to permit ADRs to act on behalf of other ADRs (ACCC 2020). In addition, outsourced service providers which provide IT infrastructure, software and services to financial services providers, do not have to be ADRs.

A further step, taken on 28 February, 2021, was the transfer of the CDR rule-making power and responsibility for designation of additional CDR sectors from the ACCC to the Financial Services Minister, and Australian Treasury. However, the ACCC remains the lead regulator for the CDR (ACCC, 2021), responsible for:

- Accrediting entities to receive data;
- Managing an online register of ADRs and DHs;
- Providing education and guidance on the CDR;
- Recommending to government future sectors to be brought within the CDR; and
- Compliance and enforcement activities (other than in relation to the CDR Privacy Safeguards, which are the responsibility of the OAIC).

Future development of Open Banking (CDR-B)

Consultation is under way on a proposal for professional advisors to receive consumer data through CDR systems, subject to consumer consent, without the need for those advisors to become ADRs.

A "Future Directions" review in late 2020 proposed some further steps (Australian Treasury, 2020). These included the enablement of agents for individual consumers (ACCC, 2020), and additional set-and-forget payment consents by consumers. It is also envisaged that greater powers will be delegated to some agencies and the Minister. Some weakening of accreditation standards is proposed for lower-risk activities. It appears that representatives of ADRs can have a weaker form of accreditation than ADRs themselves. Leakage of CDR data to non-accredited parties is also now intended, at least in the case of "low risk services for public benefit" and "insights data derived from CDR data". For these changes to take effect, it would appear that further amendments to legislation, Rules and standards may be required.

A8-5 EXTENSION OF CDR

It is envisaged that CDR is replicable in other industry sectors, and that ADRs may disclose "equivalent data" on to other ADRs, both within and beyond the banking sector. The energy sector has already been formally designated under the CDR legislation, and work has already commenced on drafting Rules and standards for CDR-E. Telecommunications has been officially nominated as the next sector for the CDR.

There also appears to be an attempt to extend the range of consumer data beyond that which has been designated to date. This includes consumer "consent and authorisation data".

A8-6 CONSUMER SAFEGUARDS

The CDR scheme includes features expressed in legislation and delegated legislation that are significantly more protective of consumers' privacy interests than the *Privacy Act* and Australian Privacy Principles. A useful summary of consumer safeguards is in (Australian Treasury 2020, pp 147-180, esp. privacy on pp 175-180), including the 3-page table extracted below (pp 150-151) – see Figure A8-2. See also (OAIC, 2020). These safeguards may, however, be now under threat.

Consumer concerns about CDR

Consumer and privacy advocates have, through a long series of consultation processes, submitted substantial, detailed critiques of the CDR proposition, design and safeguards. Some aspects of these submissions have been reflected in the legislation, rules and standards as they were in the third quarter of 2020.

However, advocates have many outstanding concerns about such aspects as the practicality of consent, data minimisation, the potential abuse of cross-sectoral data as CDR is extended, and sensitive data (see 'Issues' below).

Moreover, there is a complex and confusing overlap between the 13 CDR Privacy Safeguards on the one hand, and the 13 Australian Privacy Principles, on the other. (The OAIC's Guidelines run to 200 pages). OAIC has the lead role in handling privacy related CDR complaints, but the interface between the OAIC and ACCC responsibilities will only become clear once the CDR-B regime starts to operate on a significant scale.

From the scheme's design and the framing of some of the "Future Directions" Recommendations (Australian Treasury 2020), the question arises as to whether and how consumers would be able to seek enforcement action and remedies where breaches occur, what degree of delay they may suffer, and what degree of success they may have. A right to complain through internal dispute resolution and external dispute resolution mechanisms is far less than a right of action, and there appears to be no means for a consumer, or a consumer advocacy organisation, or a class action, to force the hand of a regulatory agency to act.

