



**4 August 2023**

**To:** Technology Strategy Branch

**Email:** [DigitalEconomy@industry.gov.au](mailto:DigitalEconomy@industry.gov.au)

## Safe and Responsible AI in Australia: Response to discussion paper

1. KomplyAi® welcomes the opportunity to provide feedback to the Minister for Industry and Science, the Hon Ed Husic MP, on his discussion paper [Safe and Responsible AI in Australia](#) which aims to understand further regulatory and governance responses to maximise artificial intelligence (AI) opportunities while protecting Australians.
2. By seeking community-wide feedback, the paper is an important step towards an effective and proportionate regulatory approach, building on the valuable work of various regulatory bodies including the eSafety Commissioner, the Responsible AI Network (**RAIN**) and the NSW AI Committee. Please find our responses to the paper's questions below.
3. We have included a definition section and further information about AI at the end of our submission for explanatory guidance. We have also included a number of annexes **attached** which provide a greater level of detail about global laws intersecting with AI.

### **ABOUT KOMPLYAI**

4. KomplyAi is an Australian based, owned and operated technology start up supporting the rapid and safe adoption of AI technologies through an innovative governance, risk and compliance (**GRC**) platform, and the development of other micro tools in AI education. KomplyAi was formally founded in 2022 in Australia to solve the global shortage of AI compliance solutions with the aim to better democratise access to AI knowledge and tool-age.

**We are on a mission to ensure AI is always built to the highest ethical and responsible standards.**

5. We have been undertaking research into AI technologies and global laws intersecting with AI in higher risk verticals for a number of years. KomplyAi is a member of the U.S. Massachusetts Institute of Technology's Computer Science and AI Laboratory Start-up Connect Plus Program, in the Machine Learning & AI category. Currently, KomplyAi has been approved as the sole Australian technology company in the category of "AI GRC", for inclusion in the global Ethical AI Database alliance, and the global Catalogue of AI Tools & Metrics by Organisation for Economic Co-Operation & Development ('**OECD.AI**').
6. **Our risk assessment tools, and compliance documents were developed with AI experts from around the globe**, amongst others, Australia's Gradient Institute, a recognised leader in responsible AI, and an inaugural member of the Australian Government's Responsible AI Network.
7. Currently, we understand that we are the only Australian technology company in GRC providing an enterprise level platform solely targeting AI technologies.
8. **KomplyAi aims to contribute to this process for feedback by supporting with our expertise in AI and GRC and our 'front line' experience in developing technologies in this field. We are uniquely positioned to support the Government's investigation of these issues, and any ongoing piloting exercises.**
9. KomplyAi's founder, Kristen Migliorini, has also been a deep technology lawyer and intellectual property litigator, for over two decades, engaged in risk and compliance activities, and technology development, in a number of senior inhouse legal roles, including for a top 4 bank and G08 university. **Previously, Migliorini was involved with DFAT and the Department of Defence in the development of dual use technology and sanctions legislative drafting, and higher education, sector wide compliance tool-age.** She further undertook sponsored sector research about whether or not Australia would be put in a disadvantageous position vis-à-vis global counterparts such as the U.S., in areas such as quantum computing, as it related to the proposed legislative reforms on controls of intangible transfers of dual use technologies. With a particular focus on the treatment of fundamental research and development and statutory exclusions to those activities.
10. Migliorini's experience in deep technologies, her **engagement as part of extensive industry piloting for earlier proposals for the Defence Trade Controls laws, and the permitting system and controls, that were advocated for, and resulted, provide some useful experience here.** Some analogous positions to the debate on safe and responsible AI. **Particularly the intersections with the use of AI in dual use technologies, potential nefarious uses of this technology, and intangible transfers of those technologies across international borders<sup>1</sup>. Managing risk in an increasingly globalised world.**

---

<sup>1</sup> Kristen Migliorini, 'Artificial Intelligence (Ai)—An Australian Perspective' (2021) LVI(No. 3) *les Nouvelles - Journal of the Licensing Executives Society*.

## EXECUTIVE SUMMARY

Our position on how Australia should tackle the challenges of AI has become more nuanced since we first wrote about these policy issues under the previous Government's AI framework. That's for two main reasons: **(1) the advent of more sophisticated foundation models being deployed on market, and the downstream flooding of generative AI tools being deployed globally, agnostically, and on mass; and (2) forming deeper experience in developing AI compliance technologies and better understanding the downstream impact of impending global laws on organisations.** We have greater technical insights to some of the common pitfalls, and 'front line' experience, and visibility about how **businesses (of varying sizes and sectors) are dealing with developing and using AI, including as their activities intersect with an impending legal regime, such as the European Union AI Act.**

Our original policy focus was on the importance of global interoperability and parity with overseas countries because of the extraterritorial application of laws in AI from some regions such as the European Union. **However, as we more closely consider global laws, Australia's unique position vis-à-vis AI, we believe that there is a different way; a way that represents coherence with responsible AI, and global harmonisation efforts largely in respect to alignment on prohibited AI activities.**

**Australia has the opportunity to do things differently here and come out on top. At the same time, ensure that it is not a testing ground for AI that has serious public consequences that will be difficult to wind back.**

Of note, we recommend that **Australia take a different approach to narrower use case determinations of higher risk activities intersecting with AI, and introduce a "technology passport," an accreditation or licensing regime. This would be attached to prescribed organisations' developing, procuring, deploying, or exporting AI.** Into the future, other emerging forms of technology, can be anticipated under this regime.

We believe that this could **better enable technology fluidity, neutrality, and create fewer barriers that unnaturally confines AI, and its multiple layers and intersections with other emerging forms of technology, to sectors, activity types, and a level of proscription, that should rather be connected to fundamental baseline corporate governance requirements, that better address issues of public safety.**

**The focus is not on the level of risk that the technology may create based on ever changing use cases, but creating a system for companies to facilitate a competitive safety advantage that would better foster customer up-take.** Risk classification systems and prescribed high risk determination based on use cases may create artificial and inherent consumer distrust, and subsequent business hesitancy to innovate in those use cases. **Government intervention could rather form as an incentive for good corporate governance in data privacy, cyber security, risk and quality management etc. and better promote safe innovation and trust.**

In our view, **Australia does not have the administrative resources currently to facilitate a legislative regime in AI matching the scale and pace of changes to the technology**

**landscape that would be required by a product based approach. A regime that is ill equipped to deal with these changes at pace, and to curb market behaviours that present real harm, is not good for anyone.** Traditional forms of technology and supporting Government and agency administrative infrastructure are diametrically different to AI and what we are seeing in market now. Arguably, the legal assessment of whether an organisation has met its licensing requirements or conditions largely based on baseline requirements of good corporate governance may also better facilitate Australia's immediate resourcing impediments.

There would, however, be **clear licensing exclusions for certain categories, such as start-ups and SMEs, that meet specific safety criterion, and are not otherwise involved in prohibited AI activities.** In our experience, start-ups and SMEs that are not well funded or positioned with in house technical capabilities across a wide breadth of areas (cyber, data privacy, responsible AI, IP), will not be in a position to meet some of the more robust compliance obligations under the EU AI Act.

**A start-up or SME company could still choose whether or not it voluntarily complies with the aforementioned regime (much like privacy laws).** Where it does, they could be **provided Government funding support, and further economic incentives such as priority co-development opportunities in Government procurement and access to those contracts, or other expediated programs that provide a tangible economic incentive to good, safety behaviours.** However, this will also be largely driven by the insurance companies, and their requirements to support indemnification of start-ups and SMEs in AI, under their insurance policies' requirements.

Australia should also closely consider some of the **exemptions that are being finalised in the European Union for two key areas: (1) research and development activities that are non-prejudicial to commercial activities; and (2) the treatment of collaborative development of open source AI components and placing them in open repositories**<sup>2</sup>. The complexities that are being explored in R&D, open source and the treatment of the open source ecosystem, including as it intersects with the build and testing of foundation models, should be a key area of focus for the Government.

**We want to ensure that Australia is not put in a disadvantageous position in this respect, and create further competition barriers for smaller players.** We have some existing useful frameworks for management of these areas in Australia.

We also support **legislative intervention in the form of mandatory and public reporting of AI harm. Commencing, the central aggregation of this data, to better enable preventive data analysis that will lead to fewer societal harms.**

We advocate for these changes to be in a principal piece of AI legislation. We also implore the Government to take a **holistic and cross departmental approach to AI, and its intersections with other forms of existing legislation that are arguably misaligned with AI and other emerging technologies, and present legal uncertainties. Amongst others, intellectual**

---

<sup>2</sup> Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts [2021], art 2(5d).

**property, anti-discrimination, data privacy and consumer and competition laws.** Our submission focuses on the treatment of changes to IP laws.

**Finally, we have an opportunity as a sovereign nation to determine how we shape our future as it intersects with novel and emerging technologies, and we must take that responsibility seriously.** There are obvious and well researched significant economic benefits that AI can generate, that we need to take advantage of<sup>3</sup>. However, there are certain AI activities where the outcomes of those activities do not have a place in Australian society. We advocate for strong and clear prohibitions on certain types of AI activities. We set those out in **Annexure C.**

We explain how we could do things differently in Australia and achieve this goal.

1. 'Front line' observations about AI compliance impact on Australian businesses
11. **KomplyAi's current technology supports organisations based on the most up-to-date international frameworks for responsible AI, such as the OECD and the U.S. NIST.** We have also developed a risk rating system, and a supporting intelligent workflow engine as part of our technology to aid organisations to comply with the requirements of the impending draft European Union AI Act. For example, to undertake and automatically generate the governance artefacts required under those draft laws. We have undertaken research with responsible AI experts to determine the technical meaning of those requirements, and the practical application of how organisations may comply with them.
12. From a practical point of view, this has provided KomplyAi with invaluable insights to those draft laws, such as potential compliance burden, and costings, and the required level and breadth of expertise for resourcing such adherence. **Providing insight, for example, to the much debated question of whether or not those required governance structures and risk mitigations may in fact hinder the growth and prospering of AI innovation.**
13. So far, based on our research and testing while building out our technologies, we believe that well-funded medium, to growth, and large enterprise, companies, particularly those with existing in house expertise, won't be significantly impacted by changes akin to the European AI Act, i.e., from an overall compliance costing perspective. With the technologies that are emerging (and aided by in house capacities), many of these organisations are well placed in GRC, and with levels of automation in governance technologies into the future, that will create extreme efficiencies. We are already building these. Those versed in intersecting areas of data privacy and cyber security, existing models for quality, risk and data assessments and assurances, will likely adapt well.

---

<sup>3</sup> Michael Chui et al, The economic potential of generative AI: The next productivity frontier, (Report, McKinsey & Company, 14 June 2023).

14. Despite AI technologies (in particular foundation models) that require a different approach and where there are quite novel risks (some unknown), the required evaluations are not insurmountable. Many requirements, in any event, draw upon usual and good practice for technology builds, in conceptualisation, development and testing (e.g., technical documentation generation, such as instructions for use, risk and quality management plans, and data management plans etc.) and are part of a well-funded organisations' normal risk mitigations when developing, sourcing or using technologies. **In any event, to understand how AI systems works it is necessary to have sufficient documentation, most importantly how the model was trained.** We are of the strong view that these assessments, in time, will and should become part of an organisations' technology hygiene, like data privacy and cyber security.
15. However, our initial observations are that for start-ups and SMEs, in the immediate future, particularly those where there is no technical founder, and little in house expertise in AI, other than a level of experimentation, and outsourcing of it, the **costs involved in engaging the human expertise for the level of evaluations required under the draft European AI Act, are likely cost prohibitive and out-of-reach for this category.** Instructively, the draft European AI Act, has made some key allowances for start-ups and SMEs for their compliance, and other priority access to regulatory sandboxes, and reduced regulatory penalties. We don't have data to make determinative observations about how that will alleviate start-up and SME burden. It may greatly assist. Deploying and using a system like ours, which dramatically expedites this process, and reduces costs, greatly assist this category. However, there are likely other ways to address this category within Australia that the Government should explore.
16. **The impact on this category of start-ups and SMEs is notably** further exacerbated by our national skills shortages in these technical areas of AI in Australia and the **extremely** high costs involved in engaging with specialists in this market. **In our experience, AI expert consultants, in responsible AI, and whom we have engaged with cost anywhere between \$650.00 to \$2,500 AUD per hour and upwards. The engagement of these experts and the breadth of skills required to comply for smaller business is at this present time prohibitive and likely seriously impactful for innovators within our country.** Potentially serving as another means of market dominance for the large players that are well placed to bear new compliance costs.
17. **We believe it is imperative for Australia to think differently about how we address these AI challenges for smaller players in our country.** Notably, KomplyAi would be happy to provide the Government with access to our platform to better understand the breadth of expertise required in this area of evaluation and testing, and its intersection with smaller business. **Providing useful data about how to address these very real challenges of ensuring that smaller players are not disproportionately impacted by any AI changes in law.**

## 2. The AI landscape has changed

18. The **AI landscape has *significantly changed* since at least 30 November 2022**, with the release of OpenAI's ChatGPT, an AI chatbot application based on the initial large language model GPT-3.5, and the global AI race that has ensued. Today, companies, and individuals in their millions are relying on generative AI tools to create human level text, images, videos and audio at a scale that is unprecedented.

