

# **DESPS ADVISORY NOTICE 07/2007**

## **ESP CLAIMS**

### **PRIVACY ISSUES**

*DESPS Advisory Notices provide advice or more detailed explanations concerning aspects of the ADF Reserves Employer Support Payments (ESP) Scheme.*

Personal information collected as part of the ESP claims process is protected by the *Privacy Act 1988 (Cth)* (the Act). Under the Act, there are specific rules regarding the collection, security and storage, access to, use and disclosure of personal information.

The following guidance is provided to inform ESP Delegates and Clerks about privacy issues relating to the ESP scheme.

### **GENERAL GUIDANCE**

When a claimant submits an ESP claim, they provide information as part, or in support, of that claim. This notice is intended to provide a general understanding of the issues that could be encountered by ESP delegates and clerks when dealing with personal information and the impact of the Act on the way in which that information is handled.

General guidance is provided relating to:

- Collection of information
- Access to information
- Storage of information
- Use of information
- Disclosure of information

Specific guidance is provided covering the following issues:

- Tax file numbers
- Provision of copies of ESP claim forms to a Reservist's unit
- Dealing with approaches by claimants to Ministers and/or MPs
- Requesting further information from claimants
- Releasing information to Reservists regarding their employer's claims
- Releasing information to employers regarding their Reservist's service

### **INFORMATION**

#### **INFORMATION PRIVACY PRINCIPLES**

Information Privacy Principles (IPPs) are detailed in the Act. They apply to Commonwealth agencies<sup>1</sup>, including Ministers and Departments – essentially anyone involved in the public sector at the Commonwealth level. It is unlawful for an agency to do an act, or engage in a practice, that breaches an IPP.

---

<sup>1</sup> Defined at Section 6 of the Act.

Key IPPs are:

- **IPPs 1, 2 and 3 – Collection:** Personal information should be collected in a manner which is fair and lawful, and not intrude unreasonably on the individual.
- **IPP 4 – Storage and Security:** Personal information shall be reasonably protected against unauthorised access, use, modification or disclosure.
- **IPPs 6 and 7 – Access and Alteration:** Generally an individual has a right to access personal information held about themselves and to have such records altered if incorrect.
- **IPPs 8, 9 and 10 – Use:** Personal information shall be used only for the purpose to which the information relates unless an IPP 10 lawful exception applies. The information must be relevant to the purpose.
- **IPP 11 – Disclosure:** Personal information shall not be disclosed to any person, body or agency outside Defence unless one of the IPP 11 disclosure purposes has been met (e.g. is reasonably expected, has been consented to or is authorised by law).

Copies of the IPPs are provided at Annex A to this Advisory Notice.

## NATIONAL PRIVACY PRINCIPLES

National Privacy Principles (NPPs) are also detailed in the Act. They apply to some private sector organisations<sup>2</sup>. However, small business operators with an annual turnover of \$3M or less are exempt.

The NPPs are generally similar to the IPPs but also include:

- **NPP 2 – Use and Disclosure:** Allows, under Section 7B(3), organisations to disclose personal information which is contained on an employee record about their current or former employees.
- **NPPs 7 – Identification:** Regulates the way in which private sector organisations identify individuals.
- **NPP 8 – Anonymity:** Allows individuals to elect to remain anonymous wherever this is lawful and practicable.

The NPPs can be downloaded from <http://www.privacy.gov.au/act/npps/index.html>.

## COLLECTION

Collection of personal information for ESP purposes should be conducted in a fair, lawful and unobtrusive manner, in accordance with IPPs 1, 2 and 3.

### Opening ESP Correspondence

Where correspondence is visually identifiable as relating to an ESP claim, it should be passed unopened by registry or mail staff to a person associated with the administration of ESP claims.

---

<sup>2</sup> Defined in Section 6C of the Act as: (a) an individual; or (b) a body corporate; or (c) a partnership; or (d) any other unincorporated association; or (e) a trust.

Where correspondence is not visually identifiable as relating to an ESP claim, it should be passed to a person associated with the administration of ESP claims as soon as it is identified as relating to an ESP claim.