For example, CDR describes compliance and enforcement actions, but "does not discuss how the OAIC will apply its complaint handling powers or the process for making a CDR consumer complaint" (CDR, 2020a, p 2). It is unclear to what extent AFCA will perform external dispute resolution functions. The "CDR Regulatory Action Policy" (OAIC, 2020) makes it apparent that the channel available to a consumer may be a complaint firstly to the relevant company, and then to OAIC under Section 36 of the *Privacy Act*. The OAIC Section 36 complaint process includes a great many hurdles. OAIC has always claimed to be under-resourced even in relation to its many existing responsibilities, and the process is commonly protracted. The OAIC does not have a strong record of finding in favour of complainants. And the OAIC has a very limited record of making section 52 determinations as a result of Section 36 complaints – which is a necessary condition for an appeal against the OAIC's findings.

Further, given the many instances in which the "Future Directions" report found it necessary to recommend that consultation be undertaken, it may be that consultation with consumer advocacy organisations is not baked into CDR processes, but depends on fresh invitations each round.

Business concerns about CDR-B

The banking sector, at least that large part of it that comprises the big four banks, has concerns about the design of the CDR regime, including:

- Conflict with existing statutory obligations under e.g. banking law, AML/CTF, Privacy Act;
- Conflicts with existing complaints regimes for banking (AFCA, OAIC) and for other sectors, if and when cross sectoral CDR data emerges (ACCC, Energy Ombudsmen, TIO, OAIC);
- Unreasonable assumptions about new participants being able to achieve banking-level data security standards; and
- Leakage of banking data to non-ADRs.

While some of these concerns are shared by consumer advocates, resistance to CDR by dominant incumbent businesses can be expected in any sector in which CDR is introduced, given that CDR is expressly designed to increase competition and encourage new entrants to established markets.

Consent templates

An approach that may assist consumers to deal with the complexity is the creation of template consent choices for particular categories of consumers, with defaults pre-set to reflect their likely preferences, identified through consultation with consumer advocates. Note that Recommendation 6-20 in (Australian Treasury, 2020) envisages something like consent templates:

> *"Industry and consumer groups should be encouraged to develop and endorse standard wording for consumer Data Right consents for specific purposes, and accredited persons should be permitted to display these endorsements in their consent processes through icons, descriptions, links or other appropriate methods."*