### 3. Government intervention is required

19. **We strongly believe that Government *inaction* in AI could result in *disproportionately negative consequences* for Australia. Government intervention is required to address the tangible and intangible harm of AI.** That intervention should take a more *holistic approach* to maximising AI opportunities while protecting Australians. Obviously one weapon in its *intervention arsenal* is the introduction of new legislation. **To use a form of legislative intervention as a means of better elevating safe innovation in Australia is strongly advocated for here in our submission.** It is required in the form of a principal piece of legislation that governs AI. **Non regulatory, ethical AI principles have been globally ineffective, and the commentary around those principles generally unpersuasive to the market<sup>4</sup>.** We note that KomplyAi has advocated for Government intervention in the form of principal AI legislation since the previous Coalition Government released a paper on AI in early 2022.
20. **Our research (*including the curation of data repositories of relevant global laws intersecting with AI in high risk vertical sectors*) has shown there are many existing laws that talk to AI.** There are some obvious existing laws that require more immediate attention to better facilitate AI research and innovation, and ensure safety. We cite a number of those below, including the importance of ensuring our intellectual property laws<sup>5</sup> are brought in line with modern technologies and are up-to-date.
21. **Generally speaking, we believe a risk based and proportionate response to AI is appropriate.** Australia should also take this as an opportunity to elevate innovation in AI in this country, and truly prioritise its public benefits. **Australia should focus on distinguishing AI harms that have occurred, from those that we suspect may occur (existential harms), but allowing malleability for the latter to be readily addressed<sup>6</sup>.**

### 4. AI harm data is lacking but AI legislation could address this

---

<sup>4</sup> Kristen Migliorini, 'Artificial Intelligence (AI)—An Australian Perspective' (2021) LVI(No. 3) *les Nouvelles - Journal of the Licensing Executives Society*, 184, 188.

<sup>5</sup> *Copyright Act 1968* (Cth), *Patents Act 1990* (Cth).

<sup>6</sup> Researchers at the Center for Security and Emerging Technology report state that: "tracking efforts by AIIIS and AIAAIC suggest that the number of harms experienced in relation to AI systems has grown rapidly over the past 5-10 years": Mia Hoffmann and Heather Frase, 'Adding Structure to AI Harm', *Center for Security and Emerging Technology* (Issue Brief, July 2023), 6.



22. The form such legislation should take is a vexed issue, arguably requiring more research in view of the fast changing nature of the AI landscape, and the tremendous advances that have recently occurred and will continue to occur. **Analyses of AI harm requires reliable data on harm incidents. However, currently there is no Australian or global and comprehensive public repository of such incident reporting, nor any impetus for an organisation to interpret certain harms as AI harms and publicly report them**<sup>7</sup>. Monitoring and examining AI harms is critical to mitigating those harms, including to provide an improved understanding of the cause of harms, and better *preventative* measures. For example, better understanding emergent AI model abilities that may or may not materialise. **Legislation could be a means of obtaining such data of AI harms by way of reasonable, mandatory disclosures and a public database that is machine readable and readily searchable to the public.** The European Union has proposed this and so too has the Canadian Government in a particular form<sup>8</sup>.
23. In **Annexure A**, we have included information about the European Unions' recently updated risk management requirements for foundation models under the EU AI Act, and undertaken a comparison with those *voluntary actions* that the large U.S. technology companies (Amazon, Anthropic, Google, Inflection, Meta, Microsoft, and OpenAI) have agreed to, under the recent Biden administration announcement<sup>9</sup>.
24. We have also made a further comparison with a recent study undertaken by Stanford University's Centre for Research on Foundation Models (June 2023) about the current status of compliance of some of the key players in the foundation model arena in those areas under the current draft EU AI Act<sup>10</sup>. It's clear based on the Stanford study that further work is required for those companies to ensure compliance under the impending laws. Based on the study there is an absence of open information and documentation that will be required under those laws.

## 5. Australia's approach should be flexible and iterative

25. There are a number of factors clearly supporting the view that Australia's approach to legislating AI should be flexible and iterative. **It is currently impossible to predict every possible use case for AI, and more importantly the highest risk categorisation of AI harm based on a use case model like the European Union**<sup>11</sup>. While the European Union has made recent changes to better accommodate foundation model risks, and ascribed

---

<sup>7</sup> Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts [2021], arts 51, 60, 62.

<sup>8</sup> Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts [2021], arts 51, 60.

<sup>9</sup> White House, FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI, 21 July 2023.

<sup>10</sup> Rishi Bommasani et al, Do Foundation Model Providers Comply with the Draft EU AI Act? (Stanford Center for Research on Foundation Models, 2023).

<sup>11</sup> Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts [2021], art 6.



responsibilities based on an organisation or individuals' role in that AI value chain, we are still in a place of learning. **The intersecting harms based on the advanced level of foundation models, with capabilities that enable them to be adapted, and integrated at scale into countless, third party, downstream AI systems, is not fully known.** The general purpose nature of these foundation models, the financial benefits, and the ongoing accelerated investment to make these models even more capable by large technology companies (and their own self learning capabilities, models teaching models), means this is not an issue of 'hype' that will easily go away.

26. There are many ways flexibility and iteration can be achieved by the Government to ensure an appropriate balance is achieved with AI. **Targeted interim measures addressing the greatest immediate harms to Australians, which may mean the Government looks to enforce the application of existing laws, and its current enforcement powers, and provide better clarification as part of a cross Government taskforce.**<sup>12</sup> These existing laws include data privacy, anti-discrimination, consumer protection, competition, critical infrastructure, cyber security, intellectual property, and defence based laws<sup>13</sup>.
27. In this regard, we emphasise the importance of co-ordination between regulatory authorities. Many key AI risks are not unique to any one industry, vendors may offer products or services into multiple markets and cross-sectoral use cases may emerge. Regulatory co-operation will help mitigate risks of regulatory arbitrage, duplication of rules and unwarranted differences of approach between sectors. **An inconsistent patchwork of laws, application of laws, and enforcement action is the very worst thing that can happen to AI innovation in this country.**
28. Further, we recommend provisioning in an enabling act for an initial **piloting period with key stakeholders**<sup>14</sup>. **This would be followed by a formal review of the legislation within a stated time period, or triggered by a particular future event that may be tied to emergent societal harms.**

## 6. Coherence, not conformity

29. **We strongly agree the Government should be looking for a form of coherence not conformity with global counterparts, based on our differences as a country. Annexure B of this submission sets out a list of global laws and those we agree or disagree with as they relate to constructing Australia's AI framework. We also indicate whether a level of coherence with those laws is required instead.**
30. The sometimes uncomfortable truths as a smaller, thriving, but geographically isolated nation, are that we are currently heavily dependent on IP imports, including as part of

---

<sup>12</sup> FTC, CFPB, EEOC and DOJ, Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems (April 2023).

<sup>13</sup> Federal Trade Commission Act of 1914, Sherman Antitrust Act of 1890, Civil Rights Act of 1964, Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Consumer Product Safety Act of 1972.

<sup>14</sup> Defence Trade Control Act 2012 (Cth), s74A(3).

extremely complicated global AI supply chains. We also have an undersupply of AI skills and talent (particularly for unique testing and evaluation of AI systems in specialist areas), and a clear imbalance in innovation funding (Government and venture) as compared to countries like the U.S., and China<sup>15</sup>. We are also arguably in a **new age of geopolitical instability that should form part of any weighting of views about technologies that can be powerfully used in that context**. AI cyber weaponry, AI deployed in critical infrastructure, and large amounts of compute power provided to unverified end users, need to be high on the Government agenda for Australian consideration<sup>16</sup>. In this regard, we fully support the Government in a more **holistic and co-ordinated regulatory approach to its consideration of laws intersecting with AI**. These areas cannot be viewed in isolation from one another and as siloed activities within Government Departments. **Historically, we do not believe there has been a form of generalised technology that cuts across such a large number of Government Departments, regulators, nor existing areas of the law, at this scale, and with this level of potential societal impact.**

## 7. Embedding coherence into laws

31. **How should coherence be practically implemented? We have undertaken research about the status of global laws, and standards intersecting with AI, and harmonisation efforts. Further, we have considered the important weighting of Australia as a sovereign nation.** Australia's own cultural nuances may be incompatible or irreconcilable with other countries' laws requiring a different approach. For example, is the identification of risk, variously based on models of AI risk characterisation, and prescriptive (or more loosely framed) risk mitigations for those harms, the best way for Australia to regulate<sup>17</sup>? **Is the original European AI regulatory model, which could be said to be**

---

<sup>15</sup> OECD Data, Australia < <https://data.oecd.org/australia.htm> >

<sup>16</sup> An expanded "Know Your Customer" or KYC for AI services such as that proposed by Microsoft, which builds on the same concept used in for high risk financial services, including for cloud operators where AI is being deployed for sensitive uses: Microsoft, Governing AI: A Blueprint for the Future (Report, 25 May 2023), 5-7.

<sup>17</sup> For example, Europe has only recently implemented new rules for foundational models and generative AI systems, which are applicable regardless of whether the systems are deemed high risk or not: Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts [2021], art 28b.

Brazil has proposed a risk based-framework, regulating three levels of risk for AI systems, excessive risk, high risk and non-high risk: Bill No. 2338 of 2023 (On the use of Artificial Intelligence systems) [2023]

China has announced regulations that will be implemented in 2023, governing generative AI and other AI technologies: Cybersecurity Administration of China et al, Interim Measures for the Management of Generative Artificial Intelligence Services [July 2023]; State Internet Information Office Ministry of Industry and Information Technology of the People's Republic of China Order No. 12 of the Ministry of Public Security of the People's Republic of China, Provisions on the Administration of Deep Synthesis of Internet Information Services [November 2022].

Canada has also proposed regulatory measures targeting high-impact AI systems: Artificial Intelligence and Data Act 2022 (Bill C-27, Digital Charter Implementation Act 2022)

**singularly focused on product safety mechanisms, flexible enough to accommodate new forms of powerful emerging AI technology (or significantly more advanced forms of existing technology)?** Annexure D of this submission sets out those use cases that are considered to be high risk under the EU AI Act, and a comparison to Canada's Bill C 27 where high impact AI systems are determined by way of an assessment of a number of useful criterion.

## 8. Prohibited AI activities

32. **Firstly, we strongly advocate for a *prohibition section* not unlike the EU AI Act that focuses on the negative and reprehensible outcomes of AI on end users; members of the public, such as children, the elderly, marginalised and more vulnerable users.** We have a strong history in Australia of legislating in this manner, and ensuring safety of end users, and in particular more vulnerable users, in a technology neutral setting. We are a trusted country for innovation. There are global debates about whether such prohibition is anti-innovation and a deterrent to international investment in Australia. We don't agree.
33. **In fact, we believe prohibition will attract the best innovators to our country and within, spurred on by a vibrant consumer base and buoying market that trusts AI products and sees their inherent value.** In the discourse of public debate, the factual truths of these issues is sometimes lost under the weight of hype. In our strong view, the **current EU approach and the explanatory information citing example use cases, is arguably clear in its intent to prohibit AI activities that are on the absolute *highest end of impacting users' fundamental human rights, health and safety***<sup>18</sup>. We believe

---

<sup>18</sup> Latest technological advances include new sensors capturing bio signals and the development of brain-computing interfaces which translate brain activity into machine readable input. These technologies are potentially highly intrusive, allowing for detection of thought or intent and possibly influencing the operation of the human brain.

For example, a Spanish supermarket chain has implemented a facial recognition system to detect people with restraining orders and to prevent them from entering the shop. The supermarket's CCTV collects facial images of customers entering a shop, and the software creates biometric templates, which are then compared with the templates of persons that are not allowed to enter the premises. Another example is facial recognition that is used to record the working hours of employees at construction sites.

In the U.S., the National Center for Border Security and Immigration (BORDERS), a United States Department of Homeland Security Center of Excellence has developed an Automated Virtual Agent for Truth Assessment in Real-time (AVATAR). This system conducts fully automated interviews at the border during which it analyses a traveller's nonverbal and verbal behaviour, such as eye movement, gestures and pitch. The AVATAR then rates the person's credibility and sends the result to a border control officer. In collaboration with EU's border agency FRONTEX, the system was also tested at the airport in Bucharest. The use of these biometric deception detection systems is highly contested, as they are not based on sound science but rather on a chain of assumptions about the relationship between biometric indicators and internal intentions.

However, biometric techniques and AI are also used for controversial medical purposes. In a recent U.S. experiment, social media photos were analysed, using algorithmic facial recognition, metadata components and colour analysis to identify predictive markers of depression.

there are AI activities that do not currently have a place in Australian society and are a cause of great concern. **We do not need to be the testing ground for these types of technologies that are currently and will be prohibited in other likeminded countries.**

34. For example, the prohibition on ***subliminal techniques*** at **Article 5(1)(a)**:

***Subliminal techniques (covert or manipulative methods, with the objective to greatly influence, by impairing, abilities to make informed decisions)***

*"The placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective to or the effect of materially distorting a person's or a group of persons behaviour by appreciably impairing the person's ability to make an informed decision, thereby causing the person to take a decision they would not have taken or otherwise in a manner that causes or is likely to cause that person, another person or group of persons significant harm<sup>19</sup>".*

35. In **Annexure C** of this submission, we set out the currently proposed wording in the EU AI Act and we provide some examples of those activities in real life scenarios. **We are of the strong view that there isn't a place for those prohibited AI activities in our Australian society, and there should be a discussion about where our national lines are drawn, for reasons of public safety.** When we talk about public safety, we do not simply mean tangible harm that is physical or observable damage, but also intangible harms that cannot generally be observed, including those that may not be readily observable at this point in time and in more vulnerable demographics such as our children (e.g., resulting mental or psychological harm caused by AI over-reliance and algorithmic nudges).