Where possible, ESP claims or correspondence concerning ESP claims should be opened by persons associated with the administration of ESP claims.

### Fax Machines

Where possible, fax machines used for the receipt of ESP claims or ESP correspondence should be located in the immediate vicinity of personnel administering ESP claims, in order to limit casual access by others to a claimant's personal information or the possibility of the documentation being misplaced.

Where fax machines are not located in close proximity to personnel administering ESP claims, delegates should consider the feasibility of re-locating existing fax machines or acquiring an additional fax machine for ESP use.

If it is not possible to have a fax machine located in close proximity to ESP clerks, delegates should ensure that internal work procedures are put in place requiring faxed correspondence concerning ESP to be passed immediately to ESP administrators following its receipt.

If it is not possible to have a fax machine located in close proximity to ESP administrators, and an ESP administrator is aware that a claimant may fax ESP related documents, the administrator should advise the claimant to ring him or her before faxing the documents, so that ESP personnel (where possible) may be waiting to collect the document off the fax machine.

### Mail

In accordance with Defence requirements for Staff-In-Confidence information, correspondence containing ESP claim forms (whether completed or partially completed) sent through either internal or external mail should be double-enveloped to prevent unauthorised access to these records.

## **ACCESS**

### Work Areas

ESP administrators' work areas should preferably be self-contained, and located away from any direct walkway. This is to prevent claim files from casual observation by persons who do not have a need to access the personal information (and also to minimise the opportunity for non-ESP staff to listen to phone calls by ESP staff that may disclose personal information).

Ideally, desks should be positioned in such a way as to further inhibit the possibility of unauthorised access to ESP related personal information.

Unless a work areas are is secured in a way that denies access to non-ESP staff, ESP claim files and related documentation should be cleared away at the end of each day, and stored in accordance with the guidelines below.

## **STORAGE**

ESP records, as they contain personal information, should be protected from unauthorised access, use, modification or disclosure.

### Hard copy documentation

Appropriate policies and procedures should be put in place to limit access to ESP documents to those people who have a legitimate need. ESP records containing personal information should not be left unattended in insecure areas or in locations where they may be viewed by unauthorised persons.

Physical files should be stored (e.g. in separate lockable filing cabinets or security containers) so that access is limited to persons who are involved in processing ESP claims and who need access in order to do their jobs. If this is not presently available, delegates should consider additional measures to provide this control of access (e.g. those parts of the compactus or filing cabinets containing ESP files might be pushed together and padlocked to prevent unauthorised access).

Hard copy documents containing ESP personal information should be secured at COB each day by placing them in a lockable, limited access area (to which ESP staff control access), such as a locked office, a lockable filing cabinet or security container.

Documentation which contains personal information related to ESP should not be left unsecured overnight.

### Electronic Information

Electronic ESP information which is stored on shared drives should only be accessible by ESP staff.

IT or document records management systems used by multiple personnel should have a separate, restricted access workgroup for ESP claims and associated ESP documentation.

Correspondence regarding ESP claims should not be scanned into an electronic document records management system unless the correspondence can be stored in a limited access IT area and there are procedures in place to limit access to those people who have a legitimate need. If no policies and procedures are in place to limit access to personal information that is stored electronically, correspondence should not be scanned and kept electronically in a document records management system.

Further information on implementing a limited access area within an electronic document records management system should be available from local Defence IT staff.

## **USE**

In accordance with the ESP Privacy Statement on all ESP claim forms, personal information contained in ESP claim forms or provided in supporting documentation may be used for the processing of ESP claims. This information may also be used for employer support activities.

Delegates may provide information concerning claimants to local Defence Reserves Support State/Territory Offices or State/Territory committees of the Defence Reserve Support Council for use in employer support activities.

Personal information should not be used by any person not associated with the ESP scheme, or provided for use to any other Defence personnel, for any other purpose unless a lawful exception under IPP 10 applies (refer Annex A).

