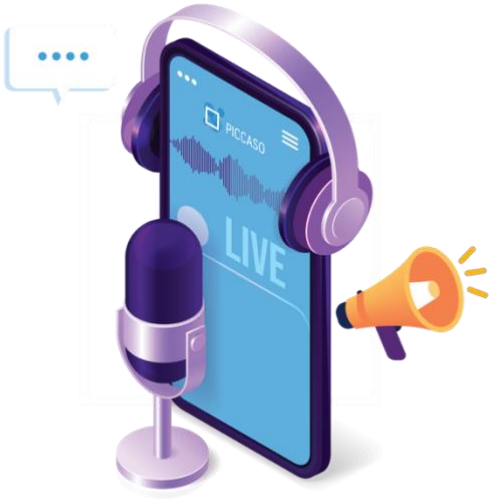
PICCASO

Privacy & Security Insights with PICCASO



Managing Third Party Supplier Risk- a Data Privacy Perspective

Kirsten Mycroft

PICCASO Advisory Board Member

Chief Privacy & Data Ethics Officer

BNY Mellon

Sponsored by

PrivacyCulture

Managing Third Party Supplier Risk- a Data Privacy Perspective

Introduction

Effective third-party outsourcing arrangements can offer organisations valuable opportunities, such as the rapid scaling of business operations and technology infrastructure, access to specific industry expertise and innovation, improved resilience of critical systems, operational efficiencies, and cost reduction.

However, working with third parties also introduces risks that need to be managed appropriately.

This short piece highlights some of the potential risks associated with outsourcing the processing of personal data to third parties and offers practical tips for managing those risks.

Five key potential data privacy risks:

- ***Accountability*** – Are respective roles and responsibilities, and personal data processing instructions, restrictions and liabilities clearly articulated in a contract that conforms to applicable regulatory requirements? Is this understood by all parties and do the day-to-day processing activities align with expectations?
- ***Privacy and Security by Design*** – Is a "privacy and security by design" approach in place when sharing personal data with the supplier? Has the supplier implemented appropriate technical and organisational controls to protect the confidentiality, integrity and availability of the personal data throughout its lifecycle, including upon termination of the relationship?
- ***Compliance*** – Can the supplier meet the data privacy obligations (regulatory, contractual, corporate policy) that attach to the personal data in question, both now and as those obligations evolve over time? How is this measured and what is the supporting evidence?
- ***Resilience*** – is the supplier financially sound? Are their products and services resilient to threats such as cybersecurity attacks, environmental threats, labour actions, critical market events, etc.
- ***Artificial Intelligence*** (AI) – do vendor-provided AI solutions or the AI solutions being used by suppliers meet your requirements for ethical, responsible, compliant AI? What data has been used to train the AI model in question, and what access will the vendor in question have to company confidential information? Who owns the output of the AI model?

Five practical tips to take on board:

1. **Teamwork makes the dream work.** Third parties typically provide a host of different services to organisations, from payroll through to technology infrastructure and facilities management. Where they exist, it makes sense for data privacy leaders to leverage central sourcing/procurement functions, and associated operating models and governance frameworks, to manage data privacy risks alongside other third-party risks in a holistic, coordinated fashion. As with most components of a successful data privacy program,

standing up an effective, sustainable third-party data privacy risk management capability requires collaboration with partners such as Legal, Risk and Compliance, Cybersecurity, Business Supplier Managers and Sourcing/Procurement. Assurance work by Internal Audit or other compliance testing functions can be helpful in identifying control gaps.

2. **Third party suppliers are not created equal.** It's important to identify which suppliers represent the greatest risk to the organisation. This is a foundational capability that enables the implementation of proportionate supplier control assessments, risk decisions and ongoing monitoring efforts. Consider factors like volumes and sensitivity levels of personal data, the nature of the relevant service, the extent of cross-border data transfers, and the status/credibility of relevant supplier certifications, e.g. in cybersecurity.

3. **Third party risk management is the gift that keeps on giving.** A one-off data privacy assessment at supplier onboarding won't cut it. In this fast-paced world (more on that in the next tip), supplier relationships aren't static. From the nature of the personal data shared and the technology used in the outsourcing arrangement, to the 'state of the art' in cybersecurity and regulatory expectations, aspects of the supplier relationship are likely to change over time. Comprehensive risk and control assessments of every third-party supplier every year is not pragmatic or realistic for most companies, but there is a balance to be struck. The frequency and extent of third-party supplier monitoring should be proportionate to the risk those suppliers represent (see tip 2). Suggestions to tackle this challenge include:

    a. Tiering third party supplier engagements based on risk profile and defining the frequency and extent of monitoring per tier.

    b. Regularly reviewing the tiering criteria and allocation across the supplier population.

    c. Retaining metadata per supplier engagement to quickly identify engagements impacted by regulatory change, contract uplift requirements or market/industry events.

    d. Digitising contracts and the contract management lifecycle to enable the rapid identification of contractual obligations relevant to data use restriction or data incident analysis, provide auditability and robust record keeping, and achieve greater consistency in contractual terms and negotiating positions.

4. **Jack be nimble, Jack be quick.** As with most risk management disciplines, data privacy and broader organisational approaches to third party risk management need to evolve over time – sometimes quickly and tactically – to account for changes in the technology, regulatory, economic, and business landscape. Recent regulatory drivers include new requirements for cross-border personal data transfers and operational resilience. In the technology space, the increasing accessibility and capability of artificial intelligence (AI) is driving organisations to consider how third-party risk management must evolve to account for new/nuanced risks posed by AI solutions that are produced by, or integrated into, third party supplier products and services.

5. **Be prepared.** When (not if!) one of your third party suppliers experiences a data privacy incident, such as a cybersecurity attack, unexpected outage or human processing error, the ability to respond effectively and reduce the impact of the incident will – to a large extent – be dependent upon the extent to which you and your supplier have thought through what could go wrong in advance and implemented a robust, up-to-date incident response plan.

Conclusion

Whilst companies can outsource personal data processing activities, they can't outsource accountability for the protection of that personal data and the privacy rights of the impacted individuals. Prioritising the management of third-party risk as a core part of the enterprise data privacy program and the organisation's broader approach to risk management is an essential component of demonstrating accountability for data privacy, operating a resilient business, and maintaining stakeholder trust.

PICCASO

Listen now on:

Spotify®

Google Podcasts

YouTube

Apple Podcasts

About us:

We are a UK based non-for-profit privacy special interest group, led by seasoned volunteers who are senior leaders in privacy and data protection.

The primary aim of PICCASO is to create a community of professionals that share the value of exchanging 'know how', insights, clarity and explanation on specific privacy and data protection topics designed to distinguish between legal requirements, operational implementation, and strategic objectives, with the aim of greater understanding in how to achieve optimal outcomes based on good practice and thought leadership.

The PICCASO community is drawn from across the UK, Europe, and beyond, and from all industry sectors.

Contact us:

www.piccaso.org
Bouverie House | 154-160 Fleet St | London | EC4A 2DQ
T. +44 (0) 207 112 9360 | hello@PICCASO.org
https://www.linkedin.com/company/piccaso/