## 9. Australia, doing things differently

36. Australia can learn from first movers overseas such as the European Union and its draft impending laws, including the very recent changes that were required to be made to better accommodate foundation models. This has laid an excellent and ground-breaking foundation for the rest of the world in Responsible AI. However, the political landscape of the European Union and its somewhat complicated legal system, including the entirety of

---

In the edtech sector, in China there have also been reports concerning the use of facial recognition software in Chinese Schools that monitors the students' behaviour and gives the teachers feedback on the students' concentration levels.

Christiane Wenderhorst and Yannic Duller, Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces (Study, European Parliament, August 2021).

<sup>19</sup> Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts [2021], art 5(1)(a).

the *New Legislative Framework*<sup>20</sup> supporting the AI ecosystem, and the prominence of political compromises, may not be representative of the best way for Australia.

37. Accordingly, **there are a number of areas where we propose coherence, but not conformity with impending global laws, such as the seminal European Union AI Act.** We understand that the European laws will apply extraterritorially, and enterprise in Australia with global operations are electing to comply with the EU for administrative efficiencies and as a more practical and immediate way of ensuring safe AI and preventing reputational risk. However, we have also included some proposals in our submission that would be currently unique to Australia. Constituting a level of coherence based on achieving the same objectives in responsible AI. **We have prepared a diagram below to illustrate our proposal (Annexure G).**

## 10. A “digital technology passport”

38. There are many reasons why a static use case approach to rating AI risk is challenging for Australia. For example, the fast moving pace of this technology, the complicated layering of hardware, software and open source as part of AI systems, including those that are of general application. The increasing confluence of fields of technology (such as AI and our heavily invested quantum computing industry), and the real challenges of multi-contributor supply chains to components of AI systems, and allocation of liability, which Australia is arguably at the end of. **However, there are strong foundations for Australia to be a leader in responsible AI.**

---

<sup>20</sup> The New Legislative Framework consists of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation [2008] OJ L 218, Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC [2008] OJ L 218 and Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 [2019].

Other relevant laws supporting the EU’s AI ecosystem include:

1. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277
2. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265
3. Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) [2022]
4. Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC [2023] OJ L 135.

39. Organisational level accreditation, or a form of organisation specific licensing (not unlike many already in existence in Australia) could be introduced to better promote emerging technologies, including AI, and promote us to leading in this area.
40. **We recommend creation of a digital “Technology Passport” with the ultimate aim of promoting competitive safety and engendering a form of fluidity, technology neutrality, and self-certification (with some key exclusions).** The focus should not be on the nature of technology, nor the characteristics of the technology, but the competitive advantage brought by an organisation being incentivised as a trusted player in this market for having in place safety measures in key areas to better advance its position, and that of its end users. **This will have the benefit of allowing an organisation greater scope to operate within: (1) a number of AI activities; (2) a number of roles as part of the AI value chain; (3) varied AI sub domains (and AI system components); (4) cross pollination of those sub domains; and (5) potentially other forms of emerging technology, so that Australia can move quickly to leverage those benefits.**
41. **A Technology Passport would act as a form of trust-mark and signal to the end user of these technologies that there is a solid basis on which those organisations can be trusted. We recommend the creation of a central repository of searchable details of licence holders and their activities, instructions for use, potential harms and mitigations, and reporting of AI harms. This will also have the effect of encouraging a level of consistency to many areas, such as the construction and communication of instructions for use, and transparency in explanation of AI operations and decision making, that better serves the public interest.**
42. We note not all organisations will be required to have accreditation status or an organisation specific licence because they intersect with AI as a provider, developer, deployer, exporter, and possibly a user. The criterion for accreditation or licensing would be based on a more nuanced approach to the calculation of an organisations’ engagement with high impact AI and compliance with existing laws.
43. We have set out in **Annexure E** an example of the types of areas that could be considered as part of the determination of whether, for example, a licence was required or not. **We also note there are strong existing parallels globally with these types of assessment of risk, for example, in export controls and requirements of licensing here in Australian and overseas in the U.S.<sup>21</sup>.** Organisations operating in this technology area (and deep technologies) are very familiar with those assessments and well placed from an infrastructure perspective to comply.
44. **The accreditation or licence could be for a stated period of time, or unless and until an event occurs or is triggered that may cause the licence to be, for example, amended, suspended, revoked or cancelled.** An example of such an event may be a

---

<sup>21</sup> Bureau of Industry and Security, US Department of Commerce, 'Commerce Control List' ;Bureau of Industry and Security, US Department of Commerce, ' Commerce Country Chart' (8 April 2022) ;*Defence and Strategic Goods List 2021* (Cth), part 2.



major and preventable AI malfunction or multiple occurrences of such that result in public distrust.

45. We also propose there be clear exclusions for: (1) particular organisations, such as start-ups, SMEs that are not otherwise involved in the prohibited AI activities, or intersect with particular high impact criterion. **We want to prevent the occurrence of an imbalanced system, where underfunded innovators in Australia, such as our start-ups and SMEs, that are engaging in a few, lower risk AI activity types, are not required to comply with an entire compliance regime based on a singular use case.** However, organisations that do not legally require a licence may also elect to apply for one and comply (much like current privacy laws) for market leveraging.
46. **Importantly, we also consider the European Union and its exclusion of stated activity types, such as forms of non-commercial research and development<sup>22</sup>.** This is an extremely important and not often talked about exclusion, where further information is to follow on it from the EU. However, it is certainly an area to closely follow and come to a view about in the Australian context.
47. Arguably, the present text of the EU AI Act requires some further clarification about the intersections and exclusions of R&D, opensource AI components, and the treatment of high risk AI system incorporation and foundation models<sup>23</sup>. We could write another entire submission about this area and how to treat open source and foundation models in this context, but note for present purposes, this is an area of up-most importance to this debate. We were heavily involved in similar extensive debates about exclusions to R&D under the Defence Trade Controls legislation in Australia.
48. Further, there would need to be close determination of licence applicability, consequences for noncompliance, and a potential moratorium on noncompliance for a period of time as the licence authorisation relates to existing technologies on market.
49. Infrastructure and supporting resources around such a regime would be required by the Government. Our established infrastructure and systems of approval in areas such as the Therapeutic Goods Administration ('TGA') are largely for point in time approvals, however, where technology is adapting and learning in situ (including generating new data), that review process even for one form of technology in one context could involve multiple rounds of review for significant modification, and multiple touch points, where resources do not currently exist.

---

<sup>22</sup> Europe's upcoming AI Act will not apply to research, testing and development activities regarding an AI system prior to the system being placed on the market or put into service. This is provided that these activities are conducted respecting fundamental rights and the applicable Union law. Real-world testing of the AI systems is not included in this exemption: Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act ) and amending certain Union Legislative Acts [2021], art 2(5d).

<sup>23</sup> Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act ) and amending certain Union Legislative Acts [2021], arts 2(5d), 6, 28b.



50. In view of the Government's limited resources and expertise in this area of AI evaluation, and the potential required re-reviews of AI technologies, this could be a useful beginning to digitise corporate compliance. **We recommend focus on the responsible actions of an organisation as it relates to their obligations for non-static technologies.** This would mean where we don't currently have the resources or expertise at the scale required to facilitate a technology based regime, Government resources largely become an assessment of whether or not an organisation is meeting its required thresholds and standards (due diligence) as opposed to technologies, and re trained or modified technologies, or the interrogation of large algorithms and their impact.

51. **It would also arguably better enable more efficient cross border flows of AI technologies.** For example, through a form of AI and blockchain certification of the AI supply chain and multiple unknown parties contributing technologies to an AI system, and digital exchanges of information, and the reporting of areas of concern in real time for action to be taken in the public interest (e.g., expedited removal of technology from market and across the globe where it presents a serious threat).

## 11. Reflecting an international landscape & growing calls for cross border AI safety mechanisms

52. **This Australian system could evolve as and when the international landscape does. For example, if we hypothesised there will be the future introduction of an International AI Treaty, an international governing body on AI, and a level of global consensus on the highest impact areas.** In these eventualities, Australia would already be well placed from an infrastructure point of view to facilitate exchange of information and cross border flows of its technologies as part of exporting responsible AI. This is not unlike the global Wassenaar Arrangement, and its co-ordination and agreement of a list of dual use and munitions technologies, and requirements, on those frontier technologies that could do the most harm. **Areas to be considered in the context of AI are disinformation at scale and uncontrollable superhuman intelligence.**

53. Mechanisms for the safe and efficient use and trade of these technologies across international borders is an important imperative to get right.

## 12. Mandatory & public reporting of AI harms

54. In addition, we support pointed requirements for mandatory and public reporting of AI harm data, such as major AI malfunctions (not unlike data breaches and reporting of cyber incidents as it relates to critical infrastructure), and transparency about reasonably foreseeable risks, and organisational mitigations of those risks.

13. Australian innovators (start-ups and SMEs) shouldn't be unduly impacted

55. **As previously noted, ensuring start-ups and SMEs are prioritised and not disproportionately affected by AI laws, is something that needs to be closely considered in the Australian context.** Particularly in view of the current market dominance of large global technology companies.

56. Larger and well positioned upstream companies not only have the resource, and infrastructure to easily comply with impending laws such as the EU AI Act, they are also in a privileged position as the original developers of many forms of seminal AI technologies, including foundation models, with knowledge that the public is not privy to.

57. **From a safety point of view, companies should generally remain accountable for commercialisation of technologies they place on market, particularly where they have knowledge that those technologies, such as foundation models, will be incorporated at scale into downstream applications in multiple contexts.** Where this is reasonably foreseeable, subject to intervening acts and the responsibilities of downstream stakeholders, there should be sureties about the technology and its operation during the entirety of the AI life cycle.

58. The European Union has managed the treatment of start-ups and SMEs and ensuring innovation in a number of ways, including priority access to regulatory sandboxes, and exclusion from more prescriptive compliance requirements. This includes **a recently added provision that basically voids the legality of contractual provisions unilaterally placed on smaller players by larger technology providers excluding their legal liability and squarely placing it on the smaller players**<sup>24</sup>. Again, our competition experts would need to consider the strengths and weaknesses of such a provision, and also how it compares to existing provisions under our existing competition law relating to, for example, our unfair terms provisioning in standard form contracts. On first view, this provision appears that it is more targeted and could potentially put start-ups and SMEs in a stronger position.

59. **These areas are explored further in Annexure F, with nomination of our preferences for treatment.**

14. Existing laws in need of updating (IP laws are completely outdated)

60. There are many existing laws intersecting with AI that require changes. For the purposes of this submission, we won't focus on all of them.

---

<sup>24</sup> Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts [2021], arts 1(ea), 28(a), 29a(4), 43(4a), 53a, 71(1).

61. **Of key focus to us is our intellectual property legislative framework. In our strong view, it is outdated and in need of changes to better accommodate for new forms of technologies like AI that were not contemplated when these laws were first written. We note that is a theme that is not unique to Australia and its IP laws. This is a theme that is being faced by many jurisdictions globally.**
62. The continued uncertainties of IP laws (in particular copyright and patent laws), which, like in most countries around the world, are being hotly debated, are not beneficial for any side of the fence. Many existing copyright laws (and exclusions to them such as “fair use” in the US) are being tested through current litigation<sup>25</sup> especially in the US. The uncertainties and legal debates amongst academics, lawyers and AI experts needs to be better addressed. Uncertainty in these laws facilitates single or potential multiple judge-based decisions, and decisions that become persuasive in our jurisdictions and court cases.
63. **Changes to our IP laws, however, require broader review and public consideration and Government intervention for legislative amendment. Wherever the changes eventually end up.**
64. There are some recent examples of other jurisdictions attempting to deal with these vexed issues, and balancing the rights of copyright owners with developers, providers and users of AI systems requiring large amounts of trained data. The European Union, for example, requiring certain disclosures of the copyrighted data that has been used to train AI as part of public documentation<sup>26</sup>.
65. One area that could be usefully focused upon in Australia is a mechanism for Government (and supporting agencies) to better support the advancement of foundation models that are in our public interests. This could mean **better facilitating a process for copyrighted data protection practices, for example, infrastructure, standard licensing regimes and formulaic and benchmarked fees for reproduction and use, or avenues for facilitated and expedited digital negotiation procedures (in particular circumstances), for copyright owners, for the reproduction of their protected copyrighted data in foundation models.** In circumstances such as alleged reproduction of that copyrighted material by an organisation that is developing foundation models or other forms of AI, that do not otherwise fall within an existing exemption, this would require recompense.
66. Foundation models are usually trained on billions, if not hundreds of billions, of parameters requiring large amounts of training data and computing power. There is current research looking at ways to reduce these requirements, and associated costs, but this is very much the case at this present time. **Foundation models when safe could be incredibly beneficial for society and advancing and solving some of our greatest global problems, therefore, we believe there is absolute value in creating an environment that better enables the collation of the best data to inform these models, which takes**

---

<sup>25</sup> *Andersen et al v. Stability AI Ltd. et al*, Docket No. 3:23-cv-00201 (N.D. Cal. Jan 13, 2023); *Getty Images (US) Inc v. Stability AI Inc.* 1:2023cv00135 (2023).

<sup>26</sup> Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts [2021], art 28b(4)(c).

**into consideration issues of representation, diversity, and prevention of mass bias and misinformation etc.** There are many incumbent and well established markets for information sharing and buying in copyright law consistent with this model.

67. **Uncertain laws, litigation, disgruntled and impacted copyright owners, and incomplete datasets, with resulting consequences such as bias perpetuated on mass, is in no way a reasonable or stable way to continue these technological advances.**

68. Data privacy, anti-discrimination and consumer and competition laws are fundamental areas to closely review as part of broader changes here. For the purposes of this submission, we don't intend to interrogate these areas but are in a position to do so upon request.