## **DISCLOSURE**

Personal information is not to be disclosed outside Defence, for any purpose other than for the efficient administration of the ESP scheme, unless a lawful disclosure under IPP 11 applies (refer Annex A).

Delegates may provide information concerning claimants to local Defence Reserves Support State/Territory Offices or State/Territory committees of the Defence Reserve Support Council for use in employer support activities.

## **SUMMARY OF GENERAL GUIDANCE**

The above advice is provided as “best practice” guidelines which should, wherever possible, be implemented in all ESP locations.

Where implementation of this guidance is currently impractical, delegates should endeavour to make amendments to their administrative processes or work locations, as soon as practicable, to achieve maximum compliance with these guidelines and ensure the requirements of the Privacy Act are met.

## **GUIDANCE CONCERNING SPECIFIC SITUATIONS**

### **TAX FILE NUMBERS**

The Tax File Number guidelines 1992 (issued by the Privacy Commissioner) govern the storage, use and disclosure of tax file numbers (TFNs). Provision of a claimant’s TFN is not specifically required by the Defence Determination; however, tax documents are acceptable forms of evidence often used to establish eligibility to ESP:

- A claimant may provide their individual and/or business tax return and ATO Notice of Assessment as proof that their business is operating/trading and/or provides them with their Principal Source of Income (PSI), in accordance with Section 3B(1) of the Defence Determination.
- A delegate may require that a claimant provide their personal tax return and ATO Notice of Assessment in order to substantiate evidence provided in support of an ESP application, in accordance with Section 3B(2C) of the Defence Determination.

Normally, the TFN will not have been obscured or removed. In this circumstance, ESP delegates and clerks have a responsibility to comply with the TFN guidelines with regard to storage, use and disclosure of TFNs.

Key TFN Guidelines are:

- **Guideline 2 – Use and Disclosure:** TFNs are not to be used or disclosed to any unauthorised person to establish or confirm the identity of an individual for any purpose. TFNs may not be recorded separately except where such an action is authorised by law<sup>3</sup>.
- **Guideline 5 – Collection:** TFN information shall only be requested or collected from individuals where authorised by law.
- **Guideline 6 – Storage and Security:** TFN recipients shall ensure that the information is protected by reasonable safeguards to prevent unauthorised access, use, modification, disclosure and other misuse.
- **Guideline 7 – Incidental provision of TFNs:** When an individual chooses to provide a TFN for a purpose not authorised by law, the individual shall not be prevented from obscuring or removing the TFN. If the TFN has not been obscured/removed, the recipient shall not record, use or disclose it.

The TFN Guidelines can be downloaded from <http://www.privacy.gov.au/act/tfn/>.

#### Procedures for documentation containing TFNs

TFNs on tax returns, ATO Notices of Assessment, or other documentation should be protected to prevent loss, unauthorised access, use, modification, disclosure or other misuse in accordance with Guideline 6.

Access to records that contain a TFN should be restricted to persons undertaking duties related to the processing of ESP claims.

Hard copy documents with unobscured TFNs should be stored in a locked filing cabinet or compactus with restrictions on access, or another similar facility.

Electronic copies of such documents should be stored in restricted access folders. If there are no policies in place to limit access to people who have a legitimate need for the information, these documents should not be scanned into document management systems.

TFNs on Individual tax returns should only remain unobscured until such time as the delegate is satisfied that the ATO Notice of Assessment wholly substantiates the tax return, at which point the TFN should be obscured on both documents.

- When an Individual tax return and Notice of Assessment are received together, the TFN should be obscured once the tax return and Notice of Assessment have been confirmed as relating to each other. A notation should be added to the Notice of Assessment confirming this.
- If an Individual tax return is received without the Notice of Assessment, the TFN should not be obscured until the Notice of Assessment has been received

---

<sup>3</sup> “Law” with reference to TFNs includes taxation, assistance agency or superannuation law.

and confirmed as relating to the tax return. A notation should be added to the Notice of Assessment confirming this.

When Company, Trust and Partnership tax returns are received, the TFN should be obscured on receipt in accordance with TFN Guideline 6 (as these types of tax return are not normally accompanied by an ATO Notice of Assessment – see DESPS Advisory Notice 03/2006 for further information).

