How to use this document

This case study considers a common type of outsourcing arrangement: where a Victorian public sector (**VPS**) body wishes to utilise an online service delivery model for a new program or initiative (in this case, a training course that is delivered online). 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 professional development team for a Victorian Government body that is responsible for certifying and regulating professionals in a particular industry sector (your **Organisation**).

Your Organisation identified an emerging skills gap affecting a large number of professionals in your area, and your team has been asked to develop a training and awareness program to respond to this challenge.

Your team decided that the program will include a voluntary online training course available at no charge. The training course will ask professionals to self-rate their knowledge in the area, and then complete a test to assess their skill level.

The training course will then give the professional feedback on their performance, a report that summarises their answers and compares them against the initial self-assessment, and the average scores of other professionals who also took the test. The professional will then be invited to sign up to a mailing list for further updates and training materials.

Senior managers in your Organisation also wish to receive statistics about the participation / uptake rate for the online training course, and general trends about the performance of the professionals who complete the course. This will be used to assess the effectiveness of the online training course within the broader education program, and to guide the development of further training materials.

You are approached by a corporate training consultancy to assist with the project. If engaged, the consultancy would act as a contracted service provider (**CSP**). The CSP developed similar solutions for other Australian regulators, and offered your team an "all in one" package for this project. In addition to helping your team to design the training course, the CSP will also develop and manage the website that will host the training course (the **Website**).

The CSP has provided you with a copy of its standard terms and conditions. The CSP mentions that its terms and conditions have previously been acceptable to other Victorian Government agencies.

What are your Organisation’s responsibilities in this scenario?

What are your Organisation's responsibilities in this scenario?

The Website will collect information about the professionals that undertake the online training course including their initial self-assessment, and their actual performance. It will also collect contact details of the professionals that sign up for the mailing list.

While this is information about the individuals 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 ensure that the professionals completing the online training course are properly informed about how their data will be used. Your Organisation is also required to ensure that the method of collection is fair, and that your Organisation does not collect more information than is necessary for its functions and activities. You should take steps to ensure that the CSP (and the stakeholders within your Organisation) are aware of, and will comply with, these parameters.*

The Website is being used to collect information for your Organisation. This information will constitute "public sector data", and the Victorian Protective Data Security Standards (**VPDSS**) will apply.

The CSP manages the Website (and collecting data through the Website) for your Organisation. Your Organisation has responsibility under the VPDSS for ensuring that the Website is secure, and that the CSP handles any data collected through the Website in a secure manner.

*Among other things, the VPDSS requires your Organisation to assess the security value of the data that is being collected through the Website, 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 Website data has a BIL of level 2 ("Limited") or higher, your Organisation is responsible to notify OVIC of any data breach affecting that data.*

Complying with the IPPs and VPDSS requires a co-ordinated effort from many different stakeholders within your Organisation including the IT and 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 help you conduct due diligence on the CSP. Depending on the outcome of due diligence, you may need to de-scope or restructure aspects of the CSP's proposed scope of work. The Victorian Government is currently working to establish more streamlined procurement processes for government IT projects, which will provide access to pre-vetted technology solutions and panels of approved suppliers. Contact your Organisations' IT procurement team or the Enterprise Solutions Branch in the Department of Premier and Cabinet for further information.

Breaching privacy and data security controls can have serious consequences. Data breaches can cause serious reputational damage, negatively impact stakeholder relationships, and put affected individuals at risk of further harm (such as identity fraud). OVIC has a range of powers under the PDP Act to investigate data breaches and other misuses of personal information and public sector data.

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 risk mitigation strategies during the (i) pre-contract (due diligence / requirements gathering); (ii) contracting; and (iii) operational phases.

**Risk 1: The Website may not meet Victorian Government data security standards**

***Description of risk***

While the CSP said it has worked with Victorian Government agencies previously, this does not guarantee the CSP has appropriate security standards in place for the specific needs of this project. Data security requirements should be assessed on a case-by-case basis.

The VPDSS requires your Organisation to assess the security value of the data that is being collected through the Website, and implement proportionate security controls to ensure that the data receives 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 to determine the BIL rating of the Website data.

