



SIBENCO
LEGAL & ADVISORY

PRIVACY TRAINING

Susan Bennett
Sibenco Legal & Advisory
e: susan.bennett@sibenco.com
p: +61 409 480 840
[🐦 @sibenco](https://twitter.com/sibenco)

Privacy



A strong **privacy culture** is critical for ensuring personal information security

Privacy champions essential for strong privacy culture

Personal Information



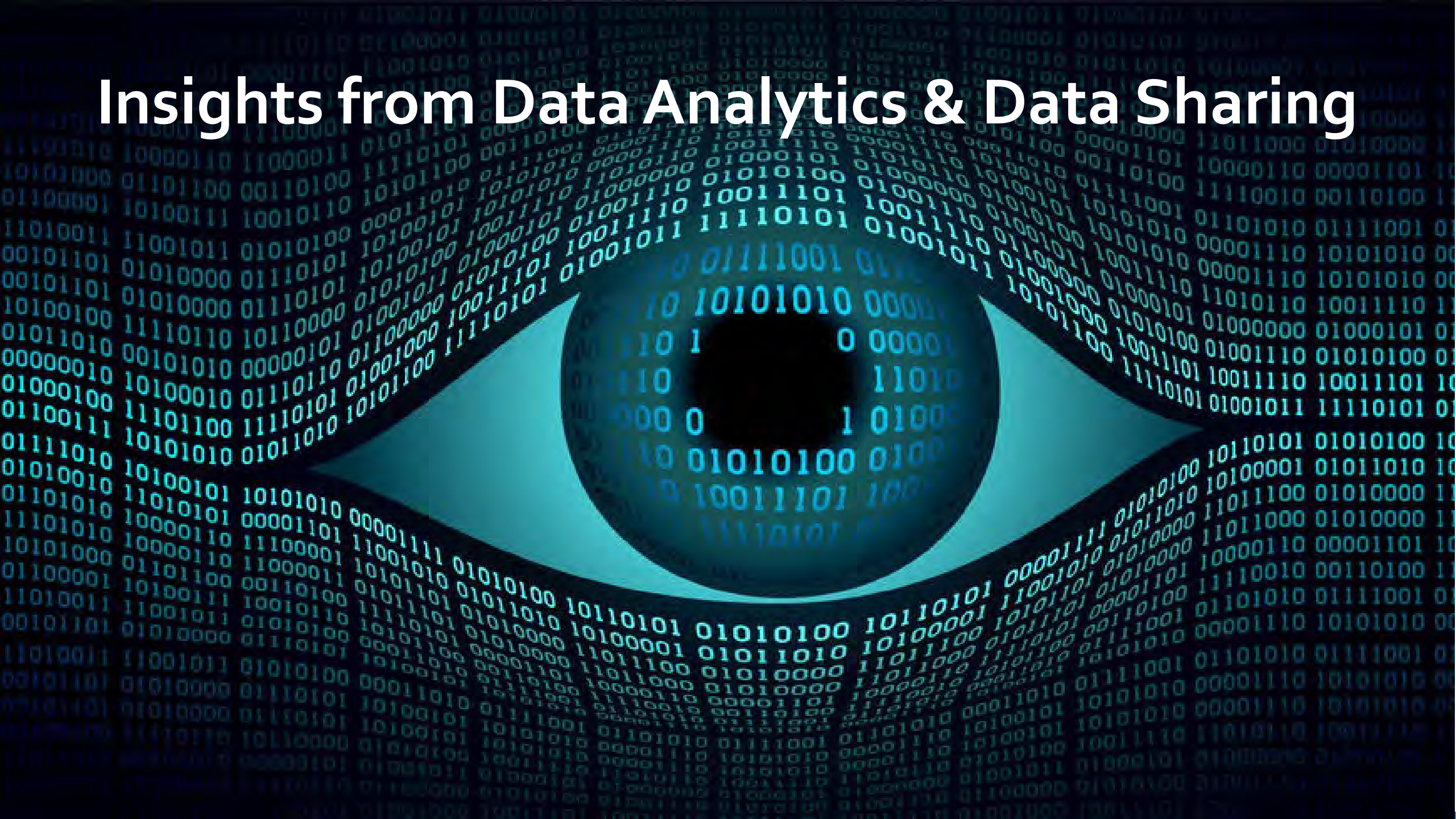
Personal Information



Global Digital Economy – data flows



Insights from Data Analytics & Data Sharing



Information

**Freedom of
Information**

FOI Act 1982

Privacy

Privacy Act 1988



Privacy now in focus

Cambridge Analytica & Facebook

Cambridge Analytica scandal: the biggest revelations so far

Since Christopher Wylie blew the whistle in the Observer, developments have been rapid. Here's what we know about the analytics firm, Facebook and Trump's election team



▲ Cambridge Analytica whistleblower: "We spent \$1m harvesting millions of Facebook profiles" - video

Cambridge Analytica and Facebook: The Scandal and the Fallout So Far

Revelations that digital consultants to the Trump campaign misused the data of millions of Facebook users set off a furor on both sides of the Atlantic. This is how The Times covered it.



Cambridge Analytica's Facebook data was accessed from Russia, MP says

by Donie O'Sullivan, Drew Griffin and Patricia DiCarlo @CNNTech
July 27, 2018, 6:50 PM ET



Cambridge Analytica's Facebook data was accessed from Russia, MP says

The now infamous Facebook data set on tens of millions of Americans gathered by a Cambridge University scientist for a firm that went on to work for Donald Trump's 2016 campaign was accessed from Russia, a British member of parliament tells CNN.

The Cambridge Analytica Files

A year-long investigation into Facebook, data, and influencing elections in the digital age



- Revealed / 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**
- The Brexit whistleblower / Did Vote Leave use me? Was I naive?**
- Facebook told me it would act swiftly on data misuse - in 2015**
- Revealed: Steve Bannon's psychological warfare tool: meet the data war whistleblower**
- Christopher Wylie goes on the record to discuss the role he played in exposing the profiles of millions of Facebook users in order to help the Conservative Party**
- Facebook's work of shame / The Cambridge Analytica fallout**
- Politicians can't control the digital giants with rules drawn up for the analogue era**
- Investigations spend seven hours at Cambridge Analytica HQ**
- Former Cambridge Analytica exec says she wants lies to stop**
- The shady data-gathering tactics used by Cambridge Analytica were an open secret**
- Zuckerberg apologizes for the Cambridge Analytica scandal, outlines next steps**

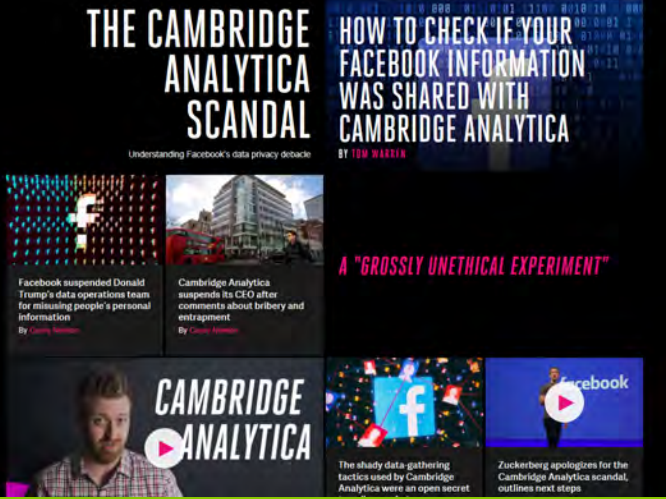
THE CAMBRIDGE ANALYTICA SCANDAL

Understanding Facebook's data privacy debate

HOW TO CHECK IF YOUR FACEBOOK INFORMATION WAS SHARED WITH CAMBRIDGE ANALYTICA

BY TOM WARREN

A "GROSSLY UNETHICAL EXPERIMENT"



- Facebook suspended Donald Trump's data operations team for misusing people's personal information
- Cambridge Analytica suspends its CEO after comments about bribery and entrapment

Facebook Cambridge Analytica Scandal: 10 Questions Answered

TECH • FACEBOOK



By BLOOMBERG April 10, 2018

Cambridge Analytica & Facebook

How Cambridge Analytica Exploited the Facebook
Data of Millions

New York Times

PageUp – June 2018

NEWS

LOCATION: Sydney, NSW [Change](#)

[Home](#) [Just In](#) [Politics](#) [World](#) [Business](#) [Sport](#) [Science](#)

[Print](#) [Email](#) [Facebook](#) [Twitter](#) [More](#)

Bank details, TFNs, personal details of job applicants potentially compromised in major PageUp data breach

By Pat McGrath and Clare Blumer, ABC Investigations
Updated 7 Jun 2018, 12:07pm

The personal details of thousands of Australians have potentially been compromised, with HR company PageUp, which counts Telstra, NAB, Coles, Australia Post, Aldi and Medibank as clients, revealing a massive data breach.

