Evolving legal landscape for Australian businesses operating in the UK and EU

This article was first published in the LexisNexis Privacy Law Bulletin, issue 22.02.

Australian businesses providing B2C or B2B digital services in the United Kingdom (**UK**) or the European Union (**EU**) must consider new regulatory frameworks concerning various aspects of digital services such as artificial intelligence (**AI**), online safety, data and data privacy, and cyber security.

AI regulation

The AI Act (**AIA**) will apply to any Australian businesses that develop, use, import, or distribute an AI system in the EU. From 2 February 2025, various provisions became effective.

Firstly, AI systems which pose unacceptable risk designed for manipulation and deception, harmful exploitation of age or other vulnerabilities, social scoring in unrelated social contexts, predicting delinquency, data scraping for facial recognition, emotion recognition, biometric categorisation and real time remote biometric identification are prohibited under Article 5.

The recent guidelines adopted by the European Commission[1] suggest a broad interpretation of these prohibited categories. Australian businesses developing AI systems which edge on "prohibited AI practices" should anticipate enquiries about how their service either satisfies an exemption or falls outside these prohibitions.

Secondly, there is an obligation to ensure "*a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf*". This means that a base level of AI literacy must be ensured across the organisation and specialist knowledge for key stakeholders. The Dutch data protection authority identifies four steps in ensuring AI literacy, including identification, goal setting, implementation and evaluation.[2]

The EU's AI Office will have finalised a general-purpose AI (**GPAI**) code of practice by 9 May 2025 under AIA. Its third draft[3] elaborates on the detailed technical documentation and transparency requirements (including details about training data) under article 53, and the safety obligations for GPAI with systemic risk under article 55 of AIA. These obligations will become effective on 2 August 2025.

Australian services offered in the EU and UK have long had a duty to provide meaningful information about automated decision-making under Articles 12-14 and 22 of GDPR. In

[1] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) (link).
[2] Get started with AI Literacy, Autoriteit Persoonsgegevens, February 2024 (link).
[3] General-Purpose AI Code of Practice, European Commission (link).

the recent case of *Dun & Bradstreet Austria*,[4] it was clarified that transparency and explainability must enable the person to understand the link between their personal data and the automated decision and to verify the accuracy of the decision. Such information cannot be withheld on the basis that it constitutes a trade secret but the controller can disclose such information to a court or a regulator who will determine the level or required disclosure.

The proliferation of AI features adopted by service providers could raise GDPR compliance issues for Australian businesses providing services in the EU and UK. When appointing service providers who will handle UK and EU data, Australian businesses must ensure that their Article 28 data processing terms adequately curtail any unauthorised data use by those providers for AI model training.

Online safety

Australian businesses will already be familiar with the Australian Online Safety Act 2021 effective from January 2022. It applies to social media, communication services, games, app stores, search engines, and other designated services as well as device manufacturers and providers.[5]

Service providers must operate an effective complaints procedure for end-users to flag any offensive content. Some of the Basic Online Safety Expectations (BOSE)[6] on providers include taking reasonable steps to ensure service safety and proactively minimising access to unlawful or harmful material.

Similarly, services provided by an Australian business to a client, customer or user in the EU may be caught by the **Digital Service Act** (**DSA**)[7] if there is a substantial connection to the EU. Such connection may exist if a significant number of EU customers are served or if EU member states are targeted.

Effective since 17 February 2024, the DSA applies to all "*intermediary services*". Despite the deceptive label, this definition is very broad and will include most B2C and B2B digital services, including 'mere conduit', 'caching' or 'hosting' services. The 'hosting' category captures any physical, network, or application layer hosting services, including any cloud computing, web hosting or any peer-to-peer service.

Australian providers which are in scope must, among other things:

- Designate a single point of contact for users and authorities in the EU.
- Appoint a legal representative and notify the Digital Services Coordinator authority.

[4] C-203/22 CK v Magistrat der Stadt Wien / other party: Dun & Bradstreet Austria GmbH (link).
[5] Equipment Online Safety Code (Class 1A and Class 1B Material) (link).
[6] Online Safety (Basic Online Safety Expectations) Determination 2022 amended on 31 May 2024 (link).
[7] 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)

- Implement technical capabilities to block and remove content.
- Regulate content in the service in a diligent, objective and proportionate manner by enforcing terms and conditions and operating a takedown procedure.
- Restrict users who engage in certain online behaviour and provide a statement of reasons.
- Ensure the traceability of traders featured in online marketplaces.
- Implement appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors.
- Report illegal content to law enforcement authorities.
- Publish an annual transparency report on content moderation and enforcement.