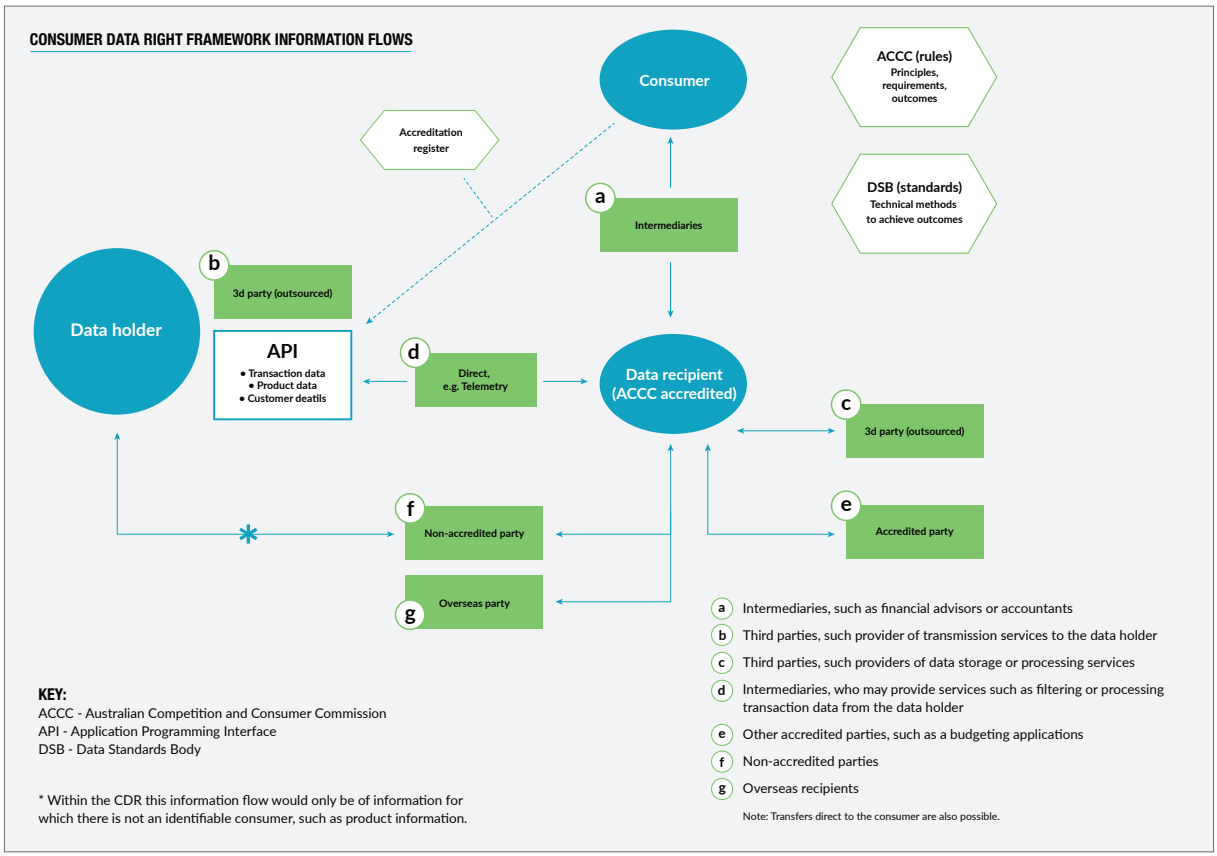
A8-7 SOME KEY ISSUES ARISING IN CDR-B

- The consent process has enormous complexity (DSB, 2020, pp 32-114) and comprises 3 phases: Consent (to a request from an ADR), Authenticate (connect to a DH), and Authorise (confirm sharing of CDR data from DH to ADR). The consent process has been designed and emphasised as a source of trust, but may also act as a barrier to use of CDR because of its complexity.
- Consumers are expected to enter into and understand an entire new ecosystem and process to take advantage of CDR, separate from their existing relationship with a DH, for example a bank in CDR-B). This raises the question as to how realistic it is to expect significant uptake.
- Consumer access to their own data – a declared objective of CDR – has not yet been implemented or even designed, partly because the risk exists of providers stepping around the safeguards by demanding consumers acquire their own copy of the data and provide that to requesting business or outsourced provider. Consumers are consequently dependent at least for now on the weak, highly qualified Privacy Act right of subject access (Australian Privacy Principle 12), which can also involve a fee (at the discretion of the entity).
- The subject access right in the CDR scheme is restricted to DHs, so that once CDR data reaches an ADR or any outsourced provider, or the proposed intermediaries, consumers are entirely dependent on the *Privacy Act* provisions, with all the exemptions, exceptions and bureaucracy they entail.
- There are ongoing fundamental and entrenched information asymmetries, resulting in power asymmetry between consumers and participating businesses, and potential use of CDR in the interests of businesses rather than of consumers.
- Strict sector-specific security standards, particular in banking, cease to apply to personal data disclosed to CDR participants (CDR data).
- The possibility exists of CDR data being applied by ADRs to secondary uses. (For example, the DSB process documents provide for opt-in for marketing).
- Data leakage, and consumer confusion, may arise from the provision in the design of the ecosystem for ADR and DH "brands" separate from the legal ADR and DH entities themselves. This is not only difficult to explain to consumers, but it also creates great difficulty in unambiguously assigning legal liability for compliance with CDR Rules and Standards.
- The possibility exists of third party access to and use of CDR data by non-accredited entities, with lesser or even no regulation or consumer protections.
- There appears to be a strong possibility of the use of pseudo-de-identification as a means of avoiding CDR controls and safeguards. For example, by removing explicit

identifiers, ADRs might claim they can release rich, multi-column data-records to non-accredited domestic or overseas parties (as allowed under the CDR Rules on condition of de-identification). Such data-sets harbour strong potential for re-identification by matching with other data.

