



Privacy Impact Assessment: Department of Education and Training and VET Student Loans Ombudsman File Transfer Process

January 2019

Privacy Impact Assessment Report – Contents

1. Threshold assessment.....	4
2. Plan the PIA.....	5
3. Describe the project.....	5
4. Identify and consult with stakeholders.....	6
5. Map information flows	7
6. Privacy impact analysis and compliance check.....	9
7. Privacy management - addressing risks.....	14
8. Recommendations	14
9. Sign off.....	15

PRIVACY IMPACT ASSESSMENT

Role of OAIC

Note: The Privacy Act gives the Information Commissioner (IC) a power to direct an agency to provide a PIA to the OAIC, if the Commissioner considers that a proposed activity or function of the agency might have a significant impact on the privacy of individuals. (s33D Privacy Act) This includes when the agency proposes to engage in a new activity or function, or substantively change an existing activity or function e.g., a substantive change to the system that delivers an existing function or activity.

What is a Privacy Impact Assessment (PIA)?

A Privacy Impact Assessment (PIA) is a systemic assessment of a project that may have privacy implications. The term project includes:

- ◆ policy proposals
- ◆ new or amended legislation, programs, systems or databases
- ◆ new methods or procedures for service delivery or information handling
- ◆ changes to how information is stored

The PIA identifies the impact the project might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating adverse impacts. It will go beyond assessing the project's risk of non-compliance with privacy legislation and identify controls to mitigate the risk.

This PIA will also consider the broader privacy implications and risks, including whether the planned uses of personal information in the project will be acceptable to the community.

This PIA should be prepared with reference to the Commonwealth Ombudsman's Privacy Impact Assessment Guidelines (attached to the [Privacy Policy](#)).

DET and VSLO file transfer process

The Office of the Commonwealth Ombudsman (the Office) and Department of Education and Training (DET) are required to share information relating to complaints about VET student loan scheme providers, undertaken under the Office's VET Student Loans Ombudsman (VSLO) function.

To date, this has predominantly involved DET sending the Office lists of student whose student loan debts have been re-credited as a result of tuition assurance or compliance action. This information has been used to minimise duplication of work between the two agencies.

DET previously transferred this information to the Office by encrypted USB, however has recently started using a secure file transfer service (SFTS).

Following the passage of the *Higher Education Support Amendment (VET FEE-HELP Student Protection) Bill 2018*, the Office will now make recommendations to DET to re-credit VET FEE-HELP debts. This will involve transferring personal information to DET via the SFTS.

This PIA focuses on how the Office will share complainants' personal information with DET via the SFTS, predominantly for the new VET FEE-HELP remedy but also for complaints that interact with DET's tuition assurance and compliance actions.

1. Threshold Assessment

- a) Will any personal information be collected? If yes, record a brief description of the personal information that will be collected, used or disclosed (such as name, address, date of birth, health information etc.).

Complainants' personal information is collected by dispute resolution officers (DROs) when a complaint is made, and is recorded in Resolve.

Data, including personal information, will be extracted from Resolve and sent to DET through the SFTS as a CSV file as the basis of the Office's recommendations for re-credits through the new VET FEE-HELP remedy.

Personal information to be sent to DET includes full legal name, date of birth, email address, residential address, phone number, Commonwealth Higher Education Student Support Number (CHESSN) issued by DET, and the student identification number issued by the education provider. Information on the nature of the student loan debt will also be transferred.

2. Plan the PIA

General Description

Name of Program: DET and VSLO file transfer process	
Date: 2 January 2019	
Name of Section/Branch: VET FEE-HELP Remedy Team, Industry Branch	
PIA Drafter: Claire Roberts	
Email: claire.roberts@ombudsman.gov.au	Phone: 02 6276 0108
Program Manager: Tim O’Mahony	
Email: tim.omahony@ombudsman.gov.au	Phone: 02 6198 9436

Definition – Project: For the purpose of this document, the term project is intended to cover the full range of activities and initiatives that may have privacy implications including:

- policy proposals,
- new or amended legislation, programs, activities, systems or databases,
- new methods or procedures for service delivery or information handling
- changes to how information is stored

3. Describe the Project

A PIA needs a broad ‘big picture’ description of the project. It should be kept fairly brief.

This project focuses on the Office transferring personal information to DET by a SFTS as recommendations for re-credits under the new VET FEE-HELP remedy. Information will only be transferred to DET with complainants’ consent. Personal information will be collected in accordance with the Office’s normal complaints processes.

