How to use this document

This case study considers a common type of outsourcing arrangement: where a Victorian public sector (**VPS**) body wishes to engage a commercial data analytics provider to analyse Victorian Government data. This case study 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 is intended to be read in conjunction with the *Guidelines for Outsourcing in the Victorian Public Sector - Checklist* and *Accompanying Guide*, which provide more detailed implementation guidance. You may also wish to refer to the *Short form Model Terms for Contracted Service Provider agreements.*

Scenario

You work in the Policy, Strategy and Performance branch of a Victorian Government body (your **Organisation**). Your team is asked to systematically review theservice quality of a particular service that is funded by your Organisation (the **Project**). To assist with this task, you have access to an archive of historical performance reviews and evaluation reports for that service. These documents mention the names of various service providers and staff who were involved in the delivery of the services.

One of your objectives is to identify common trends and themes in the performance reviews and evaluation reports, so that these can be analysed as part of the broader assessment. This analysis will primarily be used for internal reporting purposes, to assist with strategy development and service planning within your Organisation. Following this, your team will prepare a final, public-facing report to summarise the key findings of the review and the initiatives that your Organisation is implementing in response.

The document archive you have been provided with is quite sizeable. This presents a challenge for your team, as the structure and format of the reports has changed several times over the years. The reports also vary in their length and level of detail. To expedite the analysis and help your team to meet the project timeframes, your team is considering whether to engage a data analytics provider who can use software to automate the review process.

You identify a commercial data analytics company (the **CSP**) with the right type of analytics software for the Project. You have an initial meeting with the CSP, and they indicate that they can analyse the document archive (the **Input Data**) and produce the following deliverables (the **Data Outputs**):

(a) a searchable index that highlights commonly occurring keywords and phrases in the documents (which may include service provider and staff names); and

(b) statistical tables of aggregated data that can be included in your final public-facing report.

What are your Organisation's responsibilities in this scenario?

The Input Data consists of historical performance reviews and evaluation reports, some of which contain the names of individual staff members.

While this is information about the staff in their professional capacity, it is still "personal information" under the PDP Act. Consequently, the Information Privacy Principles (**IPPs**) apply:

*Among other things, the IPPs require your Organisation to take reasonable steps to protect the Input Data against unauthorised access, modification, disclosure, misuse, or loss. This includes a requirement to protect any data that has been "de-identified" against the risk of unauthorised re-identification (as re-identification would disclose the identity of the individuals).*

The historical performance reviews and evaluation reports that comprise the Input Data are government records that are held by your Organisation. These records are "public sector data", and the Victorian Protective Data Security Standards (**VPDSS**) apply. Under the VPDSS, your Organisation is still accountable for the Input Data while held by the CSP.

*Among other things, the VPDSS requires your Organisation to assess the security value of the Input Data that is being provided to the CSP, and to take steps to secure that data in a manner that is consistent with other data of the same classification. Your Organisation must assess the security measures that the CSP is offering, and consider whether these meet the requisite standard.*

*If the Input Data is assessed to have a BIL of level 2 (“Limited”) or higher under the VPDSS classification system, your Organisation is also responsible for notifying OVIC of any data breach affecting that data.*

Complying with the IPPs and VPDSS requires a co-ordinated effort from many different stakeholders in your Organisation including the information security teams (to assess the CSP's security offering and monitor on-going security risks), legal and procurement (to ensure that appropriate contractual obligations are imposed on the CSP), and records management (to advise on how your Organisation should store and manage the data once it is received back from the CSP).

These stakeholders can assist you to conduct the necessary due diligence on the CSP. If the CSP is not able to meet the standards required by the VPDSS, you may need to consider using an alternative provider.

There may be alternative options that you can consider within the Victorian public service. Many Victorian Government departments now have their own in-house data analytics teams, such as the Centre for Victorian Data Linkage (**CVDL**) within the Department of Health and Human Services (**DHHS**). The Victorian Centre for Data Insights (**VCDI**) has also been established to support the Victorian public service in delivering data projects. VCDI's team of data and policy specialists are available to partner with Victorian public service organisations to conduct projects that require data analytics tools and expertise.