All tax returns and Notices of Assessment (where applicable) are to be secured in accordance with all other privacy requirements as outlined above.

## **UNIT COPIES OF ESP CLAIM FORMS**

Units are not required to keep copies of ESP claim forms on Reservist's personal files, in relation to Defence service commenced after 31 Aug 05. This requirement in relation to earlier claims (contained at Para 50(h) of DI(G)PERS 05-30 and Para 81(i) of DI(G)PERS 05-37) was omitted from DI(G)PERS 05-42.

Except for the COs of Air Force Reserve Squadrons and 1AFDS, unit COs are no longer ESP delegates.

Apart from ESP claims from self-employed Air Force Reservists, claims should be submitted directly to ESP delegates.

ESP claims from self employed Air Force Reservists should be submitted to the claimant's Air Force Reserve Squadron who will check the claim for completeness prior to forwarding it to the appropriate Air Force delegate for self employed Reservist claims.

Unless a claim is submitted by the claimant (or by the Reservist on behalf of the claimant) to the Reservist's unit, copies of the claims should not be provided to the unit. Such distribution may lead to an interference with privacy.

If a claim is submitted to an Army or Navy Reserve unit, the claim should be date stamped with the receipt date by the unit and forwarded promptly to the appropriate ESP delegate. Copies should not be retained at unit level.

There is no requirement for claims to be sighted by unit COs before submission and such a procedure is not authorised and is not to be implemented.

If COs are aware that a claimant has submitted an ESP claim and have concerns regarding the claimant's eligibility, they should raise these concerns with the relevant ESP delegate. In order to obtain a complete picture of a situation (whether this situation has been drawn to the delegate's attention by the CO or otherwise), a delegate may discuss with a CO those details regarding a claim as are necessary for the delegate to determine whether or not to approve a claim or to take further action.

If fraud or fraudulent misrepresentation is suspected, it should be reported to the Service Police or Inspector General immediately, through the correct channels (i.e. through the chain of command or line management). This applies to delegates, COs or

any other Defence member. In the event that fraud is suspected with regard to ESP claims, the Director ESP Scheme should also be informed.

## **MINISTERIAL INVOLVEMENT**

A claimant who approaches a Minister or their Member of Parliament (MP) to request investigation or action on their behalf concerning their ESP claim is impliedly consenting to Defence providing relevant information about their claim, including non-sensitive personal information, to the Minister and/or through the Minister to the MP.

Any personal information which is disclosed to the Minister or MP should be limited to information which is relevant to the case and necessary for the Minister to reply to the constituent's request.

If the disclosure of sensitive personal information (for example, information relating to the claimant's health or religious background) is necessary in order for the Minister to fully comprehend the situation, and the claimant's request to the Minister for enquiry or action on their behalf is not ambiguous, such information can be disclosed.

However, not all approaches by claimants to Ministers or MPs can be taken as impliedly consenting to Defence providing relevant information about their claim to the Minister and/or MP. Approaches can generally be classified at one of three levels of ambiguity with regard to implied consent for disclosure:

- **Unambiguous** – for example, a claimant who requests investigation or action on their behalf concerning their ESP claim;
- **Discretionary** – for example, a claimant who details issues they may have experienced with the ESP scheme or their particular claim, but does not explicitly request that the Minister or MP intervene on their behalf; and
- **Ambiguous** – for example, a claimant who complains about the ESP Scheme generally but does not seek or expect any resolution to eventuate from their complaint in respect of their own ESP claim.

If a claimant writes to a Minister or MP complaining that the administrative processes surrounding the ESP Scheme are causing their claim to be delayed excessively, and requesting that the Minister or MP inquire on their behalf about the delay in processing their claim, this request is considered to be unambiguous. In this case, the claimant expects a resolution of their grievance as a direct result of the Minister or MP's inquiries. The claimant is impliedly consenting to Defence providing relevant information about the claimant and/or their claim, including personal information, to the Minister and/or through the Minister to the MP. Where an unambiguous request is received, only relevant personal information necessary for the Minister to understand the situation should be disclosed.