MUST READ: [MICROSOFT DECLARES WINDOWS 10 APRIL 2018 UPDATE READY FOR BUSINESS](#)

PageUp could face class action over potential data mishandling

Centennial Lawyers is considering launching a class action lawsuit against the HR SaaS provider after it suffered a malware attack and possible resulting data breach.

How the PageUp Hack is Highlighting HR's Data Protection Problems

by Guest Contributor on June 14, 2018

FINANCIAL REVIEW

Home / Technology

Jun 8 2018 at 12:54 PM
Updated Jun 8 2018 at 12:54 PM

[Save article](#) [My Saved Articles](#) [Print](#) [License article](#)

PageUp data breach forces Coles, Aus Post and more to close careers websites



Karen Cariss, co-founder and chief executive of PageUp, was forced to address a data breach on Wednesday.



HR Software company PageUp victim of a Data Breach, experts fear a domino effect

June 6, 2018 By Pierluigi Paganini

[My Page](#) [Like 13](#)

[G+](#)

HR Software Firm PageUp is the last victim of a data breach, the company has 2.6 million active users across over 190 countries.

The Sydney Morning Herald

BUSINESS COMPANIES CYBER SECURITY

PageUp data breach: ABC, Asahi, Myer, Macquarie pull jobs pages

By Jennifer Duke
11 June 2018 – 4:52pm

Australians hoping to apply for a new job on the long weekend may have found their plans scuppered, with a swathe of businesses pulling down their careers pages after the PageUp data

BANK INFO SECURITY

[Breach Notification](#), [Breach Response](#), [Data Breach](#)

HR Service Provider PageUp Discloses Data Breach

Customers Include Aldi, Lindt, Australia Post, Commonwealth Bank and Telstra

Jeremy Kirk (@Jeremy_kirk) · June 7, 2018 · 0 Comments

[Twitter](#) [Facebook](#) [LinkedIn](#) [Credit Eligible](#)

[Get Permission](#)

PageUp faces customer losses, lawsuits after data breach

[G+](#) [f](#) [t](#) [in](#) [v](#)

PageUp - Universities

Universities impacted

Universities victims of data breach at PageUp incl: Melbourne, RMIT, UNSW, Macquarie, ANU, Tasmania.

Reported that 'malicious code executed inside PageUp's systems'.

Major universities hit by data breach affecting thousands of job applicants at top firms

By [Michael Koziol](#)

8 June 2018 - 4:54pm



5 [View all comments](#)

Leading universities including Melbourne and Macquarie have become the latest victims of a major data breach at human resources firm PageUp, forcing them to suspend their job boards and urge applicants to check their affairs for unusual activity.

PageUp People, which manages recruitment for ASX200 firms including AMP, Telstra and Coles, revealed it had detected "unusual activity" on its IT infrastructure last month and received "some indicators that client data may have been compromised".

The breach is under investigation by the government-run Cyber Security Centre. PageUp advised there was "no evidence that there is still an active threat, and the jobs website can continue to be used" - though many of its clients were being more cautious.



ANU says 'sophisticated operator' stole data in new cyber breach

By [Max Koslowski](#) and [David Wroe](#)

Updated June 4, 2019 — 4:48pm, first published at 11:33am



36 [View all comments](#)

Up to 200,000 students and staff of the Australian National University have had personal data stolen in a "sophisticated" cyber attack that echoes a similar breach last year attributed to the Chinese government.

The university has admitted the hackers stole data stretching back 19 years that included bank details, passport information and academic records of current and former students and staff.



TODAY'S TOP STORIES

FEDERAL BUDGET

There's one thing politicians just can't resist when the economy goes bad



MONEY APPS

Hours before Afterpay boss took to the stage, he was tapped over potential counter-terrorism breach



TRUMP DIPLOMACY

On Iran, Trump tweets like a hawk but - thankfully - acts like a dove



ANU data breach stretching back 19 years detected

Updated 4 Jun 2019, 5:02pm

The Australian National University has been hit by a massive data hack, with unauthorised access to significant amounts of personal details dating back 19 years.

A sophisticated operator accessed the ANU's systems illegally in late 2018 but the breach was only detected two weeks ago, the university said in a statement.

Based on student numbers over that time, as well as staff turnover, the university has estimated approximately 200,000 people were affected by the breach.

"We believe there was unauthorised access to significant amounts of personal staff, student and visitor data extending back 19 years," ANU vice-chancellor Brian Schmidt said.

"Depending on the information you have provided to the university, this may include names, addresses, dates of birth, phone numbers, personal email addresses and emergency contact details, tax file numbers, payroll information, bank account details, and passport details. Student academic records were also accessed."

However, Professor Schmidt said the hack had not accessed credit card details, travel information, medical records, police checks, workers' compensation information, vehicle registration numbers, and some performance records.



PHOTO: The hacker accessed personal details of staff, student and visitor data at Australian National University. (ABC News: Niki Challis)

RELATED STORY: [Doubts over data safety after ANU hack](#)

RELATED STORY: [Chinese hackers infiltrate systems at ANU](#)

RELATED STORY: [Where Australia ranks on the list of state-sponsored hackers](#)

Key points:

- ANU vice-chancellor Brian Schmidt said the university had been made aware of the breach two weeks ago
- Professor Schmidt said there had been unauthorised access to "significant amounts" personal data
- IT upgrades put in place after a different breach last year helped detect the incident

Australian Catholic University staff details stolen in fresh data breach

By [Carrie Fellner](#)

June 17, 2019 – 3.36pm



The Australian Catholic University has revealed the sensitive personal information of staff members has been stolen in a cyber attack, in the second significant security breach revealed in a month to have occurred at one of the country's tertiary institutions.

In an email circulated on Monday afternoon, the university confirmed a number of staff email accounts and some university systems had been compromised in a phishing attack on May 22.



Tuesday, 18 June 2019 08:50

Attackers use phishing to gain access to ACU staff data Featured

The Australian Catholic University has been hit by a data breach, with the attacker(s) using a phishing email to trick users into revealing their credentials on a fake ACU login page. The ACU has three public websites, with the main one running on Linux, while two others, which allow staff to log in, run on Windows Server 2008.

NEWS

Laptops holding 30 years' worth of student data stolen from UWA



By George Nott

CIO |

29 JULY 2019 22:25 AEST

The laptops – which were taken in a break-in at a UWA administration building – contain the Tax File Numbers and student identification numbers of people who applied to study at the university between 1988 and January 2018.

“Separately, and in varying degrees of completeness, there are also details across the laptops from applicants who may have provided the University with information such as names, dates of birth and passport numbers to obtain a confirmation of enrolment,” Vice-Chancellor Professor Dawn Freshwater”

'Alarming' Data Breach Exposes 50,000 Students In Ticketing Website Bungle

NAME
CONTACT DETAILS
DATE OF BIRTH
BANK DETAILS



Get, an online service used by a numerous clubs, societies, and student organisations around Australia, has suffered a major data breach, potentially



Tech start-up investigating 'potential data leak' on online ticketing platform

By [Ben Nielsen](#) and [Rebecca Puddy](#)

Posted 10 Sep 2019, 7:10am

Student claims 'insane' amount of information available

Claims about the system vulnerability emerged over the weekend, after a University of Canberra software engineering student posted on social media.

The student, who asked to remain anonymous, told the ABC he found the data when applying for a club membership. "[The website] showed a list of all the people that were part of that society, which seemed a bit strange to me," the student said. He said a quick online search found the personal data of about 200,000 users dating back more than a year. "I looked at the information that was being sent from Get to my computer ... it's things like name, phone number, date of birth, addresses, student number.