## 15. Quotas established by Government for "very large" foundation model providers (benefit Australia AI ecosystem)

69. Finally, to further elevate AI innovation, we could use this opportunity for Government intervention (regulatory or non-regulatory) to support smaller players in the Australian AI ecosystem, or public and underfunded institutions that are currently grappling with AI uptake and use (such as public hospitals, schools and Universities requiring AI skills and computing power). Support here could take the form of **introducing positive innovation quotas, with prescribed organisations required to meet those quotas by, for example, providing free access to AI technologies or capabilities which better promote equality in digital divides, both in impoverished and gender and culturally diverse settings.**

## 16. Australia requirements (diagram)

70. **See Annexure G.**

## CONCLUSION

71. We strongly agree Government intervention in the form of new laws in AI is required. There are impressive models coming from overseas in how new laws in responsible AI should be modelled, and some proposing to apply extraterritorially to Australian businesses. International interoperability is important, but we believe that the regulatory focus should arguably shift by moving toward coherence with responsible AI internationally, and at the same time accommodating our unique AI needs as a country.

72. Australia could take an approach that arguably incentivises good and fair corporate governance standards, and supporting risk mitigations undertaken by an organisation, by way of a licensing regime. This will allow for technological fluidity, and rapid application for

the real life complexities of AI, and its layered, morphing, and generalised status. This should be coupled with clearly defined prohibitions on particularly reprehensible AI activities and outcomes, where those technologies do not have a place in Australian society.

73. We also recommend inclusion of additional means of mandatory notifications and disclosures that are publicly available, which allows for better data about AI harms, for prevention rather than cure.
74. This, arguably, results in trust markers that may better incite consumers in AI uptake and support our economy, further opening the doors to both rapid global exports and generation of more complex combinations of AI and other emerging technologies, that will form part of advancing layers of solutions and are efficiently managed. In other words, we believe risks should be mitigated in a flexible and adaptive manner.

End.

## Key Defined Terms

1. **AI System:** "A machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments"<sup>27</sup>."
2. **Foundation Model:** AI model that is trained on broad DATA at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks<sup>28</sup>.
3. **Generative AI:** Foundation models used in AI systems specifically "intended to generate, with varying levels of autonomy, content such as complex text, images, audio, or video"<sup>29</sup>.
4. **Large Language Model:** "A type of artificial intelligence model that has been trained through deep learning algorithms to recognise, generate, translate, and/or summarise vast quantities of written human language and textual data"<sup>30</sup>.
5. **Machine Learning:** A branch of AI and computer science which focuses on development of systems that are able to learn and adapt without following explicit instructions imitating the way that humans learn, gradually improving its ACCURACY, by using ALGORITHMS and statistical MODELS to analyse and draw inferences from patterns in DATA"<sup>31</sup>.
6. **Provider:** " A natural or legal person, public authority, agency or other body that develops an AI SYSTEM or that has an AI SYSTEM developed and places that system on the market or puts it into service under its own name or trademark, whether for payment or free of charge"<sup>32</sup>.

***AI Component should be defined.***

---

<sup>27</sup> Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts [2021], art 3(1).

<sup>28</sup> Ibid, art 3(1)(c).

<sup>29</sup> Ibid, art 28b(4).

<sup>30</sup> European Commission, Knowledge Centre on Interpretation (Webpage).

<sup>31</sup> Estévez Almenzar M. et al, *Glossary of Human-Centric Artificial Intelligence* (JRC Science for Policy Report, Publications Office of the European Union, 2022), 40.

<sup>32</sup> Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act ) and amending certain Union Legislative Acts [2021], art 3(2).

# Tables of evidence for AI submission

## Annexure A

Global analysis of foundation model controls (legislative and voluntary, and research analysis about current compliance adherence by major foundation model providers)

Foundation Model Harms	Draft EU AI Act Mitigation (legal requirements, related Articles) <sup>33</sup>	Voluntary Measures Agreed by U.S. tech companies (comparative to the EU AI Act) <sup>34</sup>	Stanford University Research grading Foundation Model Providers of the Current EU AI Act (10 major foundation model providers (and their flagship models) for the 12 AI Act requirements on a scale from 0 (worst) to 4 (best)) <sup>35</sup>
Potential biased outcomes and increased susceptibility to adversarial attacks	Continuous risk assessment and risk mitigation (Article 28b (2)(a))	On a broad scale, companies will invest in cybersecurity and implement the NIST AI Risk Management Framework.  The companies will also work toward sharing information among companies and governments regarding trust and safety risks,	On a 40-point scale for risk mitigation, the average score for the top 10 foundation model providers was 16.

<sup>33</sup> Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts [2021], art 28b.

<sup>34</sup> White House, FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI, 21 July 2023.

<sup>35</sup> Rishi Bommasani et al, Do Foundation Model Providers Comply with the Draft EU AI Act? (Stanford Center for Research on Foundation Models, 2023).



		dangerous or emergent capabilities, and attempts to circumvent safeguards.	
Harm of inaccurate or misleading output	Using quality datasets (Article 28b (2)(b))	The companies commit to prioritising research on the societal risks that AI systems can pose, including on avoiding harmful bias and discrimination, and protecting privacy.	On a 40-point scale for using quality data sources, the average score for the top 10 foundation model providers was 22.
Violation of legal safeguards and harm to users' rights	Compliance by design, capabilities and limitations (Article 28b (2)(c))	Some companies such as Microsoft will ensure a layered safety-by-design approach so that models remain safe, secure, and within human control. They will also support the development of a licensing regime to regulate the secure development and deployment.	On a 40-point scale for design and development with appropriate levels of performance, the average score for the top 10 foundation model providers was 27.
Biases, errors, or vulnerabilities in the model leading to unexpected or unreliable outputs.	Extensive testing and evaluation (Article 28b (2)(c))	<p>The companies commit to internal and external security testing of all AI systems before their release.</p> <p>The companies will also share information across the industry and with governments, civil society, and academia on managing AI risks.</p>	On a 40-point scale for carrying out testing, the average score for the top 10 foundation model providers was 10.
Increased resource waste and energy consumption	Standards and environmental impact (Article 28b (2)(d))	The companies aim to develop and deploy advanced AI systems to help address society's greatest challenges, emphasising their positive impact rather than exacerbating issues.	On a 40-point scale for incorporating existing standards to reduce energy use, the average score for the top 10 foundation model providers was 15.

Misuse of the model's capabilities and limitations	Downstream technical documentation and instructions for use (Article 28b (2)(e))	<p>Companies will develop more initiatives to support downstream providers in understanding the model and its users.</p> <p>The companies also commit to developing robust technical mechanisms to ensure that users know when content is AI generated, such as a watermarking system.</p> <p>The companies will enable members of the public to lodge reports on their AI systems' capabilities, limitations, and areas of appropriate and inappropriate use.</p>	On a 40-point scale for providing technical documentation, the average score for the top 10 foundation model providers was 24.
Inconsistent or unreliable performance of the model	Quality management system (Article 28b (2)(f))	<p>The companies commit to internal and external red-teaming of models or systems in areas including misuse, societal risks, and national security concerns, such as bio, cyber, and other safety areas.</p> <p>The companies will also facilitate third-party discovery and reporting of vulnerabilities in their AI systems.</p>	On a 40-point scale for incorporating a quality management system, the average score for the top 10 foundation model providers was 15.
Unauthorised use or dissemination of copyrighted content	Disclosure of copyrighted data (Article 28b (4)(c))	We understand that there is no current commitment to disclose the use of copyrighted data.	On a 40-point scale for copyright disclosure, the average score for the top 10 foundation model providers was 7.

Decreased transparency and oversight on the model's deployment and use	Registration (Article 28b (2)(g))	<p>The companies commit to publishing reports for all new significant model public releases within scope. The reports will indicate model or system capabilities, limitations, and domains of appropriate and inappropriate use, and include discussions on societal risks, such as effects on fairness and bias.</p> <p>However, there is no clear commitment to public disclosure of serious incidents or major malfunctions on a public register.</p>	On a 40-point scale for disclosing the foundation model on the market, the average score for the top 10 foundation model providers was 9.
--	-----------------------------------	--	---

The 10 major foundation model providers considered as part of this study are:

1. OpenAi – Gpt-4
2. Cohere – Cohere Command
3. StabilityAi – Stable Diffusion v 2
4. Anthropic – Claude
5. Google – PaLM2
6. Meta – LLaMA
7. BigScience – BLOOM
8. AI21labs – Jurassic-2
9. Aleph Alpha – Luminous
10. EleutherAI – GPT-NeoX

The research was conducted by the Stanford Center for Research on Foundation Models (CRFM), Institute for Human-Centered Artificial Intelligence and released in 2023. There are some cited limitations to the research that can be found [here](#).

## Annexure B

	KomplyAi's position	KomplyAi's position	KomplyAi's position	AI Reference (region/country + law)
	Yes	No	Coherence	
Prohibited AI practices	X			<p>Europe<sup>36</sup></p> <ul style="list-style-type: none"> <li>Artificial Intelligence Act 2021, Article 5(1)(a)- AI systems that deploy subliminal techniques or use manipulative/deceptive techniques to hinder a user's informed decision making. This excludes AI systems approved for therapeutic purposes on the basis of informed user consent.</li> <li>Artificial Intelligence Act 2021, Article 5(1)(b)-AI systems that exploit vulnerabilities of a person or group of persons based on their characteristics to then distort user behaviour and potentially cause them significant harm.</li> <li>Artificial Intelligence Act 2021, Article 5(1)(ba)- Biometric categorisation systems which categorise people based on their sensitive or protected attributes. This excludes AI systems approved for therapeutic purposes on the basis of informed user consent.</li> <li>Artificial Intelligence Act 2021, Article 5(1)(c)-AI systems used for social scoring, classifying or evaluating people based on their social behaviour and the social score potentially leads to detrimental or unfavourable treatment for users.</li> </ul>

<sup>36</sup> Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act ) and amending certain Union Legislative Acts [2021], art 28b.

				<ul style="list-style-type: none"> <li>• Artificial Intelligence Act 2021, Article 5(1)(da)- AI systems that make risk assessments of people or profile people to assess risk of offending, reoffending, predicting the occurrence/re-occurrence of criminal and administrative offences.</li> <li>• Artificial Intelligence Act 2021, Article 5(1)(db)- AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage</li> <li>• Artificial Intelligence Act 2021, Article 5(1)(dc)- AI systems to infer emotions of people in the areas of law enforcement, border management, in workplace and education institutions.</li> <li>• Artificial Intelligence Act 2021, Article 5(1)(d)- 'Real-time' remote biometric identification systems in publicly accessible spaces.</li> <li>• Artificial Intelligence Act 2021, Article 5(1)(d)- AI systems analysing recorded footage of publicly accessible spaces through 'post' remote biometric identification systems, unless pre-judicially authorised and strictly necessary for the targeted search connected to a specific serious criminal offense.</li> </ul> <p><b>Brazil</b> <sup>37</sup></p> <ul style="list-style-type: none"> <li>• Bill n° 2.338/2023, Article 14(I)- AI systems employing subliminal techniques that aim to or induce a person to behave in a harmful or dangerous manner towards the health or safety or fundamental rights of people.</li> <li>• Bill n° 2.338/2023, Article 14(II)- AI systems exploiting vulnerabilities of people, such related to their age or physical or mental disability, to induce a person to behave in a harmful or dangerous manner towards the health or safety or fundamental rights of people.</li> <li>• Bill n° 2.338/2023, Article 14(II)- AI systems used by the government to evaluate, classify or rank people based on their social behavior or personality</li> </ul>
--	--	--	--	---

<sup>37</sup> Bill No. 2338 of 2023 (On the use of Artificial Intelligence systems) [2023].

				<p>traits to determine access to goods and services and public policies, in an illegitimate or disproportionate manner.</p> <p><b>Canada</b><sup>38</sup></p> <ul style="list-style-type: none"> <li>The Artificial Intelligence and Data Act (AIDA) 2022 (Bill C-27, the Digital Charter Implementation Act, 2022) does not outrightly ban AI systems that present an unacceptable level of risk, but it does create offences for certain practices: <ul style="list-style-type: none"> <li>Section 38: possessing or using personal information for the purpose of creating an AI system if the personal information was not lawfully obtained</li> <li>Section 39(a): knowingly (or with reckless disregard) using an AI system that is likely to cause serious physical or psychological harm to an individual or substantial damage to property, if such harm occurs.</li> <li>Section 39(b): making an AI system available for use with the intent to defraud the public and to cause substantial economic loss to an individual if such loss occurs.</li> </ul> </li> </ul> <p><b>US</b></p> <ul style="list-style-type: none"> <li>California: The California Fair Employment and Housing Council, on March 15, 2022, published draft modifications to its employment anti-discrimination laws that would make it unlawful for an employer or covered entity to use automated-decision systems that screen applicants or employees on the basis of a protected characteristic (subject to some</li> </ul>
--	--	--	--	---

<sup>38</sup> Artificial Intelligence and Data Act 2022 (BILL C-27, Digital Charter Implementation Act 2022), 44th Parliament, 1st session.