- There is a potential for the emergence or enhancement of one or more sectoral databases, perhaps centralised, or perhaps virtual. This is already evident in the energy sector in the form of the AEMO meter database). Alternatively a CDR project could be used as a means of legitimising existing and dubiously legal operations. Such schemes may, under some circumstances have advantages for consumers as well as for business enterprises; but there appears to be no coherent analysis, design or discussion in relation to either the principles, or the specific instance of the potentially extraordinarily intrusive AEMO database.
- These schemes harbour great potential for the initial imposition of improved safeguards, followed by the ratchetting back of privacy protections to the Privacy Act Australian Privacy Principles - with their enormous and now engrained inadequacies.
- Risks arise in relation to joint accounts for adults as well, in particular in relation to financial abuse between life-partners.
- Although accounts for which any account-holder is under 18 are currently excluded from the CDR, the risk exists of that safeguard being whittled away.
- Risks exist of CDR data being used for the exploitation of vulnerable consumers.
- A high degree of risk exists of CDR data being used for unreasonably discriminatory conduct, both based on the data itself, or where a consumer declines to provide a consent, or qualifies their consent.

Figure A8-1: Phasing of CDR-B (from CDR 2020)



This model may require updating to reflect recent changes, because the entity-set and the flows continue to be expanded, and adjustments to be made to the conditions applying to particular flows.

The key categories DH and ADR may have separate “brand entities” for CDR purposes.

The Data Standards Chair declares designated data-sets – for particular classes of data, account-types, transaction-types, consents – with technical specs developed and issued by the DSB.

DSB issues detailed CX specifications, such as user-interface layouts and processes (DSB, 2020)

Consumer dashboards, to enable consumers to manage their consents, are required to be provided by ADRs (consent management dashboard) and by DHs (authorisation management dashboard) – see guidance in DSB, 2021). (However, dashboards provide access only to meta-data, not to the transferred CDR data itself.

Figure A8-2: Extract from Australian Treasury (2020), pp 149-151

Obligation	Overview of requirements	Source of obligation
Transparency and reports to regulators	ADRs must maintain consent dashboards and CDR policies. ADRs' twice yearly reports to the ACCC and OAIC are required to include a summary of CDR complaint data	Section 56ED – Privacy Safeguard 1, Rules 1.14 and 9.4
CDR consent receipts and record keeping	Accredited persons must give the consumer a CDR receipt as soon as practicable after the consumer gives, or withdraws, a consent. ADRs must keep records, including records and explanations of consents given by consumers	Rules 4.18 and 9.3
Ongoing notification for consents	If 90 days have elapsed since a consumer last consented, used their dashboard or was notified, the accredited person must notify the consumer	Rule 4.20
Reporting to consumer	Rules can enable a CDR consumer to direct an ADR to give reports about their valid requests, and any disclosures made in response	Section 56BI
Obligations applying to data holders		
Data holder to seek authorisation to disclose	Data holders must ask consumers to authorise disclosure of requested CDR data, and to disclose required CDR data where authorised to do so	Section 56BC, Rules 4.5 and 4.6
Eligibility	Where there is no existing authorisation, a data holder is only required to seek authorisation where they reasonably believe the request is made by an accredited person on behalf of an eligible consumer[244]	Rule 4.5
Withdrawal of authorisation and record keeping	Consumers can withdraw authorisation at any time. Authorisations expire after 12 months unless renewed. Data holders must keep records, including records and explanations of authorisations given by consumers	Rules 4.25, 4.26 and 9.3
Accuracy of data	Data holders authorised to disclose must take reasonable steps to ensure data is, having regard to the purpose for which it is held, accurate, up to date and complete[245]	Section 56EM – Privacy Safeguard 11
Notification of disclosure	Data holders must take specified steps to notify CDR consumers of disclosure of CDR data[246]	Section 56EM – Privacy Safeguard 10, Rule 7.9