March 2020

Australia data breach: 90,000 staff, students, suppliers impacted at Melbourne Polytechnic

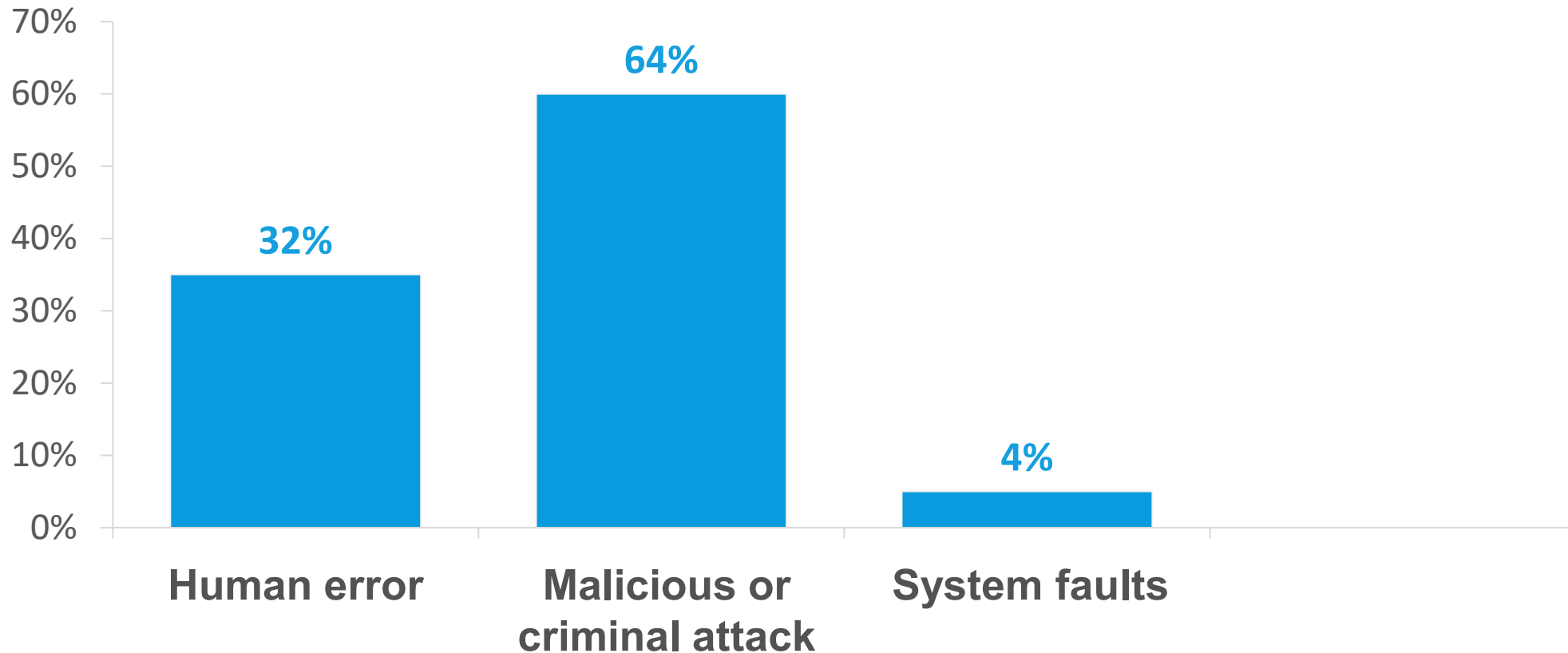


Personal data, including e-mail addresses, passwords, driver's license, passport details, and financial and health information of 90,000 staff, students and suppliers

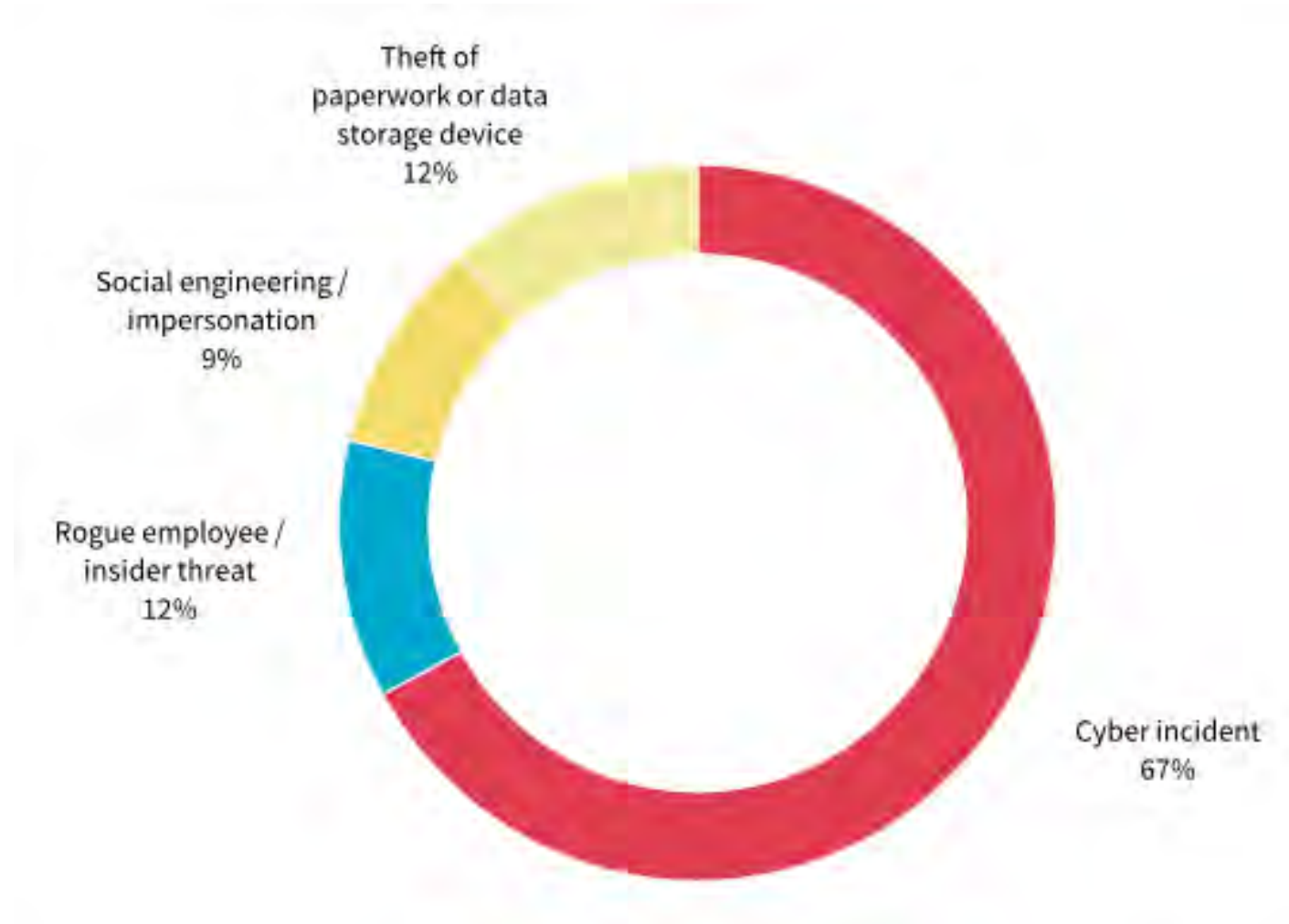


Victoria Police notified Melb Poytechnic that an individual who attended the campus in **late 2018** had 'obtained unauthorised access to Melbourne Polytechnic's computer systems by hard logging onto the network; overcoming security measures.'