If a claimant writes to a Minister or MP detailing issues they may have experienced with the ESP Scheme or their particular claim but does not explicitly request that the Minister or MP intervene on their behalf, Defence may consider this to be a discretionary request. This may constitute implied consent to disclose relevant information about the claimant and/or their claim to the Minister or MP. However,

depending on the context and sensitivity of the personal information, it may be advisable to gain express consent before disclosing the information.

However, a claimant who approaches a Minister or MP to merely complain about the ESP Scheme generally and does not expect any resolution to eventuate from the complaint, cannot normally be taken to have given implied consent for further investigation or enquiry on their behalf with respect to their claim. This would normally be considered an ambiguous request and IPP 11.1 may not authorise Defence to disclose the claimant's personal information (including personal information relating to the ESP claim) to the Minister and/or MP. In this event, express consent to disclose these records should normally be sought from the claimant before disclosing any personal information.

When queries are made direct to an ESP delegate by Ministers, MPs or their staff members, the delegate should inform DESPS of the query as soon as practicable.

### **REQUESTING FURTHER DOCUMENTATION FROM CLAIMANTS**

As ESP delegates are authorising the expenditure of public monies and are bound by the *Financial Management and Accountability Act 1997*, they must be satisfied of the eligibility of a claim before authorising an ESP payment. If a delegate believes that the evidence that has been provided is deficient, they cannot approve the claim. They may refuse the claim or request further information from the claimant to satisfy themselves of the claim's eligibility.

Specifically, Section 3B(2C) of the Determination allows the Director or a decision maker to require substantiation by way of a financial statement or tax return and associated ATO Notice of Assessment. This substantiation may be required if PSI evidence provided from a financial adviser or accountant does not wholly satisfy the Director or decision maker of the eligibility of the claimant to ESP.

When the Director or a decision maker requires that further information or substantiation be provided, it should be made clear to the claimant that failure to provide the requested information or substantiation will be considered by the Director or decision maker and may lead to a refusal of the claim.

If the claimant does not want to provide further substantiating evidence, they are not required to do so. However, in this case, the delegate should normally refuse the claim and advise the claimant of the outcome, in writing, as required by Section 9(8) of the Determination.

While such requests for further documentation are authorised by the Defence Determination, they should also be in accordance with IPPs 1-3, essentially:

- Personal information should only be collected for a purpose directly related to a function or activity of the collector.
- The collector of personal information should take such steps as is reasonable to ensure that the individual concerned is generally aware of the purpose for which the information is being collected, the areas within Defence and any parties to whom the information is likely to be disclosed, and that the collection of information is required for the delegate to be satisfied concerning the claimant's eligibility.

- The collector of personal information should take such steps as is reasonable to ensure that the information collected is relevant to the purpose and the collection does not intrude to an unreasonable extent upon the affairs of the individual concerned.

## **RELEASING INFORMATION TO RESERVISTS REGARDING THEIR EMPLOYER'S CLAIMS**

Details concerning an employer's claim should not be disclosed to a Reservist, unless that Reservist is acting on behalf of their employer (as the claimant, an employer can consent to a Reservist acting as an agent on their behalf to discuss details regarding their claim). If an employer has not consented to Defence discussing these details with the employee, a disclosure may be a breach of IPP 11.1.

Information regarding the status of an employer's claim (such as whether the claim has been approved/refused, or how much ESP is to be paid to the employer) can be released to a Reservist acting on behalf of their employer, as long as the delegate or ESP clerk is satisfied that the enquiry is coming from an authorised agent of the employer.

If there is any doubt as to the identity, authenticity or authority of an inquirer, a signed authorisation (or authorising email) from the employer should be requested prior to disclosing details of the employer's claim.

If a delegate requires further information, requests for additional information should still be made directly to the claimant, unless express consent has been given by the employer for the Reservist to supply this information on the claimant's behalf.

