MY PASS®

A NEW HORIZON ON TRUST & DATA PRIVACY

Whitepaper 2023/2024

mypassglobal.com

Date of Publication: 05 / 12 / 2023

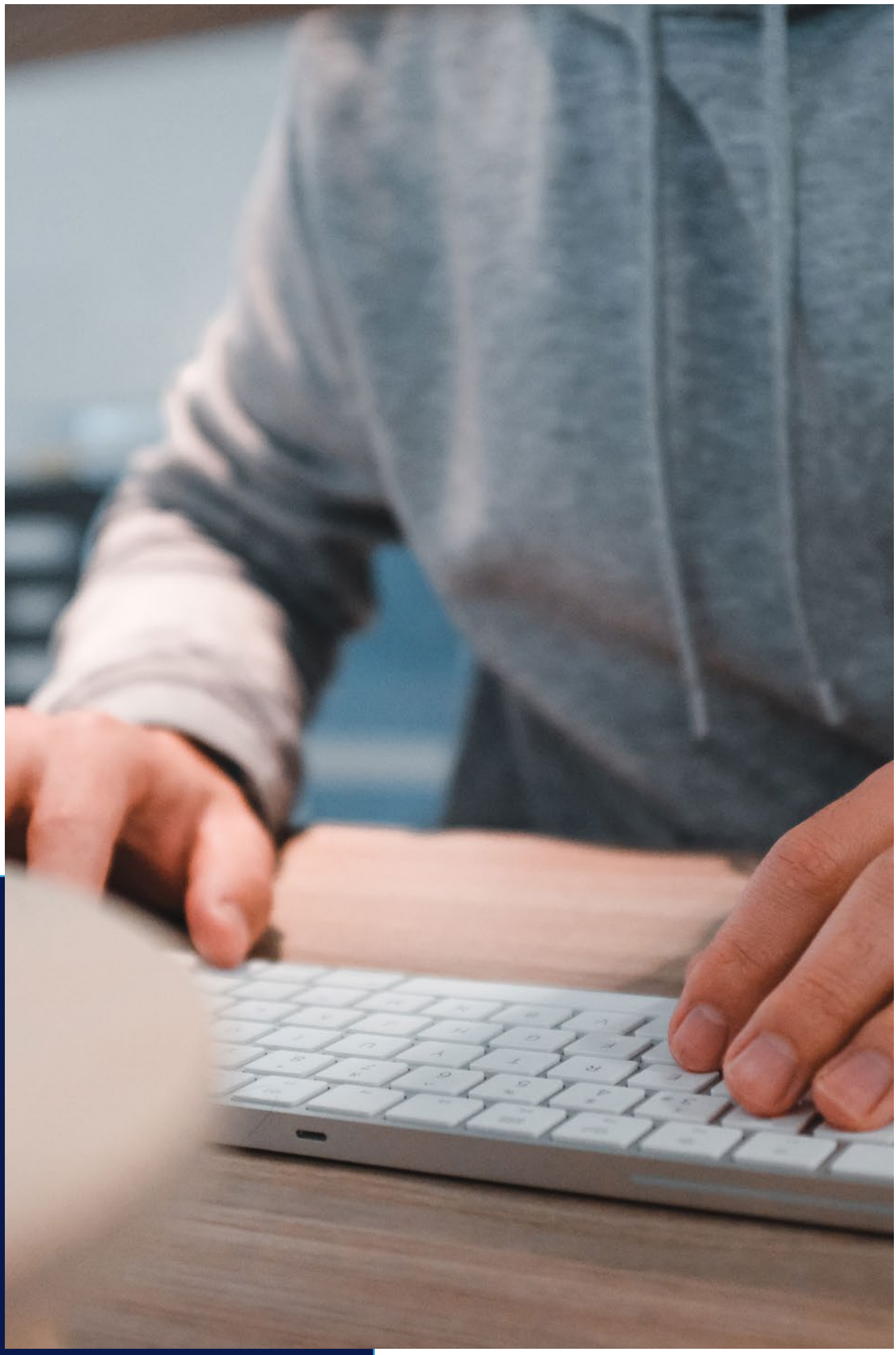
Contact: hello@mypassglobal.com

Address: 32/152 St Georges Terrace,
Perth, WA, 6000

CONTENTS

”

Australia now imposes some of the most severe financial penalties for data privacy violation in the world.



