



Privacy108
We Protect Privacy

MANAGING VENDOR PRIVACY RISK IN 2025:

A Guide To Third-Party
Supplier Privacy



June 2025
Edition 1.1

Table of Contents

1. Introduction	3
2. Why Privacy Matters	4
2.1 Defining the role of privacy	4
2.2 Privacy challenges in today's vendor relationships	5
3. Vendor Selection & Onboarding	6
3.1 Criteria for Assessing Privacy Risks in Vendor Selection	6
3.2 Best Practices for Onboarding Vendors with Privacy in Mind	8
4. Contractual Agreements & Privacy Protocols	9
4.1 Key Privacy Clauses & Legal Considerations	9
4.2 Cross-border transfers of personal data	9
4.3 Compliance With Privacy Regulations	10
5. Data Security Measures for Vendors	11
6. Ongoing Support	12
6.1 Vendor Support for Data Subject Requests (DSRs)	12
6.2 Ongoing Monitoring of Vendor Privacy Compliance	12
7. Incident Response & Data Breach Management	13
8. Exit Strategies & Transitioning	14
9. Conclusion	15



INTRODUCTION

Partnering with third-party vendors to manage your organisation's data, especially personal data, is risky. This is especially true given the complex global privacy terrain of 2025.

In this E-Guide, we dissect the essential privacy considerations crucial for organisations throughout the process of selecting, onboarding, and managing vendors. Our goal is to demystify the world of privacy and data protection, and their impact on vendor risk management.

Privacy acts as the cornerstone for preserving the integrity and confidentiality of personal data

WHY PRIVACY MATTERS

2.1 Defining the role of privacy

Privacy plays a fundamental and multifaceted role in the realm of vendor risk management. It acts as the cornerstone for preserving the integrity and confidentiality of personal data exchanged between organisations and its vendors. By ensuring the confidentiality and appropriate handling of this data, **privacy helps mitigate substantial risks to organisations including:**

- **Breach of data protection laws**
- **Data compromise**
- **Regulatory intervention**
- **Legal consequences**
- **Reputational damage**
- **Financial loss**
- **Operational disruption**
- **Trust erosion**

In a landscape increasingly shaped by stringent regulations and heightened customer expectations, privacy is not merely a legal obligation but a pivotal component in fostering trust and credibility. It also helps establish the ethical and contractual boundaries and responsibilities within vendor relationships, emphasising the need for conscientious data stewardship.

Understanding and implementing robust privacy measures in vendor relationships are integral not only to mitigate risk but also to build a foundation upon which successful and enduring vendor partnerships are built.

2.2 Privacy challenges in today's vendor relationships

Privacy challenges in today's vendor relationships are varied and complex, stemming from the intricacies of data sharing and management. Some of the key challenges include:

Vendor selection and due diligence:

Conducting thorough assessments of vendors' privacy practices, security protocols and data handling capabilities before onboarding, to ensure they meet the required standards.

Compliance with diverse regulations:

Navigating a landscape with diverse and evolving privacy regulations (like GDPR, CCPA) and ensuring that both the organisation and vendors comply with these regulations when handling data.

Complex vendor ecosystems:

Managing multiple vendor relationships, each with different privacy practices and standards, can create a challenge in maintaining a cohesive and consistent approach to data privacy across all partnerships.

Lack of transparency:

A lack of transparency in how vendors handle data can make it challenging for organisations to monitor and ensure compliance with agreed-upon privacy standards.

Data access and control:

Balancing the need to share data with vendors while retaining control over its usage and ensuring it is only accessed for authorised purposes.

Data security and breach risks:

Managing the risk of data breaches or unauthorised access, especially when data is transferred or stored by vendors, which can compromise the privacy of personal data.

Emerging technologies:

Incorporating and appropriately assessing new technologies (like AI) within vendor relationships while maintaining privacy standards, given the rapid evolution of tech capabilities.

Allocating roles and responsibilities:

Establishing clear contractual agreements that explicitly outline roles, responsibilities and compliance requirements.

Addressing these challenges demands a comprehensive approach that involves careful vendor selection, clear contractual agreements, continuous monitoring, and proactive strategies to maintain privacy standards within vendor relationships.

