

the intended uses to be made of it, except when doing so would result in the collection of inaccurate or misleading information. Employees must also be told whether the information is required by law, and, if not, that giving it is purely voluntary.

- ***Controls that conform to legal requirements must be in place to regulate the use and disclosure of employee information. Uses beyond the original purposes for which information was collected and disclosures to third parties, in particular, are circumscribed.***

Without the consent of the employee to whom it relates, personal information shall only be used for a purpose for which it was collected, or for a purpose consistent with the original purpose, or for a purpose permitted under the disclosure part of the *Privacy Act*, subsection 8(2).

Personal information shall not, without the consent of the employee, be disclosed to third parties except in the limited number of situations set out in subsection 8(2) of the *Privacy Act*. Some of these situations include the requirements of other *Acts* and Regulations, compliance with a subpoena or warrant, internal audits, and archival purposes. In many instances these provisions are permissive and the onus is on personnel administrators to determine that a particular instance of permissible disclosure of personal information is fair to the employee concerned.

Certain very sensitive personal information, such as Employee Assistance Program (EAP) data, medical files and conflict of interest declarations, should be disclosed to persons other than the official responsible (e.g. EAP Counsellor) only when compelled to do so by law or regulation that requires its disclosure.

Uses of personal information that are not listed in the personal bank descriptions in the *Personal Information Index* shall be recorded, and the record attached to the personal information. The Privacy Commissioner must be advised, and the new use must subsequently be published in the *Personal Information Index*.

Data matching and linkage involve comparing for administrative purposes personal information obtained from various sources. They are used widely in personnel administration, and generally involve the use of computers to generate more extensive profiles of individuals. Data matching is regulated by Treasury Board policy to ensure compliance with the *Privacy Act*, particularly as it relates to the *Act's* provisions dealing with the collection, use and disclosure of the personal information to be matched. Government institutions are required to give 60 days' advance notice of matching programs to the Privacy Commissioner and to describe them in the *Personal Information Index*.

- ***Government institutions should ensure that personal information is accurate and that appropriate precautions are taken to protect it.***

Personal information has a life cycle; that is, it exists from the time it is originally collected or compiled to the date it is finally disposed of. Throughout its life cycle, personal information should be current and accurate for its intended use. Adequate safeguards and protection should be provided to prevent its misuse.