Breaching privacy and data security controls for data analytics projects can have serious consequences. Data analytics projects often involve large-scale data sets with detailed and sensitive information. Unauthorised release of this information by data breach, or through re-identification of Data Outputs made publicly available, can cause serious reputational damage, negatively impact stakeholder relationships, and put affected individuals at risk of harm.

Key privacy and data security risks in this scenario

**Overview**

Discussed below are five common privacy and data security risks that should be considered in this scenario. The case study suggests mitigation strategies during the (i) pre-contract (due diligence / requirements gathering); (ii) contracting; (iii) and operational phases.

**Risk 1: Can the Project use information under the PDP Act or your Organisation’s enabling legislation?**

***Description of risk***

The PDP Act regulates the use of personal information - where persons are named, or where their identity is otherwise apparent or can be reasonably ascertained. In this scenario, the Input Data contains the names of staff members in performance reviews and evaluation reports. While these individuals may not be the primary focus of the reports, their personal information is still contained in the reports.

It is likely that your Organisation’s enabling legislation contains a secrecy or confidentiality provision that restricts you from using some or all of this information. The PDP Act also regulates when personal information can be used. Your Organisation's Privacy Officer can help you to assess whether your Project is a permitted purposeunder the PDP Act, or whether you can rely on relevant authorisations under your Organisation's enabling legislation.

Alternatively, the Input Data could be “de-identified” before it is provided to the CSP. If the Input Data is properly "de-identified", it will not be subject to the "permitted purpose" requirements of the PDP Act. However, de-identification is a difficult and technical process that generally requires more than just removing the names of the individuals from the data.

If you wish to conduct your Project on a "de-identified" basis, you should consider partnering with expert data analytics bodies such as VCDI. These experts can work with you to ensure that the correct de-identification techniques are used, based on the nature of your data and the requirements of your project.

(*Key PDP Act references: IPP 2 and 4*)

***Mitigation strategies:***

| Stage | Actions |
| --- | --- |
| Pre-contract | * Liaise with your Organisation's Privacy Officer to discuss if the Project is a "permitted purpose" under the PDP Act (which may include de-identifying the data);
* Discuss with your legal or governance team about what information can be used for the Project based on any secrecy of confientiatlity provisions;
* Identify who owns the data in your organisation and seek their approval to use and share the archive with external parties, such as the CSP; and
* If de-identifying the data, seek assistance from data analytics experts (such as VCDI).
 |
| Contract terms | * State that the CSP can only use the Input Data to perform the Project and produce the agreed Data Outputs, and that the Input Data and Data Outputs cannot be used for any other purpose;
* State that the CSP cannot combine the Input Data with any other datasets without your Organisation's consent;
* The CSP must destroy (providing proof if requested) or return all copies of Input Data and Output Data to your Organisation; and
* The CSP cannot share the Input Data with any third parties without your consent.
 |
| Operational phase | * Guard against "mission creep" by monitoring the scope of the Project and ensuring that any material changes (e.g. additional Input Data or new Data Outputs) go through an appropriate change management process; and
* At the end of the contract, ask the CSP to confirm that it (and its subcontractors) either returned or destroyed all copies of the Input Data and Output Data.
 |

**Risk 2: The CSP's facilities may not meet Victorian Government data security standards**

***Description of risk***

Your Organisation remains accountable for the Input Data while it is held by the CSP. The VPDSS requires your Organisation to assess the security value of the Input Data, and ensure security controls at a similar level of security to other Victorian Government data of the same classification.

The security value of Victorian Government data is assessed according to the potential negative outcomes that would arise if the data is compromised / misused, corrupted, or lost / unavailable. Under the VPDSS, the security value of data is described in terms of Business Impact Levels (**BILs**). Your Organisation's information security team can help you determine the BIL rating of the Website data.

Your Organisation should have a standard set of requirements for the CSP's facilities and IT infrastructure, based on the BIL rating for the data. Your Organisation can also contact OVIC or VCDI for further assistance on the types of data security features you should expect to find in a secure data analytics facility.

