CONTRACTPROBE

Data Sovereignty Issues When Choosing an AI Contract Review Tool in Australia

A recent research report [1] has highlighted data sovereignty as a key concern for lawyers intending to use AI. According to that report, data and information governance was highlighted as a key concern by those lawyers.

This white paper summarises the practical issues that arise when using offshore AI services to assist with legal work, using AI contract review as a particular example to illustrate the issues.

This white paper covers the following issues:

- ***Is your contract data processed exclusively in Australia?***
- ***Where is your supplier (or its critical subprocessors) located?***
- ***Has the legal tech tool been designed to cover Australian-specific statutes?***

The appendix additionally contains a sample Supplier due diligence questionnaire, a scoring matrix to assist in comparing different suppliers and a list of clauses that could be considered for inclusion in the services agreement.

Is your contract data processed exclusively in Australia?

Organisations wanting contracts to be reviewed by an AI solution should investigate whether their contract data is processed exclusively in Australia end-to-end. In practice, "processing" should be read broadly. It can include where the contract is uploaded, where model inference occurs, where prompts and outputs are stored (even temporarily), where logs are retained, where backups are held, and where supplier support personnel can access systems.

From a risk perspective, widely reported Australian data incidents show that oversight and incident response can be harder where key systems, subprocessors, or operational teams are located offshore. For in-house legal and procurement teams, this increases the importance of understanding the full data flow and the supplier's operational model.

Companies disclosing contracts which include personal information outside Australia also need to consider their obligations under the cross-border disclosure provisions in the Australian Privacy Act. Australian Privacy Principle 8 (APP 8) generally requires an Australian organisation to take reasonable steps to ensure that an overseas recipient handles an individual's personal information in a manner consistent with the Australian Privacy Principles, unless an exception applies.

APP 8 typically requires due diligence on the privacy laws and practices that govern the place where the data is processed, and on the supplier's actual data handling practices. Any gaps in protection may need to be addressed via appropriate contractual provisions (including security, audit, retention, and breach notification obligations).

The Privacy Act can also impose liability on Australian organisations for certain acts or practices of overseas recipients. In broad terms, section 16C can make Australian organisations accountable for misuse or mishandling of personal information by the overseas recipient. To manage this, organisations should perform due diligence on the overseas recipient's data handling practices and ensure the contract clearly allocates responsibilities and provides enforceable protections (including security requirements, audit/assurance, retention/deletion, and prompt incident/breach notification).

Due diligence questions include:

- Where is any personal information contained in the contract stored, processed, and backed up (including disaster recovery)?
- Where does model inference occur?
- Are outputs retained, and, if so, for how long?
- What logs are collected, and do they contain customer content or sensitive metadata?
- Who can access systems (including support/admin access), from where, and under what controls?
- What subprocessors are used, and where are they located?
- Is customer content used to train models (by default, opt-in, or opt-out), and what controls prevent leakage?
- What are the supplier's incident response SLAs (time to notify, time to escalate, contact points at different escalation points)?

Benefits of data being processed exclusively in Australia

- Increased ability for customers to monitor how data is handled and protected.
- Assists in compliance with Australian privacy laws and internal governance requirements.
- Reduces exposure to cross-border transfer risks (including accountability under section 16C).

Where is your supplier (or its critical subprocessors) located?

Even if data is processed in Australia, supplier location and corporate structure can materially affect the protection afforded to uploaded data. As a practical matter, where the supplier (or key subprocessors) conduct their operations mainly outside Australia, there is the risk of increased delays and complexity in incident response, time-zone coverage, and prioritisation during a crisis.

Prompt notification during a crisis is particularly important to ensure compliance with the data breach notification requirements in Part IIIC of the Australian Privacy Act. That Part requires an Australian company which experiences an eligible data breach to notify affected individuals and the Office of the Australian Information Commissioner (OAIC).

