How to use this document

This case study considers a common type of outsourcing arrangement: where a Victorian public sector (**VPS**) body grants a private contractor "read only" access to a government database to enable the contractor to perform a government function, for example processing claims. It assumes that the VPS body is subject to both Parts 3 (Information Privacy) and 4 (Protective Data Security) of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**).

This case study should be read together with the *Guidelines for Outsourcing in the Victorian Public Sector - Checklist* and *Accompanying Guide*, which provides more detailed guidance. You may also wish to refer to the *Short form Model Terms for Contracted Service Provider agreements.*

Scenario

You are part of the procurement team for a statutory authority (your **Organisation**) that processes claims under its enabling legislation.

When processing claims, your Organisation verifies claims information received from the client against information stored in a case management database operated by another agency within your Departmental portfolio (the **Database**).

Your Organisation and the portfolio agency are both "public entities" under the *Public Administration Act 2004* (Vic).

Clients in the Database include both sole traders and bodies corporate. Their records contain a range of information, including financial details. The portfolio agency generated the information in the client record, and manages the protective markings in the Database.

Your Organisation accesses the Database under a Memorandum of Understanding (**MoU**) with the portfolio agency. The MoU was made in the late 1990s, and is a brief document that outlines the purpose of the access arrangements. It does not address subcontracting or refer to any specific operational policies or procedures for the Database.

Your Organisation works closely with the portfolio agency, and operational level issues about data use are generally managed through open communication and working arrangements between the parties.

Your Organisation now wishes to outsource steps in the claims processing workflow to a private contracted service provider (**CSP**), whose personnel will need to access the Database to process claims.

What are your Organisation's responsibilities in this scenario?

The Database contains information about individual sole traders. Although this is information about individuals in their professional capacity, it is still "personal information" under the PDP Act. Consequently, the Information Privacy Principles (**IPPs**) apply.

*IPPs limit the purposes for which personal information can be used and disclosed. The CSP and its staff must understand and comply with these limitations when accessing the Database.*

The Database is a "public sector data system" under the PDP Act, and records in the Database are "public sector data". Consequently, the Victorian Protective Data Security Standards (**VPDSS**) also apply.

*The VPDSS requires your Organisation to take a holistic approach to identifying and managing potential risks to the client service record information across the following areas: ICT, personnel, physical and environment, and information. Your Organisation must consider what new risks might arise in each of these areas as a result of the CSP having access to the Database.*

In this scenario, your Organisation and the portfolio agency must ensure that Database access is provided to the CSP securely. Your Organisation is also responsible for ensuring that the CSP's staff only access and use the Database for authorised purposes.

Complying with the IPPs and VPDSS requires a co-ordinated effort from many different stakeholders in your Organisation, including procurement, risk management, contract managers, IT security, legal, and compliance / audit teams. Breaching privacy and data security controls can have serious criminal, contractual, and reputational consequences.

Key privacy and data security risks in this scenario

**Overview**

In this scenario, when a CSP is given access to a Victorian Government database, four common privacy and data security risks are explored. The case study suggests risk mitigation strategies during the (i) pre-contract (due diligence / requirements gathering); (ii) contracting; and (iii) operational phases.

**Risk 1: CSP staff access the Database for unauthorised purposes, or contrary to government-specific Database policies and procedures**

***Description of risk***

CSP staff may use the Database for unauthorised purposes, or access the database beyond what is needed to perform claims processing. For example, looking up a friend, relative, or celebrity for personal reasons, or copying parts of the Database to create their own version of the client's service record for convenience.

CSPs and their staff may not be familiar with Victorian government requirements like protective markings, statutory secrecy provisions, and retention / disposal requirements for public records.

Your Organisation must ensure the CSP and its staff clearly understand the scope and limits of access, and have mechanisms to regularly audit and verify appropriate Database use in practice. In past matters, staff have been unaware of what constitutes unauthorised access (and that unauthorised access is unlawful). It is also helpful to formally document the working arrangements between your Organisation and the portfolio agency, so that these requirements can be flowed down to the CSP.