Your Organisation should have a standard set of requirements for the Website (and its back-end IT infrastructure), based on the BIL rating for the data. If not, your Organisation can contact OVIC or the Enterprise Solutions Branch in the Department of Premier and Cabinet for further assistance. A good starting point for assessing the CSP's data security capabilities is to consider the Australian Signal Directorate's "Essential Eight" and the Victorian Government's *Cloud Information Security Guidance[[1]](#footnote-1)*.

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

***Mitigation strategies:***

| Stage | Actions |
| --- | --- |
| Pre-contract | * Liaise with your Organisation's information security team to confirm the security value (BIL) of the data that will be published and collected through the Website;
* 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;
* If the CSP cannot meet data security requirements, consider de-scoping and re-allocating certain portions of the scope of work (for example, by using approved Victorian Government IT infrastructure to host a Website designed by the CSP); 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**) 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;
* The CSP should commit to maintaining at least the same level of security during the contract term, and should not remove or degrade existing security controls;
* The CSP must provide appropriate information security assurance during the contract term (e.g. certification and/or audits); and
* Identify any contractual terms that assign data security roles and responsibilities to your Organisation (e.g. identity and access management roles). Ensure that these terms are acceptable to your Organisation's IT operations team.
 |
| Operational phase | * Liaise with your IT operations and information security teams to ensure that the CSP and the Website are added to any relevant IT project registers.
* Monitor the CSP's compliance with the agreed data security requirements using the assurance mechanisms in the contract (e.g. certification / audit processes).
 |

**Risk 2: The CSP may be using subcontractors to provide the IT infrastructure for the Website**

***Description of risk***

Unless the CSP is a dedicated technology solutions company, it is likely that the CSP will be using third party subcontractors to provide the IT infrastructure for the Website. These subcontractors may include web hosting service providers, website developers, and IT support service providers.

Subcontracting arrangements can create additional challenges from a data security and privacy compliance perspective where they reduce your Organisation's ability to maintain direct oversight of the entities actually responsible for securing and managing your data. Subcontractor arrangements can also increase compliance requirements for the project - for example, where the subcontractor or its IT infrastructure are located outside of Victoria.

You should work with your Organisation's IT and information security teams to seek details from the CSP about its proposed subcontracting arrangements. The CSP should contractually assure you that the substantive data security commitments they agree to will be followed by their subcontractors.

(*Key PDP Act references: IPP 2.1, 4.1; VPDSS 4, 8 and 10*)

***Mitigation strategies:***

| Stage | Actions |
| --- | --- |
| Pre-contract | * Discover the CSP's proposed subcontracting arrangements, then liaise with your IT operations and information security teams to decide if subcontractors are appropriate (e.g. is the subcontractor a reputable provider in its own right?);
* Ask the CSP what information security assurance it can provide in relation to its subcontractors (e.g. certifications / audit reports); and
* Confirm where the Website and its data will be hosted. If this location is outside of Victoria, consult with your Organisation's privacy officer.
 |
| Contract terms | * The CSP should be responsible for ensuring that all subcontractors implement data security measures that are consistent with those set out in the CSP contract;
* Ideally, the CSP should only subcontract with your Organisation's consent; and
* If the CSP has agreed to provide information security assurance in relation to its subcontractors (e.g. certifications / audits / stress tests), this requirement should be included in the CSP contract.
 |
| Operational phase | * Monitor and periodically audit the CSP's compliance with the agreed data security requirements for subcontractors using the assurance mechanisms in the contract (e.g. certification / audit / stress test). If the CSP does not have the right to directly audit its subcontractors' compliance with the agreed data security requirements, consider whether other mechanisms are available (such as obtaining copies of independent audit reports).
 |

**Risk 3: 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. In practice, this will cover a fairly broad range of data. OVIC considers that data will have a BIL of level 2 if the data breach would cause even "***limited*** *harm/damage to government operations, organisations or individuals*"[[2]](#footnote-2).

If the CSP will be managing the Website for your Organisation, you will need to ensure that the CSP has adequate measures in place to prepare for, detect, and prevent potential data breaches. The CSP should also be ready to respond if a data breach does occur, and should use reasonable technical and operational measures to mitigate the impact of any data breach. Your Organisation should assess the CSP's level of data breach readiness as part of your information security due diligence.