(*Key PDP Act references: IPP 4.1; VPDSS 2, 4, 8, 10, 11 and 12*)

***Mitigation strategies:***

| Stage | Actions |
| --- | --- |
| Pre-contract | * Liaise with your Organisation's information security team to confirm the security value (BIL) of the Input Data that will be provided to the CSP for the Project;
* Analyse the CSP’s information security capability by working with your Organisation's information security team to assess if it meets the relevant BIL rating; and
* Ensure there is a secure method for transferring data between your Organisation and the CSP. For example, consider using Transport Layer Security (**TLS**) or Virtual Private Networks (**VPN**) with protected access.
 |
| Contract terms | * The CSP should apply the specific security controls, industry standards and other security requirements that are agreed during the due diligence process;
* If the Input Data is highly sensitive, consider seeking individual confidentiality undertakings from the CSP data analysts performing the work; and
* The CSP must provide appropriate information security assurance during the contract term (e.g. certification and/or audits).
 |
| Operational phase | * Ensure that the CSP is added to your register of third-party data arrangements; and
* Monitor the CSP’s compliance with the agreed data security requirements using the assurance mechanisms in the contract (e.g. certification / audit processes).
 |

**Risk 3: The Project may not be using best practice data handling techniques**

***Description of risk***

The PDP Act requires your Organisation to take “reasonable steps” to protect the Input Data against unauthorised disclosure, and to ensure the accuracy, completeness, and currency of the Data Outputs produced using the Input Data. These "reasonable steps" requirements are designed to operate flexibly, so that they can keep up with new developments and best practices in the data analytics industry.

Government data analytics experts use a range of techniques, tools, and frameworks to improve the safety and quality of data analytics projects. For example, the Five Safes Framework[[1]](#footnote-1) provides a model for assessing and managing the risks associated with data sharing and access. The Five Safes Framework is commonly used in data analytics projects that involve confidential or sensitive data.

Applying safe data handling techniques depends on the sensitivity of the data and the potential impact of a breach or security failure. If the Input Data has a high BIL rating, consider using one or more of these best practice frameworks or contacting data analytics experts, like VCDI, for advice.

(*Key PDP Act references: IPP 2.1, 3 and 4; VPDSS 4, 5, 10, 11 and 12*)

***Mitigation strategies:***

|  |  |
| --- | --- |
| Stage | Actions |
| Pre-contract | * Consider the volume, sensitivity and BIL rating of the Input Data you are providing to the CSP and if you should work with a data analytics expert to determine whether a best practice framework (such as Five Safes) should be applied.
 |
| Contract terms | * The CSP should contractually commit to implementing any agreed actions arising out of your discussion with them.
 |
| Operational phase | * Monitor the CSP's compliance with the agreed actions using the assurance mechanisms in the contract (e.g. project steering meetings / audit processes); and
* Check the quality of the Data Outputs that you receive from the CSP, to ensure that they are accurate and complete before you put them to operational use.
 |

**Risk 4: The CSP may not be adequately prepared for a data breach**

***Description of risk***

Under the VPDSS, your Organisation is required to notify OVIC of any data breach involving public sector data with a BIL of level 2 ("Limited") or higher. Data has a BIL of level 2 if the data breach would cause even "***limited*** *harm/damage to government operations, organisations or individuals*"[[2]](#footnote-2).

While the CSP holds the Input Data and conducts the analysis, you must ensure that the CSP has adequate measures in place to prepare for, detect, and prevent data breaches. The CSP should be ready to respond if a data breach does occur, and should use reasonable technical and operational measures to mitigate the impact of any such data breach. Your Organisation should assess the CSP's level of data breach readiness as part of your information security due diligence and procurement.

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

***Mitigation strategies:***

|  |  |
| --- | --- |
| Stage | Actions |
| Pre-contract | * Assess the CSP's data breach readiness with your IT and information security teams including whether the CSP uses appropriate technical measures to mitigate the impact of a potential breach (for example, encrypting data in transit and at rest, and using appropriate data / application segregation techniques).
 |
| Contract terms | * The CSP must implement suitable practices, procedures and technological measures to detect, prevent, and mitigate security incidents;
* The CSP must notify you of suspected or confirmed data breaches, and comply with your Organisation's incident response policies; and
* The CSP must investigate and remediate all data breaches, and co-operate with your Organisation on the data breach response (including any regulatory notifications).
 |
| Operational phase | * Monitor and periodically audit the CSP's compliance with the data security using the assurance mechanisms in the contract (e.g. certification / audit / stress test); and
* Ensure that your team is aware of your Organisation's data breach response plan and the relevant contacts in your Organisation's IT and information security teams.
 |

**Risk 5: The Data Outputs may not be properly de-identified**

***Description of risk***

In this scenario, the Data Outputs include statistical tables (derived from the Input Data) that your team intends to include in the final, public-facing report. Where statistical tables are derived from personal information, there is a potential risk that the data in the tables could be reverse-engineered to "re-identify" the relevant staff members.