(*Key PDP Act references: IPP 1.1, 2.1 and 4.1; VPDSS 2, 3, 4, 5 and 10*)

***Mitigation strategies:***

|  |  |
| --- | --- |
| Stage | Actions |
| Pre-contract | * Conduct an information security risk assessment of the CSP to assess their maturity level and capacity to meet information handling requirements;
* Use technical configurations on databases to ensure that the CSP only has access to the relevant information in the client record (e.g. on a "need-to-know" basis), for example, it may be sufficient for the CSP to "sight" the relevant information from the Database (rather than printing / copying records);
* Consider if the Database can log access of the Database by individual users, and whether the Database should include this functionality;
* Develop a written services description / workflow document that explains how the CSP staff should use the Database when processing a claim;
* Consider appropriate "on-boarding" training program for CSP staff and who is responsible for conduct of this training; and
* Consider if Database users should undergo security clearances / background checks.
 |
| Contract terms | * The CSP should commit to an agreed services description / workflow document, and ensure that its staff only access the Database for the purpose of providing the Services (and for no other purposes);
* Specify the level of access and whether the CSP can extract / edit information;
* CSP staff can only use the Database once they have been approved having shown that they completed training and security clearances / background checks;
* The CSP should be required to notify your Organisation of any suspected or confirmed misuse of the Database by its staff. The Contract could specify a timeframe to notify, make serious misuse a contract default, or impose abatements for breaches; and
* Your Organisation should have contractual rights to directly monitor and to require audit of the CSP's access and use of the Database.
 |
| Operational phase | * Your Organisation, CSP or an independent third-party auditor should periodically (annually or biennially) audit the CSP's access to the Database to identify any instances of unauthorised use;
* Ensure and review technological configurations and restrictions identified during the pre-contract stage (e.g. disable printing functionality);
* Consider how the CSP will be notified of policy updates / new policies during the term of the outsourcing arrangement; and
* If the Database administrator maintains a register of third party CSPs with access to the Database, ensure that the CSP is added to that list.
 |

**Risk 2: Insufficient IDAM (Identity Access Management) planning and controls**

***Description of risk***

Your Organisation should maintain visibility of which CSP staff have access to the Database, and for what purposes. This will assist your Organisation to appropriately monitor their usage of the Database, and identify any cases of suspected or actual misuse. CSP staff should have their access to the Database promptly revoked once they no longer require access. For example, because they change jobs, or move to a different role within the CSP.

Identity and Access Management (**IDAM**) refers to the combination of policies, procedures and technical measures implemented to achieve these objectives. To be effective, IDAM requires continued management during the life of the outsourcing arrangement. IDAM problems can arise where the CSP does not promptly notify your Organisation about staff turnover / role changes, or where your Organisation does not conduct regular audits to supervise use of the Database by CSP staff.

(*Key PDP Act references: IPP 4.1, VPDSS 4, 5 and 10.*)

***Mitigation strategies:***

|  |  |
| --- | --- |
| Stage | Actions |
| Pre-contract | * Work with technical and operational stakeholders to ensure that a suitable IDAM strategy is implemented to manage the CSP's access.
 |
| Contract terms | * The CSP must notify your Organisation of CSP personnel with access to the Database, and promptly notify your Organisation of any changes in its user base;
* The CSP should ensure that its staff do not share their access credentials; and
* If the Database has an IDAM policy and procedures document, consider including this in the contract.
 |
| Operational phase | * Promptly remove access CSP users who no longer require access; and
* Conduct periodic reviews of the authorised user list (for example, every three months) to confirm that it remains accurate and up to date.
 |

**Risk 3: Insufficient oversight and auditing of CSP usage of the Database**

***Description of risk***

It is important for your Organisation to oversee the CSP during the contract. The security controls, training and documentation that are implemented at the start of the arrangement may need to be updated due to staff turnover, operational changes, or the emergence of new types of security threats. Regular audits are important to ensure CSPs actively manage their responsibilities under the contract.

(*Key PDP Act references: IPP 4.1, VPDSS 2, 3, 4 and 5.*)

***Mitigation strategies:***

|  |  |
| --- | --- |
| Stage | Actions |
| Pre-contract | * Configure the Database to maintain audit logs of individual users' access to the Database, and to produce reports flagging any unusual usage patterns; and
* Develop a plan to conduct periodic audits of the CSP's use of the Database.
 |
| Contract terms | * The CSP should commit to co-operate with, and participate in, the audit process and promptly address any issues identified through the audit;
* Ensure that privacy and data security issues are added as agenda items for any governance forums / performance review meetings with the CSP;
* Consider whether the CSP should be required to provide an annual attestation of its compliance with their privacy and data security obligations; and
* The CSP should nominate a suitably qualified authorised representative to liaise with your Organisation on privacy and data security issues.
 |
| Operational phase | * As part of handover to operations, ensure that contract managers and other relevant stakeholders are made aware of the audit mechanisms in the contract and the schedule for conducting audits;
* Ensure that the outsourcing arrangement is noted in any relevant risk registers maintained by your Organisation or the Database administrator; and
* During the term of the outsourcing, conduct regular audits of the CSP's usage of the database and discuss the results with the CSP.
 |

**Risk 4: CSP login details / access credentials compromised by a third party**

***Description of risk***

Once the claims processing function is outsourced, your Organisation will have less visibility of whether CSP staff are handling their access credentials (such as log-in details and passwords) securely. Data breaches can occur where a CSP's access credentials are compromised by a malicious third party and used to gain unauthorised access to a database. Technical and operational security controls can be implemented to minimise this risk and mitigate the potential damage of any data breach.