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

***Mitigation strategies:***

| Stage | Actions |
| --- | --- |
| Pre-contract | * Work with your IT and information security team to assess the CSP's level of data breach readiness as part of procurement; and
* Consider whether the CSP is using appropriate technical measures to mitigate the impact of a potential breach (e.g. encrypting data in transit and at rest, and using appropriate data / application segregation techniques).
 |
| Contract terms | * The CSP should be required to implement suitable practices, procedures, and technological measures to detect, prevent, and mitigate security incidents;
* The CSP should be required to notify your Organisation of suspected or confirmed data breaches, and comply with your Organisation's incident response policies; and
* The CSP should be required to 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 agreed data security requirements 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 4: Ownership and control of the Website data may not be clearly defined or understood**

***Description of risk***

The CSP may wish to retain data collected through the Website (such as the mailing list and the users' test scores) for the CSP's own commercial purposes.

CSPs should not retain public sector data for their own commercial purposes. Here the professionals participate in the online training course expecting that they are dealing with a Victorian Government body and expecting their data will only be used for public purposes.

(*Key PDP Act references: IPP 1, 2.1, 3, 4.2, 5 and 6 VPDSS 1, 2, 3, 7 and 8.*)

***Mitigation strategies:***

|  |  |
| --- | --- |
| Stage | Actions |
| Pre-contract | * Confirm with the CSP that all data collected through the Website is owned by your Organisation, and cannot be retained or used by the CSP for ancillary purposes.
 |
| Contract terms | * Clarify that the CSP can only handle the Website data to provide the services, and may not use the data for the CSP's (or any third party's) commercial purposes;
* The CSP must delete or return (providing proof on request) Website data to your Organisation at the end of the contract term (subject to statutory requirements); and
* As the CSP does not have any direct relationship with the users and manages the Website on behalf of your Organisation, the CSP should refer any access / correction requests or privacy complaints that it receives from the users to your Organisation.
 |
| Operational phase | * At the end of the contract term, ask the CSP to confirm that it (and each of its subcontractors) has returned or deleted Website data.
 |

**Risk 5: The Website users may not fully understand how their data will be used**

***Description of risk***

The primary purpose of the online training course is to deliver training to the professionals and provide them with feedback on their performance. However, your Organisation also wishes to use the Website data for certain ancillary purposes such as gathering statistics about participation / uptake rate and general performance trends.

IPPs 1 and 10 in the PDP Act govern how information can be collected from the professionals who use the Website, including requiring that professionals be notified about how their information will be used and, in some cases, obtaining their consent. IPP 1 also prohibits your Organisation from collecting more information than is necessary for your functions and activities. The Website should be designed with these requirements in mind. Your Organisation's privacy officer can provide you with guidance on how this can be achieved.

(*Key PDP Act references: IPP 1 and 10; VPDSS 1, 2, 3 and 8*)

***Mitigation strategies:***

|  |  |
| --- | --- |
| Stage | Actions |
| Pre-contract | * Liaise with your Organisation's privacy officer to ensure that the proposed Website design complies with the requirements of IPPs 1 and 10. This includes developing an appropriate "privacy collection notice" to explain how the data will be used, and ensuring that the Website has mechanisms to seek user consent where necessary.
 |
| Contract terms | * The CSP must design and implement the Website in accordance with the requirements developed during the pre-contract stage.
 |
| Operational phase | * Before the Website goes live, undertake testing to ensure that the Website is functioning correctly (e.g. the privacy collection notice is accessible and user consents are being recorded correctly).
 |

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 Website and the data collected in a manner that is consistent with the requirements of the IPPs - for example, the IPP 4.2 requirement to avoid retaining client personal information for longer than is needed; and
* Your Organisation has complied with its own obligations in relation to the data that is collected through the Website - for example, the notification requirements in IPP 1.3.

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 manage the Website and the data collected in a manner that complies with 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; and
	+ your Organisation has identified and assigned relevant information security roles and responsibilities to the CSP under the contract - see VPDSS 8 element E8.040; and
* Your Organisation is able to comply with its VPDSS obligations in relation to the data that is collected through the Website, once that data is returned to your Organisation by 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. <https://www.vic.gov.au/cyber-security-standards-and-guidelines> [↑](#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)