

§ 806b.37

The recycling sales contract must contain a clause requiring the contractor to safeguard privacy material until its destruction and to pulp, macerate, shred, or otherwise completely destroy the records. Originators must safeguard Privacy Act material until it is transferred to the recycling contractor. A Federal employee or, if authorized, a contractor employee must witness the destruction. This transfer does not require a disclosure accounting.

Subpart K—Privacy Act Exemptions

§ 806b.37 Exemption types.

There are two types of exemptions permitted by 5 U.S.C. 552a:

(a) A *General exemption* authorizes the exemption of a system of records from most parts of the Privacy Act.

(b) A *Specific exemption* authorizes the exemption of a system of records from only a few parts.

§ 806b.38 Authorizing exemptions.

Denial authorities may withhold records using Privacy Act exemptions only when an exemption for the system of records has been published in the FEDERAL REGISTER as a final rule. Appendix D lists the systems of records that have published exemptions with rationale.

§ 806b.39 Requesting an exemption.

A system manager who believes that a system needs an exemption from some or all of the requirements of the Privacy Act will send a request to Air Force Chief Information Officer/P through the Major Command or Field Operating Agency Privacy Act Officer. The request will detail the reasons for the exemption, the section of the Act that allows the exemption, and the specific subsections of the Privacy Act from which the system is to be exempted, with justification for each subsection.

§ 806b.40 Exemptions.

Exemptions permissible under 5 U.S.C. 552a (subject to §806b.38 of this part):

(a) *The (j)(2) exemption*. Applies to investigative records created and main-

32 CFR Ch. VII (7–1–05 Edition)

tained by law-enforcement activities whose principal function is criminal law enforcement.

(b) *The (k)(1) exemption*. Applies to information specifically authorized to be classified under the DoD Information Security Program Regulation, 32 CFR part 159.

(c) *The (k)(2) exemption*. Applies to investigatory information compiled for law-enforcement purposes by nonlaw enforcement activities and which is not within the scope of Sec. 806b.40(a) of this part. However, the Air Force must allow an individual access to any record that is used to deny rights, privileges or benefits to which he or she would otherwise be entitled by Federal law or for which he or she would otherwise be eligible as a result of the maintenance of the information (unless doing so would reveal a confidential source).

(d) *The (k)(3) exemption*. Applies to records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C. 3506.

(e) *The (k)(4) exemption*. Applies to records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8.

(f) *The (k)(5) exemption*. Applies to investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information, but only to the extent such material would reveal the identity of a confidential source. This provision allows protection of confidential sources used in background investigations, employment inquiries, and similar inquiries that are for personnel screening to determine suitability, eligibility, or qualifications.

(g) *The (k)(6) exemption*. Applies to testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal or military service, if the disclosure would compromise the objectivity or fairness of the test or examination process.

(h) *The (k)(7) exemption.* Applies to evaluation material used to determine potential for promotion in the Military Services, but only to the extent that the disclosure of such material would reveal the identity of a confidential source.

Subpart L—Disclosing Records to Third Parties

§ 806b.41 Disclosure considerations.

The Privacy Act requires the written consent of the subject before releasing personal information to third parties, unless one of the 12 exceptions of the Privacy Act applies (see § 806b.47). Use this checklist before releasing personal information to third parties: Make sure it is authorized under the Privacy Act; consider the consequences; and check the accuracy of the information. You can release personal information to third parties when the subject agrees in writing. Air Force members consent to releasing their home telephone number and address when they sign and check the “Do Consent” block on the AF Form 624, Base/Unit Locator and Postal Service Center Directory⁷(see Air Force Instruction 33-329, *Base and Unit Personnel Locators*⁸).

§ 806b.42 Social rosters.

Before including personal information such as spouses names, home addresses, home phones, and similar information on social rosters or directories that are shared with groups of individuals, ask for signed consent statements. Otherwise, do not include the information. Consent statements must give the individual a choice to consent or not consent, and clearly tell the individual what information is being solicited, the purpose, to whom you plan to disclose the information, and that consent is voluntary. Maintain the signed statements until no longer needed.

⁷ <http://www.e-publishing.af.mil/formfiles/af/af624/af624.xfd>

⁸ <http://www.e-publishing.af.mil/pubfiles/af/33/afi33-329/afi33-329.pdf>.

§ 806b.43 Placing personal information on shared drives.

Personal information should never be placed on shared drives for access by groups of individuals unless each person has an official need to know the information to perform their job. Add appropriate access controls to ensure access by only authorized individuals. Recall rosters are FOUO because they contain personal information and should be shared with small groups at the lowest levels for official purposes to reduce the number of people with access to such personal information. Commanders and supervisors should give consideration to those individuals with unlisted phone numbers, who do not want their number included on the office recall roster. In those instances, disclosure to the Commander or immediate supervisor, or deputy, should normally be sufficient.

§ 806b.44 Personal information that requires protection.

Following are some examples of information that is not releasable without the written consent of the subject. This list is not all-inclusive.

- (a) Marital status (single, divorced, widowed, separated).
- (b) Number, name, and sex of dependents.
- (c) Civilian educational degrees and major areas of study (unless the request for the information relates to the professional qualifications for Federal employment).
- (d) School and year of graduation.
- (e) Home of record.
- (f) Home address and phone.
- (g) Age and date of birth (year).
- (h) Present or future assignments for overseas or for routinely deployable or sensitive units.
- (i) Office and unit address and duty phone for overseas or for routinely deployable or sensitive units.
- (j) Race/ethnic origin.
- (k) Educational level (unless the request for the information relates to the professional qualifications for Federal employment).
- (l) Social Security Number.

§ 806b.45 Releasable information.

Following are examples of information normally releasable to the public