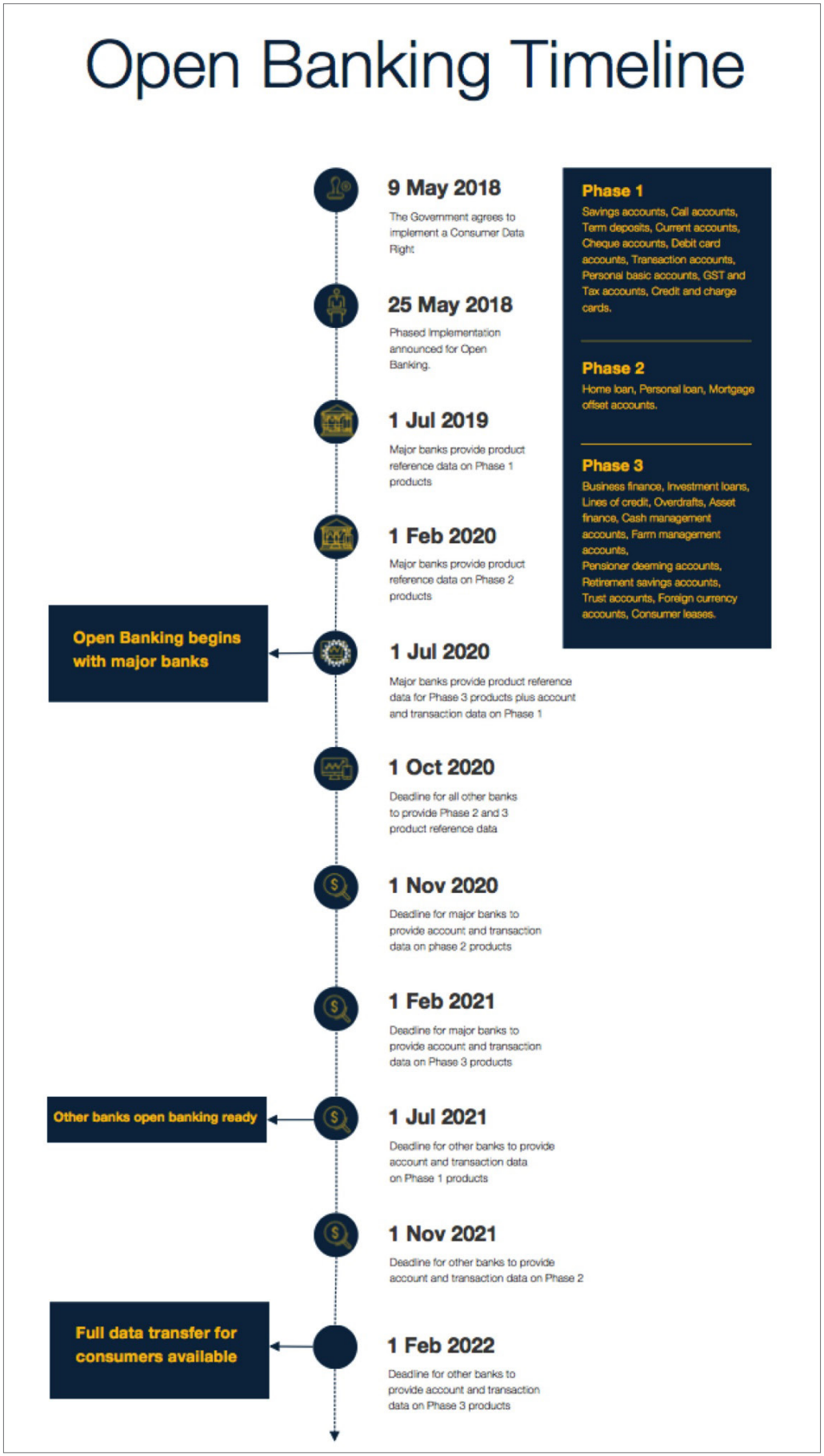
Obligation	Overview of requirements	Source of obligation
Permitted refusal to disclose	Data holders can refuse to seek authorisation for or disclose CDR data in some circumstances, including to prevent physical or financial harm or abuse	Rules 3.5 and 4.7
Transparency and reports to regulators	Data holders are required to maintain consent dashboards and CDR policies. Data holders' twice yearly reports to the ACCC and OAIC are required to include a summary of CDR complaint data	Section 56ED – Privacy Safeguard 1, Rules 1.15 and 9.4
Reporting to consumer	Rules can enable a CDR consumer to direct a data holder to give reports about the consumer's valid requests, and any disclosures made in response	Section 56BI
Specific conduct prohibitions		
Holding-out	A person must not hold out that they are accredited if they are not	Sections 56CC and 56CD
Misleading and deceptive conduct	A person must not mislead another person into believing that a person is a CDR consumer, is making a valid request or consent, or satisfies other disclosure criteria	Sections 56BN and 56BO
Avenues for redress		
Range of remedies	Remedies include suspension or revocation of accreditation, injunctions for breach of the CCA or Rules, infringement notices, substantial civil penalties,[247] and fines for offences.	Various
Internal and external dispute resolution (EDR)	ADRs and data holders must meet internal dispute resolution requirements and be a member of a recognised EDR scheme for consumer complaints	Rules 5.12, 6.1 and 6.2
Direct rights of action	Consumers can take action to recover loss or damage arising from a contravention of the privacy safeguards or Rules relating to privacy or confidentiality of CDR data, certain CCA CDR prohibitions, or a contravention of a civil penalty provision of the Rules. Actions on behalf of consumers are also supported.	Sections 56EY, 82 and 87