				<p>exceptions). Assembly Bill 331 aims to prohibit the use by deployers of automated decision tools that contributes to algorithmic discrimination.<sup>39</sup></p> <ul style="list-style-type: none"> <li>• Colorado: Bill Colo. Rev. Stat. § 10-3-1104.9 prohibits insurers from using external consumer data and information sources, as well as any algorithms or predictive models that use ECDIS, in a way that unfairly discriminates based on race, color, national or ethnic origin, religion, sex, sexual orientation, disability, gender identity or gender expression.</li> <li>• Maryland: H.B. 1202 (2023) bans the use of “a facial recognition service for the purpose of creating a facial template during an applicant’s interview for employment,” unless the applicant signs a waiver.</li> <li>• New York City, Local Law 2021/144 (2021) to amend the administrative code of the city of New York, in relation to automated employment decision tools: Employers and employment agencies are prohibited from using automated employment decision tools unless they has been subjected to a “bias audit” within the last year and the results of the most recent bias audit and the “distribution date of the tool” have been made publicly available on the employer’s or employment agency’s website.</li> </ul> <p>China<sup>40</sup></p> <ul style="list-style-type: none"> <li>• Interim Measures for the Management of Generative Artificial Intelligence Services 2023 (proposed), Article 4- Content generated by generative artificial intelligence must not contain subversion of state power, overthrow</li> </ul>
--	--	--	--	---

<sup>39</sup> California Assembly Bill 331, Automated decision tools (2023)

<sup>40</sup> Cybersecurity Administration of China et al, Interim Measures for the Management of Generative Artificial Intelligence Services [July 2023]; State Internet Information Office Ministry of Industry and Information Technology of the People's Republic of China Order No. 12 of the Ministry of Public Security of the People's Republic of China, Provisions on the Administration of Deep Synthesis of Internet Information Services [November 2022].



				<p>of the socialist system, incitement to split the country, undermine national unity, promote terrorism, extremism, and promote ethnic hatred and ethnic discrimination, violence, obscene and pornographic information, false information, and content that may disrupt economic and social order.</p> <ul style="list-style-type: none"> <li>Regulations on the Administration of Deep Synthesis of Internet Information Services 2022, Article 6- No company or person is permitted to use 'deep synthesis' technologies to create, duplicate, share, or spread information that is forbidden by laws or administrative rules. This includes the generation and dissemination of fake news. These services are not permitted to be used for activities that risk national security, harm the nation's reputation, infringe on public interests, or disrupt the economy. Any activities that break laws, administrative regulations, disrupt social order, or infringe on others' rights are strictly prohibited. <ul style="list-style-type: none"> <li>Article 23- Deep synthesis technology is defined as "technology that uses deep learning, virtual reality, and other synthesis algorithms to generate text, images, audio, video, and virtual scenes."</li> </ul> </li> </ul>
Risk based & proportionate response and ensuring innovation in AI (as a stated objective)	X			<p><b>Europe</b></p> <ul style="list-style-type: none"> <li>Artificial Intelligence Act 2021, Article 6(1)- AI systems will be considered high risk if they are safety components or products covered by Union legislation and if they are required to undergo a third-party conformity assessment related to risks for health and safety.</li> <li>Artificial Intelligence Act 2021, Article 6(2)-AI systems will be considered high risk if they fall under one or more of the critical areas and use cases referred to in Annex III, only if they pose a significant risk of harm to the health, safety or fundamental rights of people. AI systems used in managing or operating critical infrastructure will be high-risk if they pose a significant risk of harm to the environment.</li> </ul>

				<ul style="list-style-type: none"> <li>Artificial Intelligence Act 2021, Article 16-List of obligations for providers of high risk AI systems to follow, before placing their AI systems on the market.</li> </ul> <p><b>Brazil</b></p> <ul style="list-style-type: none"> <li>Bill n° 2.338/2023, Article 13- Providers of AI systems should conduct a preliminary assessment to classify the degree of risk carried by their systems as 'Excessive' or 'High'.</li> <li>Bill n° 2.338/2023, Article 17- The "high risk" category identifies 14 unique AI uses, including systems for social aid, employment decisions, critical infrastructure operation like water and electricity, biometric identification, and autonomous vehicles.</li> <li>Bill n° 2.338/2023, Articles 19 and 20- Providers of High risk AI systems will have to adopt governance measures, follow documentation requirements, register the AI systems for evaluation, carry out rigorous testing, establish data management and risk control measures and implement human oversight.</li> </ul> <p><b>UK</b></p> <ul style="list-style-type: none"> <li>The UK currently has a risk-based approach to regulate AI. The Government also indicated in June 2023 that it will adopt a pro-innovation approach that encourages regulation on a sectoral basis. More details to come. <sup>41</sup></li> </ul> <p><b>Canada</b> <sup>42</sup></p> <ul style="list-style-type: none"> <li>AIDA, Section 7- A person who is responsible for an artificial intelligence system must assess whether it is a high-impact system.</li> </ul>
--	--	--	--	---

<sup>41</sup> Department for Science, Innovation and Technology and Office for Artificial Intelligence, AI regulation: a pro-innovation approach (Policy Paper, 29 March 2023).

<sup>42</sup> *Artificial Intelligence and Data Act 2022* (BILL C-27, *Digital Charter Implementation Act 2022*), 44th Parliament, 1st session.

				<ul style="list-style-type: none"> <li>AIDA, Section 8- Providers of high-impact systems must establish measures to identify, assess and mitigate the risks of harm or biased output that could result from the use of the system.</li> <li>AIDA, Section 9- Providers of high-impact systems must establish measures to monitor compliance with the risk mitigation measures they implement.</li> <li>AIDA, Sections 11(1) and (2)- Providers of high-impact systems or those who manage their operation, must publish on a publicly available website a plain-language description of the system.</li> <li>AIDA, Section 12- Providers of high-impact systems must notify the Minister if the use of the system results or is likely to result in material harm.</li> </ul> <p>USA</p> <ul style="list-style-type: none"> <li>The U.S. federal government's AI risk management is generally not directly risk-based. While the 2019 executive order (EO 13859) and subsequent OMB guidance suggest a risk-based approach, other initiatives like the AI Bill of Rights (non-binding) don't strictly follow this type of framework for AI regulation.<sup>43</sup></li> </ul>
Risk scoring system, such as "High, Medium, Limited or Low"			X	<p>Australia</p> <ul style="list-style-type: none"> <li>The government is currently considering a framework where AI systems are classified as low risk, medium risk and high risk.</li> </ul> <p>Europe</p> <ul style="list-style-type: none"> <li>The European Parliament has adopted a risk-based framework of classifying AI Systems as prohibited, high risk, limited risk and low risk.</li> </ul>

<sup>43</sup> Executive Office of the President, 'Executive Order 13859: Maintaining American Leadership in Artificial Intelligence' (11 February 2019); White House, 'Blueprint for an AI Bill of Rights' (October 2022).

				<p><b>Brazil</b></p> <ul style="list-style-type: none"> <li>• Bill nº 2.338/2023 proposes three levels of risk for AI systems, which are similar to the European Union AI Act: (i) excessive risk, in which the use is prohibited; (ii) high risk; and (iii) non-high risk. Before deploying or using the AI system, it shall pass a preliminary self-assessment analysis conducted by the AI provider to classify its risk level.</li> </ul> <p><b>UK</b></p> <ul style="list-style-type: none"> <li>• The UK currently does not have a risk-based approach to regulate AI. The Government indicated in June 2023 that it will adopt a pro-innovation approach that encourages regulation within the industry.<sup>44</sup></li> </ul> <p><b>Canada</b></p> <ul style="list-style-type: none"> <li>• While Canada doesn't follow a strict risk-based framework like the EU's AI Act, the AIDA does outline requirements for 'high impact' AI systems, along with other less impactful systems.</li> </ul> <p><b>USA<sup>45</sup></b></p> <ul style="list-style-type: none"> <li>• The U.S. federal government's AI risk management is generally not directly risk-based. While the 2019 executive order (EO 13859) and subsequent OMB guidance suggest a risk-based approach, other initiatives like the AI Bill of Rights (non-binding) don't strictly follow this type of framework for AI regulation.</li> </ul>
--	--	--	--	--

<sup>44</sup> Department for Science, Innovation and Technology and Office for Artificial Intelligence, AI regulation: a pro-innovation approach (Policy Paper, 29 March 2023).

<sup>45</sup> Executive Office of the President, 'Executive Order 13859: Maintaining American Leadership in Artificial Intelligence' (11 February 2019); White House, 'Blueprint for an AI Bill of Rights' (October 2022).

Narrow use cases established for <b>high risk</b> characterisation and compliance requirements		X		<p><b>Europe</b></p> <ul style="list-style-type: none"> <li>Artificial Intelligence Act 2021, Annex III- AI systems falling under each critical use case will automatically be considered high risk (paraphrase below): <ul style="list-style-type: none"> <li>Biometric and biometrics-based systems</li> <li>Systems used in the management and operation of critical infrastructure</li> <li>Systems used in education and vocational training</li> <li>Systems used in employment, workers management and access to self-employment</li> <li>Systems used to determine access to and enjoyment of essential private services and public services and benefits</li> <li>Systems used in law enforcement</li> <li>Systems used in migration, asylum and border control management</li> <li>Systems used in administration of justice and democratic processes</li> </ul> </li> </ul>
More generalised criterion to determine <b>high impact</b> AI systems and compliance requirements			X	<p><b>Canada</b></p> <ul style="list-style-type: none"> <li>The Government considers the following to be among the key factors to be examined in determining which AI systems would be considered to be high-impact<sup>46</sup>: <ul style="list-style-type: none"> <li>Evidence of risks of harm to health and safety, or a risk of adverse impact on human rights, based on both the intended purpose and potential unintended consequences;</li> <li>The severity of potential harms;</li> <li>The scale of use;</li> </ul> </li> </ul>

<sup>46</sup> Government of Canada, The Artificial Intelligence and Data Act (AIDA) – Companion document (2023).

				<ul style="list-style-type: none"> <li>○ The nature of harms or adverse impacts that have already taken place;</li> <li>○ The extent to which for practical or legal reasons it is not reasonably possible to opt-out from that system;</li> <li>○ Imbalances of economic or social circumstances, or age of impacted persons; and</li> <li>○ The degree to which the risks are adequately regulated under another law.</li> </ul>
Specific requirements for <b>foundation models</b> and compliance requirements based on the organisations' role in the AI supply chain			X	<p><b>Europe</b></p> <p><b>Foundation models</b></p> <ul style="list-style-type: none"> <li>• Artificial Intelligence Act 2021, Article 28b- Providers of foundation models, need to, prior to making them available on the market, ensure that they are compliant with the following requirements (paraphrase below):             <ul style="list-style-type: none"> <li>○ Continuous Risk Assessment and Risk Mitigation</li> <li>○ Using Quality Datasets</li> <li>○ Compliance-by-Design</li> <li>○ Standards and Environmental Impact</li> <li>○ Technical Documentation</li> <li>○ Overall Quality Management</li> <li>○ Registration</li> </ul> </li> <li>• The requirements apply regardless of whether foundation models are provided as standalone models or embedded in another AI system, or provided under free and open source licences, as a service, as well as other distribution channels.</li> </ul>

				<b>AI supply chain</b> <ul style="list-style-type: none"> <li>Artificial Intelligence Act 2021, Article 28- Any distributors, importers, deployers or other third parties involved in the AI value chain will be classified as AI system providers if they: <ul style="list-style-type: none"> <li>Brand a high-risk AI system already on the market with their name or trademark, or</li> <li>Substantially modify an existing high-risk AI system, keeping it high-risk, or</li> <li>Substantially modify a general purpose AI system, making it high-risk if it wasn't before.</li> </ul> </li> <li>The original provider must supply the new provider with the AI system's technical documents and other necessary information based on the acknowledged state of the art, aiding them in fulfilling their AI Act obligations.</li> </ul>
Specific requirements for <b>generative AI</b> and compliance requirements based on the organisations' role in the AI supply chain			X	<b>Europe</b> <ul style="list-style-type: none"> <li>Artificial Intelligence Act 2021, Article 28b- Providers of foundation models that involve generative AI, need to, prior to making them available on the market, ensure that they are compliant with the following: <ul style="list-style-type: none"> <li>Transparency obligations</li> <li>Extensive testing to ensure adequate safeguards against the generation of content in line with Union law</li> <li>Documentation and publication of detailed summaries of the data used to train the generative AI system, where such training data is protected under copyright law.</li> </ul> </li> </ul>
Proportionate treatment for <b>start-ups and</b>			X	<b>Europe</b>



<b>SMEs</b> & competition protection measures for smaller innovators				<ul style="list-style-type: none"> <li>• Artificial Intelligence Act 2021, Article 28(a): Unfair or anti-competitive contractual terms unilaterally imposed on an SME or startups will not be binding.</li> <li>• Artificial Intelligence Act 2021, Articles 1(ea) and 53a(2)(c): The AI Act will introduce measures to foster innovation, emphasizing support for SMEs and start-ups. It provides that European Member States will establish regulatory sandboxes and measures to lessen regulatory burdens on SMEs and start-ups. Access to all AI regulatory sandboxes is intended to be free of charge for SMEs and startups.</li> <li>• Artificial Intelligence Act 2021, Article 53a(3): Sandbox participants, especially SMEs and start-ups, will receive pre-deployment guidance on AI Act requirements, assistance with standardization and certification, and access to Digital Single Market resources like Testing Facilities, Digital Hubs, and Centres of Excellence.</li> <li>• Artificial Intelligence Act 2021, Article 43(4)(a): Third-party conformity assessment fees will be tailored for SMEs according to their size and market share.</li> <li>• Artificial Intelligence Act 2021, Article 29(a)(4): Start-ups and SMEs with high risk AI systems will not be required to carry out extensive consultations with different stakeholders when performing a fundamental rights impact assessment.</li> <li>• Artificial Intelligence Act 2021, Article 11(1): SMEs and start-ups can create alternative documentation fulfilling the objectives of the technical documentation requirements.</li> </ul>
---	--	--	--	---

