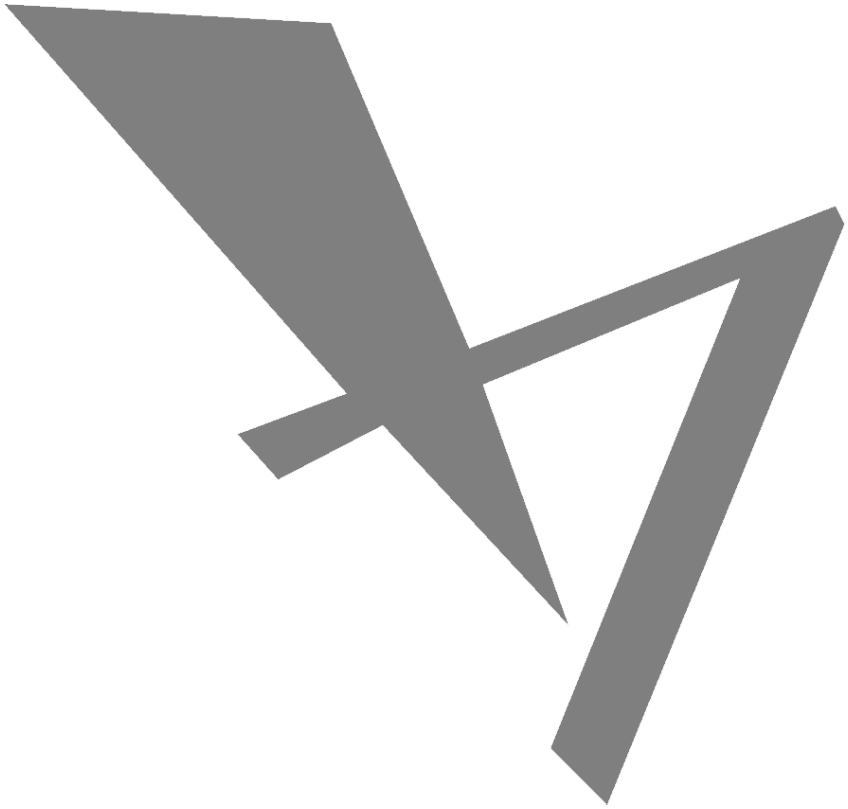
AESBUS PRIVACY CENTER

PRIVACY NOTICE

Overview of Privacy Act of 1974: Collection, Disclosure & Access Denial of Personally Identifiable Information (PII)

JANUARY, 2023



PRIVACY NOTICE — OVERVIEW OF PRIVACY ACT OF 1974: COLLECTION, DISCLOSURE & ACCESS DENIAL OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Aesbus (the "Company") has an excellent reputation for conducting business in an ethical and responsible manner. We have worked hard to develop this reputation and are committed to maintaining it by conducting our business activities honestly and in full compliance with the privacy regulations, laws, and business practices applicable to each location where we do business.

As key company stakeholders and employees, we should be aware of our stance on privacy issues, so that we can act accordingly. The **Overview of Privacy Act of 1974: Collection, Disclosure & Access Denial of Personally Identifiable Information (PII)** incorporates Aesbus' guidelines regarding privacy and data security within our company and with our clients, customers, suppliers and governmental entities. It is our intention that these policies, standards and rules guide our common values and culture and equally important, our actions and behavior in all business environments and circumstances.

All Aesbus employees that receive a copy of the **Overview of Privacy Act of 1974: Collection, Disclosure & Access Denial of Personally Identifiable Information (PII)** are expected to comply with its directives. You are encouraged to consult with your manager, or as appropriate, senior management of the Company prior to taking any action whenever the proper course of conduct with regard to privacy or data security is in doubt. Any failure to adhere to this Privacy Notice may result in disciplinary action, up to and including termination of employment. All employees in receipt of this Privacy Notice are expected to report violations of this Privacy Notice to any member of Aesbus management. Failure to report any violations, or to cooperate in the investigation of any alleged violation is, in itself, a violation of this Privacy Notice.

Please report privacy and Privacy Notice violations to Coni Fox, VP of Human Resources, coni.fox@aesbus.com or Earl Castor, President, earl.castor@aesbus.com.

Enactment of Privacy Act of 1974

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, (the Privacy Act) is a public sector law that regulates the use of Personally Identifiable Information (PII) by the United States Government. Specifically, it establishes rules, similar to the Fair Information Practice Principles that determine what information may be collected and how it may be used in order to protect the personal privacy of U.S. citizens.

U.S. federal agencies maintain vast amounts of PII data, and they use that data to make decisions about all of us that affect our lives in major ways. The Privacy Act applies to federal agencies like the Internal Revenue Service, the Department of Health and Human Services, the Social Security Administration, the Department of Homeland Security, federal law enforcement agencies, and more.

The U.S. Congress enacted the Privacy Act to protect individuals against invasions of personal privacy by requiring federal agencies maintaining PII data to ensure the accuracy of such information and to prevent its misuse.