Figure A8-3: Extract from Australian Treasury (2019, pp 149-151)

Table 7.1: Key existing consumer protections under the CDR regime

Obligation	Overview of requirements	Source of obligation
Requirements on accredited persons, ADRs, or those seeking accreditation		
Accreditation is mandatory	To have CDR consumer data disclosed to them, third parties must be accredited[240]	Sections 56BC and 56BD
Accreditation criteria	Accredited persons must meet requirements regarding insurance, being a fit and proper person, information security, internal and external dispute resolution, and comply with any conditions imposed	Sections 56BH and 56CA, Rules[241] – Parts 5 and 7, Schedules 2 and 3
Consent to request CDR data	Accredited persons must have consumer consent to request CDR consumer data. Consent should be voluntary, express, informed, specific as to purpose, time limited and easily withdrawn. Accredited persons must ask for consent in compliance with the Rules	Section 56EF – Privacy Safeguard 3, Rules – Part 4
Data minimisation principle	Accredited persons may only collect and use CDR consumer data reasonably needed to provide the requested good or service	Rules 4.4 and 4.12
Protection of CDR data	ADRs must take specified steps to protect CDR data from misuse, interference, loss, and unauthorized access, modification or disclosure	Section 56EO – Privacy Safeguard 12
Notification of disclosure	ADRs are to take steps specified in the Rules to notify consumers of disclosure of CDR consumer data	Section 56EM – Privacy Safeguard 10
Deletion or de-identification	Consumers can request deletion of CDR data[242]	Section 56BAA
	ADRs must destroy or, with the consumer's consent, de-identify redundant data. Data becomes redundant when use permissions expire[243]	Section 56EO – Privacy Safeguard 12
Use and disclosure restrictions	CDR consumer data cannot be used for direct marketing except as authorised by the Rules	Section 56EJ – Privacy Safeguard 7, Rules 4.11, 7.5 and 7.6
	Consent cannot be requested to on-sell CDR data (unless de-identified) or to use CDR data to identify, compile insights or profile another identifiable person	Rule 4.12

Figure A8-4: Open Banking Timeline (Extract from ABA (2021))



Appendix 9: Glossary

ACCC – Australian Competition and Consumer Commission

ACL – Australian Consumer Law

Accreditation Register – the register required under s.56CE(1) of the *CDR Act*

ADI – Authorised Deposit-Taking Institution under the Banking Act, administered by APRA