				<b>Brazil example</b> <ul style="list-style-type: none"> <li>The government provides federal initiatives to assist startups, such as business mentoring, financial investment guidance, business modeling, infrastructure, and training support.<sup>47</sup></li> </ul>
<b>General requirements for transparency, explainability etc., applying to lower and limited risk AI</b>	X			<b>Europe</b> <ul style="list-style-type: none"> <li>Artificial Intelligence Act 2021, Article 4a- All operators which fall under the AI Act are encouraged to adopt the following general principles: <ul style="list-style-type: none"> <li>'human agency and oversight'</li> <li>'technical robustness and safety'</li> <li>'privacy and data governance'</li> <li>'transparency'</li> <li>'diversity, non-discrimination and fairness'</li> <li>'social and environmental well-being'</li> </ul> </li> <li>The Act translates the general principles into specific requirements for providers and operators of high-risk AI systems.</li> </ul>
Central AI governing body	X			<b>Europe</b> <ul style="list-style-type: none"> <li>Artificial Intelligence Act 2021, Article 56- Established an independent body called the 'European Artificial Intelligence Office' (AI Office) with the seat located in Brussels.</li> <li>Artificial Intelligence Act 2021, Article 56b- The AI Office is responsible for undertaking wide a range of tasks such as supporting the implementation of the AI Act, monitoring its effective application, promote AI literacy, serve as a mediator in discussions about the AI Act's application, coordinate joint</li> </ul>

<sup>47</sup> Government of Brazil, Startup Point (Website) <<https://www.gov.br/startuppoint/pt-br>>

				<p>investigations, contribute to the effective cooperation with the competent authorities of third countries and with international organisations etc.</p> <p><b>Canada</b></p> <ul style="list-style-type: none"> <li>AIDA, Section 33(1)- Artificial Intelligence and Data Commissioner is established to assist in the enforcement of the proposed law. In addition to administration and enforcement of the Act, the Commissioner's work will include supporting and coordinating with other regulators to ensure consistent regulatory capacity across different contexts, as well as tracking and studying of potential systemic effects of AI systems in order to inform administrative and policy decisions.</li> </ul> <p><b>UK</b></p> <ul style="list-style-type: none"> <li>The Office for Artificial Intelligence, a unit within the Department for Science, Innovation and Technology, is responsible for overseeing implementation of the National AI Strategy.</li> </ul> <p><b>USA</b></p> <ul style="list-style-type: none"> <li>The National Artificial Intelligence Initiative Office, located in the White House Office of Science and Technology Policy (OSTP), is legislated by the <i>National Artificial Intelligence Initiative Act</i> (DIVISION E, TITLE LI, SEC. 5102) to coordinate and support the National AI Initiative.</li> </ul>
Changes to laws behind the introduction of an AI principal piece of legislation	X			<p><b>Europe</b></p> <ul style="list-style-type: none"> <li>AI Liability Directive 2022/0303 (proposed)</li> <li>Cybersecurity Regulation 2022/0085 (proposed)</li> </ul>

<p><b>(general updates to data privacy, anti-discrimination, intellectual property, consumer protection, competition laws, product safety, cyber security, and export controls)</b></p>				<ul style="list-style-type: none"> <li>• Cyber Resilience Act 2022/0272 (proposed)</li> <li>• Cyber Solidarity Act 2023/01099 (proposed)</li> <li>• Data Act 2022/0047 (proposed)</li> <li>• Data Governance Act 2022/868</li> <li>• European Health Data Space 2022/0140 (proposed)</li> <li>• Regulation on data collection for short-term rental 2022/0358 (proposed)</li> <li>• Harmonisation of GDPR enforcement 2023/0202 (proposed)</li> <li>• Interoperable Europe Act 2022/0379 (proposed)</li> <li>• Copyright Directive 2019/790</li> <li>• Design Directive 2022/0392 (proposed)</li> <li>• Standard essential patents 2023/0133 (proposed)</li> <li>• Compulsory licensing of patents 2023/0129 (proposed)</li> <li>• General Product Safety Regulation 2023/988</li> <li>• Digital Services Act 2022/2065</li> </ul>
---	--	--	--	--

				<ul style="list-style-type: none"> <li>• Digital Market Act 2022/1925</li> <li>• Digital Operational Resilience Act 2022/2554</li> <li>• Crypto-assets Regulation 2023/1114</li> <li>• Financial Data Access Regulation 2023/0205 (proposed)</li> <li>• Payment Services Regulation 2023/0210 (proposed)</li> </ul> <p>Australia</p> <ul style="list-style-type: none"> <li>• <i>Privacy Act 1988</i> (Cth)</li> <li>• <i>Online Safety Act 2021</i> (Cth)</li> <li>• <i>Patents Act 1990</i> (Cth)</li> <li>• <i>Copyright Act 1968</i> (Cth)</li> <li>• <i>Data Availability and Transparency Act 2021</i> (Cth)</li> <li>• <i>Treasury Laws Amendment (Consumer Data Right) Act 2019</i> (Cth)</li> <li>• <i>Disability Discrimination Act 1992</i> (Cth)</li> <li>• <i>Racial Discrimination Act 1975</i> (Cth)</li> </ul>
--	--	--	--	--

			<ul style="list-style-type: none"> <li>• <i>Sex Discrimination Act 1984</i> (Cth)</li> <li>• <i>Age Discrimination Act 2004</i> (Cth)</li> <li>• <i>Competition and Consumer Act 2010</i> (Cth)</li> <li>• <i>Privacy and Personal Information Protection Act 1998</i> (NSW)</li> <li>• <i>Health Records and Information Privacy Act 2002</i> (NSW)</li> <li>• <i>Government Information (Public Access) Act 2009</i> (NSW)</li> <li>• <i>Data Sharing (Government Sector) Act 2015</i> (NSW)</li> <li>• <i>State Records Act 1998</i> (NSW)</li> <li>• <i>Anti-Discrimination Act 1977</i> (NSW)</li> <li>• <i>Workplace Surveillance Act 2005</i> (NSW)</li> <li>• <i>Surveillance Devices Act 2007</i> (NSW)</li> <li>• <i>Health Services Act 1997</i> (NSW)</li> <li>• <i>Fair Trading Act 1987</i> (NSW)</li> </ul> <div>UK</div> <ul style="list-style-type: none"> <li>• <i>Data Protection Act 2018</i></li> </ul>
--	--	--	--

				<ul style="list-style-type: none"> <li>• UK GDPR</li> <li>• Data Protection &amp; Digital Information (No.2) Bill</li> <li>• Consumer Rights Act 2015</li> <li>• The Computer Misuse Act 1990</li> </ul> <p><b>Singapore</b></p> <ul style="list-style-type: none"> <li>• <i>Personal Data Protection Act 2012</i></li> <li>• <i>Customs Act 1960</i></li> <li>• <i>Regulation of Imports and Exports Act 1995</i></li> <li>• <i>Public Sector (Governance) Act 2018</i></li> <li>• <i>Registered Designs Act 2000</i></li> <li>• Model Artificial Intelligence Governance Framework 2020</li> <li>• <i>The Principles to promote Fairness, Ethics, Accountability and Transparency 2018</i></li> </ul> <p><b>USA</b></p> <ul style="list-style-type: none"> <li>• AI Bill of Rights 2022</li> </ul>
--	--	--	--	--

				<ul style="list-style-type: none"> <li>• Executive Order 13960 Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government</li> <li>• Executive Order 13859 Maintaining American Leadership in Artificial Intelligence</li> <li>• Executive Order 13985 on Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government</li> <li>• National AI R&amp;D Strategic Plan 2023</li> <li>• Bill for the Data Care Act 2022</li> <li>• John S. McCain National Defense Authorization Act for Fiscal Year 2019</li> <li>• National AI Initiative Act of 2020</li> <li>• Advancing American AI Act of 2021 (proposed)</li> <li>• AI Training Act of 2021</li> <li>• Fair Credit Reporting Act of 1970</li> <li>• Equal Credit Opportunity Act of 1974</li> </ul>
--	--	--	--	---



				<p><b>Canada</b></p> <ul style="list-style-type: none"> <li>• <i>Consumer Privacy Protection Act (proposed)</i></li> <li>• Artificial Intelligence and Data Act 2022 (Bill C-27, the Digital Charter Implementation Act, 2022)</li> <li>• Canada Consumer Product Safety Act ( SC 2010, c. 21)</li> <li>• Privacy Act ( RSC , 1985, c. P-21)</li> <li>• Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)</li> <li>• Critical Cyber Systems Protection Act 2022 (proposed)</li> </ul> <p><b>Brazil</b></p> <ul style="list-style-type: none"> <li>• Bill of Law No. 21, of 2020 (Establishes foundations, principles, and guidelines for artificial intelligence development and application in Brazil and establishes other provisions)</li> <li>• Bill No. 5051, of 2019 (Establishes the principles for the use of Artificial Intelligence in Brazil)</li> <li>• Bill No. 872 of 2021 (Provides for the ethical frameworks and guidelines that underlie the development and use of Artificial Intelligence in Brazil)</li> <li>• General Data Protection Law</li> </ul>
--	--	--	--	---

				<ul style="list-style-type: none"> <li>• Decree No. 9,573/2018 (National Policy for the Security of Critical Infrastructures)</li> <li>• Decree No. 11,200/2022 (National Plan for the Security of Critical Infrastructures within the Federal Public Administration)</li> <li>• Decree No. 9,637/2018 (National Information Security Policy)</li> <li>• Decree No. 10,222/2020 (National Cybersecurity Strategy)</li> <li>• Brazilian Civil Code - Law No. 10,406/02</li> <li>• Brazilian Consumer Protection Code (CDC) - Law No. 8,078/90</li> <li>• Internet Legal Framework - Law No. 12,965/14</li> <li>• Brazilian Criminal Code - as amended by Law No. 12,737/12</li> <li>• Interception of Telephone Communication Law - Federal Law 9,296/96</li> <li>• Complementary Law No. 105/01</li> <li>• Brazilian Information Access Law - Federal Law N° 12,527/11</li> <li>• Good Payer's Registry Law - Federal Law N° 12,414/11, amended by Complementary Law No. 166/2019</li> <li>• Brazilian Securities and Exchange Commission Resolution ("CVM") No. 35 of 2021</li> </ul>
--	--	--	--	--

## Annexure C

### Global approach to prohibited AI activities

Prohibited AI Activities	Government Explanatory Memoranda <sup>48</sup>	Real Life Examples <sup>49</sup>	Region/country laws
<p>AI systems that employ subliminal techniques, manipulative, or deceptive methods to significantly distort an individual's or group's behaviour by hindering their ability to make informed decisions and thus, potentially causing significant harm.</p> <p>The ban on AI systems using subliminal techniques does not apply to those used for approved therapeutic purposes, provided specific informed consent is obtained from exposed individuals or their legal guardians.</p>	<p>AI systems designed to significantly distort human behaviour, potentially leading to physical or psychological harm, are to be prohibited. These systems could use imperceptible subliminal techniques or exploit individual vulnerabilities to cause such distortions, potentially resulting in significant harm over time. This applies even if the provider or deployer didn't intend to cause significant harm, as long as the harm results from manipulative or exploitative AI practices.</p>	<p>Using a device emitting sound at an inaudible frequency to lessen fatigue in truck drivers, enabling them to drive for extended periods.</p>	<p>European Union: Artificial Intelligence Act 2021</p>
<p>AI systems that exploit vulnerabilities of a person or a group, including</p>	<p>AI systems may exploit vulnerabilities related to individual traits like</p>	<p>Cambridge Analytica, a political consulting firm, used Facebook data</p>	<p>European Union: Artificial</p>

<sup>48</sup> Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act ) and amending certain Union Legislative Acts [2021], recitals.

<sup>49</sup> Christiane Wenderhorst and Yannic Duller, Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces (Study, European Parliament, August 2021).