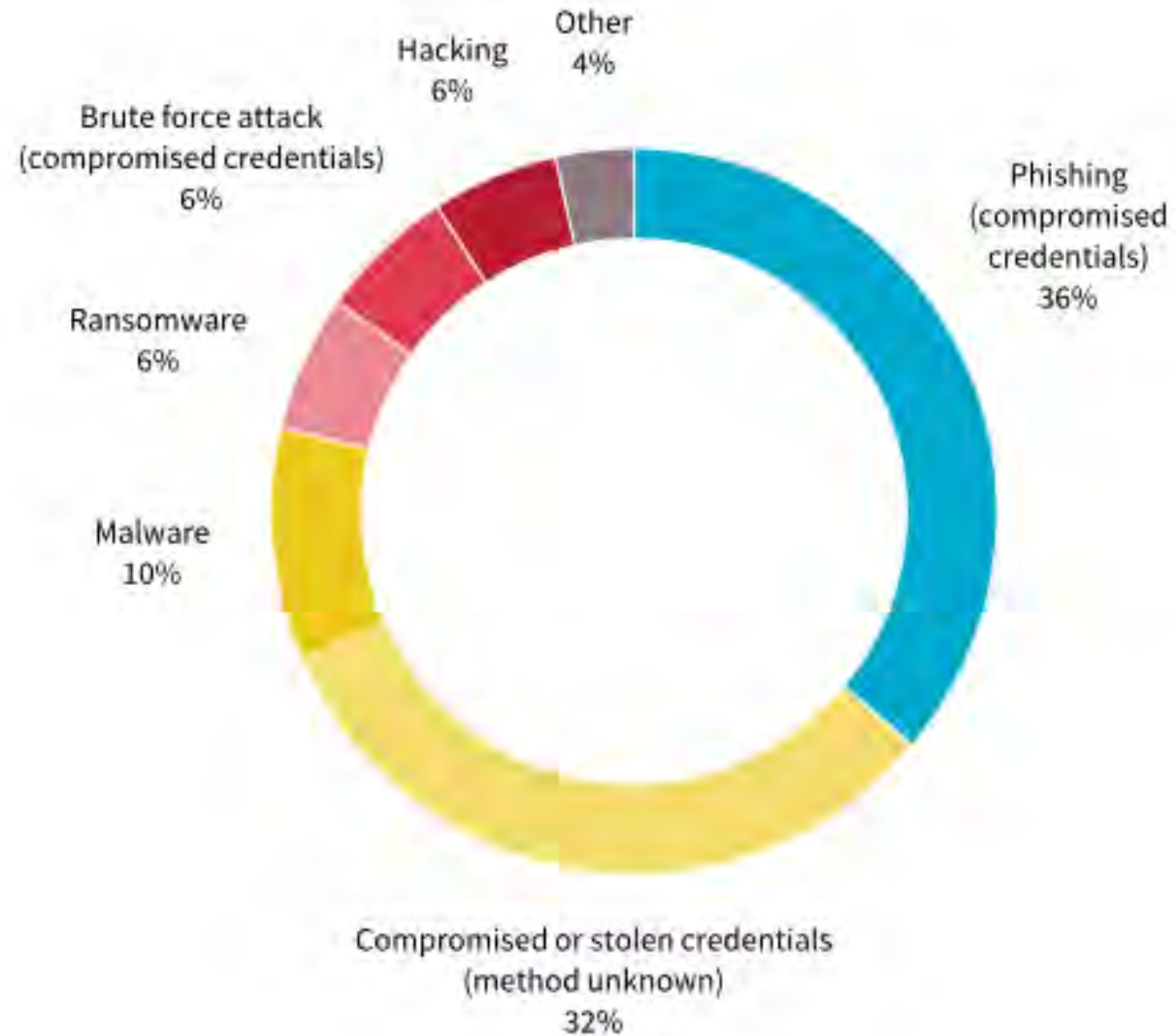
Data Breach Causes – OAIC, 28 Feb 2020



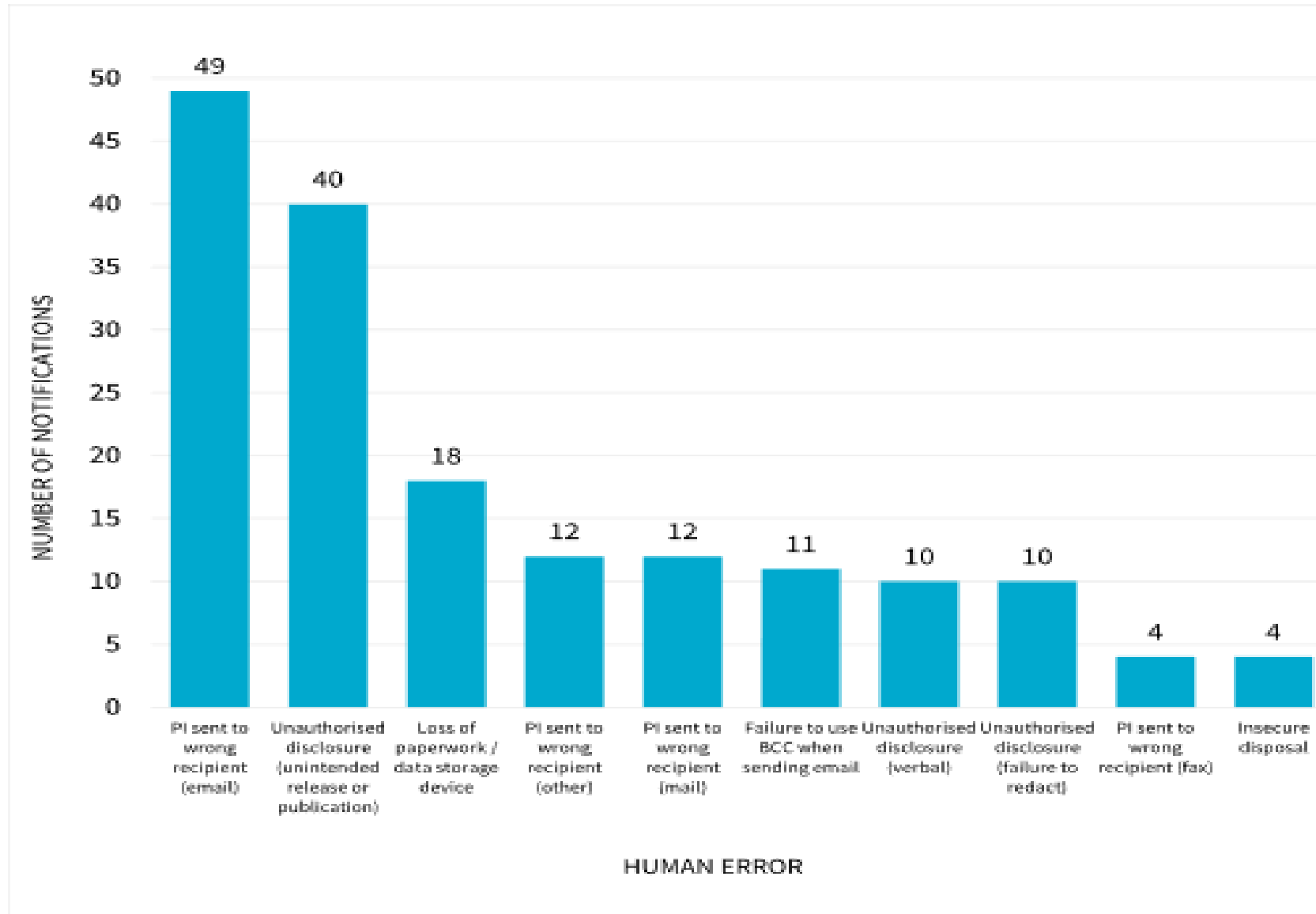
Malicious or criminal attacks



Cyber incident



Human Error Causes – OAIC, 28 Feb 2020

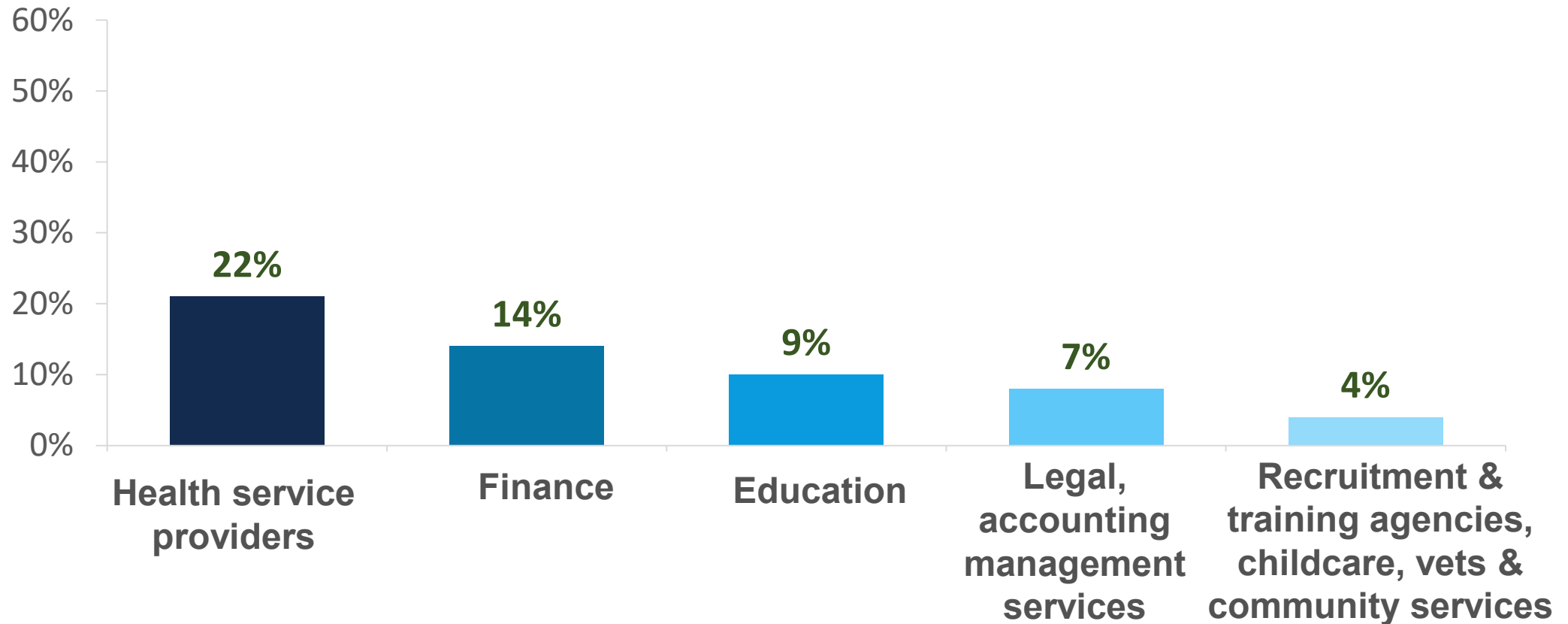


Data Breach



- A data breach happens when personal information is accessed or disclosed **without** **authorisation** or is lost.

Top 5 Sectors – July to Dec 2019



OAIC report – 1st 12 months of NBD Scheme



- **964 data breach notifications**
- From 1 April 2018 to 31 March 2019

- **114 data breach notifications**
- for financial year 2016/2017

OAIC report – 19% increase in 2019



- **537 data breach notifications**
- From 1 July 2019 to 31 December 2019

- **460 data breach notifications**
- From 1 January 2019 to 30 June 2019

What do you do if you identify a data breach of personal information?



Notify the ANU Privacy Officer



Data breach notification

You must notify affected individuals and OAIC when a data breach involving personal information is likely to result in serious harm



- Enables students, staff and affected individuals to take any steps required to protect themselves from risk that may occur as a result of the data breach.
- Assist to mitigate any damage and reflect positively on the University's reputation.

Serious Harm



The types of PI involved more likely to cause serious harm include:

sensitive information – e.g. health

documents commonly used for ID fraud
e.g. Medicare number, student number,
driver license, passport details

financial information

a combination of types of PI that allows more
to be known about the individuals

Nature of Harm



Examples likely to result in serious harm include:

identity theft

significant financial loss

threats to an individual's physical safety

loss of business or employment opportunities

humiliation, damage to reputation or relationships

workplace or social bullying or marginalisation

Notify the ANU Privacy Officer



Process for managing a data breach



When are affected individuals and OAIIC notified of data breach?



Assessment - As Short a Time as Possible



Section 26WH(2): An organisation must take all reasonable steps to complete the assessment within 30 calendar days after the day it became aware of the grounds that caused it to suspect an eligible data breach.

But....

wherever possible entities to treat 30 days as a maximum time limit ..., and endeavour to complete the assessment in a much shorter timeframe, as the risk of serious harm to individuals often increases with time.

Assessing a Suspected Data Breach

The assessment:

Must be
reasonable
and
expeditious

and

Entities may
develop their
own
procedures for
assessing a
suspected data
breach

General Data Protection Regulation (GDPR)

How Europe's GDPR will affect Australian organisations

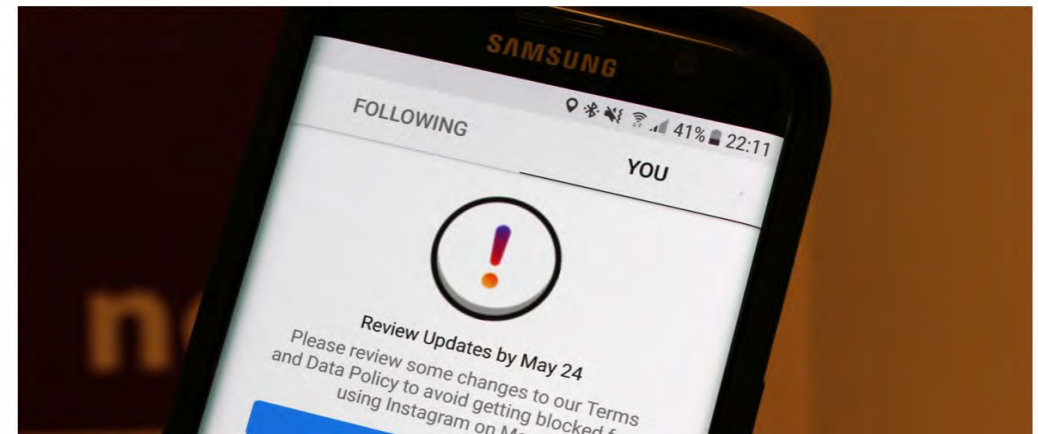