If an employer wishes to authorise a Reservist to inquire about ESP claims for Defence service rendered by other employees, a signed consent should be sought from the employer prior to disclosing any details regarding claims for service rendered by other Reservists. This situation is most likely to arise if the employer has submitted several ESP claims in relation to service by a number of Reservists.

A standard authorisation form for use in these circumstances is at Annex B.

## **DETAILS CONCERNING A RESERVIST'S SERVICE**

Sometimes, employers will not claim for periods of service undertaken by a Reservist employee, for which they may be entitled to ESP.

In these situations, the exact dates of the Reservist's service should not be disclosed to their employer, unless *the individual concerned has consented to the disclosure, or one of the other provisions of IPP11.1 applies*. This is because the dates that a Reservist has undertaken Reserve service are personal information of the Reservist.

In circumstances where there are additional periods of service which may be eligible for ESP (noting that the member must have been released on an appropriate type of leave and met all other eligibility criteria), it is suggested that delegates and clerks use the following wording to ascertain whether employers are eligible for ESP over any other periods:

*“Please note it is not uncommon that employers may not claim all eligible periods of Defence service. If you have a record of having released your Reservist on military leave or LWOP (or another form of leave which is not accrued) to render Defence service for any continuous period of five days or more (please note, this may include weekends and public holidays), please advise of the dates, and whether you would like to claim ESP for any or all relevant periods.”*

This wording should offer some guidance to employers, while safeguarding the privacy of the dates on which the Reservist rendered Defence service. Alternatively, express consent can be given by the Reservist under IPP 11.1(b) to discuss the member’s service dates with their employer.

Such situations should be handled in the same way that disclosure of information to an appropriate agent is handled – if in doubt, written consent should be requested prior to the disclosure. If written consent has been provided to release the Reservist’s service details, exact dates of possible ESP entitlement can be discussed with the employer.

A standard authorisation form for use in these circumstances is at Annex C.

### **Further queries**

If delegates or clerks have any queries about this topic (or about any aspect of the ESP Scheme), they are encouraged to ring the ESP Help Line on 1800 001 696.

*Doug Stedman*

**M.D. STEDMAN**

Director ESP Scheme

**22 October 2007**

### **Annexes:**

- A. Information Privacy Principles
- B. Reservist’s Consent Form
- C. Employer’s Consent Form

## **Division 2—Information Privacy Principles**

### **Section 14 Information Privacy Principles**

The Information Privacy Principles are as follows:

## **Information Privacy Principles**

### **Principle 1**

#### **Manner and purpose of collection of personal information**

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:
  - (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
  - (b) the collection of the information is necessary for or directly related to that purpose.
2. Personal information shall not be collected by a collector by unlawful or unfair means.

### **Principle 2**

#### **Solicitation of personal information from individual concerned**

Where:

- (a) a collector collects personal information for inclusion in a record or in a generally available publication; and
- (b) the information is solicited by the collector from the individual concerned; the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:
  - (c) the purpose for which the information is being collected;
  - (d) if the collection of the information is authorised or required by or under law—the fact that the collection of the information is so authorised or required; and
  - (e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

### **Principle 3**

#### **Solicitation of personal information generally**

Where:

- (a) a collector collects personal information for inclusion in a record or in a generally available publication; and
- (b) the information is solicited by the collector;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

- (c) the information collected is relevant to that purpose and is up to date and complete; and
- (d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

## **Principle 4**

### **Storage and security of personal information**

A record-keeper who has possession or control of a record that contains personal information shall ensure:

- (a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and
- (b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

## **Principle 5**

### **Information relating to records kept by record-keeper**

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:
  - (a) whether the record-keeper has possession or control of any records that contain personal information; and
  - (b) if the record-keeper has possession or control of a record that contains such information:
    - (i) the nature of that information;
    - (ii) the main purposes for which that information is used; and
    - (iii) the steps that the person should take if the person wishes to obtain access to the record.
2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.
3. A record-keeper shall maintain a record setting out:
  - (a) the nature of the records of personal information kept by or on behalf of the record-keeper;
  - (b) the purpose for which each type of record is kept;
  - (c) the classes of individuals about whom records are kept;
  - (d) the period for which each type of record is kept;
  - (e) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and
  - (f) the steps that should be taken by persons wishing to obtain access to that information.