The Privacy Act limits the creation of government secret data files on individuals and strictly controls the dissemination of PII maintained by federal agencies. The Government informs the public about record systems covered by the Privacy Act by publishing notices in the Federal Register. The record systems are referred to as Privacy Act systems of records and the notices provide a description of particular systems of records.

Scope

The Privacy Act is a public sector law which lays down a code of fair information practice that regulates the collection, maintenance and dissemination of PII about individuals that is maintained in records systems by U.S. federal agencies.

The Privacy Act applies only to U.S. citizens and immigrants who are lawfully admitted for permanent residence in the United States.
It applies only to personal information maintained by U.S. federal agencies, or by private companies on behalf of U.S federal agencies.

The Privacy Act does NOT apply to PII data collected about persons outside the United States, nor does it protect the privacy of an individual’s records that are maintained by the private sector, such as credit report, bank account and medical records or even local or state government records such as driver’s license information.

As with the U.S. Freedom of Information Act, federal agencies can withhold certain PII "exempted" under the Privacy Act. Examples include information concerning national security or criminal investigations.

Privacy Act Definitions, Roles & Systems

The **Overview of Privacy Act of 1974: Collection, Disclosure & Access Denial of Personally Identifiable Information (PII)** contains the guidelines and procedures put in place by Aesbus (the "Company") to protect the personal information of individuals on whom Aesbus maintains systems of records that are subject to the Privacy Act. This Privacy Notice applies only to Aesbus systems of records that are subject to the Privacy Act and from which information is retrieved by name or a personal identifier, such as the Social Security Number (SSN).

The Privacy Notice provides information on how individuals can obtain, correct, and control the dissemination of their personal information. The Policy is designed as a source of information and guidance for:

- Individuals who are the subjects of records
- Managers and supervisors who use the records
- System managers who manage Privacy Act systems and the information in the systems
- Vendors and contractors who provide support services for systems containing personal information
- Management officials who have responsibilities for carrying out functions under the Privacy Act

Definitions of Privacy Act Terms

The Privacy Act establishes controls over what PII data is collected, maintained, used and disseminated by U.S. federal government agencies, or private companies on behalf of such agencies.

The terms in this section are defined to ensure consistency and common understanding when used in a Privacy Act context:

Individual means a citizen of the United States or a legal resident alien on whom Aesbus maintains records that are subject to the Privacy Act.

Record means any item, collection, or grouping of information about an individual which contains the individual's name or other **Personal Identifier** such as number or symbol, fingerprint, voiceprint, or photograph. The information may relate to education, financial transactions, medical conditions, employment, or criminal history collected in connection with an individual's interaction with Aesbus.

System of records means a group of records under Aesbus' control from which information is retrieved by the name of an individual, or by any number, symbol, or other identifier assigned to that individual.

Routine use means disclosure of a record for the purpose for which it is intended.

Request for access means a request by an individual to obtain or review his or her record or the information in the record.

Disclosure of information means providing a record or the information in a record to someone other than the individual of record.

Exempt record means a record that may not be obtained by an individual because they are exempted under the Privacy Act.

Solicitation means a request by an individual for an individual's personal information to be included in a system of records for a specified purpose.

Program/system manager means the Aesbus manager who is responsible for a system of records and the information in it.

Information Technology (IT) system (also known as electronic information system) means the equipment and software used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Personally identifiable information (personal information in identifiable form) means data within an IT system or online collection that permits the identity of an individual to whom the information applies to be reasonably inferred; information that identifies the individual by name or other unique identifier or by which an individual is identified in conjunction with other data elements such as gender, race, birth date, geographic indicator, and similar personal information. Information permitting the physical or online contacting of a specific individual is considered information in identifiable form.

Privacy Impact Assessment (PIA) means the process for evaluating privacy issues in an electronic information system, including examining the risks and effects of collecting, maintaining, and disseminating information in identifiable form, and identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information. The process consists of gathering data on privacy issues from a project, identifying and resolving privacy risks, and obtaining approval from agency privacy and security officials. Completion of the PIA process results in the PIA Report.

Privacy Act Roles and Responsibilities

Program Officials: Responsible for ensuring that the systems of records in their program areas meet the requirements of the Privacy Act and security policy and regulations. Responsibilities include:

- Ensuring that the program systems of records are necessary, relevant to the program, and authorized.
- Identifying the need for and proposing the establishment of new or revised systems of records to accomplish program mission or functions.
- Proposing the cancellation of outdated or obsolete systems of records.

- Identifying and proposing for exemption the systems that meet nondisclosure criteria under the Privacy Act.
- Ensuring that all contractors providing program systems of records services follow Privacy Act and security requirements.
- Identifying systems requiring Privacy Impact Assessments (PIAs), coordinating on developing the PIAs, and resolving any privacy issues.