A company which has provided contracts which contain personal information to an external supplier will need to ensure that the company is promptly informed about any data breaches, so that it can in turn notify its own customers about the breach.Where personal information is provided to an external supplier, the customer should ensure it is promptly informed of relevant incidents so it can meet its own notification obligations.

An additional risk that may be relevant in some circumstances is the compelled disclosure of data pursuant to the laws of a foreign country. Those laws can require an overseas company which (either directly or through subsidiaries) is holding information in Australia, to disclose that information in accordance with requests by a foreign government. The US Cloud Act and its enabling legislation in Australia[2] is an example of such a law.

Due diligence questions include:

- What is the supplier's corporate structure (parent entities and key group companies)?
- Are there contractual commitments to notify disclosure requests (where lawful) and to minimise disclosures?
- Can the customer require onshore-only access for sensitive information?
- Which jurisdictions can compel the supplier and its critical subprocessors (including cloud providers) to hand over the customer's information?

Benefits of supplier being located in Australia

- Australian-based providers are more likely to be familiar with Australian legal requirements and client expectations; geographically they can offer support during Australian business hours, which can be critical in a crisis.
- Australian suppliers may be more likely to operate policies and controls aligned with Australian privacy and security expectations.
- Reduces exposure to foreign legal compulsion risk (subject to the supplier's subprocessor choices).

Has the legal tech tool been designed to cover Australian specific statutes?

Many generative AI tools have been trained predominantly on data from outside Australia. Accordingly, they may not be well suited to analysing material in the Australian legal context. Australian organisations operate under statutes and regulatory expectations that in some cases are unique to Australia or that treat key issues differently to other jurisdictions. Large language models that have not been trained to recognise these differences are more likely to produce incomplete or incorrect outputs.

As an example in the privacy context, Australian Privacy Principle 11.1 requires an organisation to take reasonable steps to protect personal information from misuse, interference and loss. When information is being disclosed to a third party, this duty can extend to taking steps at the time of disclosure to ensure the information will be treated appropriately by the third party after disclosure[3]. Consequently, a legal tech tool reviewing a contract that deals with the disclosure of personal information should be able to identify this risk and recommend measures to manage it (for example, strengthening security obligations, audit/assurance and breach notification, and—where appropriate—allocating risk through indemnities and related contractual protections). Legal tools not attuned to Australian legal requirements might overlook this extension of responsibility.

As an example of the type of clause that might be needed, contracts that are drafted by overseas suppliers will typically not include robust language to protect the personal information that has been disclosed to them. The contract will accordingly need to be reviewed to check if it contains language such as the following (illustrative only):

> *Upon the occurrence of a Security Incident, the Supplier must:*
>
> > *(a)promptly notify the Customer of the incident and provide the Customer on an ongoing basis with full details of the incident as those details become known to the Supplier;*
> >
> > *(b) promptly take all actions that are necessary in order to minimise the adverse consequences of the incident on the Customer;*
> >
> > *(c)promptly take all actions that are necessary in order to prevent the reoccurrence of that Security Incident or of similar incidents; and*
> >
> > *(d)provide the Customer on an ongoing basis with full details of the steps that the Supplier is taking under paragraphs (b) and (c).*
>
> *"Security Incident" means any actual or suspected incident that results in, or may result in, misuse, interference, loss, unauthorised access, unauthorised modification or unauthorised disclosure of any data provided by the Customer to the Supplier, or generated by the Supplier in the course of providing services under this Agreement, including any incident that constitutes an eligible data breach under Part IIIC of the Privacy Act 1988 (Cth).*

Benefits of the legal tech tool being designed to cover Australian Specific Statutes

- Increased accuracy due to the tool being trained on Australian-sourced data and patterns.
- More likely to be designed to address issues raised by Australian laws and procurement expectations.

Conclusion

Lawyers need to weigh these security, privacy and governance factors when selecting AI contract review tools. Choosing a solution that keeps contract data onshore (where required) and is tailored to Australian law can reduce the risk of disclosing information to an AI tool.

