



AVUE DIGITAL SERVICES

ENSURING DATA SECURITY AND PRIVACY

Federal agencies, federal employees, and the public are rightly concerned about the privacy of personal data. Avue shares that concern. Accordingly, Avue is committed to ensuring that Avue Digital Services (ADS) remains a secure system, and to doing Avue's part in enabling ADS subscriber agencies to meet their obligations under the Privacy Act and all laws relating to federal data. This white paper provides information on ADS security measures, who accesses data using ADS, and how privacy laws relate to ADS. These are the highlights:

- Agency use of ADS is fully compatible with the Privacy Act and other laws.
- ADS employs stringent physical, electronic, and personnel security measures to keep the risk of security breach exceedingly low.
- When ADS is used, personally identifiable data is accessed only by persons who provide it and by properly authorized Avue personnel and government officials.

ADS SECURITY FEATURES

What are the basic security requirements for Federal Government automated information resources? OMB Circular A-130, *Management of Federal Information Resources*, requires agencies to implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. The security provided must be at least commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

What security features are incorporated in ADS? ADS includes a dynamic system of security features made up of multiple layers to protect the integrity and confidentiality of ADS data and data transmissions. ADS Data Centers include state-of-the-art security management and firewall technology to provide ADS protection on a 24 x 7 basis. All data transmitted to and from an ADS Data Center are protected by Secure Sockets Layer (SSL) v3 128-bit encryption. Additional security, such as an encrypted Virtual Private Network (VPN) tunnel can be provided at the subscribing agency's election. ADS is secured by 24 x 7 intrusion detection monitoring, which provides response to numerous threats, and monthly incident reporting. ADS enforces restricted access to ADS based on user IDs, passwords, and permissions created and maintained by Avue in cooperation with the subscriber agency. ADS Data Centers physical security are maintained by video surveillance cameras, security breach alarms, motion-detection equipment and 24-hour personnel. ADS Data Center access is provided via a key-card system with mandatory pre-approved access lists and mandatory sign in/sign out procedures.

Should agencies be concerned about their control over electronic documents? Control issues will always exist regardless of whether paper-based or electronic-based processes are used. For example, with paper-based processes someone could leave a hard copy of a disciplinary document on a printer or copying machine, or in a trash bin, or fax or send a hard copy to the wrong addressee—all of which may result in a sensitive document falling into the wrong hands. Many control features have been embedded in ADS to mitigate risks of unauthorized access to documents. For example, only those persons with a valid password are authorized to view Workforce Management documents. System Administrators, designated by the agency, define relationships between users (e.g., an HR professional as an advisor to a specific

manager) so that one user can view another's ADS files and documents. In this way, ADS electronic documents are far more secure than paper documents.

If an ADS user deletes a file created in ADS, can the deleted file be “found” by a computer expert? All files created through ADS are stored in an ADS Data Center and not on a user's local disk. When a user file is deleted, that file is totally removed from the ADS database and cannot be recovered from the database. User files are, however, backed up on a regular basis in case of accidental deletion or catastrophic damage to the Data Center. A particular file may be restored from a backup tape at the agency's request, unless the pertinent tapes have been overwritten. Backup tapes are overwritten on a regular basis as they are cycled through the backup schedule. The ADS Data Center backup schedule is included in the ADS Master Services Agreement.

PRIVACY ISSUES

Who accesses what data using ADS?

The public: The public can only access public-domain information, such as job postings and position descriptions, not information about any individuals.

Job applicants (including those who are current federal employees): In addition to viewing public data, applicants can voluntarily submit, view, and edit information **about themselves** that they provide for application purposes.

Government officials whom the agency has designated as having a need to know consistent with the Privacy Act: The subscriber agency, not Avue, determines which agency officials will have access to what data, and Avue scrupulously maintains password-protected user access privileges to implement those decisions. The access privileges enable the agency to associate specific domains of information with specific user groups, so that giving access to certain information does not

require access to be given to other data that the individual does not need in order to do his or her job. Thus, for example, agency managers evaluating candidates for a position would be able to view application data only for that position. As another example, for subscribers using the Performance Optimization Module (POM), only those officials authorized to view performance evaluations would be given access to such data in ADS.

Avue personnel: Avue personnel build and continually enhance ADS, particularly the ADS software and databases. These databases contain data and a logical structure developed by Avue, as well as public domain data; and, depending upon the ADS module involved, may include information on individuals. Avue personnel generally do not participate in any functions involving data on individuals and do not have access to such data. Where ADS involves functions using data on individuals (for example, individual performance reviews), access to such data is limited to a very small number of Avue personnel that have appropriate security clearances. In addition, all Avue personnel are bound by strict confidentiality obligations rigorously enforced by Avue.

Who determines who has access to individually identifiable information?

Agencies control who accesses such information supplied by the applicant or employee, as well as any individually-identifiable data that the agency itself supplies in conjunction with ADS. Therefore, ***an agency's use of ADS does not entail any broader access to private information than what would occur without ADS.*** Indeed, ADS has tremendous security advantages over traditional, paper-based, non-automated agency methods, since users have to identify themselves to gain access and there is an electronic audit trail of who accessed what, and when they did it.

What is the Privacy Act? The Privacy Act can be described as a “code of fair information practices” that regulates the collection, maintenance, use, and dissemination of personal information by federal government agencies. Not all federal files are subject to the

Privacy Act—the Act applies only to “systems of records” under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Whether a system is a system of records depends on whether there is an indexing or retrieval capability using identifying particulars that is built into the system and the agency does, in fact, retrieve records about individuals by reference to some personal identifier. If the Privacy Act applies, the personal information may not be disclosed except for “routine uses” specified in a public government notice concerning the system of records. In addition, individuals may request access to their own information, and information may be disclosed with the individual's consent. The Privacy Act also requires agencies to account for disclosures of covered records.