Chief Information Officer (CIO): Responsible for implementing IT security management in the Company, with overall responsibility for the Aesbus IT Security Program and for security policy on electronic privacy data. Responsibilities include:

- Overseeing security policy for privacy data.
- Ensuring review of Privacy Impact Assessments (PIAs) for information security considerations.
- Ensuring that PIAs are part of Aesbus' system development life-cycle guidance for Information Technology.

System Architects, Developers/Designers: Responsible for ensuring that the system design and specifications conform to privacy standards and requirements and that technical controls are in place for safeguarding personal information from unauthorized access. Responsibilities include establishing system protection controls (e.g., access, retrieval, storage, user restrictions).

Legal General Counsel: Responsible for providing legal advice and assistance on Privacy Act matters and Aesbus systems of records. Responsibilities include:

- Assisting program and system managers to determine the applicable statute or regulation for a new or revised system of records.
- Reviewing the Privacy Act notice for applicable legal citations, routine uses, and other legal aspects of establishing or revising the system.
- Approving each notice for publication.
- Advising management on appropriate actions involving Aesbus systems of records, including release of information, appropriate use of information, and appeals.
- Providing legal opinions on all Privacy Act issues as needed.

Supervisors and Employees: Responsible for ensuring that the personal information they use in carrying out their official duties is protected according to Privacy Act and security requirements.

Clients/Vendors/Suppliers/Contractors: Aesbus clients, vendors, suppliers, and contractors performing work directly in relation to the Privacy Act are subject to the same laws and regulations and are therefore responsible for ensuring the privacy and security of systems they design, develop, maintain, operate, or use and for system data. They are accountable for any violation that may occur due to oversight or negligence and may be subject to civil or criminal penalties under the Privacy Act.

Disclosure of Information in a Privacy Act System of Records

No Personally Identifiable Information (PII) stored in a Privacy Act system of records may be disclosed to anyone other than the individual of record without the written consent of that individual, except when specifically allowed under the Privacy Act.

Disclosures that are allowed under the Privacy Act include:

- To Aesbus management and employees in the performance of their official duties.
- Under the Freedom of Information Act, where applicable.
- For routine uses cited in the system of records Federal Register notice to the Bureau of the Census for statistical purposes and only if the record is unidentifiable by individual.
- To the National Archives and Records Administration (NARA) when the record warrants permanent retention because of historical or other national value as determined by NARA to law enforcement agencies in civil or criminal cases.
- In emergencies affecting an individual's health or safety.
- Under a court order.
- To a consumer reporting agency if specifically authorized by law.

Accounting of Disclosures

The program/system manager must keep a record of any disclosure of PII from a Privacy Act covered system for five years or for the life of the record, whichever is longer, except when no accounting of disclosure is needed as noted below.

Note: No accounting of disclosures is needed when the disclosure is:

- To Aesbus management or employees in the performance of their official duties.
- Required under the Freedom of Information Act (FOIA).
- Required for law enforcement purposes.

Collection and Use of PII

PII must be collected directly from the individual of record whenever possible, and used only for the purpose for which it is intended. If the information needs to come from a third-party, the individual's written permission is required.

Accuracy of PII

Personally Identifiable Information (PII) provided by individuals must be accurate and complete. Program/system managers must ensure that the information in the system is relevant, necessary, and timely.

Standards of Conduct on PII

Aesbus employees have a duty to protect the security of PII stored in a Privacy Act system of records by:

- Ensuring the accuracy, relevance, timeliness, and completeness of records.
- Avoiding any unauthorized disclosure, verbal or written, of records.
- Not collecting PI data unless authorized.
- Collecting only the PI data needed to perform an authorized function.
- Collecting PI data directly from the individual whenever possible.
- Maintaining and using records with care to prevent any inadvertent disclosure of PI data.

Protection of PII

Program/system managers must establish physical, administrative, and technical safeguards for PII stored in a Privacy Act system of records. The safeguards must ensure the security and confidentiality of records, protect against possible threats or hazards, and permit access only to authorized persons.

Paper records will be placed in secured locations. Electronic systems will use passwords, identity verification, detection of break-in attempts, firewalls, encryption, and/or other security measures determined to be appropriate by the responsible system and program managers.

Access and Release of Privacy Act Records

Requests for Personally Identifiable Information (PII) stored in a Privacy Act system of records must be submitted in writing to Aesbus at Aesbus.privacy@aesbus.com.

Specifically, requests must include the following details in the email:

- That it is a “Privacy Act Request”
- Requester’s full name and address
- A description of the records requested
- A brief description of the nature, time, and place of the Requester’s association with Aesbus and any other information that may facilitate locating the requested records

Denial of Access to Privacy Act Records

Access to PII stored in a Privacy Act system of records will be denied in those instances that Aesbus has specifically exempted pursuant to the Privacy Act.

Aesbus legal counsel will advise on appropriate actions involving access and release of information or denial of information.