Disclaimer: This paper is provided for general information only and does not constitute legal advice. Organisations should obtain advice for their specific circumstances

References

1. Legal Innovation Report 2026, pg. 9, available for download at https://www.legalfestival.com/.
2. https://www.ag.gov.au/international-relations/international-crime-cooperation-arrangements/international-production-order-framework .
3. For an example where the contractual clause was not included and a breach occurred, see the report on the DonateBlood.com.au data breach, available at https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-decisions/Investigation-inquiry-reports .

Appendix A – Minimum Due Diligence Pack

A1. Supplier due diligence questionnaire (AI contract review tools)
Data location, processing and retention

1. Where is the customer contract stored, processed and backed up (primary, backup, disaster recovery)?
2. Where does model inference occur? Is any processing performed outside Australia?
3. Does the supplier retain the uploaded contract, any associated metadata or the generated outputs? If so, for how long? Can retention be configured or disabled?
4. What logs are collected? Do they include uploaded contract, any associated metadata or the generated outputs?
5. What subprocessors are used (including cloud providers), and where are they located? Provide a current list.

Access controls and operational security

1. Who can access customer data (roles), from where (in what countries), and under what access controls (MFA, privileged access management, just-in-time access)?
2. Is onshore-only support available for sensitive matters? Can offshore access be contractually excluded?
3. What are your encryption controls (in transit and at rest), key management model, and tenant isolation approach?
4. What security certifications/assurance do you maintain (e.g., AS/NZS ISO/IEC 27001, 27002 and 27701), and what is the scope?

Model training and leakage controls

1. Is customer content used to train or fine-tune any models (default, opt-out, opt-in)?
2. What technical and contractual controls prevent customer content leakage into other customers' outputs?
3. Do you use third-party foundation models? If so, which ones, and what are the data handling terms?

Incident response and breach notification

1. at are your incident response SLAs (time to notify, time to triage, escalation contacts)?
2. How do you support customers' notifiable data breach obligations (Part IIIC), including evidence and reporting?
3. Do you provide an audit trail of access and actions taken on customer content (who/what/when)?

A2. Example scoring matrix to compare suppliers

Score each item 0–3 (0 = not met, 1 = partially met, 2 = met, 3 = exceeds). Content and suggested weighting is illustrative.

- Data processed and stored exclusively in Australia (weight 3)
- Supplier incorporated in Australia (weight 2)
- Supplier and its subprocessors provide all relevant services exclusively from Australian locations (weight 3)
- Express commitment that the information provided is not used to train any Large Language Models (weight 3)
- Express commitment that the uploaded contract is deleted promptly after processing is completed (weight 2)
- Express obligation to comply with the notifiable data breach scheme in Part IIIC of the Privacy Act (weight 2)
- Express obligation to report all data breaches (including those not covered by Part IIIC) promptly (weight 2)
- Independent security assurance (AS/NZS ISO/IEC 27001, 27002 and 27701) covering the data processing site and any data storage facilities (weight 2)
- No foreign country disclosure obligations (including by subprocessors) (weight 3)
- Australian legal-context capability (Australia-specific statutes covered) (weight 2)

Max score: 72

A3. Contract schedule clauses to request (high level)

The customer should consider requesting request warranties/undertakings covering:

- Data location and processing: define permitted locations for storage, processing, backups and support access.
- Subprocessors: prior notice and approval rights; onshore restrictions where required; up-to-date subprocessor list.
- Security controls: encryption, access controls, segregation, vulnerability management, and audit rights/assurance.
- Retention and deletion: retention periods, deletion SLAs, and handling of logs containing customer content.
- Training prohibition: no training or fine-tuning using customer content except with explicit written consent.
- Incident response and notification: notification timelines, cooperation obligations, and support for Part IIIC compliance.
- Sovereignty and legal process: commitments to minimise disclosure, challenge overbroad requests where lawful, and notify the customer where permitted.
- Audit and reporting: access logs, activity audit trail, and periodic assurance reporting.