Failure to comply with the data protection regulations could result in a €20 million fine, and Australian organisations with links to Europe will not be exempt.

By Asha McLean | July 12, 2017 -- 23:37 GMT (09:37 AEST) | Topic: Security

Facebook, Google face first GDPR complaints over 'forced consent'

Natasha Lomas @riptari / May 25, 2018

Comment



Max Schrems files first cases under GDPR against Facebook and Google

European data protection bodies vow to work with Irish colleagues on complaints

© Fri, May 25, 2018, 08:03 | Updated: Fri, May 25, 2018, 18:15

Derek Scally in Berlin



Privacy campaigner Max Schrems accused the tech giants of 'coercing' users to accept data policies

European data protection bodies have promised to work closely with their Irish colleagues on multi-billion-euro complaints filed by Austrian privacy campaigner Max Schrems against Facebook and Google.

SECURITY

The Game of Lawsuits – Another One Filed Against Facebook Over Data Misuse



By Rafia Shaikh

May 30, 2018

12
SHARES

f SHARE

t TWEET

SUBMIT

EU- GDPR



The biggest change to Europe's privacy laws in 20 years

Enforced from 25 May 2018

Penalties of up to 4% of global turnover or €20 million, whichever is higher



Notification of Data Breach under GDPR



Under the GDPR, notification must be made where a data breach is likely to **'result in a risk for the rights and freedoms of individuals'**.






Notification must be made **within 72 hours** of first having become aware of the breach.



Data processors are required to notify their customers and the controllers **'without undue delay'** after first becoming aware of a data breach.



GDPR applies to Australian orgs that -

-  are data processors or controllers with an establishment in the EEA
-  offer goods or services to individuals in the EEA
-  monitoring the behavior of individuals in the EEA, where that behavior takes place in the EEA

Personal Information



Mandatory Data Breach Reporting



NDB Scheme

Australia's notifiable data breach (NDB) scheme
- 23 February 2018

APP entities – incl orgs with \$3m turnover, health care providers, ANU, private tertiary education providers, & breaches of TFNs



Global trend

EU - General Data Protection Regulation (GDPR) - 25 May 2018

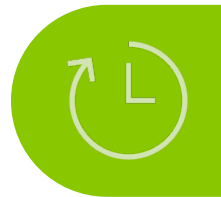
Australian orgs incl education providers, tertiary institutes if they are operating in the EU or offering goods & services to EU residents – i.e. prospective or current students or alumni residing in EU



Notification of Data Breach under GDPR



Under the GDPR, notification must be made where a data breach is likely to **'result in a risk for the rights and freedoms of individuals'**.



Notification must be made **within 72 hours** of first having become aware of the breach.



Data processors are required to notify their customers and the controllers **'without undue delay'** after first becoming aware of a data breach.

Controllers and Processors

Controllers

Determine the purpose and means of processing personal data.

