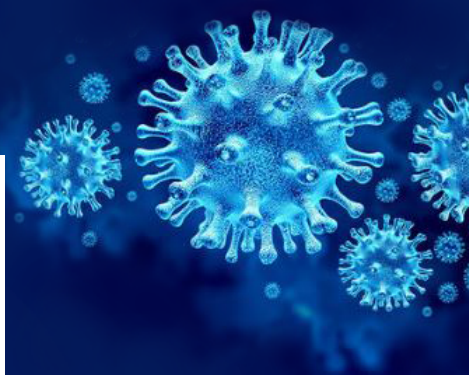
PRIVACY UPDATE

Privacy Awareness Week

This year Privacy Awareness Week (PAW) will be held from 3– 9 May. The theme is 'Make privacy a priority'. AGS has signed up as a PAW supporter. Signing up as a PAW supporter and distributing PAW materials is one way agencies and Privacy Champions can seek to meet their obligations under s 11(4) of the Australian Government Agencies Code to promote a culture of privacy that values and protects personal information.

To coincide with PAW, AGS is running a full day FOI and Privacy Forum. This forum is held once every 2 years and includes a mix of significant and contemporary topics in information law. For more information see here.



Privacy and COVID-19 vaccinations

The OAIC has released guidance for entities on privacy obligations in relation to COVID-19 vaccination information. The guidance emphasises that:

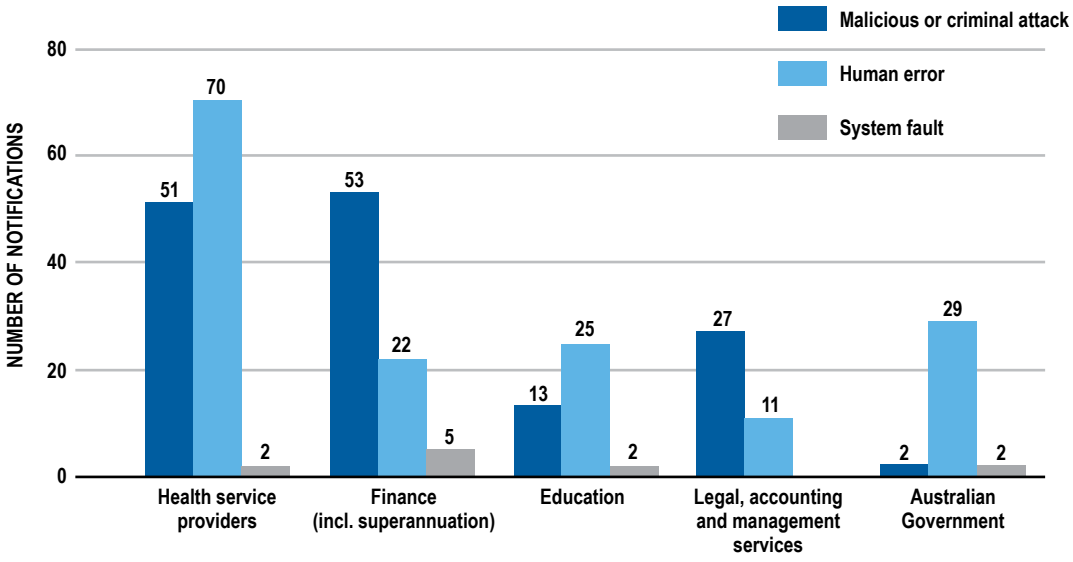
- the collection of vaccination information should only occur in very limited circumstances
- only the minimum amount of personal information that is reasonably necessary to maintain a safe workplace should be collected
- agencies must only collect vaccination information about employees with consent and where the collection is reasonably necessary for the agency's functions and activities, unless an exception applies.

Depending on the circumstances, collection may be authorised under the *Workplace Health and Safety Act 2011* (see *AIT18 v Australian Information Commissioner* (2018) 267 FCR 93, which AGS has summarised here). If your agency does collect vaccination information, you must tell your staff the type of personal information collected and how it will be handled. Consent must be current and informed.

Notifiable Data Breach report
JULY–DECEMBER 2020

Australian government agencies featured in the NDB report for the first time as one of the top 5 industry sectors reporting data breaches to the OAIC, notifying 6% of all breaches (33 in total). Only 58% of notifications from the Australian government were made to the OAIC within 30 days of the entity becoming aware of the incident.