01/ Introduction

Our whitepaper is for:

- Anyone interested in data protection, cyber security or the changing data privacy landscape
- Operational leaders
- Executives at organisations with large contracting workforces

What you'll learn

- Past, present and future of data privacy in Australia
- The media's influence on public perception
- The social and economic impacts of data breaches
- The MyPass approach
- How to proactively plan for the new privacy reforms

Jason Van
Chief Technology Officer, MyPass

Jason has been addressing complex challenges with innovative technology for thirty years, including time at the federal government and twenty years in commercial enterprises.

Since the 1990s, Jason has focused his career on thinking about what privacy means for an individual, and what people need out of the systems they interact with. He has brought a wide array of products to market, from design all the way through to inception, and the systems he has engineered have all had a strong emphasis on the protection of the individual's privacy against the evolving backdrop of regulations in Australia and around the world.

02/ The Current State of Data Privacy

In the digital age, cyber security is a concern that directly impacts the daily lives of Australian citizens. Australia is a prime target for cyber criminals, with millions of Australians experiencing breaches of personal data in recent years (Department of Home Affairs, 2023). As emerging technologies continue to reshape our digital environment, the stakes in safeguarding our people and businesses have reached unprecedented heights.

There is currently a junction of conflicting regulation whereby companies are forced to find balance. On one side, modern laws like GDPR (General Data Protection Regulation) are championing individual control over personal data. However, there are still reactive policies designed for data retention that require companies to store consumer data for up to 30 years. This tension between individual privacy and regulatory compliance has become a high-stakes balancing act that keeps managers, executives, and boards on their toes.

Amid changing legislation and heightened public awareness, how does a company navigate these conflicting imperatives?

At MyPass, we've taken a proactive approach to find balance in this complex regulatory environment. This whitepaper shares a viewpoint on this critical balancing act, with a focus on the challenges and strategies relevant to the Australian landscape.

We will explore privacy in an ecosystem that demands more personal data than ever before - data that must be both safeguarded for individual privacy and stored long-term for compliance. We will provide key insights and examples that have shaped the current state of affairs. We will also outline MyPass' ongoing strategies that have guided our approach to privacy and data retention over the years and into the future.

03/ Year 2022: the 'Line in the Sand'

The old landscape: The risk of the past and the (lack of) measures to protect us

Before 2022, data privacy in Australia was shaped by a lack of strict oversight and accountability. News outlets didn't report on weak measures with the intent to publicly shame, so the business community didn't suffer pressure or urgency to enhance their protocols. The Office of the Information Commissioner wasn't adequately resourced to investigate and publicise privacy breaches, which only added to the lax attitudes. The results were a lack of transparency and accountability that left consumers in the dark about the extent of breaches affecting them.

Penalties were lenient compared with other forms of commercial non-compliance. Knowing that the financial repercussions would be minimal meant organisations weren't motivated to prioritise data privacy.

In November 2022, the Australian government passed an updated Privacy Penalty bill [or Privacy Legislation Amendment] that increased the maximum penalties for serious or repeated privacy breaches from $2.22 million to $50 million. **With the passage of this bill, Australia now imposes some of the most severe financial penalties for data privacy violation in the world.**

The role of the media and the change in public perception

Recent high-profile cases of leaked data and cyber attacks received an uproar of public attention, showing that these issues will no longer be swept under the rug. Recent attacks indicate an escalation, not just in scale but in ambition. Historical breaches were discreet, but the new wave of attacks have evolved to be more hostile and involve hefty ransoms. Now in 2023, 24% of all breaches involve ransomware—maliciously encrypting data and demanding a ransom to return or unlock it.

No longer a brief mention in a newspaper, contemporary media takes an active role in scrutinising these attacks. Journalists investigate compromised data and explore the ramifications for the general public. With the additional implementation of government issued digital IDs, we're now at a tipping point where the dynamics of data breaches, public scrutiny, and corporate accountability are shifting. Businesses and regulators alike need to adapt to this new landscape where cyber threats are escalating, and public scrutiny is intensifying. Ignoring this reality will only lead to harsher consequences down the road. The genie is out of the bottle, and there's no putting it back.

> The Department of Home Affairs' current "pay no ransom" stance might deter some, but history tells us that cyber-attackers adapt and evolve, they don't just disappear.
> - Jason Van

04/ The Future of Data Privacy in Australia

Privacy regulations in Australia

In 2021, a proposed amendment (Dreyfus 2022) was brought before the Senate to increase privacy penalties to a not-so-insignificant $10 million, but it didn't gain traction. Over the next year, following three very public privacy incidents, there would be a stark shift, with penalties of $50 million AUD readily accepted by 2022. Interestingly, even as penalties surged, there was little resistance. Instead, the sentiment was acceptance coupled with a lack of clarity, leaving businesses unsure how to comply.