VENDOR SELECTION & ONBOARDING

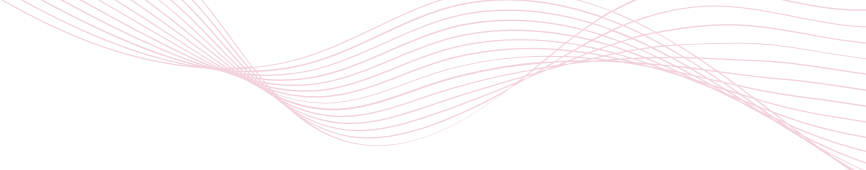
3.1 Criteria for Assessing Privacy Risks in Vendor Selection

When evaluating vendor privacy practices, several key criteria can be considered to ensure the vendor meets the required standards for handling personal data securely:

- 1 Data handling protocols:** assess the vendor's protocols for data collection, storage, use and transmission. Ensure they comply with relevant regulations and align with industry best practices. Also check they align with your own organisational requirements, for example, does the vendor's solution support single-sign-on or multi factor authentication?
- 2 Security measures:** evaluate the vendor's security infrastructure, including encryption methods, access controls, authentication processes and any certifications or compliance with security standards (like ISO 27001). Again, check that those practices align with your organisational requirements.
- 3 Incident response plan:** enquire about their preparedness and response plans in the event of a data breach. A clear and effective plan showcases their commitment to managing and containing potential data incidents.

Assessing privacy risks during vendor selection is a pivotal stage in establishing a secure and compliant partnership. It involves:

- Understanding the scope and nature of the data they'll handle.
- Assessing their track record in maintaining data privacy.
- Scrutinising their protocols for data use and storage, access control, encryption methods, and incident response plans.
- Examining their past performance, including any history of data breaches or non-compliance with privacy regulations.

- 
- 4 **Vendor compliance and audits:** request details on their past compliance with privacy and security regulations and any history of audits conducted on their data handling practices.
 - 5 **Contractual agreements:** scrutinize the terms of their agreements, ensuring they include clear and comprehensive clauses pertaining to data privacy, confidentiality and obligations regarding data protection.
 - 6 **Transparency and communication:** assess the vendor's transparency in sharing information about their privacy and security practices, willingness to engage in open communication regarding security protocols and their responsiveness to enquiries concerning data security.
 - 7 **Location of data storage:** Many organisations, particularly those in highly regulated industries, must comply with specific data residency requirements. This means that data must be stored within a particular jurisdiction to comply with regulatory standards. Choosing a vendor with data storage facilities in a jurisdiction with strong privacy laws is important. This strategic choice not only facilitates adherence to legal requirements but also establishes a foundation for heightened data protection.

3.2 Best Practices for Onboarding Vendors with Privacy in Mind

Onboarding vendors with a focus on privacy involves a series of strategic steps to ensure a secure and compliant partnership from the outset. Here are some best practices:

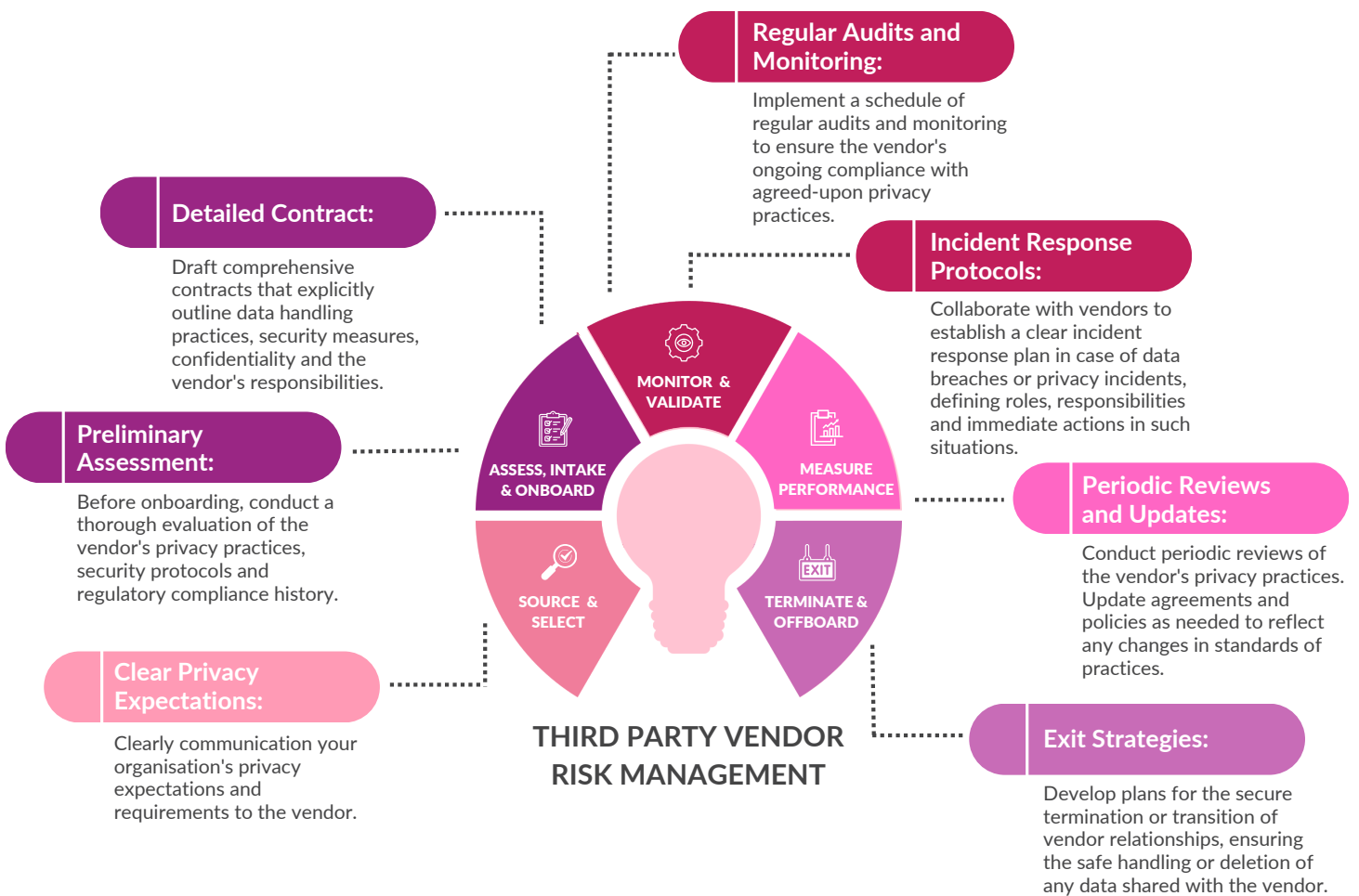


Diagram 1 – Best Practices for Onboarding Vendors



CONTRACTUAL AGREEMENTS & PRIVACY PROTOCOLS

4.1 Key Privacy Clauses & Legal Considerations

Crafting effective contracts with a strong emphasis on privacy is crucial in ensuring a privacy protective and compliant vendor partnership. These contracts should delineate obligations, responsibilities and standards for the handling, processing and safeguarding of personal data.

Clear definitions of what constitutes personal data, how it should be managed, and the purpose for which it can be used are essential components. It is especially important to be clear on what rights of use the vendor may have (if any) to the personal data. Explicit clauses about data security measures, encryption standards, access controls, and the vendor's commitment to compliance with relevant data protection laws should be detailed.

Moreover, these contracts should also have a mechanism to deal with data incidents. Regular audit reporting requirements, and provisions for updating the contract to align with evolving privacy regulations should also be included.

Having clauses that address privacy not only establish a clear framework for privacy but also serve as a legal mechanism to hold both parties accountable, ensuring the secure and responsible handling of personal data throughout the vendor relationship.

4.2 Cross-border transfers of personal data

The cross-border transfer of personal data introduces an additional layer of scrutiny, as various jurisdictions enforce distinct legal requirements. For instance, certain jurisdictions necessitate the implementation of data processing agreements (DPAs) or standard contractual clauses (SCCs) with vendors. DPAs and SCCs serve as contractual instruments that establish a legal foundation for the secure and privacy-compliant handling of personal data by vendors operating in different geographic locations; they delineate the obligations and responsibilities of vendors, ensuring that the vendor complies with the privacy standards mandated by the relevant jurisdiction.

4.3 Compliance With Privacy Regulations

Vendor compliance with key data privacy regulations and laws is fundamental in ensuring the secure and lawful processing of personal data. Adherence to regulations like GDPR, CCPA, HIPAA, or any industry-specific standards is paramount in maintaining the trust and integrity of vendor relationships.



TIP

Understand the data privacy regulations and laws that apply to your operations. Then, prioritise vendors who commit to comply with those regulations and laws, or equivalent laws that provide a comparable level of data protection.

This approach ensures that your chosen vendors align with the requisite legal frameworks, mitigating risks and fostering a culture of trust and accountability in the handling of personal data.