<p>characteristics of such individual's or group's known or predicted personality traits or social or economic situation, age, physical or mental ability, with the objective or to the effect of materially distorting the behaviour of that person or a person pertaining to that group in a manner that causes or is likely to cause that person or another person significant harm.</p>	<p>personality, age, or health to significantly alter behaviour, potentially causing substantial harm over time to individuals, others, or larger groups.</p>	<p>to build profiles of millions of users, inferring personality traits from their online activities. The firm allegedly used this data to deliver customised political ads during the 2016 U.S. Presidential Election and Brexit referendum, with claims of influencing voters. This case triggered widespread discussions on data privacy, AI ethics, and the risks of manipulation.</p>	<p>Intelligence Act 2021</p>
<p>Biometric categorisation systems that categorise natural persons according to sensitive or protected attributes or characteristics or based on the inference of those attributes or characteristics.</p> <p>The prohibition of such systems does not apply to AI systems intended to be used for approved therapeutic purposes on the basis of specific informed consent of the individuals that are exposed to them or, where applicable, of their legal guardian.</p>	<p>AI systems that categorise individuals based on sensitive or protected characteristics, such as gender, race, political orientation, or religion, can be highly intrusive, violate human dignity, and risk causing discrimination.</p>	<p>Companies are increasingly employing AI tools to evaluate job applications, assessing candidates based on various criteria like qualifications and skills. However, if the data used to train AI systems contains biases, such as gender or racial bias, the tools might undervalue applicants from certain groups. For example, if an AI tool was trained on data from a tech industry traditionally dominated by men, it might unfairly downgrade applications from women, reinforcing existing gender imbalances.</p>	<p>European Union: Artificial Intelligence Act 2021</p>

AI systems that are used for the social scoring, evaluation or classification of people or groups based on their social behaviour and that social score leads to detrimental or unfavourable treatment.	AI systems that provide social scoring can lead to discriminatory results and exclusion of certain groups, infringing on rights to dignity and non-discrimination. These systems evaluate individuals based on a multitude of data points and time occurrences related to their social behaviour, potentially resulting in disproportionate or unjust treatment in unrelated contexts.	China's Social Credit System assigns a score to citizens based on their financial behaviour, legal compliance, and social interactions, impacting various aspects of their lives, such as loan eligibility or travel rights.	European Union: Artificial Intelligence Act 2021
AI systems used for assessing the risk of individuals or groups committing or recommitting crimes, based on profiling or assessment of personality traits, locations, or past criminal behaviour.	AI systems used by law enforcement for predictions or risk assessments, based on profiling or past behaviour data, pose a risk of discrimination. These systems can violate human dignity and the principle of presumption of innocence and particularly target certain marginalised individuals or groups.	Predictive policing software used by U.S. law enforcement, that operates on past crime data to forecast future crime hotspots and guide police resource allocation. However, such systems have sparked concerns due to its potential to perpetuate existing policing patterns, resulting in the over-policing of communities of colour.	European Union: Artificial Intelligence Act 2021
AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage	The widespread and untargeted collection of biometric data from social media or CCTV footage to build facial recognition databases fosters a sense of mass surveillance and can result in severe infringements of fundamental rights, including privacy violations.	Clearview AI, a company uses facial recognition technology to scrape images on the web to create a searchable biometric database. A user can upload a snapshot of any person, and in response the system generates additional matches from the internet using biometric comparison. It was	European Union: Artificial Intelligence Act 2021

		<p>found that global law enforcement agencies were using Clearview AI, without sufficient oversight or disclosure. This revelation triggered a wave of lawsuits, with some focusing on the potential harm that Clearview's technology could inflict on survivors of domestic and sexual violence, undocumented immigrants, and marginalised communities. These groups unknowingly found themselves subjected to Clearview's 'face printing', potentially facing severe repercussions from the company's wide-ranging surveillance activities.</p> <p>Another example is of supermarket chains in Spain that have introduced a facial recognition system to identify and prevent individuals with restraining orders from entering their stores. The system uses the store's CCTV to capture facial images of incoming customers. These images are then converted into biometric templates, which are cross-referenced with the templates of individuals</p>	
--	--	---	--

		prohibited from entering the premises.	
AI systems to infer emotions of a natural person in the areas of law enforcement, border management, in workplace and education institutions.	There are serious doubts about the scientific validity of AI systems designed to detect emotions or physical features such as facial expressions or voice. These technologies often face issues of reliability and specificity, as emotions vary significantly among individuals and cultures. The use of such systems, particularly in contexts like law enforcement or education, can lead to misuse due to reliability issues. Therefore, deploying AI systems intended to detect emotional states in these contexts is prohibited.	AI systems are being used to suggest activities that align with a learner's cognitive abilities and provide real-time feedback, eliminating the need for a human teacher. These systems depend on analysing student performance data collected via IoT devices. However, there are concerns about practices like the use of facial recognition in Chinese schools to monitor student behaviour and concentration levels. Such collection and analysis of learning activities can seriously intrude on children's privacy, as the data can reveal detailed insights about a child's development, mental state, preferences, and weaknesses.	European Union: Artificial Intelligence Act 2021
The use of 'real-time' and 'post' remote biometric identification systems in publicly accessible spaces.	The use of AI systems for 'real-time' remote biometric identification in public spaces can infringe on personal rights and freedoms, create a sense of constant surveillance, and dissuade people from exercising their fundamental rights. Technical inaccuracies can lead to biased, potentially discriminatory results, especially regarding age, ethnicity, sex,	Law enforcement agencies around the world use real-time and remote biometric identification technology to locate suspects in public spaces. Incorrect predictions could not only result in discriminatory outcomes but can also threaten individual autonomy and self-determination, as the constant fear of being evaluated and monitored can alter public behaviours.	European Union: Artificial Intelligence Act 2021

	<p>or disabilities. These 'real-time' systems are prohibited due to their immediate impact and limited opportunities for checks or corrections.</p> <p>Similarly, AI systems used for post-analysis of recorded public space footage are also prohibited, except when pre-judicial authorization is obtained for law enforcement in the context of a specific serious criminal offense.</p>	<p>The broad effects that mass surveillance can have on a population's behaviour are also strikingly evident when observing China's social credit score system, which penalises its citizens for non-adherence to societal norms.</p>	
--	---	---	--



## Annexure D

### Global approach to a risk-based metric for controlling AI harms: high risk classifications

Use case	Sector	High Risk Classification	Region/country laws
<b>HIGH RISK</b>			
Biometric identification of natural persons	Biometric and biometrics-based systems	See Figures 1-3 below	European Union: Artificial Intelligence Act 2021, annex III
AI systems intended to be used to make inferences about personal characteristics of natural persons on the basis of biometric or biometrics-based data, including emotion recognition systems	Biometric and biometrics-based systems		
AI systems intended to be used as safety components in the management and operation of road, rail and air traffic	Management and operation of critical infrastructure		
AI systems intended to be used as safety components in the management and operation of the supply of water, gas, heating, electricity and critical digital infrastructure	Management and operation of critical infrastructure		
AI systems intended to be used for the purpose of determining access or materially influence decisions on admission or assigning natural persons to educational and vocational training institutions	Education and vocational training		
AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to those institutions	Education and vocational training		

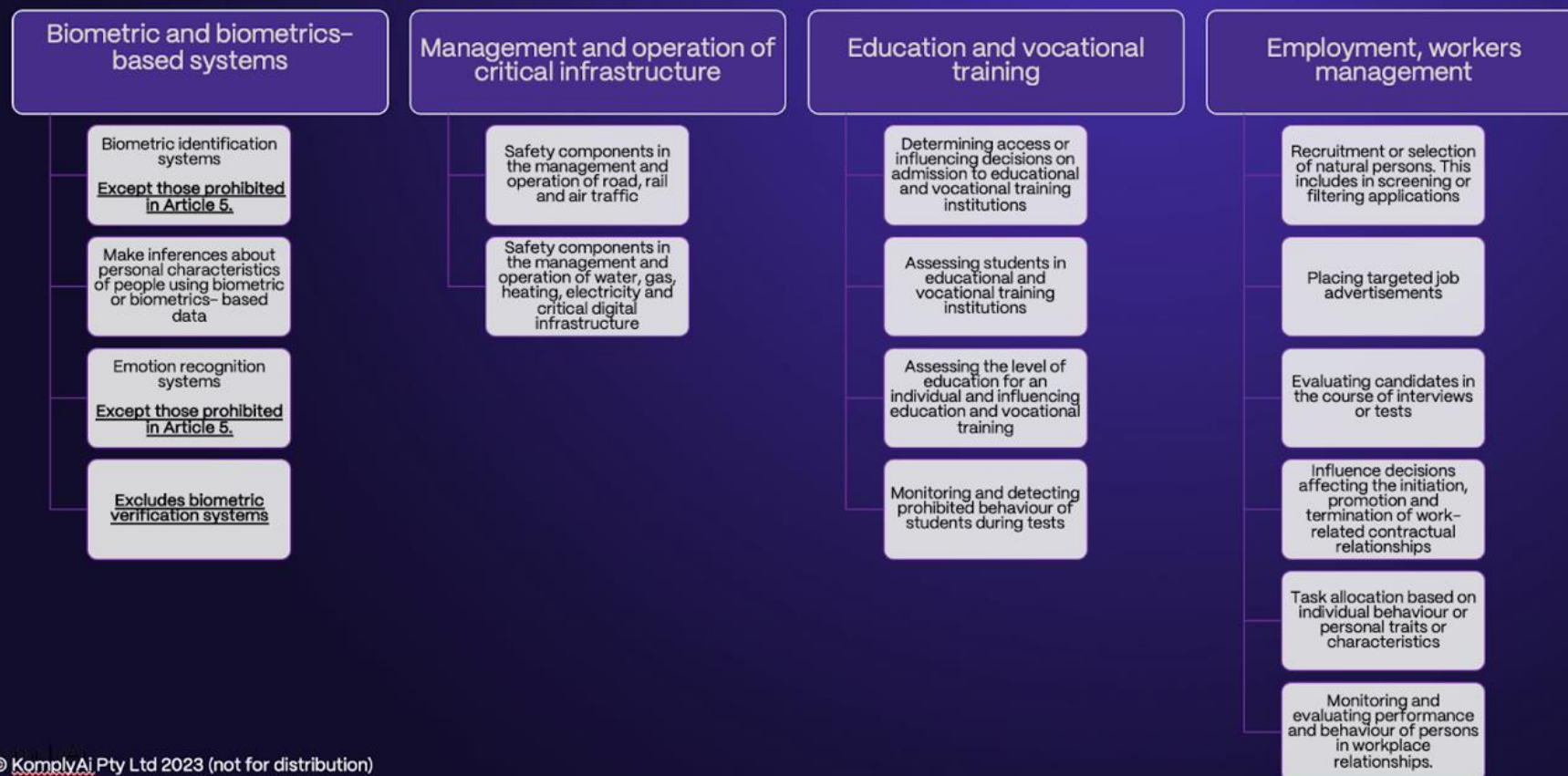
AI systems intended to be used for the purpose of assessing the appropriate level of education for an individual and materially influencing the level of education and vocational training that individual will receive or will be able to access	Education and vocational training		
AI systems intended to be used for monitoring and detecting prohibited behaviour of students during tests in the context of/within education and vocational training institutions	Education and vocational training		
AI systems intended to be used for recruitment or selection of natural persons, notably for placing targeted job advertisements, screening or filtering applications, evaluating candidates in the course of interviews or tests	Employment, workers management and access to self-employment		
AI systems intended to be used to make or materially influence decisions affecting the initiation, promotion and termination of work-related contractual relationships, task allocation based on individual behaviour or personal traits or characteristics, or for monitoring and evaluating performance and behavior of persons in such relationships	Employment, workers management and access to self-employment		
AI systems intended to be used by or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, including healthcare services and essential services, including but not limited to housing, electricity, heating/cooling and internet, as well as to grant, reduce, revoke, increase or reclaim such benefits and services	Access to and enjoyment of essential private services and public services and benefits		
AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud	Access to and enjoyment of essential private services and public services and benefits		
AI systems intended to be used for making decisions or materially influencing decisions on the eligibility of natural persons for health and life insurance	Access to and enjoyment of essential private		

	services and public services and benefits		
AI systems intended to evaluate and classify emergency calls by natural persons or to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by police and law enforcement, firefighters and medical aid, as well as of emergency healthcare patient triage systems	Access to and enjoyment of essential private services and public services and benefits		
AI systems intended to be used by or on behalf of law enforcement authorities, or by Union agencies, offices or bodies in support of law enforcement authorities as polygraphs and similar tools ; insofar as their use is permitted under relevant Union and national law	Law enforcement		
AI systems intended to be used by or on behalf of law enforcement authorities, or by Union agencies, offices or bodies in support of law enforcement authorities to evaluate of the reliability of evidence in the course of investigation or prosecution of criminal offences	Law enforcement		
AI systems intended to be used by or on behalf of law enforcement authorities or by Union agencies, offices or bodies in support of law enforcement authorities for profiling of natural persons in the course of detection, investigation or prosecution of criminal offences	Law enforcement		
AI systems intended to be used by or on behalf of law enforcement authorities or by Union agencies, offices or bodies in support of law enforcement authorities for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data	Law enforcement		
AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies as polygraphs and	Migration, asylum and border control management		

similar tools insofar as their use is permitted under relevant Union or national law			
AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State	Migration, asylum and border control management		
AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features	Migration, asylum and border control management		
AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies to assist competent public authorities for the examination and assessment of the veracity of evidence in relation to applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status	Migration, asylum and border control management		
AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies in migration, asylum and border control management to monitor, surveil or process data in the context of border management activities, for the purpose of detecting, recognising or identifying natural persons	Migration, asylum and border control management		
AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies in migration, asylum and border control management for the forecasting or prediction of trends related to migration movement and border crossing	Migration, asylum and border control management		

AI systems intended to be used by a judicial authority or administrative body or on their behalf to assist a judicial authority or administrative body in researching and interpreting facts and the law and in applying the law to a concrete set of facts or used in a similar way in alternative dispute resolution	Administration of justice and democratic processes		
AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda This does not include AI systems whose output natural persons are not directly exposed to, such as tools used to organise, optimise and structure political campaigns from an administrative and logistic point of view	Administration of justice and democratic processes		
AI systems intended to be used by social media platforms that have been designated as very large online platforms within the meaning of Article 33 of the Digital Services Act (EU) 2022/2065, in their recommender systems to recommend to the recipient of the service user-generated content available on the platform	Administration of justice and democratic processes		
<b>HIGH IMPACT</b>			
		See Figures 4-5 below	AIDA Canada

# High Risk: AI Systems in Annex III (1)



© KomplyAi Pty Ltd 2023 (not for distribution)