Files will be transferred using the SFTS provided by the Department of Jobs and Small Business. DET has implemented the use of a secure file sharing service to mitigate the risks of improper use and release of DET’s data. This secure method of transfer, outlined in DET’s Information Security Policy and Data handling and Transfer Policy (attached), ensures that DET’s methods for transfer of information and data are secure (encrypted), controlled and accredited for use as per the requirements of the Australian Government’s Information Security Manual.

4. Identify and consult with stakeholders

The Office consulted with DET's IT security team and legal staff in relation to this project. Consultation was also undertaken with the Office's Principal Lawyer and members of the ICT Team. No concerns were raised with the use of the SFTS system.

Provide key privacy elements

Personal information to be transferred to DET by the SFTS comprises:

- information from the complainant regarding their current name, address, phone number and email address
- information extracted from DET's Higher Education Information Management System (HEIMS), to allow DET to process re-credits through HEIMS
- the Office's reason for recommending DET re-credit a student loan debt, denoted by an alphanumeric code that correlates with an agreed investigation process
- that the complainant has complained to the Office

None of this information is sensitive, as outlined in the APPs.

Most of the information to be transferred to DET is DET's own data on the student, collected by DROs from HEIMS. Very little information on the nature of complainants' circumstances or complaints will be shared with DET through the SFTS. The nature of the data means that third parties will not understand some of the data fields if they obtain the data as the fields are coded, although it is unlikely a third party could access the system given the security provisions of the SFTS.

Some personal information to be transferred was collected by the Office under s 8(3) of *the Ombudsman Act 1976*.

Any transfers of personal information from the Office to DET will be undertaken only with complainants' consent.

The information will be disclosed in accordance with the Memorandum of Understanding between DET and the VSLO during the establishment of the VSLO's function. This MoU will be updated in February 2019 and will reference this PIA.

5. Map Information Flows

Describe and map the project's personal information flows.

VERIFICATION

Complainants' identity is verified by the Office on first contact, including name, address and date of birth. These identifiers are then compared with HEIMS, to verify the details of the student debt. DET have confirmed the use of three identifiers is consistent with their practices.

COLLECTION

Personal information is collected by online form or phone, as per the standard practices of the Office. A new VSLO-specific online form will be used from March 2019. A separate PIA is being developed for this online form.

Information is also collected from HEIMS once a complainant's identity is verified.

Consent is sought from complainants to share their details with DET for the purposes of re-crediting their student loans debts, and this consent is documented in Resolve.

USE

Personal information is collected for the purposes of investigating VSLO complaints, as per the Office's standard practices.

For the purposes of this new project, the Office will share information with DET as a recommendation to re-credit a VET FEE-HELP debt under the new VET FEE-HELP remedy. DET requires this personal information to make a decision on whether to re-credit the debt and then to process re-credits in HEIMS.

DISCLOSURE

The recent amendment ss 20ZM(1)(ca) of the *Ombudsman Act 1976* allows the Office to make recommendations to DET to re-credit VET FEE-HELP debts. This power has been delegated to the EL1 level.

Complainants' consent will also be received before disclosing information.

INFORMATION QUALITY

The quality of the personal information collected will be ensured through the data validation process and adherence to the VET FEE-HELP Remedy Team's Standard Operating Procedures and the Quality Assurance Framework.

Complainants are asked to provide up to date contact information before the personal information is transferred to DET, to improve the efficiency of the re-credit process. This information is taken from Resolve, in the person contact details, so will have been validated by the Office.

If a complainant's details are not accurate or up to date they will be given an opportunity to provide updated information to DET. If DET are unable to contact the complainant, DET will ask the Office to do so.

Other data will be extracted from HEIMS for data matching processes at DET. DET will contact the Office if any data does not match.

Therefore, there are limited consequences to complainants beyond a slight delay in processing their re-credits if their personal information is not accurate or up to date.

SECURITY

DET's Information Security Policy and Data handling and Transfer Policy, outlines that the SFTS is secure (encrypted), controlled and accredited for use as per the requirements of the Australian Government's Information Security Manual.

Access to complaint files, and the personal information contained within, is undertaken with the Office's standard practices

RETENTION AND DESTRUCTION

Data will be retained and destroyed in accordance with the Office's standard practices. Individual complaints data will be retained in Resolve, with recommendations files to be retained in Objective.