4. A record-keeper shall:
  - (a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and
  - (b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

## **Principle 6**

### **Access to records containing personal information**

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

## **Principle 7**

### **Alteration of records containing personal information**

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:
  - (a) is accurate; and
  - (b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.
2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.
3. Where:
  - (a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and
  - (b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

## **Principle 8**

### **Record-keeper to check accuracy etc. of personal information before use**

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

## **Principle 9**

### **Personal information to be used only for relevant purposes**

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

## **Principle 10**

### **Limits on use of personal information**

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:
  - (a) the individual concerned has consented to use of the information for that other purpose;
  - (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
  - (c) use of the information for that other purpose is required or authorised by or under law;
  - (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
  - (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.
2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

## **Principle 11**

### **Limits on disclosure of personal information**

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:
  - (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;
  - (b) the individual concerned has consented to the disclosure;
  - (c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;
  - (d) the disclosure is required or authorised by or under law; or
  - (e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.
2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the

protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

### **Section 15 Application of Information Privacy Principles**

- (1) Information Privacy Principles 1, 2, 3, 10 and 11 apply only in relation to information collected after the commencement of this Act.
- (2) Information Privacy Principles 4 to 9, inclusive, apply in relation to information contained in a record in the possession or under the control of an agency, whether the information was collected before, or is collected after, the commencement of this Act.

### **Section 16 Agencies to comply with Information Privacy Principles**

An agency shall not do an act, or engage in a practice, that breaches an Information Privacy Principle.

Employer's Name \_\_\_\_\_

(Postal Address) \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

ESP Delegate \_\_\_\_\_

(Postal Address) \_\_\_\_\_

\_\_\_\_\_

I, \_\_\_\_\_ (Employer's Name)

of \_\_\_\_\_ (Business Name),

give my consent to the Department of Defence to provide information on my claim under the

ESP Scheme to \_\_\_\_\_ (Agent's Name),

of \_\_\_\_\_ (Agent's Address),

for the purposes of administering the claim under the ESP Scheme submitted for Defence

service rendered by \_\_\_\_\_ (First Reservist's Name)

(Reservist's PMKeyS number [if known]) \_\_\_\_\_,

between \_\_\_\_\_ (First Claimed Date)

and \_\_\_\_\_ (Last Claimed Date).

(Delete the following fields if not required)

\_\_\_\_\_ (Second Reservist's Name)

(Reservist's PMKeyS number [if known]) \_\_\_\_\_,

between \_\_\_\_\_ (First Claimed Date)

and \_\_\_\_\_ (Last Claimed Date).

(If additional space for further Reservists is required, please attach extra page[s] as necessary)

Signed \_\_\_\_\_

Name \_\_\_\_\_

Date \_\_\_\_\_

Reservist's Name \_\_\_\_\_

(Postal Address) \_\_\_\_\_

\_\_\_\_\_

ESP Delegate

(Postal Address) \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

I, \_\_\_\_\_ (Reservist's Name)

\_\_\_\_\_ (Reservist's PMKeyS number),

of \_\_\_\_\_ (Reservist's Address),

give my permission for the Department of Defence to disclose details of my Reserve service to my employer:

\_\_\_\_\_ (Employer's Name),

of \_\_\_\_\_ (Business Name),

Please tick one of the following to indicate how long you want this arrangement to last

during Financial Year(s) \_\_\_\_\_; or

between \_\_\_\_\_ (Start Date)

and \_\_\_\_\_ (End Date); or

indefinitely.

These details could include the dates that I rendered Defence service, the type of service and any other information that is considered necessary to disclose to my employer for the purposes of administering my employer's claim under the Employer Support Payment Scheme.

Signed \_\_\_\_\_

Name \_\_\_\_\_

Date \_\_\_\_\_

Original to ESP Delegate