DATA SECURITY MEASURES FOR VENDORS

Data security is an integral component of data protection laws, emphasising the safeguarding of personal data against unauthorised or unlawful use and against accidental loss, destruction or damage. When selecting vendors, it is imperative to prioritise those that adhere to stringent data security measures to ensure compliance with regulatory requirements.

Some tips for vendor selection include evaluating their encryption standards, access controls and commitment to compliance with data protection laws. Collaboration with the information security team is essential in this process, as their expertise can help identify vendors that meet the organisation's security standards. Working closely with the information security team ensures a thorough assessment of potential risks and helps confirm that chosen vendors align with robust data protection practices, helping to strengthen the overall security posture of the organisation.



ENCRYPTION PROTOCOLS

Vendors should implement robust encryption methods for both stored and transmitted data.

ACCESS CONTROL MEASURES

Utilise stringent access controls to limit data access to authorised personnel only. This involves implementing multi-factor authentication, role-based access, and regular reviews to ensure access is appropriate and up to date.

SECURITY UPDATES & PATCH MANAGEMENT

Vendors need to regularly update and patch their systems, applications and software to address known vulnerabilities and security weaknesses.

SECURE STORAGE & TRANSMISSION

Ensure that personal data is stored in secure environments, employing strong data centre security measures, firewalls, and encryption during data storage and transmission.

INCIDENT RESPONSE PLANNING

Develop and regularly test a comprehensive incident response plan to address and mitigate data breaches swiftly and effectively.

Diagram 2 – Best Practices for Securing Data with Vendors

ONGOING SUPPORT

6.1 Vendor Support for Data Subject Requests (DSRs)

You should give due consideration to the role that vendors may need to play to help your organisation successfully fulfil data subject requests. As individuals exercise their rights to access, rectify or erase their personal data, vendors may need to have robust mechanisms in place to support your organisation to respond to these requests.

Ongoing support for data subject requests involves regular communication, ensuring that individuals are kept informed about the status and outcomes of their requests.

6.2 Ongoing Monitoring of Vendor Privacy Compliance

As the regulatory landscape continues to evolve, it is important for organisations to vigilantly assess and ensure their vendors consistently adhere to privacy standards for the duration of the partnership. Regular monitoring enables proactive identification and mitigation of potential privacy risks.

As part of your regular audits of your vendors, you should:

- Track their external certifications (i.e., has their ISO 27001 certification been renewed? Is a new SOC 2 Type 2 report available?)
- Re-send your vendor privacy and security questionnaire and ask for confirmation that nothing has changed
- Ask for current audit reports at preset intervals. These dates should be carefully followed so it's essential your team has processes in place to ensure the audits are obtained at the set intervals
- Confirm when the vendor's team last received privacy training, what the training involved and when the next training is scheduled
- Query whether they have planned penetration testing and phishing tests and request that they confirm the results once the tests have taken place



Continuous monitoring involves:

- Leveraging automated tools
- Regular audits
- Periodic reviews of the vendor's security controls with privacy regulations

INCIDENT RESPONSE & DATA BREACH MANAGEMENT

Numerous data protection laws impose mandatory data breach notification obligations, underscoring the significance of pre-planning with vendors to navigate such situations effectively. Here are some practical tips for pre-planning to help streamline breach responses and mitigate potential risks associated with data incidents:

Establish Key Contacts

Maintain an updated list of key contacts at your vendors, including designated individuals for data security and incident response. Having direct communication lines ensures swift and effective collaboration during a data incident.

Define Roles

Clearly define the roles and responsibilities of both your organisation and the vendor in the event of a breach. Ensure there is a shared understanding of who does what during each phase of incident response.

Conduct Regular Training

Provide regular training to your team on incident response procedures. Familiarity with the processes can lead to quicker and more effective responses when a breach occurs.

Back-up Communication Lines

Establish alternative communication channels in case there is system downtime or communication failures. This could include back-up email addresses, phone numbers, or secure messaging platforms to ensure continuous contact during an incident.

Evaluate Vendor Incident Response Plans

Request and review your vendor's incident response plan. Ensure that it aligns with your organisation's expectations and standards, and address any discrepancies or areas of improvement.

Maintain Legal Compliance

Regularly review and update contracts to incorporate the latest legal requirements for reporting and responding to data breaches in the jurisdictions where you operate.