Further obligations apply to 'online platforms', 'very large online platforms' (VLOPs) and 'very large online search engines' (VLOSEs). Their compliance will be overseen by the European Commission[8] while member state authorities will watch over all other providers. The European Board for Digital Services is expected to release guidance and codes of conduct. Concurrently, the **Digital Markets Act** (**DMA**) applies to very large platforms, so called "gatekeepers", and helps establish a level playing field in the digital space. The recent voluntary Hate Speech Code of Conduct[9] emphasises transparency reporting on the measures adopted.

The UK Online Safety Act 2023 applies to "user-to-user services" with a significant number of UK users, targeting the UK market or posing a material risk of significant harm to users.

A code of practice issued by the UK's Office of Communications (**Ofcom**)[10] requires service providers, among other things, to:

- Appoint an accountable individual.
- Implement a content moderation function, including ability to review, assess and remove content.
- Implement user complaints systems and processes.
- Investigate suspected illegal content.
- Update terms of service to explain the use of proactive technologies and other matters.
- Remove accounts of proscribed organisations such as terror groups.

Ofcom has significant investigatory powers. In 2024, TikTok was fined £1.875m for failing to provide accurate information about its parental controls.[11] Recently, OnlyFans was

[8] COMMISSION DECISION (EU) 2025/628 of 31 March 2025 laying down internal rules concerning the provision of information to data subjects and the restrictions of certain data-subjects' rights in relation to the processing of personal data by the Commission for the purpose of the supervision, investigation, enforcement and monitoring under DSA (link).
[9] Code of Conduct on Countering Illegal Hate Speech Online +, European Commission, 20 January 2025 (link).
[10] Illegal content Codes of Practice for user-to-user services, Ofcom, 24 February 2025 (link).
[11] TikTok fined £1.875m for providing inaccurate data on safety controls (link).

fined £1.05m[12] for failing to adequately respond to requests abouts age-assurance. OnlyFans took over one year to discover a discrepancy with its age-assurance vendor.

Online safety is often associated with content moderation. Content moderation could give rise to human rights issues including an interference with privacy, freedom of speech, access to information, and others. Each of the discussed online safety regimes anticipates content moderation which can be reactive or proactive. However, a careful balance must be struck between peoples' rights and freedoms and any adopted content moderation measures and objectives.

As any global indiscriminate monitoring of all user content would likely be unlawful, proactive measures typically include measures at user account level such as age verification and age assurance, protective account settings including smart content filters, regulating recommender systems, etc.

The DSA explicitly states that no general monitoring, active fact-finding or proactive action duty is imposed. However, it also encourages a provider's own-initiative investigations into suspected illegal content. The DSA anticipates that member state authorities may issue orders to providers to act against specific items of illegal content, which may include proactive measures in a targeted way. Similarly, the Australian regime expects proactive steps to detect and remove seriously harmful content like child sexual exploitation or terrorism content. However, it does not refer to the blanket monitoring of all user communications across a network.

Nevertheless, there is a greater shift to proactive monitoring as relevant privacy-preserving technologies become available and as codes of practice are updated. The UK regime anticipates the deployment of perceptual hash matching technology, where technically feasible,[13] to remove child sexual exploitation material. The recent voluntary Code of Conduct on Disinformation[14] refers to anti-deepfake policies '*such as warning users and proactively detect such content*'. Following endorsement by major providers, the code will become a Code of Conduct under the DSA and auditable from 1 July 2025.

Whilst Australian penalties are capped at AUD$782,500 for corporations, the UK fines go up to £18m or 10% of qualifying worldwide revenue. The DSA leaves enforcement to member states and fines under national law must not exceed 6 % of the offending corporation's preceding year's annual worldwide turnover. Under the UK regime, directors and senior managers can be held criminally liable for non-compliance.
Unlike the Australian or UK regimes, the DSA also provides for a direct right of action allowing affected individuals to bring proceedings.

[12] Ofcom fines provider of OnlyFans £1.05 million (link).
[13] Illegal content Codes of Practice for user-to-user services, Ofcom, 24 February 2025 (link).
[14] The Code of Conduct on Disinformation, European Commission, 13 February 2025 (link).

Data and data privacy

Most Australian businesses will host data of their UK/EU clients. If servers are located outside of the client's country, for example, in Australia, the client and the service provider may be engaging in an international data transfer. If the GDPR rules on international data transfers are not followed, affected individuals could claim damages.

In *Bindl v European Commission*, the CJEU held that putting the user "*in a position of some uncertainty*" about whether their data may have been processed, was actionable. The court awarded $400 in damages.[15] Australian business must remember that data transfers are not a low risk area of compliance.