They are the principal party with responsibilities including - collecting and managing consent and enabling rights under the GDPR.

Processors

Means the organisation which processes personal data on behalf of the controller.

The obligations on data processors under the GDPR are new.

Controllers to only use processors providing 'sufficient guarantees to implement appropriate technical and organizational measures' that will meet the GDPR requirements.

Rights of Individuals Under the GDPR

**Right of
access**

**Right to
be
informed**



**Right to
object**

**Right to
withdraw
consent**

**Right to
rectification**

**Right
to restrict
processing
(in certain
circumstances)**

**Right
to object
to automated
decision making
(in certain
circumstances)**

**Right to
erasure / be
forgotten**

**Right
to data
portability**

GDPR Data Breach Penalties

BA faces £183m fine over passenger data breach

ICO says personal data of 500,000 customers was stolen from website and mobile app



▲ A British Airways data breach in 2018 compromised customers' credit card information. Photograph: Frank ©2020 Sibenco Pty Ltd

Marriott to be fined nearly £100m over GDPR breach

ICO imposes fine after personal data of 339 million guests was stolen by hackers



▲ Marriott said it would appeal against the fine. Photograph: Reuters

GDPR Penalties

Facebook fined for data breaches in Cambridge Analytica scandal

Firm fined £500,000 for lack of transparency and failing to protect users' information



▲ Facebook's co-founder, chairman and chief executive, Mark Zuckerberg, prepares to testify before Congress about Cambridge Analytica. Photograph: Chip Somodevilla/Getty Images

GDPR Penalties

Google fined record £44m by French data protection watchdog

CNIL found that company failed to offer users transparent information on data use



€14.5 Million GDPR Fine for Non-compliant Data Retention Schedule

Real estate company fined € 14.5 million in Germany for violating GDPR principle of privacy by design

📅 November 8, 2019 🗨️ Posted by Dissent 📁 Breaches, Non-U.S.

Lars Lensdorf and Ulrike Elteste of Covington & Burling write:

“

On October 30, 2019, the supervisory authority (“SA”) of a € 14.5 million fine against the real estate company Deutscher Wohnen SE for storing personal data of tenants without Art. 6 GDPR) and for not implementing the GDPR principle of privacy by design (Art. 5 and 25(1) GDPR) (press release in German). It is the highest GDPR fine imposed so far this year.

First multi-million dollar GDPR fine

Thursday, November 14, 2019 - 13:59

A German real estate company, die Deutsche Wohnen SE (Deutsche Wohnen) has received the highest GDPR fine to date for ‘over retention’ of personal data, €14.5 million.

On November 5, 2019, the Berlin Commissioner for Data Protection and Freedom of Information announced it has imposed the highest fine issued in Germany since the EU General Data Protection Regulation (“GDPR”) became applicable.

After conducting onsite inspections in June 2017 and March 2019, the Berlin Commissioner noticed that Deutsche Wohnen SE was retaining personal data of tenants for an unlimited period, without examining whether the retention was legitimate or at all necessary. In some cases, it was possible to access personal data of affected tenants, some of which were years old, without the data serving the purpose of the original data collection.

COMPARISON	EU GDPR	Australian Privacy Act
Who does this apply to?	Data processing activities of businesses, regardless of size, that are data processors or controllers	Most Australian Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than \$3 million, all private health service providers and some small businesses.
What does it apply to?	Personal data – any information relating to an identified or identifiable natural person: Art 4(1)	Personal information (PI) – information or an opinion about an identified individual, or an individual who is reasonably identifiable: s 6(1)
Jurisdictional link	Applies to data processors or controllers: <ul style="list-style-type: none"> with an establishment in the EU, or outside the EU, that offer goods or services to individuals in the EU or monitor the behaviour of individuals in the EU: Art 3 	Applies to businesses: <ul style="list-style-type: none"> incorporated in Australia, or that ‘carry on a business’ in Australia and collect PI from Australia or hold PI in Australia: s 5B
Accountability and governance	Controllers generally must: <ul style="list-style-type: none"> implement appropriate technical and organisational measures to demonstrate GDPR compliance and build in privacy by default and design: Arts 5, 24, 25 undertake compulsory data protection impact assessments: Art 35 appoint data protection officers: Art 37 	APP entities must take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs and to enable complaints: APP 1.2 Businesses are expected to appoint key roles and responsibilities for privacy management and to conduct privacy impact assessments for many new and updated projects
Consent	Consent must be: <ul style="list-style-type: none"> freely given, specific and informed, and an unambiguous indication of the data subject's wishes which, by a statement or by a clear affirmative action, signifies agreement to processing: Art 4(11) 	Key elements: <ul style="list-style-type: none"> the individual is adequately informed before giving consent, and has the capacity to understand and communicate consent the consent is given voluntarily the consent is current and specific: OAIC’s APP GLs
Data Breach notifications	Mandatory data breach notifications by controllers and processors (exceptions apply): Arts 33-34	From 22 February 2018, mandatory reporting for breaches likely to result in real risk of serious harm
Individual rights	Individual rights include: <ul style="list-style-type: none"> right to erasure: Art 17 right to data portability: Art 20 right to object: Art 21 	No equivalents to these rights. However, business must take reasonable steps to destroy or de-identify PI that is no longer needed for a permitted purpose: APP 11.2. Where access is given to an individual’s PI, it must generally be given in the manner requested: APP 12.5
Overseas transfers	Personal data may be transferred outside the EU in limited circumstances including: <ul style="list-style-type: none"> to countries that provide an ‘adequate’ level of data protection where ‘standard data protection clauses’ or ‘binding corporate rules’ apply approved codes of conduct or certification in place: Chp V 	Before disclosing PI overseas, a business must take reasonable steps to ensure that the recipient does not breach the APPs in relation to the information: APP 8 (exceptions apply). The entity is accountable for a breach of the APPs by the overseas recipient in relation to the information: s 16C (exceptions apply)
Sanctions	Administrative fines of up to €20 million or 4% of annual worldwide turnover (whichever is higher): Art 83	Powers to work with entities to facilitate compliance and best practice, and investigative and enforcement powers: Parts IV and V

Processing Personal Data

You must have a valid lawful basis in order to process personal data.

Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.

There are six available lawful bases for processing.

You must determine your lawful basis before you begin processing, and you should document it. You should not swap to a different lawful basis at a later date without good reason.

If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

6 Lawful Bases for Processing

Consent

The individual has given clear consent for you to process their personal data for a specific purpose.

Contract

Necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Legal obligation

Necessary for you to comply with the law (not including contractual obligations).

Vital Interests

Necessary to protect someone's life.

Public task

Necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

Legitimate interests

Necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.*

International Transfers



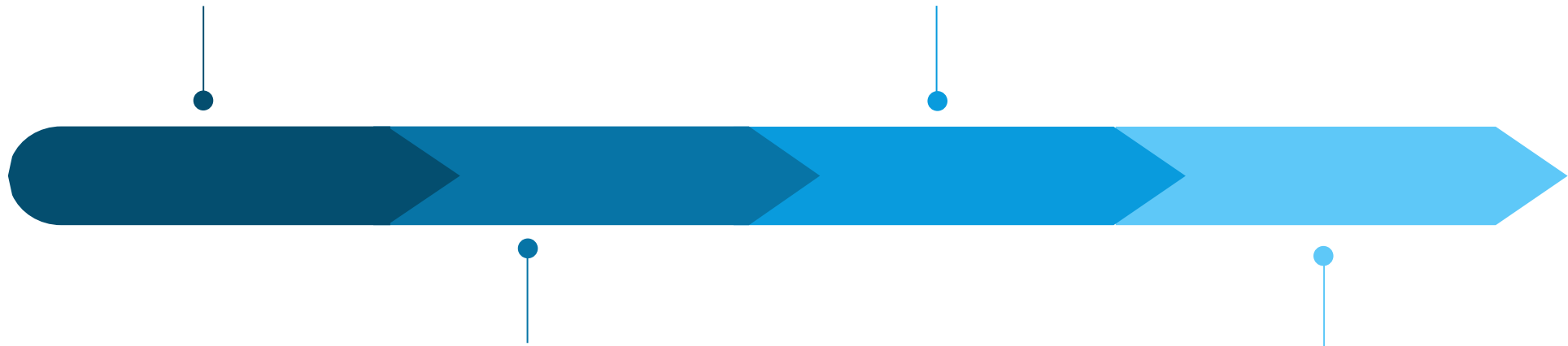
Transfers may take place to a third country or international organisation where the EU Commission has decided that it ensures ‘an adequate level of protection’ (Article 45(1)).