And more changes are coming...

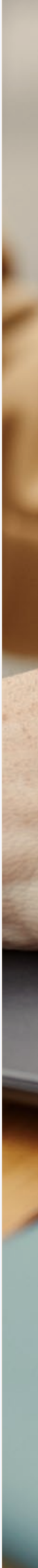
The Attorney-General released the Privacy Act Review Report in February 2023, as a formal review of the Privacy Act (1988). In September 2023, the government released its response to the Privacy Act Review Report (Attorney-General's Department 2023) agreeing to most of the recommendations. Many reforms are expected to start rolling out in 2024. The Australian government recognises that cyber attacks are accelerating, with malicious activity targeting Australians growing faster than ever before. The 2023-2030 Australian Cyber Security Strategy outlines the urgency for change, with a strategic plan to mitigate risks and increase resilience within this scope (Australian Government Department of Home Affairs, 2023). The Department of Finance is now managing the Trusted Digital ID Framework (TDIF) that seeks to provide a uniform framework across those organisations creating and managing digital identities. Integral to the strategy is the development of new laws and voluntary codes to support technology that is 'secure-by-design' (Tech Council of Australia 2023).

Steps to consider:

There are proactive steps your company can take ahead of the Privacy Act reforms, such as implementing robust data governance processes and controls (Rountree et al. 2023).

Suggested actions

1. Know your existing suite of privacy documentation
2. Assess your data governance frameworks managing the collection and use of information
3. Understand your consent frameworks
4. Identify usage of technical data not currently captured in privacy frameworks
5. Implement governance over automated decision-making processes
6. Prepare for operational impact of individual rights, including on systems and procurement
7. Review or implement data retention and destruction frameworks
8. Implement Privacy Impact Assessments for high-risk activities



05/ The Social and Economic Implications of Data Privacy

The government now calculates the cost that privacy breaches pose to taxpayers and the wider community (Office of the Australian Information Commissioner 2023). While 95% of data breaches are financially motivated, the social impact is significant. There have been cases of businesses compensating for the societal problems they have contributed to, such as identity theft, weaknesses in our healthcare systems and even national security concerns.

The cost of cyber crime on Australian businesses is growing by 14% per annum (Australian Signals Directorate, 2023). One recent high-profile example saw the offending company reimburse its customers for the cost of replacing their ID documentation - a costly exercise all round.

For individuals, leaked personal data, identity theft and financial scams can have severe and long-lasting consequences. For companies, the expanding net of regulations have real-world implications, including higher costs, increased training, enhanced support structures, and complex processes.

As individuals with data, and as citizens in our world, we know the importance of protecting our data in the face of technological advancements and threats. As organisations, we shoulder the burdens related to these increased costs, but we can also be at the forefront of making these changes for the right reasons.

”

It’s in everyone’s interest to ensure that compliance isn’t driven purely by the fear of penalties, but also by a genuine desire for a more private digital world.

06/ Privacy Reimagined

In recent years, leading tech companies like Apple have demonstrated that prioritising privacy isn't just a moral stance; it's a viable commercial strategy. The trajectory is clear: privacy management is permanently tightening. With increased regulatory scrutiny and public awareness, a structured approach to privacy is becoming the new normal.

The MyPass way

MyPass stands for the democratisation of personal data. We believe it's the imperative of an individual to own their data and choose who can access it. MyPass' Skills Passport is a first-in-kind solution that offers bottom-up data ownership. The benefits of this include self-determination for workers, but also real-time visibility and a drop in administrative costs for the companies they work for.
Industry is increasingly turning to a single source of truth dataset, and a collaborative industry standard to manage the safety and compliance of workers.

"Approximately 25% of the Australian Energy and Resources sector trusts MyPass to ensure the right workers with the right skills are performing their tasks on site, and this figure is growing daily."

Rigorous IT security and data privacy processes

MyPass has held the ISO 27001 certification since 2018 and is audited annually by an independent certification body. We have implemented a comprehensive set of security controls, including risk assessment and treatment, asset management, human resources security, access control, and operations security. MyPass focuses on continuous improvement, employee training and awareness, third-party risk management, security metrics and reporting, and regular security audits and assessments. Our privacy model and secure architecture are built to reduce exposure to potential data breaches and associated cyber crime.

At the core of the MyPass philosophy is something we call "opt-in privacy by design." With GDPR legislation reinforcing the expectation of individually owned and controlled data, the burden of regular re-permissions and manual updates falls on those maintaining personal data. Our technology complies in full with GDPR and similar models. This will become increasingly vital as we integrate with other ecosystems like Australia's Digital Identity Framework and the Digital Transformation Agency. MyPass leads the way in safeguarding the privacy of personal information. Our ISMS is our "licence to operate," not just a box-ticking exercise. MyPass is passionately building a reputation around the way we do business and our responsibility towards Information Security.