Separately, effective from 12 September 2025, the EU's Data Act (**DA**) is intended to increase fairness in the allocation of data value. It imposes an obligation on operators of connected products and related services, including Australian operators in the EU in this space.

Providers will have to make data available free of charge to their consumer or business users or a third party designated by the user. The DA expands the user's right to portability to not only actively provided data but also passively observed data.

Services must be designed for easy access by the user. This will apply to all personal data, non-personal data and underlying raw data, for example, user commands, transactions, movement in app, access logs, security scans, metadata, search queries, results returned, time stamps, login and password reset logs, SQL logs, time spent on page, virtual assistant data collected when on, on standby and off, diagnostic data. Excluded are derived data and analytics outputs.

The DA imposes significant restrictions on data holders, who must not use data to derive insights about the economic situation, assets and production methods of the user or to undermine the user's commercial position on the markets.

Further, the DA regulates cloud, edge and other service providers by prohibiting lock-in contracts, unilateral degradation of service during contract term and enables the seamless porting of data to a new provider.

Cyber security

Australian businesses involved in manufacturing, importing, or distributing connected devices in the UK must comply with the UK's Product Security and Telecommunications Infrastructure Act 2022 (**PSTIA**). Effective from April 2024, the requirements include regulations regarding passwords, channels for notifying the manufacturer, software

[15] Case T-354/22, Bindl v European Commission (link).

update periods, and statements of compliance. These requirements do not apply to excluded products such as smart meters.

The EU's Cyber Resilience Act (**CRA**), passed in October 2024 and effective from 11 December 2027, mandates specific cybersecurity obligations for products with digital elements available in the EU. These requirements encompass security measures, design considerations, vulnerability management, and market oversight. The obligations for vulnerability reporting by manufacturers commence on 11 September 2026, while provisions pertaining to conformity assessment bodies take effect from 11 June 2026.

The Digital Operational Resilience Act (**DORA**)[16] effective on 17 January 2025 is aimed at enhancing operational resilience of digital systems in the financial sector. It requires, among other things, information and communication technology (**ICT**) risk management and governance, risk mapping, anomaly detection, incident management, crisis communication, recovery, resilience testing, supply chain risk management, reporting and protocols for information sharing.

The EU's second Network and Information Security Directive (**NIS 2**) became effective on 18 October 2024. Despite many member states missing the transposition deadline, NIS 2 sets significant new obligations for critical services and infrastructure providers. Australian businesses serving these providers may also face new supply chain (including third and fourth party) risk assessment requirements.

The extraterritorial nature of these laws, results in an increased risk for Australian providers. In additions, even Australian B2B providers could be liable for regulatory penalties. The recent settlement for £3.07m[17] between the UK's Information Commissioner's Office (**ICO**) and a software company represents a shift from the traditionally held view that processors are less at risk of penalties.

During a ransomware incident in August 2022, unauthorized individuals gained access to several health and care systems through a customer account that lacked multi-factor authentication (**MFA**). Although MFA was offered as an optional feature to customers, the ICO indicated that failing to implement it constituted a breach of the data processor's security obligations under the GDPR.

The GDPR will directly apply not only to B2C providers offering goods or services to UK or EU consumers or monitoring their behaviour, but it may also directly apply to B2B providers whose data processing 'relates' to that of their business customer.[18] This increases the risk of a GDPR penalty for Australian B2B providers, even if they are not established in the UK or EU.

Future trends

[16] REGULATION (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector, etc. (link).
[17] Software provider fined £3m following 2022 ransomware attack, 27 March 2025 (link).
[18] Clearview wins appeal against ICO fine in tribunal (link).

The regulatory focus on cyber security and online safety, particularly child safety, seems to be at its peak as comprehensive regulatory frameworks emerge. We start seeing comprehensive regulatory guidance which will likely only become more complex over time as new digital risks and new ways to mitigate them emerge.

Separately, various data sharing frameworks are now effective. Ensuring easy access to data and interoperability of systems through APIs and by other secure means will be essential for compliance.

The extraterritorial effect of digital regulations and cross-border cooperation in regulatory enforcement will likely result in organisations seeking global solutions to their compliance requirements.

As the EU builds its pillars of digital regulation, we can expect more complexities and guidance in relation to seemingly opposing objectives, such as data protection on the one hand and data sharing fostering innovation on the other.

Alexander Dittel is a Principal in **Data Privacy, Cyber and Digital** at KHQ Lawyers

30 April 2025