ACCESS AND CORRECTION

Access to and correction of personal information in Resolve will be undertaken in accordance with the Office's standard practices. Complainants will also be sent a summary of Office's recommendation to DET for their own records.

Requests to access and correct information retained in HEIMS will be referred to DET as the data custodians.

Complainants can access and correct their personal information under the *Freedom of Information Act 1982* and the *Privacy Act 1988*.

6. Privacy Impact Analysis and Compliance Check

PRIVACY IMPACT ANALYSIS

The privacy impact analysis should attempt to determine whether the project has acceptable privacy outcomes, or unacceptable privacy impacts.

The use of DET's SFTS relies on the Office's existing processes for the collection and storage of data, along with consent from complainants before personal data is transferred.

The security measures associated with the SFTS are strong and mean privacy breaches are unlikely. The SFTS is more secure than email.

The personal information disclosed to DET will only be used for the purpose of processing re-credits under the new VET FEE-HELP Remedy.

By sharing personal information with DET under this project, complainants will only have positive consequences, through re-crediting their VET FEE-HELP debts. They will not be negatively impacted in any way.

ENSURING COMPLIANCE

You will need to consider whether your project complies with each of the Australian Privacy Principles (APPs).

#	Description of the privacy principle <i>(These can be deleted from your final report if they're not relevant to your project)</i>	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
1	<p>Principle 1 – Open and transparent management of personal information</p> <p>The agency must have a clearly expressed and up to date APP privacy policy about the management of personal information by the agency.</p>	<p>The Office has an up to date APP privacy policy.</p> <p>Additionally, complainants' consent is obtained before personal data is transferred to DET. Complainants are advised what data will be transferred and for what purpose.</p>	<i>Complies</i>	

PRIVACY IMPACT ASSESSMENT – DET and VSLO file transfer process

#	Description of the privacy principle <i>(These can be deleted from your final report if they're not relevant to your project)</i>	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
2	<p>Principle 2 – Anonymity and pseudonymity</p> <p>Individuals must have the option of not identifying themselves, or of using a pseudonym, note exceptions to this rule apply.</p>	<p>Anonymous complaints are not possible for this project as personal data is required for the data sharing tasks between the Office and DET, including DET processing the Office's recommendations for re-credit.</p>	<i>Complies</i>	
3	<p>Principle 3 – Collection of solicited personal information</p> <p>Limits apply to only collect information where the information is reasonably necessary for or directly related to one or more of the agency's functions or activities.</p>	<p>The Office will only collect personal information required to allow DET to make a decision on whether to re-credit a debt, and data to process the re-credit in HEIMS.</p>	<i>Complies</i>	
4	<p>Principle 4 – Dealing with unsolicited personal information</p> <p>Determine whether or not the agency could have collected the information under APP 3. If not, where it is lawful and reasonable to do so destroy or de-identify the information.</p>	<p>The Ombudsman will not retain any unsolicited personal information that is not required to investigate a complaint or make a recommendation to DET to re-credit a debt.</p>	<i>Complies</i>	
5	<p>Principle 5 – Notification of the collection of personal information</p> <p>Inform the person what information you are collecting, the purpose or use of the information and how they may access or complain about the use of the information. Also inform them if the agency is likely to disclose the information to overseas recipients.</p>	<p>Complainants are informed of the need to collect personal information upon lodging a complaint.</p> <p>Complainants are referred to the Ombudsman Privacy Policy hosted on www.ombudsman.gov.au and may also request a physical copy be sent to them.</p>	<i>Complies</i>	