The adequacy decisions under the current Directive remain in force under the GDPR and those determined by the EU Commission to provide ‘an adequate level of protection’ - eg New Zealand and Japan.

International Transfers

Approved binding corporate rules that enable transfers within a multinational group of companies

Approved code of conduct pursuant to Article 40, and the recipient gives binding and enforceable commitments to apply appropriate safeguards



Standard data protection contractual clauses approved by the EU Commission

Approved certification mechanism pursuant to Article 42, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards

Accountability & Governance

The GDPR sets out expanded accountability and governance requirements including that data controllers must:



Demonstrate that they comply with all the principles set out in Article 5(1) of the GDPR.



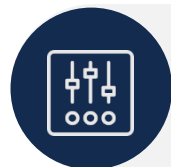
Implement appropriate technical and organizational measures to ensure compliance with the GDPR, including implementation of data protection policies



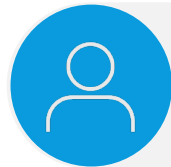
Implement 'data protection by design and by default'.



Implement appropriate technical and organizational 'measures to ensure a level of security appropriate to the risk'.



Data protection impact assessment for high risk processing



Appoint a Data Protection Officer (DPO)

Accountability & Governance



Demonstrate that they comply with all the principles set out in Article 5(1) of the GDPR.

These principles relate to the processing of personal data which include: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality.



Implement 'data protection by design and by default'.

The controller is required at the outset to determine the means for processing data, as well as at the time of processing to implement appropriate technical and organizational measures to ensure it complies with the GDPR and protects the rights of individuals. This includes ensuring that only personal data collected and processed is for the specific purpose of the transaction, personal data is stored no longer than it is required and that access to personal data is restricted.



Implement appropriate technical and organizational measures to ensure compliance with the GDPR, including implementation of data protection policies (Article 24).



Implement appropriate technical and organizational 'measures to ensure a level of security appropriate to the risk'.

This includes as appropriate: de-identification and encryption of personal data; ongoing confidentiality, integrity and availability and resilience of processing systems and services; ability to restore the availability and access to personal data; and a process for regularly testing, assessing and evaluating the effectiveness of the measures implemented to ensure security.

Accountability & Governance



Demonstrate that they comply with all the principles set out in Article 5(1) of the GDPR.

These principles relate to the processing of personal data which include: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality.



Implement appropriate technical and organizational measures to ensure compliance with the GDPR, including implementation of data protection policies (Article 24).

Accountability & Governance



Implement ‘data protection by design and by default’.

The controller is required at the outset to determine the means for processing data, as well as at the time of processing to implement appropriate technical and organizational measures to ensure it complies with the GDPR and protects the rights of individuals.

This includes ensuring that only personal data collected and processed is for the specific purpose of the transaction, personal data is stored no longer than it is required and that access to personal data is restricted.



Implement appropriate technical and organizational ‘measures to ensure a level of security appropriate to the risk’.

This includes as appropriate:

- de-identification and encryption of personal data;
- ongoing confidentiality, integrity and availability and resilience of processing systems and services;
- ability to restore the availability and access to personal data;
- and a process for regularly testing, assessing and evaluating the effectiveness of the measures implemented to ensure security.

Accountability & Governance



Data protection impact assessment for high risk processing

A data protection impact assessment is required before processing personal data for processing which is likely to result in a high risk to the rights and freedoms of individuals.



Appoint a Data Protection Officer (DPO) if the organisation falls within a category where a DPO is mandated.

This includes: public authorities, organizations carrying out large scale systematic monitoring of individuals (e.g. online behavior tracking) or organizations carrying out large scale processing of special categories of data or data relating to convictions and offences.

DPO's are required to have 'expert knowledge' of data protection law and practices.

The DPO must 'directly report to the highest management level', must not be instructed in the exercise of their tasks and must not be dismissed or penalized for performing their tasks (Article 38(3)).

Global Digital Economy – data flows



Changes to Privacy Act ahead



Federal Government announcement in March 2019 that:

- OAIC will be provided with an additional \$25 million over three years to give it the resources it needs to investigate and respond to breaches of individuals' privacy
- Amendments to Privacy Act will be drafted for consultation.

The challenge of Shadow IT




Home » IT Leadership

OPINION

Hillary Clinton is now the face of shadow IT

Even if the former secretary of state set up a private mail server purely for the convenience of using a single phone for both government work and personal use, Hillary Clinton is now the poster child for the dangers of rogue IT. Intentions aside, a move like Clinton's puts the security of confidential data at risk.

[Twitter](#) [Facebook](#) [LinkedIn](#) [Google+](#) [Reddit](#) [StumbleUpon](#) [Email](#) [Print](#)

 **By Tom Kaneshige**
Senior Writer, CIO |
MAY 12, 2015 10:55 AM PT

What We Know About the Investigation Into Hillary Clinton's Private Email Server

By ALICIA PARLAPIANO | UPDATED OCT. 28, 2016

On Oct. 28, the F.B.I. director, James B. Comey, said that the bureau had recently uncovered new emails potentially related to the investigation into the private email server. The latest emails were found after the bureau seized at least one electronic device once shared by Anthony D. Weiner and his estranged wife, Huma Abedin, an aide to Mrs. Clinton. [RELATED ARTICLE](#)

30,000 initially turned over by Mrs. Clinton's lawyers, deemed work-related, returned to the State Department in December 2014.

- **8 chains** included **"top secret"** information
- **36 chains** included **"secret"** information
- **8 chains** included **"confidential"** information, the lowest level of classification
- **2,000 emails** have since been classified **"confidential"**
- The F.B.I. director, James B. Comey, said that a very small number of emails had classified markings when they were sent.

14,900 additional work-related emails that Mrs. Clinton did not turn over to the State Department, uncovered by the F.B.I. during the course of its investigation.

Comply with ANU Policies

- **Acceptable Use of IT Policy**
- **Code of Conduct**
- **Records & Archive Management Policy**
- **Research Data Management Policy**



Do you know what everyone is doing?





Privacy & Research

PI and Research

Australian Privacy Act 1988 (Cth)

Australian Privacy Principles (APPs)

**Australian Code of Responsible
Conduct of Research 2007**

Sets out the principles and responsibilities that underpin the conduct of Australian research

**National Statement on Ethical
Conduct in Human Research (2007)**

Consists of a series of guidelines made in accordance with the NHMRC Act 1992

ANU Code of Research Conduct

Sets out compliance requirements re research records at the University

Research Data Management Policy

Data management plan and management of data throughout the research and lifecycle of data

Australia – Re-identification of dataset



THE SIMPLE PROCESS OF RE-IDENTIFYING PATIENTS IN PUBLIC HEALTH RECORDS

In late 2016, doctors' identities were decrypted in an open dataset of Australian medical billing records. Now patients' records have also been re-identified - and we should be talking about it

By Dr Vanessa Teague, Dr Chris Culnane and Dr Ben Rubinstein, University of Melbourne

In August 2016, Australia's federal Department of Health published medical billing records of about 2.9 million Australians online. These records came from the Medicare Benefits Scheme (MBS) and the Pharmaceutical Benefits Scheme (PBS) containing 1 billion lines of historical health data from the records of around 10 per cent of the population.

These longitudinal records were de-identified to protect a person's identity from being connected to the government's [open data website](#).




ENGINEERING & TECHNOLOGY

Featured

 **Dr Vanessa Teague**
School of Computing and Information Systems, Melbourne School of Engineering, University of Melbourne

 **Dr Chris Culnane**
School of Computing and Information Systems, Melbourne School of Engineering, University of Melbourne

 **Dr Benjamin Rubinstein**
Senior Lecturer, School of Computing and Information Systems, Melbourne School of Engineering, University of Melbourne

Engineering and IT

Research reveals de-identified patient data can be re-identified

18 December 2017

Health record details exposed as 'de-identification' of data fails

One in 10 Australians' private health records have been unwittingly exposed by the Department of Health in an embarrassing blunder that includes potentially exposing if someone is on HIV medication, has terminated a pregnancy, or is seeing a psychologist.