MyPass keeps data more secure than traditional systems

Traditional workforce compliance management typically involves sharing PI and PII via email. Generally, this information is then stored in unsecure locations like shared drives, spreadsheets and in data silos. This approach puts organisations at risk of serious privacy and data breaches, not to mention the administrative effort involved in maintaining worker records. In contrast, MyPass' user-owned data model is 'privacy by design.' Individuals own and manage their personal data in their digital Skills Passport. They can then share access to their profile with employers and registered training organisations via a permission structure, giving them heightened visibility and control.

Extra security features in MyPass

- Role-based access helps to keep data safe
- 'Sensitive' certification status to prevent the file being viewed or downloaded by anyone without the correct permissions
- Search constraints designed to prevent any form of worker poaching between companies using MyPass
- To discourage password sharing, MyPass has not capped your number of administration users
- Back-up and recovery capabilities
- Support model and SLAs
- Security and privacy protocols (PD/SPD, data encryption)
- Secure sharing methods, both peer-to-peer and between individuals and organisation

Transparency through bi-annual publications

MyPass publishes bi-annual reports on our cybersecurity outcomes. These reports coincide with our annual ISO27001 audits and aim to offer transparent insights into our cybersecurity and privacy performance. This reduces the operational burden for our customers who currently spend significant time completing bespoke cybersecurity documentation. By taking these proactive steps, we offer a clear, transparent, and secure approach to managing cybersecurity and privacy.

The buck stops here

MyPass is a win-win for individuals and businesses alike. Our Skills Passport provides a democratic framework for individuals to control, manage and share their own data, with the peace of mind that their data is managed securely. Connected organisations have access to real-time and verified worker compliance data, but don't bear the responsibility to keep it safe - that's on MyPass.

And finally, privacy isn't just a compliance requirement; it's a commitment to safeguarding the identities and data of everyone who interacts with MyPass. For that reason, MyPass does not sell or share data with third party companies and this will not change, you have our word.

07/ The Official MyPass Position

We have witnessed the evolution from the lax regulatory environment to one marked by penalties and public attention. MyPass, with its commitment to 'privacy by design' and robust adherence to international standards, holds a proactive stance in this evolving domain.

As we look to the future, it's clear that the conversation around data privacy is far from over. Upcoming reforms and tech advancements will continue to shape this landscape, making it vital for companies to stay agile and informed.

Our commitment at MyPass is unwavering: to uphold the highest standards of data privacy and security, ensuring that personal data remains in the hands of its rightful owner - the individual. In doing so, we are not just complying with regulations; we are fostering a culture of trust and responsibility, essential for the digital age.