Recent advances in data science and technology have made it easier to re-identify individuals, particularly unit level data, even where there is only a limited amount of starting data. Consequently, any statistics or data that you intend to make publicly available should go through a robust de-identification process to ensure that individuals cannot reasonably be re-identified.

Assessing and managing re-identification risk is a highly technical matter. OVIC or a Victorian Government data analytics expert, such as VCDI, can provide further advice about how you can manage this risk.

(*Key PDP Act references: IPP 2.1 and 4.1; VPDSS 2 and 3*)

***Mitigation strategies:***

|  |  |
| --- | --- |
| Stage | Actions |
| Pre-contract | * If any of the statistical tables are derived from personal information, consider whether it is necessary to publish those tables in the final report;
* If you wish to publish the tables, determine who is responsible for ensuring that the statistical tables will be de-identified to an appropriate standard;
* If the CSP does not commit to performing the de-identification work, liaise with a Victorian Government data analytics expert (such as VCDI); and
* Ensure that the de-identification process is conducted using a structured de-identification decision making framework (such as CSIRO Data 61's De-identification Decision-Making Framework[[3]](#footnote-3)).
 |
| Contract terms | * If the CSP performs de-identification, specify the relevant de-identification standards, techniques and methodology that must be used.
 |
| Operational phase | * Make a record of the steps taken to de-identify the statistical tables before publishing them in the final public-facing report;
* Check that you have complied with your Organisation's data release and publication policies including the appropriate data custodian approvals; and
* Consider having the de-identification work reviewed by an independent data analytics expert (such as VCDI or CSIRO Data 61).
 |

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, with the aim of ensuring that the outsourcing arrangement meets the following general objectives:

**Objectives - Privacy compliance**

* The CSP agrees (and has the necessary know-how and operational capacity) to manage the Input Data and Data Outputs in a manner that is consistent with the requirements of the IPPs - for example, the IPP 4.2 requirement to avoid retaining the Input Data (or Data Outputs) for longer than is needed; and
* Your Organisation has taken the necessary steps to ensure that the Data Outputs can be used by your Organisation for the intended purposes without breaching the PDP Act - for example, by ensuring that any data that you include in the final public-facing report has been properly de-identified to a standard that is appropriate for publication.

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 may also wish to consider conducting a Privacy Impact Assessment, which provides a structured process for systematically considering and addressing the requirements of the IPPs.

**Objectives - Data security compliance**

* The CSPs agree (and have the necessary know-how and operational capacity) to manage the Input Data and Data Outputs in a manner that complies with the requirements of the VPDSS;
* Your Organisation has addressed the requirements of VPDSS 8 (Third Party Arrangements), including:
	+ your Organisation has undertaken an information security risk assessment of the CSP's service offering and addressed any residual risks prior to finalising the arrangement - see VPDSS 8 element E8.030;
	+ your Organisation has documented its information release management requirements - see VPDSS 8 element E8.070; 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; and
* Your Organisation has taken the necessary steps to ensure that the Data Outputs will be managed in accordance with the requirements of the VPDSS once you receive them from the CSP.

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.

1. See, e.g., Australian Institute of Health and Welfare, ‘The Five Safes Framework’ (<https://www.aihw.gov.au/about-our-data/data-governance/the-five-safes-framework>) and Australian Bureau of Statistics, ‘Managing the Risks of Disclosure: the Five Safes Framework’ ([http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1160.0Main%20Features4Aug%202017](http://www.abs.gov.au/ausstats/abs%40.nsf/Latestproducts/1160.0Main%20Features4Aug%202017)). [↑](#footnote-ref-1)
2. Refer to the current VPDSF BIL table on the OVIC website <https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/> for further information. [↑](#footnote-ref-2)
3. See: <https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decision-making-framework/> [↑](#footnote-ref-3)