ADR – Accredited Data Recipient – defined (in an obscure manner) in s.56AK of the *CDR Act*

AFCA – Australian Financial Complaints Authority, which operates EDR for General Insurance

AFSL – Australian Financial Services Licence

ALRC – Australian Law Reform Commission

AP – Accredited Person under s.56CA(1) of the *CDR Act*

API – Application Programming Interface – Software, including data-structures, designed for use in interacting with other software

APPs – Australian Privacy Principles, expressed in the *Privacy Act*

APP entity – An agency or organisation subject to the Australian Privacy Principles as defined under the *Privacy Act 1988*

APRA – Australian Prudential Regulation Authority

ASIC – Australian Securities and Investments Commission

ASIC Act – *Australian Securities and Investments Commission Act 2001*

CCA – *Competition and Consumer Act 2010*

CDR – Consumer Data Right

CDR-B – Consumer Data Right applied to Banking. Also 'Open Banking'

CDR-E – Consumer Data Right applied to Energy.

CDR-GI – Consumer Data Right applied to General Insurance. Also 'Open Insurance'

CDR-T – Consumer Data Right applied to Telecommunications

CDR Act – *Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth)*, which inserted a new Part IVD into the *Competition and Consumer Act 2010 (Cth)*

CDR Consumer(s) – See the highly complex definition in s.56AI(3) of the *CDR Act*

CDR Data – includes not only data within a class specified in the designation instrument for the particular industry sector, but also data derived wholly or partly from that data. See the highly complex definition in s.56AI(1) of the *CDR Act*

CDR Entity – includes a DH, an ADR and a DG, as per s.56ED(1) of the *CDR Act*

CDR Participant – s.56AL(1) of the *CDR Act*

CDR Policy –a policy a CDR entity must have and maintain under s.56ED(3) of the *CDR Act*

CDR Register – a register of Accredited Data Recipients (ADRs) and Data Holders (DHs)

Code Participant – a general insurance industry participant that is a signatory to the General Insurance Code of Practice.

Consumer Dashboard – an online service that allows a consumer to manage and view details about consents they have provided

Corporations Act – *Corporations Act 2001*

CX – Consumer Experience, referring to user interface layout, appearance and processes

Designation – A legislative instrument creating consumer rights in relation to access to and transfer of a class of data within a specific sector

DG – Designated Gateway under s.56AL(2) of the *CDR Act*

DH – Data Holder – an organisation that holds data, and supplies it at the request of the ADR. See s.56AJ of the CDR Act

DSB – Data Standards Body under s.56FJ(1) of the *CDR Act*, responsible for the development of common technical standards for CDR

DSC – Data Standards Chair, the authority for CDR Data Standards, responsible for the DSB

EDR – External dispute resolution

GDPR – EU General Data Protection Regulation 2016/679.

GI – General Insurance

GICoP – General Insurance Code of Practice, versions of 2014 and 2020, administered by AFCA

GSP - Gateway Service Provider

IC Act – *Insurance Contracts Act 1984*

IC Act Code Review 2017 – Insurance Council of Australia, Interim Report, Review of the General Insurance Code of Practice, November 2017

ICA – Insurance Council of Australia

IDR – Internal dispute resolution

IEC – Insurance Enquiries and Complaints Scheme, which previously operated the external dispute resolution scheme for general insurance, with the role subsequently transferred to AFCA

IFBA – Insurance Fraud Bureau of Australia, the GI industry fraud investigative service

ILS – Insurance Law Service of the Financial Rights Legal Centre

IRS – Insurance Reference Service, the general insurance industry bureau for sharing claims data and insurance cover enquiries and maintaining a lengthy history

OAIC – Office of the Australian Information Commissioner

PC – Productivity Commission

PDS – Product Disclosure Statement

PIA – Privacy Impact Assessment

Privacy Safeguards (PSs) – provisions of Division 5B to 5F of Part IVD of the *CDR Act*

PSD2 – EU Payment Services Directive 2

RAAP – Register and Accreditation Application Platform – IT supporting the CDR

T&Cs – T&Cs, documents published by insurers containing the fine-print underlying insurance policies

UCT – Unfair Contracts Terms

About us and acknowledgements

ACKNOWLEDGEMENT OF COUNTRY

The Financial Rights Legal Centre acknowledges Aboriginal and Torres Strait Islander people as the traditional custodians of this land where we live, learn and work and pays respect to their Elders, past, present and future.