Figure 1



## High Risk: AI Systems in Annex II (2)

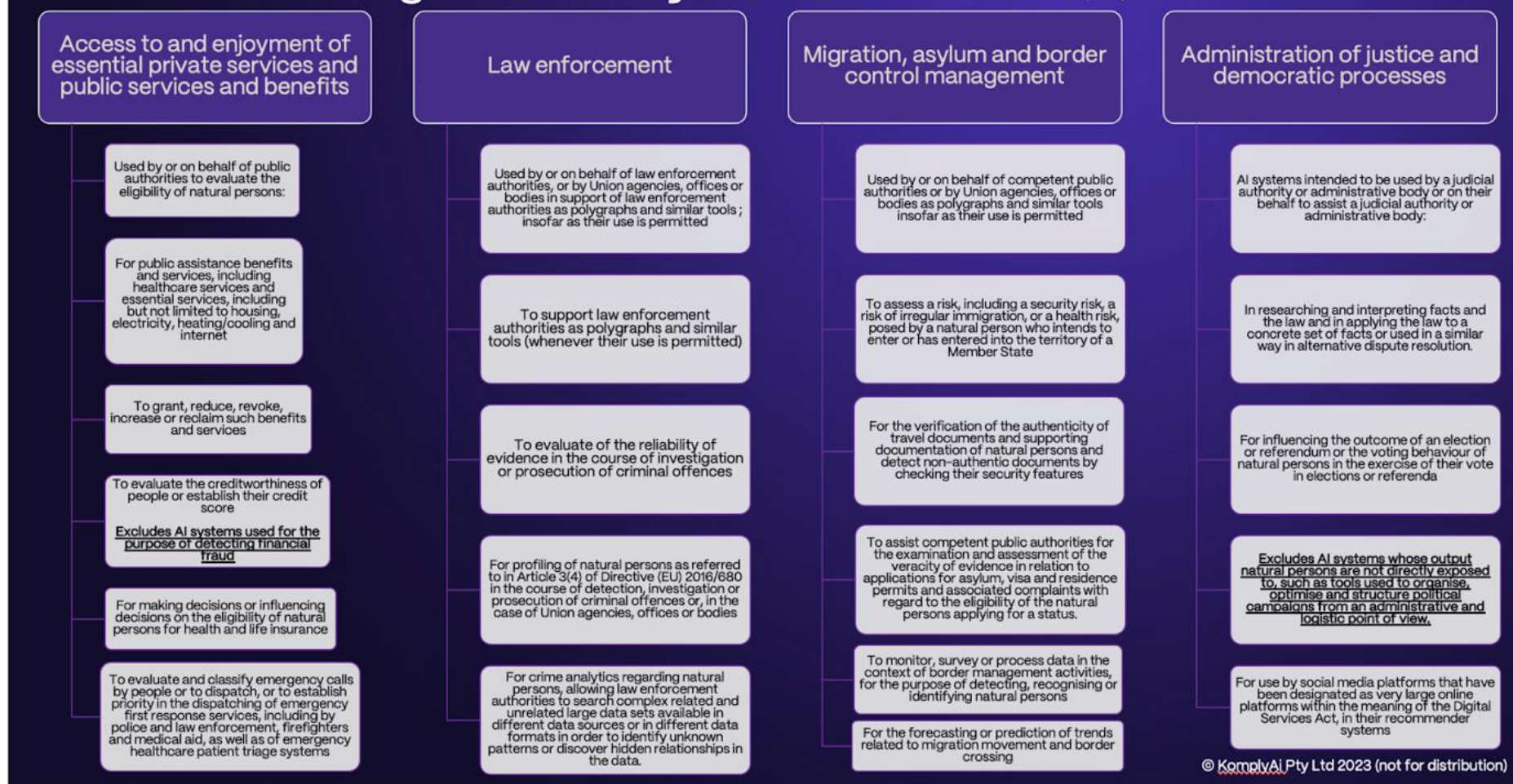


Figure 2

# High Risk Requirements – what you need to do?



© KomplyAi Pty Ltd 2023 (not for distribution)

Figure 3



# What are 'High-Impact' AI Systems?

A person who is responsible for an artificial intelligence system must, in accordance with the regulations, assess whether it is a high-impact system.

Term not defined in the Bill, the following factors are considered when determining what AI systems are high-impact

Evidence of risks of harm to health and safety, or a risk of adverse impact on human rights

Severity of potential harms caused by the system

Scale of use of the system

Severity of harms or adverse impacts

Ability to opt out from the AI system, either practically or legally

Economic or social imbalances

Age of users interacting with the AI system

Whether risks are adequately regulated under another law

© KomplyAi Pty Ltd 2023 (not for distribution)

Figure 4

<p>Requirements for "High-Impact AI Systems"</p> <p>Developers and Operators</p> <p>© KomplyAi Pty Ltd 2023 (not for distribution)</p>	1	ESTABLISH MEASURES	Identify, assess and mitigate risks of harm, biased outputs and system limitations
	2	MONITOR	Monitor compliance and effectiveness of risk related measures
	3	RECORD	Keep records with detailed information about the AI system
	4	DISCLOSURE	Publish key information about the system on a publicly available website
	5	REPORT	Notify authorities if the use of the system will cause harm

Figure 5

## Annexure E

### Classification System for Organisational Based Licensing

Organisation	Organisation size	Sector/(s) or agnostic (general)	Activity type/(s)	Technology/(ies) (sub domains, and nominated novel characteristics of AI technologies)	Data privacy impact score (e.g., sensitive data, health data)	Cybersecurity impact (e.g., critical infrastructure)	End use impact score (e.g., fundamental rights impact assessment,	End user impact score (e.g., vulnerability profile of end user)	Conditions for licence holders.
									<p>Based on a scoring mechanisms for a model AI classification. This score and its accuracy could become more intelligent over time once we have aggregated data about "AI harms" that can better facilitate our understanding of where we need targeted intervention in the form of licensing controls.</p> <p>Conditions could involve a period for licensing approval, and reviews, baseline foundational requirements for responsible AI &amp; risk management.</p>

									<p>Conditions imposed, or licence revoked for particularly serious breaches (or multiple breaches), including optionality for external algorithmic audits.</p> <p>Minister may respond and impose conditions on a licence holder where there is a serious risk of imminent harm or to prevent serious harm.</p>
--	--	--	--	--	--	--	--	--	---

Example of U.S. & Australian laws where there is a classification system for licensing and technology export activities

[Export Administration Regulations \(EAR\) \(doc.gov\)](#) & [Licences \(AUSGELs\) | Business & Industry | Defence](#)

### Commerce Country Chart

#### Reason for Control


Countries	Chemical & Biological Weapons			Nuclear Nonproliferation		National Security		Missile Tech	Regional Stability		Firearms Convention	Crime Control			Anti-Terrorism	
	CB 1	CB 2	CB 3	NP 1	NP 2	NS 1	NS 2	MT 1	RS 1	RS 2	FC 1	CC 1	CC 2	CC 3	AT 1	AT 2
Afghanistan	X	X	X	X		X	X	X	X	X		X		X		
Albania <sup>2,3</sup>	X	X		X		X	X	X	X	X						
Algeria	X	X		X		X	X	X	X	X		X		X		
Andorra	X	X		X		X	X	X	X	X		X		X		
Angola	X	X		X		X	X	X	X	X		X		X		
Antigua & Barbuda	X	X		X		X	X	X	X	X	X	X		X		
Argentina	X					X		X	X		X	X		X		
Armenia	X	X	X	X		X	X	X	X	X		X	X			
Aruba	X	X		X		X	X	X	X	X		X		X		
Australia <sup>3</sup>	X					X		X	X							
Austria <sup>3,4</sup>	X					X		X	X			X		X		
Azerbaijan	X	X	X	X		X	X	X	X	X		X	X			

## Help

Definitions  
Acronyms & Abbreviations  
Forms  
Information on the DSSL  
DEC Website  
Contact DEC  
Sanctions

## My DSSL Items

You have not added any

 Print My DSSL Items

## DSSL Search

Please enter your search query below. Your queries will be retained for the duration of this session and listed in the My DSSL Items output document for your reference. N.B. You can generate an output document without adding any items to My DSSL Items.

**Note:** Users may occasionally experience problems with the search engine not returning any results. To confirm this fault, search for the term "cyanide". If no results are returned, please notify Defence Export Controls at [dip.bss@defence.gov.au](mailto:dip.bss@defence.gov.au).

Filter by Part	Filter by Category	Filter by Sub Category	Filter by Item
PART 2 Dual Use List	All	3A - Systems, Equi...	All
	CATEGORY 3 - ELE...		3A001

Displayed below are the DSSL items that may match your search query. Any exact matches appear in bold. This search tool uses a database of commonly-used synonyms, so your specific search term may not appear in the item at all.

1 result

## Electronic components

**Item No.:** 3A001 PART 2 Dual Use List > CATEGORY 3 - ELECTRONICS > 3A - Systems, Equipment and Components

the function has been determined, is to be evaluated against the parameters of **3A001.a** ... analogue-to-digital converters and store or process the digitised data, see **3A001.a.14** ...

## Annexure F

### Treatment of start-ups and SMEs under global AI laws

Type of Support	Region/country laws
The AI Act will introduce measures to foster innovation, emphasizing support for SMEs and start-ups. It provides that European Member States will establish regulatory sandboxes and measures to lessen regulatory burdens on SMEs and start-ups. Access to all AI regulatory sandboxes is intended to be free of charge for SMEs and startups.	European Union: Artificial Intelligence Act 2021, Articles 1(ea) and 53a(2)(c)
Prospective providers in the sandboxes, in particular SMEs and start-ups, will have access to pre-deployment services such as guidance on the implementation of the AI Act requirements, to other value-adding services such as help with standardisation documents and certification and consultation, and to other Digital Single Market initiatives such as Testing & Experimentation Facilities, Digital Hubs, Centres of Excellence, and EU benchmarking capabilities.	European Union: Artificial Intelligence Act 2021, Article 53a(3)
Third-party conformity assessment fees will be tailored for SMEs according to their size and market share.	European Union: Artificial Intelligence Act 2021, Article 43(4)(a)
Start-ups and SMEs with high risk AI systems will not be required to carry out extensive consultations with different stakeholders when performing a fundamental rights impact assessment.	European Union: Artificial Intelligence Act 2021, Article 29(a)(4)
SMEs and start-ups can create alternative documentation fulfilling the objectives of the technical documentation requirements.	European Union: Artificial Intelligence Act 2021, Article 11(1)
Competent bodies may establish the conditions, requirements,	Brazil: Bill nº 2.338/2023, Article 32

communication and disclosure channels for micro or small companies/startups that are providers and operators of AI systems.	
Competent bodies may authorise the implementation of an experimental regulatory environment for innovation in AI ('regulatory sandbox') for the entities applying for it and fulfilling the requirements specified by the proposed law.	Brazil: Bill nº 2.338/2023, Article 38
AI sandbox: The UK government will remove barriers to innovation and minimise legal and compliance risks for SMEs and businesses to help AI innovators navigate the regulatory landscape. The government has established a multi-regulator AI sandbox that will test how the UK's AI regulatory framework operates and whether regulators or the government should address unnecessary barriers to innovation	UK, 'A pro-innovation approach to AI regulation' (Policy Paper, 2023)





## Annexure G

<h3>Localisation</h3> <p><b>What makes Australia different?</b></p> <ul style="list-style-type: none"> <li>• Thriving innovation communities</li> <li>• Key market advantages in other emerging technologies (quantum computing)</li> <li>• Geographically isolated</li> <li>• Dependent on IP imports</li> <li>• Extensive AI skills shortages</li> <li>• Wide community mistrust of AI (prevention of AI take-up)</li> <li>• Start-ups and SMEs underfunded comparatively to other countries</li> <li>• Geopolitical issues</li> </ul> <p><b>Risks to harmonisation approaches</b></p> <ul style="list-style-type: none"> <li>• Current administrative resources and infrastructure cannot keep pace with technological changes and requirements for ongoing and continuous product reviews</li> <li>• Impede competition in emerging, well invested growth industries</li> <li>• Impact our innovation communities</li> <li>• Unduly disadvantage start-ups and SMEs</li> <li>• Subsume other countries' cultural nuances that don't sit comfortably with Australia's way of life</li> </ul>	<h3>Coherence</h3> <p><b>What does coherence look like for Australia?</b></p> <ul style="list-style-type: none"> <li>• Clear prohibited AI activities with a focus on the outcome of those activities on citizens. Align with like-minded counterparts</li> <li>• Australia does not want to be the 'testing group' for detrimental AI</li> <li>• A different way to ensure responsible AI</li> <li>• Technology passport, focusing on good corporate governance</li> <li>• A licensing regime for organisations not products</li> <li>• Baseline foundation requirements for organisations</li> <li>• Technology neutrality and fluidity in AI and emerging technologies</li> <li>• Quickly react to international treaties about AI to facilitate trusted trade activities</li> <li>• Exclusions for start-ups and SMEs (with some exceptions based on safety)</li> <li>• Exclusions for R&amp;D activities and open source (with some exceptions based on safety)</li> <li>• Mandatory reporting of major AI malfunctions</li> <li>• Pilot proposals early (now) with industry, government, and public</li> <li>• Quotas for prescribed organisations to contribute to address safe AI and digital divide concerns</li> <li>• Cross functional departmental co-ordination in key intersecting areas such as anti-discrimination, data privacy, IP, consumer and competition protection and defence</li> <li>• Better understand operation of existing laws intersecting with AI</li> <li>• Key changes to a number of existing laws, including out-dated IP laws</li> </ul>	<h3>Harmonisation</h3> <p><b>What could parity and harmonisation look like?</b></p> <ul style="list-style-type: none"> <li>• Prohibited AI activities</li> <li>• Parity with risk classification system for responsible AI, including high risk use cases</li> <li>• Treatment of start-ups and SMEs (exclusions etc)</li> <li>• Exclusions for R&amp;D and open source in some circumstances</li> </ul> <p><b>The benefits</b></p> <ul style="list-style-type: none"> <li>• Increase interoperability where laws apply extraterritorially</li> <li>• Business efficiencies, particularly for those with a global footprint or aspirations for such</li> <li>• Cross boarder flow of technologies supported with reduced complexities for AI supply chains</li> </ul>
---	--	---