Unique patient records matching the online public information of seven prominent Australians, including three former or current MPs and an AFL footballer, were revealed in a study by the University of Melbourne's School of Computing and Information Systems.

A report published on Monday by the university's Dr Chris Culnane, Dr Benjamin Rubinstein and Dr Vanessa Teague outlines how de-identified historical health data from the Australian Medicare Benefits Scheme (MBS) and the Pharmaceutical Benefits Scheme (PBS) released to the public in August 2016 can be re-identified using known information about the person to find their record.

Health pulls Medicare dataset after breach of doctor details

By Paris Cowan
Sep 29 2016
15:27 AEST

[Updated] Researchers say govt encryption was poor.

The Department of Health has removed a research dataset based on Medicare and PBS claims from its open data portal after a team of Melbourne researchers pointed out that practitioner details could be decrypted.

The government today advised that the data was withdrawn yesterday following "an alert made in the public interest" by researcher Dr Vanessa Teague from Melbourne University on September 12.

Teague told the department that she and her colleagues had analysed 10 percent of the linked dataset and found it was possible to decrypt some of the service provider ID numbers attached to doctors.

"As a result of the potential to extract some doctor and other service provider ID numbers, the Department of Health immediately removed the dataset from the website to ensure the security and integrity of the data is maintained," the agency said in a statement.



Aussies born before 1962 with private health cover need to know this



Personal Information

What is Personal Information?

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable.

What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances.



Personal Data - GDPR



Means ‘any information relating to an identified or identifiable natural person (‘data subject’).

An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location number, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4).

The GDPR refers to sensitive personal data as ‘special categories of personal data’ (Article 9).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal Information at the University



• Student/staff - name, address, ID number

• Family details, bank account details

• Medical Info incl medicare number

• Counselling notes

• Photographs, recorded images

What are the risks?



- Risk to student and/or staff safety
- Financial loss to the student/family, and/or staff and/or University
- Reputational damage
- Loss of trust in University
- Regulatory investigation, litigation

Personal information about an individual which is apparent or can reasonably be ascertained



Redaction of name

AIN v Medical Council of New South Wales [2016] NSWCATAD 5



'While the Applicant's personal information was masked from the human eye, her personal information was able to be 'read' by the Google search engine. This resulted in a search for 'Dr [AIN]' (or similar) leading to a link to a copy of the (human eye redacted) Medical Tribunal's decision. The Respondent accepted, properly in my view, that a Google search for 'Dr [AIN]' would link the Medical Tribunal's decision to her'

De-identification of Personal Information



De-identified information is information from which identifiers have been permanently removed, or where identifiers have never been included.

De-identified information cannot be re-identified.

Personal information from linking with other information



'We have concluded that, depending on the circumstances, sources of information other than the information or opinion which contains the personal information, may be consulted to ascertain the person's identity.'

*APV and APW and Department of Finance and Services
[2014] NSWCATAD 10 at [54]*



Australian Privacy Principles (APPs)

13 Australian Privacy Principles



There are **13 APPs** and they govern standards, rights and obligations around:

- **the collection, use and disclosure of PI**
- **ANU's governance and accountability**
- **integrity and correction of PI**
- **the rights of individuals to access PI**

The Privacy Principles (APPs)

1

Open and transparent management of PI -
incls having a clearly expressed and up to date privacy policy

2

Anonymity and pseudonymity

3

Collection of PI – outlines when you can collect PI

4

Dealing with unsolicited PI - outlines steps to be taken
where unsolicited PI is received

The Privacy Principles (APPs)

5

Notification – outlines what an individual must be informed

6

Use or Disclosure – outlines the circumstances in which PI may be used or disclosed

7

Direct marketing - may only use or disclose PI for direct marketing purposes if certain conditions are met

8

Cross-border disclosure of PI - outlines steps that must take to protect PI before it is disclosed overseas

The Privacy Principles (APPs)

9

Gov't related identifier – outlines limited circumstances when a gov't identified may be adopted

10

Accuracy – reasonable steps must be taken to ensure PI is accurate, up to date and complete

11

Security - reas steps must be taken to protect PI from misuse, interference and loss, and from unauthorised access

12

Access – incls a requirement to provide access unless a specific exception applies

13

Correction – outlines the obligation to correct PI held about individuals



**Third party
providers –
technology,
contractors
&
Privacy Impact
Assessments**

What security safeguards are reasonable for contractors?

- minimise the amount of personal information given out
- audit or monitor the performance of the service provider – e.g. contractor or tech system
- control the disposal of the information or demand the return of all personal information once the service is completed
- ensure contractual provisions minimising opportunities for misuse of personal information
- include appropriate contractual clauses incl indemnity clauses to pass on the costs of any compensation due to the actions of an outside contractor/service provider.

Privacy Impact Assessments - PIAs

A PIA identifies how a new or revised project or system can have an impact on an individual's privacy, and makes recommendations for managing, minimising or eliminating those privacy impacts.

A PIA is likely to be required if:

- personal information is collected in a new way;
- personal information is collected in a way that might be perceived as being intrusive;
- personal information will be disclosed to another agency, a contractor, the private sector or to the public; or
- there is a change in the way personal information is collected, disclosed, retained, stored or secured or handled.

- [Privacy Impact Assessment Guideline](#) available on ANU website
- Examples of PIA- [Graduate search](#)
- For assistance contact the ANU Privacy Officer - privacy@anu.edu.au



Discussion

Example

Annabel's father calls Linda, who is Annabel's Masters supervisor, and says he is concerned that he hasn't heard from Annabel for 6 weeks as she usually speaks with him regularly. He is worried as she suffers from depression and would like Annabel's contact details. Can you provide Annabel's mobile number or email address to her father?



Example

ASIO contacts Anne who is senior academic, asking for information about her student John who is undertaking a PhD suspected of being involved in a terror organisation. ASIO want to know who he has been meeting with on his overseas research trips for the last 4 months. Anne hands this information over to ASIO. Should Anne have done this?



Example

A detective contacts a University staff member and asks the staff member to provide contact details for one of the University employees. They say that the disclosure is necessary for a fraud investigation and is required urgently, but is unwilling to provide further details in case it compromises the investigation.



Example

Tom, a Research Fellow, has been researching diabetes on population X and published his findings. He and another colleague are undertaking a new project relating to mental health of diabetics patients and Tom would like to use the genetic samples taken from participants from his original research and use in this new research. Can Tom use the research data in this way?



Example

An academic is seriously injured and, due to their injuries, cannot give consent. Can the University disclose the individual's health information to the treating health service where the University reasonably believes that disclosure of the information is necessary to lessen the serious threat to the individual's life posed by those injuries?



Example

Alex has been interviewing participants for his research. He is about to travel to a politically sensitive country – should Alex be collecting name of people he interviews? What steps can be taken to mitigate risks?



Example

Alex has been interviewing participants for his research in a number of politically sensitive countries. What security precautions should Alex be taking?



Example

Alex has been interviewing participants for his research both in Australia and overseas on his phone. What issues does this raise?



Example

Unfortunately, because Alex was distracted, he left his laptop at the airport? What should Alex do?



Example

Alex has realised that the ANU holds information from students that would be very useful for his research? Can Alex obtain access to this data for his research?



Example

Alex's laptop stopped working while he was overseas, he went and bought a new laptop and is now capturing his latest recordings on a cloud storage site based in the US. Does this raise any privacy concerns?



Privacy Champions & Privacy Proactive

**Be proactive,
Be prepared
and able to
quickly escalate
and respond**

- **Be able to identify when there is a data breach**
- **Escalate and notify Privacy Office immediately**
- **Embed Privacy Culture – e.g team meetings**
- **Staff training – identifying, escalating and knowing what to do in breach event**
- **Ensure suppliers comply with contractual requirements incl privacy regulations**

Personal Information



Privacy Check List

- Check - are you collecting PI?
- Check/think - do you need the PI, or all of the PI?
- Check before using and/or disclosing PI - i.e. is the use or disclosure permitted?
- Think before you send - avoid email address errors and/or wrong recipients
- Secure your computer and other devices; keep passwords safe
- Don't fall for phishing or other scams
- Be vigilant about information security



SIBENCO
LEGAL & ADVISORY

Thank you

Susan Bennett

Sibenco Legal & Advisory

e: susan.bennett@sibenco.com

p: +61 409 480 840

www.sibenco.com

 [@sibenco](https://twitter.com/sibenco)