ABOUT FINANCIAL RIGHTS LEGAL CENTRE

The Financial Rights Legal Centre is a community legal centre that specialises in helping consumers understand and enforce their financial rights, especially low income and otherwise marginalised or vulnerable consumers.

We provide free and independent financial counselling, legal advice and representation to individuals about a broad range of financial issues.

Financial Rights is one of the services operating the National Debt Helpline, which helps consumers experiencing financial difficulties. We also operate the Insurance Law Service which provides advice nationally to consumers about insurance claims and debts to insurers, and the Mob Strong Debt Help services which assist Aboriginal and Torres Strait Islander Peoples with credit, debt and insurance matters.

National Debt Helpline: 1800 007 007
Insurance Law Service: **1300 663 464**
Mob Strong Debt Help: 1800 808 488

Monday - Friday | 9.30am - 4.30pm

ecstra

Ecstra Foundation is a grant making charitable organisation committed to building the financial wellbeing of all Australians within a fair financial system.

Money matters. Ecstra is assisting Australians with resources and support to help them talk about money, to navigate through this crisis and to build future financial security.

We inform and support consumers, we engage with organisations across all sectors, we make grants to organisations to support and strengthen communities and we research, measure and evaluate outcomes to grow the evidence base of what works.

We also support community organisations on the financial frontline - those delivering direct support to Australians in financial need, but also those ensuring appropriate consumer protection frameworks and community knowledge of consumer rights and redress are available.

Ecstra works as part of the National Financial Capability Strategy led by the Australian Securities and Investments Commission (ASIC). Our initial funding, provided through the Community Benefit Payments scheme, means we will always place consumers at the centre of our work.

XAMAX Consultancy

Xamax provides leading-edge advice to corporations and government agencies regarding the strategic and policy impacts of disruptive information technologies.

Where appropriate to the client's needs, Xamax teams with a small number of other leading consultancies, in order to bring together the necessary resources and expertise. It acts as prime contractor or adopts a co-consultant role, depending on the nature of the assignment.

ABOUT THE AUTHORS

Roger Clarke

Roger Clarke is a consultant on strategic and policy aspects of advanced information technologies, including data security, identity and identification, nymity and de-identification. His consultancy CV is at http://xamax.com.au/Principal.html.

He has Honours and Masters degrees from UNSW and a PhD from the ANU. He is a Fellow of the Australian Computer Society and of the international Association for Information Systems. He has held Visiting Professorships at the Universities of Bern, Linz and Hong Kong, and continues at the ANU and UNSW.

In the privacy arena, he has conducted consultancy, research, doctoral supervision and advocacy since the mid-1970s, and has published well over 100 papers, PrePrints at http://rogerclarke.com/, citation-count at https://scholar.google.com.au/citations?user=V3s6CWYAAAAJ&hl=en&oi=ao

Nigel Waters

Nigel Waters has undertaken work on privacy matters for government agencies and businesses in Australia and overseas since 1997 – until 2019 as Principal of Pacific Privacy Consulting

He was deputy Australian Federal Privacy Commissioner from 1989-1997, and before that Assistant UK Data Protection Registrar.

Nigel is public officer of the Australian Privacy Foundation (**www.privacy.org.au**) (and Board member 1997-2013) and has represented Privacy International (**www.privacyinternational.org**) in international l fora.

Nigel holds Masters degrees from the Universities of Cambridge and Pennsylvania and from the University of Technology, Sydney.

Financial Rights
LEGAL CENTRE

Financial Rights Legal Centre
Tel (02) 8204 1386
PO Box 538
Surry Hills NSW 2010

financialrights.org.au