EXIT STRATEGIES & TRANSITIONING

Smooth vendor exits demand careful attention to privacy considerations to ensure the secure transition or termination of the vendor relationship. Key privacy considerations for a smooth vendor exit process include:

- 1 Data retrieval and transfer:** define protocols for the return or transfer of all data.
- 2 Data deletion or destruction:** establish procedures for securely deleting or destroying any residual copies of data in the vendor's possession. Ensure compliance with data retention policies and legal requirements for data erasure.
- 3 Confirmation of compliance:** obtain formal confirmation from the vendor that all data has been returned, deleted or destroyed according to the agreed-upon terms, maintaining a record of the process for regulatory compliance and auditing purposes.
- 4 Exit audits and documentation:** conduct exit audits to ensure the vendor's compliance with privacy and security measures during the exit process. Document the steps taken and maintain records for future reference.
- 5 Communication and notification:** notify relevant stakeholders, including employees, about the vendor exit and measures taken to safeguard data during and after transition.
- 6 Contractual clauses for exit procedures:** ensure that the original vendor contract includes clear clauses detailing the obligations, responsibilities and procedures for data handling and privacy during the exit process.

Aim for a seamless and secure vendor exit by addressing privacy considerations upfront



CONCLUSION

In the ever-evolving landscape of vendor risk management, prioritising privacy considerations is fundamental for establishing a secure and resilient business ecosystem. This E-Guide serves as a compass, illuminating the path of safeguarding personal data in vendor relationships.

Understanding the pivotal role of privacy not only as a legal obligation but as a foundation for trust and reliability is key. By adopting a proactive and collaborative approach, organisations can strengthen their vendor relationships, mitigating risks and ensuring the integrity of the data they steward. The insights shared in this E-Guide, from assessing vendor compliance to implementing effective exit strategies, underscore the imperative nature of a holistic and adaptive approach to vendor risk management.

It is hoped that this E-Guide helps organisations navigate the complexities of vendor relationships with confidence, resilience and a commitment to preserving privacy in an increasingly interconnected business landscape.

Prioritising privacy considerations is fundamental for establishing a secure and resilient business environment.

How Privacy 108 Can Help

Managing the risks posed by utilising third-party vendors to handle your data, is becoming increasingly complex. Privacy 108 can help your organisation identify, assess, mitigate and monitor risks posed by the interconnected network of third-party relationships.

Elevate your organisation's resilience with our expertise in:

- **Tailored Third-Party Vendor Risk Programs:** We specialise in designing customised vendor risk programs that help protect our clients' operations, brand and reputation
- **Comprehensive Vendor Risk Assessments:** We develop and conduct third-party risk assessments and help organisations define and assess proper third party controls
- **Enhanced Vendor Risk Program Maturity:** Partner with us to assess the maturity of your program in alignment with regulatory expectations and industry-leading practices.
- **Leveraging technology:** We can also explore options to provide our services leveraging the technology platforms that you already own.

You might be interested in our Vendor
Privacy Review Checklist.

Contact us now for your free copy.

Call 1300 41 20 50 or

[CONTACT US](#)

Copyright © Privacy 108 Consulting Pty Ltd

Materials developed by Privacy 108 are provided on the basis of a non-exclusive licence for non-commercial use. This document must not be resold, copied, shared, provided, assigned, transferred or licensed in any way to any third party, displayed in a public place, published on the internet or republished in any way without the prior written permission of Privacy 108.

Qualifications to this document

While prepared to the best of our ability, this document is a general guide only. It does not cover every situation that applies to your organisation, or reflect your organisation's circumstances.

This document is not legal advice, and should not be construed or relied upon as legal advice.

About Privacy 108

Privacy 108 provides legal and non-legal consultancy as well as knowledge sharing services specialising in data privacy, data governance and cyber security. Privacy 108's services include privacy impact assessments and privacy audits, the development of privacy and data-related policies and procedures, offering a range of privacy, security and data governance guidance publications, professional development and compliance training options. For more information see: <https://privacy108.com.au/>.

About the author

This E-Guide has been prepared by Dr Jodie Siganto, Founder, Privacy 108.

Dr Siganto is one of Australia's leading privacy and security experts. A qualified lawyer with over 20 years of experience, Dr Siganto advises government departments, Australian businesses and international organisations on matters related to privacy and information system security.

A passionate advocate for privacy and data protection, Dr Siganto helps organisations ensure they retain the trust of their stakeholders and the wider community, in the ways that they collect, use and secure data. She believes that the most effective solutions begin with robust and thoughtfully designed information security and privacy programs that continue to mature with practical guidance and support.