(*Key PDP Act references: IPP 4.1, VPDSS 6, 9 and 11.*)

***Mitigation strategies:***

| Stage | Actions |
| --- | --- |
| Pre-contract | * Consider what parts of the client service record the CSP requires and whether current technical configurations can restrict CSP access, or if changes are needed;
* Consider how the CSP would access the Database, and liaise with the Database administrator about ICT security settings for third party access (e.g. multi-factor authentication or VPN tunnel); and
* Consider any minimum technical security requirements for the CSP's IT systems and whether the CSP complies with relevant industry standards in information security (e.g. ISO 27001).
 |
| Contract terms | * The CSP should comply with the minimum technical security requirements for the CSP's IT systems (if any), or any industry standards that it claims to be compliant with; and
* The CSP should immediately notify your Organisation of any actual or suspected data breach, or compromise of the CSP's passwords or log-in credentials (including any data breach that affects the CSP's systems).
 |
| Operational phase | * Ensure that the outsourcing arrangement is noted in any relevant risk registers maintained by your Organisation or the Database administrator.
 |

Conclusion

The strategies above are intended to provide a starting point for privacy and data security planning, and are not exhaustive.

Privacy and data security controls should be considered on a case-by-case basis to ensure that the outsourcing arrangement meets the following general objectives for privacy and data security compliance.

**Objectives - Privacy compliance**

* The CSP agrees (and has the necessary know-how and operational capacity) to provide the claims processing service in a manner that is consistent with the requirements of the IPPs - for example, the IPP 2 requirement to only use or disclose the client information for the purposes for which it was collected (or other purposes specifically permitted under IPP 2); and
* The outsourcing arrangement is implemented in a way that addresses your Organisation's (and the portfolio agency's) continuing IPP responsibilities in relation to the Database - for example, the IPP 4 requirement to take reasonable steps to protect the Database from unauthorised access and misuse.

For further information, see "Step 4 - IPP planning and due diligence" in the *Guidelines for Outsourcing in the Victorian Public Sector - Checklist* and *Accompanying Guide*.

Your Organisation should also conduct a Privacy Impact Assessment, which provides a structured process for systematically considering and addressing the requirements of the IPPs.

**Objectives - Data security compliance**

* The CSP agrees (and has the necessary know-how and operational capacity) to provide the claims processing service in a manner that complies with the requirements of the VPDSS;
* Your Organisation has addressed the requirements of VPDSS 8 (Third Party Arrangements), including:
	+ the service agreement adequately explains how the CSP will manage risks across all four security areas (ICT, personnel, information and physical security) - see VPDSS 8 element E8.020;
	+ your Organisation has arranged to regularly monitor, review and validate the CSP's compliance with the terms of its access to the Database - see VPDSS 8 element E8.060; and
	+ your Organisation has arranged appropriate "wrap up" / disengagement arrangements upon completion or termination of the CSP's engagement - see VPDSS 8 element E8.090;
* The outsourcing arrangement is implemented in a way that addresses your Organisation's (and the portfolio agency's) continuing VPDSS responsibilities in relation to the Database - for example:
	+ the VPDSS 2 requirement to handle the client service record information in accordance with the portfolio agency's protective markings and instructions;
	+ the VPDSS 4 requirement to implement a structured process for controlling access to public sector information (including by external users, such as CSP personnel); and
	+ the VPDSS 9 requirement to notify OVIC of any data breach affecting information with a protective marking of OFFICIAL: Sensitive, PROTECTED, Cabinet-In-Confidence or SECRET (or any other information with a BIL of level 2 ("Limited") or higher).

For further information, see "Step 3 - VPDSF planning and due diligence" in the *Guidelines for Outsourcing in the Victorian Public Sector - Checklist* and *Accompanying Guide*.

Further Information

**Contact Us**

**t:** 1300 00 6842
**e:** enquiries@ovic.vic.gov.au
**w:** ovic.vic.gov.au**Disclaimer**

This fact sheet does not constitute legal advice and should not be used as a substitute for applying the provisions of the Privacy and Data Protection Act 2014, or any other legal requirement, to individual cases.