Source of data breaches – Top 5 industry sectors



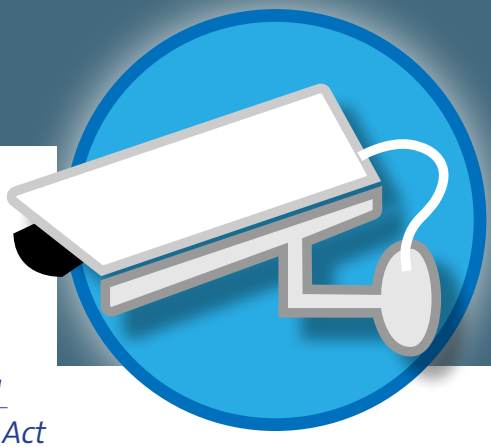
Human error was the cause of 29 out of 33 Australian government entity data breaches. The Commissioner was unable to draw a direct link between the breaches and changed business and information handling practices as a result of the Covid-19 pandemic.

Now that the scheme has been in operation for three years, the Commissioner has indicated raised expectations, including the need to be proactive in preventing data breaches, have systems to detect and respond to data breaches, and have timely responses and appropriate notifications. In one example, an entity was asked to update their notification to clarify that the 'unintended recipient' of personal information was in fact a malicious actor.

AGS has recently developed operating procedures and fact sheets for a number of agencies to assist staff to prevent and respond to some of the most common types of data breaches, drawing on our experience advising agencies as well as guidance prepared by OAIC and ACSC. We can assist you to develop a resource tailored for your agency.

Office of the Australian Information Commissioner website
— www.oaic.gov.au

Review of the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*



The *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* will amend the *Surveillance Devices Act 2004*, the *Crimes Act 1914* and associated legislation to introduce new law enforcement powers and warrants to enhance the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission's (ACIC's) ability to combat cyber-enabled serious and organised crime, including online child exploitation.

The Bill introduces:

- a data disruption warrant which enables AFP and the ACIC to access data on one or more computers and perform disruption activities for the purpose of frustrating the commission of criminal activity
- a network activity warrant to enable AFP and the ACIC to collect intelligence on criminal networks operating online
- an account takeover warrant to allow AFP and ACIC to take over a person's online account for the purposes of gathering evidence of criminal activity
- minor amendments to the controlled operations regime, to ensure controlled operations can be conducted effectively in the online environment.

The Bill gives the Inspector-General of Intelligence and Security (IGIS) oversight of these powers. The Bill amends the *Privacy Act 1988* and the *Australian Information Commissioner Act 2010* to allow the transfer of complaints, and associated information, to the IGIS that are more appropriately dealt with by the IGIS.

The Bill review was referred to the Parliamentary Joint Committee on Intelligence and Security by the Hon Peter Dutton MP, Minister for Home Affairs on 8 December 2020.

Consumer Data Right expansion

The ACCC recently introduced the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* (the Amended Rules), with the consent of the Treasurer. This followed consultation with a broad range of stakeholders.

These changes are intended to expand the Consumer Data Right Rules (the Rules) to allow greater participation in the Consumer Data Right.

The amended rules:

- expand the type of consumers who can use Consumer Data Right (CDR)
- permit accredited data recipients (ADRs), with the consumer's informed consent, to collect CDR data from, and disclose CDR data to, other ADRs who are also providing goods or services to the consumer
- allow ADRs who collect CDR data with consent to also seek the consumer's consent to de-identify some or all of the data to be used for general research purposes (subject to limitations, including de-identification in accordance with rule 1.17 which sets out a specific de-identification process)

From 1 November 2021, the major banks will enable business consumers to share their data with ADRs.

These changes build on the amendments made to the Rules, which commenced on 2 October 2020, to allow accredited intermediaries to collect CDR data on behalf of an ADR.

Consultation regarding proposed Digital Identity legislation

Late last year the Digital Transformation Agency (DTA) sought community views on proposed legislation to support an expanded Digital Identity system in Australia. The current Digital Identity system is underpinned by the Trusted Digital Identity Framework (TDIF), which imposes strict privacy, security and administrative requirements on accredited entities.

In February 2020, the DTA published a summary of the feedback. Key themes included the need for effective governance of the Digital Identity system, an appropriate liability framework and the need for legislation to enshrine key privacy and consumer safeguards.

After considering the feedback, the DTA will engage in a second round of consultation and then commence development of the draft legislation. To find out more, go to www.digitalidentity.gov.au

Privacy Act Review

Over 150 submissions have been made to the Attorney-General's Department review of the Privacy Act. A discussion paper will be released during 2021 for further consultation. Submissions have been made by a broad range of government and non-government entities, and are available here.

OAIC Consultation on updating the Guide to securing personal information

The consultation period to provide submissions on the OAIC's proposed update to the Guide to securing personal information closed on 12 March 2021. Last updated in 2018, we expect that the updated Guide will reflect changing information handling practices, and the OAIC's experience regulating the notifiable data breaches scheme. Watch this space.