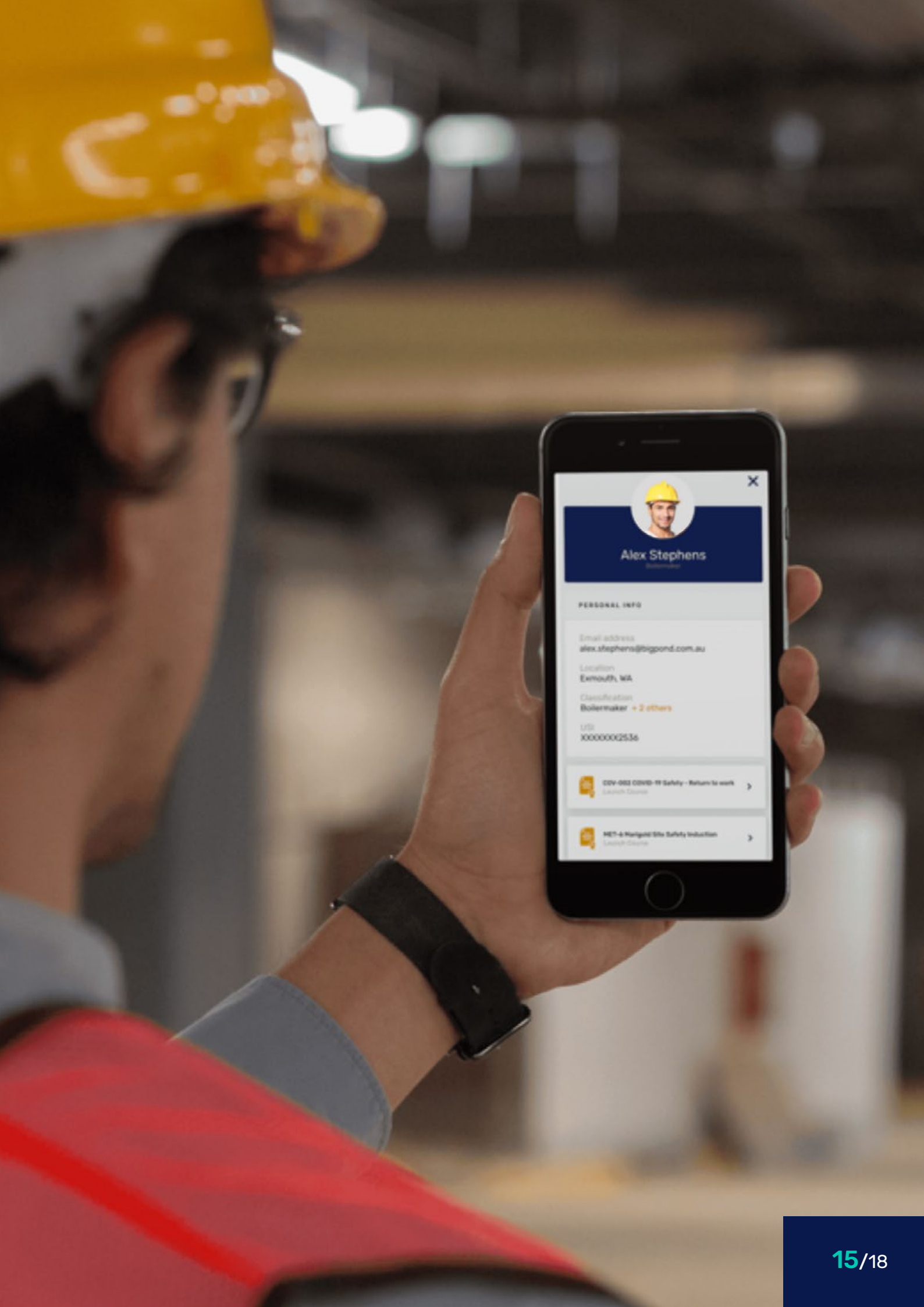
As we move forward, let us all maintain that the safeguarding of personal data is not just a legal requirement but a fundamental aspect of respecting individual rights and fostering a secure, transparent, and ethical digital ecosystem.

"At MyPass we are acutely aware of our responsibility to protect the personal information stored within our industry platform. Our clients and users trust us, and rely upon our commitment to Information Security.

"This isn't just an approach to reducing risk for our users- in fact, protecting information and data is our 'licence to operate' as a business."

Matthew Smith

Chief Executive Officer


Alex Stephens
PERSONAL INFO
Email address
alex.stephens@bigpond.com.au
Location
Exmouth, WA
Classification
Boilermaker + 2 others
USI
XXXXXX2536

08/ References

Attorney-General's Department 2023, Review of the Privacy Act 1988, Australian Government, viewed 25 October 2023, https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988

Australian Signals Directorate 2023, ASD Cyber Threat Report 2022-2023, Australian Government, Canberra, https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

Department of Home Affairs 2023, Australian Cyber Security Strategy, Australian Government, viewed 23 November 2023, https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

Dreyfus, M. 2022, Parliament approves Government's privacy penalty bill, media release, Attorney General's Department, 28 November, viewed 25 October 2023, https://ministers.ag.gov.au/media-centre/parliament-approves-governments-privacy-penalty-bill-28-11-2022#

Office of the Australian Information Commissioner 2023, Chapter 7: Civil penalties — serious or repeated interference with privacy and other penalty provisions, Australian Government, viewed 25 October 2023, https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-7-privacy-assessments

Rountree, D. Guyot, I. Tan, F. Boudsocq, F. Sheppard, L. 2023, 'Federal Government signals broad support for significant Privacy Act reforms', Allens, viewed 25 October 2023, https://www.allens.com.au/insights-news/insights/2023/10/federal-government-signals-broad-support-for-significant-privacy-act-reforms/#anchor2

Tech Council of Australia 2023, New Cyber Security Strategy Sets Australia On The Right Path To 2030, media release, Canberra, 22 November, https://techcouncil.com.au/newsroom/new-cyber-security-strategy-sets-australia-on-the-right-path-to-2030/

Verizon 2023, Data Breach Investigations Report, viewed 23 November 2023, https://www.verizon.com/business/resources/infographics/2023-dbir-infographic.pdf

This page is intentionally left blank.

mypassglobal.com