PRIVACY IMPACT ASSESSMENT – DET and VSLO file transfer process

#	Description of the privacy principle <i>(These can be deleted from your final report if they're not relevant to your project)</i>	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
6	<p>Principle 6 – Use or disclosure of personal information</p> <p>Use it for the purpose you collected it for, unless one of the exceptions applies.</p>	<p>Complainants' consent is sought to transfer details of their complaint to other government agencies for the purposes of resolving their complaint. This occurs during the initial lodgement of the complaint and may occur at other stages in the process where deemed necessary.</p>	<p><i>Complies</i></p>	
7	<p>Principle 7 – Direct marketing</p> <p>Information not to be disclosed for the purpose of direct marketing unless exceptions apply, e.g., consent.</p>	<p>The Office will not undertake direct marketing as part of carrying out the VSLO function.</p>	<p><i>N/A</i></p>	
	<p>Principle 8 – Cross-border disclosure of personal information.</p> <p>Requirement to ensure overseas recipient does not breach APPs note exceptions apply e.g., information is subject to a law similar to APP's.</p>	<p>Data will not be disclosed cross-border for the purposes of this project.</p>	<p><i>N/A</i></p>	
9	<p>Principle 9 – Adoption, use or disclosure of government related identifiers.</p> <p>Only assign unique identifiers where permitted. Agency should not disclose identifiers unless permitted.</p>	<p>A unique complaint reference number is allocated to each complaint lodged with the Office for case management purposes. This unique identifier will be included in the data transmitted to the DET in the course of making a recommendation to re-credit or not re-credit a study debt, in the event DET need to query a recommendation.</p>	<p><i>Complies</i></p>	

PRIVACY IMPACT ASSESSMENT – DET and VSLO file transfer process

#	Description of the privacy principle <i>(These can be deleted from your final report if they're not relevant to your project)</i>	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
10	<p>Principle 10 – Quality of personal information.</p> <p>Ensure information is accurate, up to date, complete and relevant prior to using it.</p>	<p>Personal information required for identification and communication purposes will be provided by the complainant or their nominated representative. This information will be validated and updated before the Office makes a recommendation to DET through the SFTS.</p>	<i>Complies</i>	
11	<p>Principle 11 – Security of personal information.</p> <p>Take care of the information and protect it against loss, modification, or unauthorised disclosure and other misuse. When no longer required either destroy or de-identify it.</p>	<p>Data will be stored in accordance with the requirements of the Australian Government Information Security Manual and the Protective Security Policy Framework published by the Attorney-General's Department.</p> <p>The Office will dispose of data in accordance with guidance set out by the National Archives of Australia (the NAA) in the <i>Archives Act 1983</i> and associated sentencing guidelines published by the NAA.</p>	<i>Complies</i>	
12	<p>Principle 12 – Access to personal information</p> <p>People have a right to see their personal information noting exceptions apply, eg., FOI exemptions.</p>	<p>Complainants who wish to access their complaint file under the Freedom of Information Act may do so in writing, and are informed of this right in the Office's privacy policy.</p>	<i>Complies</i>	
13	<p>Principle 13 – Correction of personal information</p> <p>Agency must take steps to correct personal information held, ensure information is up to date, accurate, complete and not misleading.</p>	<p>Complainants may request the Office to correct or update inaccurate records via email or verbal request and are subject to standard identity validation checks.</p>	<i>Complies</i>	

PRIVACY IMPACT ASSESSMENT – DET and VSLO file transfer process

#	Description of the privacy principle <i>(These can be deleted from your final report if they're not relevant to your project)</i>	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
14	Other privacy interests	The Ombudsman is subject to the <i>Privacy Act 1998</i> and is required to immediately notify the Office of the Australian Information Commissioner of all eligible data breaches as set out in the Notifiable Data Breach scheme.	<i>Complies</i>	

7. Privacy Management – Addressing Risks

A risk is something that could lead to the unauthorised collection, use, disclosure or access to personal information.

Use the table below to list each of the privacy risks identified and the mitigation strategies/tools that will be implemented to mitigate these. Add extra rows as required. Please specify the likelihood of the risk arising, the degree of impact it would have on individual’s privacy if it occurred and an assessment (low/medium/high) of the residual risk. It may be helpful to categorise these risks into areas such as: governance, people, process, technology.

Risk Mitigation Table					
	Identified Risk	Mitigation Strategy	Likelihood	Impact	Risk Rating
1	File may be intercepted by third parties	Utilise SFTS	Low	Low	Low
2	Personal information may be transferred to DET without consent from complainant	Standard operating procedures and quality assurance processes	Medium	Low	Low
3	File may be opened by unauthorised person at DET	File will be password protected	Low	Low	Low

8. Recommendations

Summarise the recommendations to minimise the impact on privacy based on your risk assessment.

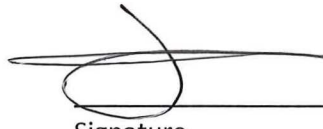
Ref	Recommendation	Agreed Y/N
R- 01		
R- 02		

Signatures

Dermot Walsh, SAO, Industry Branch

17/1/19

Date



Signature

Paul Pfitzner, Privacy Champion

17/1/19

Date



Signature