Is applicant data in the Personnel Management and Recruitment System (PMRS) Module part of a “system of records”?

In ADS this data is not accessed by name or personal identifier and so would not meet the definition of “system of records.” However, when downloaded by the agency such data may be incorporated in an agency system of records which the government has designated OPM/GOVT-5, *Recruiting, Examining, and Placement Records*.

Does ADS contain any information that is part of a “system of records”?

Yes. For example, an agency that subscribes to the Performance Optimization Module (POM) will place employee performance data into POM. Employee performance data are included in a government-wide system of records defined by OPM in a Federal Register Notice. This system of records is called OPM/GOVT-2, *Employee Performance File System Records*. Although the notice is government-wide, the system is maintained by each agency with respect to its own employees. Other OPM government-wide systems of records cover most, if not all, personnel-related information.

What safeguards and tools does ADS have to facilitate Privacy Act compliance? These fall

into two categories: security, and the individual's right to inspect and correct or supplement information on himself. As described in greater detail under the section above entitled “ADS Security Features,” ADS has sophisticated electronic and physical measures and policies in place to minimize the risk that any person would gain access to information in violation of privacy rights. ADS also facilitates the individual's exercise of rights under the Privacy Act in several ways.

Individual access – in POM, an employee has an easy means of reviewing his own personnel file. In PMRS, a job applicant controls and can view and edit his own application information. If the agency receives a verbal or written request by an employee for material in his personnel file, the agency can rapidly use POM to retrieve and print relevant data to respond to the request.

Notification of records relating to the individual – In some cases, the Privacy Act or federal employment law requires a notification to the employee, such as, for example, when a performance plan or adverse action is proposed. POM automatically generates such a notice. Agencies that do not use ADS run the risk of losing in employment litigation simply through inadvertent failures to issue written notices at the right time.

Documentation that required steps have been taken – For example, POM will document the fact that an employee has seen and had an opportunity to comment on a performance plan or adverse action.

Individual's right to correct or supplement the record – POM provides a ready means for the individual to respond to adverse or inaccurate information, as required by the Privacy Act. Such responses also become immediately available to those with a need to know. The system can even automatically notify appropriate persons when a file has been updated.

Is it permitted for a system such as ADS to process or store information which is also contained in an agency system of records?

Yes. In accordance with the Privacy Act, the OPM notices of system records relating to personnel explicitly authorize the disclosure of such information to contractors as needed. But as explained above, although there may technically be a “disclosure” to Avue, personal information is rarely seen by Avue personnel, and then only under tightly controlled circumstances.

Should an agency ADS recruitment web site contain a Privacy Act notice?

The types of information submitted by applicants through ADS are similar to those formerly submitted on paper. According to OMB’s guidance, when electronic forms supplement or replace traditional paper collections of information that form a system of records subject to the Privacy Act, the rules of the Privacy Act continue to apply. Where the Privacy Act applies in the paper-based world, the general principle is that the Act also applies in the parallel online world. **Each agency must determine for itself if its use of information gathered through ADS is subject to the Privacy Act.** For example, if an agency decides to treat the collection of applicant information as a collection of information under the Privacy Act because such information will be stored in an agency system of records, a Privacy Act notice containing the following information should be posted on the recruitment website: (1) the authority which authorizes the collection of information and whether disclosure of such information is mandatory or voluntary; (2) the principal purpose or purposes for which the information is intended to be used; (3) the routine uses that may be made of the information; and (4) the effects on the individual, if any, of not providing all or any part of the requested information. There also is a requirement for the agency to track disclosures of information contained in a system of records.

Is applicant data in the Personnel Management and Recruitment System (PMRS) Module part of a “system of records”? In ADS this data is not accessed by

name or personal identifier and so would not meet the definition of “system of records.” However, when downloaded by the agency such data may be incorporated in an agency system of records which the government has designated OPM/GOVT-5, *Recruiting, Examining, and Placement Records*.

Does ADS contain any information that is part of a “system of records”?

Yes. For example, an agency that subscribes to the Performance Optimization Module (POM) will place employee performance data into POM. Employee performance data are included in a government-wide system of records defined by OPM in a Federal Register Notice. This system of records is called OPM/GOVT-2, *Employee Performance File System Records*. Although the notice is government-wide, the system is maintained by each agency with respect to its own employees. Other OPM government-wide systems of records cover most, if not all, personnel-related information.

What safeguards and tools does ADS have to facilitate Privacy Act compliance?

These fall into two categories: security, and the individual’s right to inspect and correct or supplement information on himself. As described in greater detail under the section above entitled “ADS Security Features,” ADS has sophisticated electronic and physical measures and policies in place to minimize the risk that any person would gain access to information in violation of privacy rights. ADS also facilitates the individual’s exercise of rights under the Privacy Act in several ways.

Individual access – in POM, an employee has an easy means of reviewing his own personnel file. In PMRS, a job applicant controls and can view and edit his own application information. If the agency receives a verbal or written request by an employee for material in his personnel file, the agency can rapidly use POM to retrieve and print relevant data to respond to the request.

Notification of records relating to the individual – In some cases, the Privacy Act

or federal employment law requires a notification to the employee, such as, for example, when a performance plan or adverse action is proposed. POM automatically generates such a notice. Agencies that do not use ADS run the risk of losing in employment litigation simply through inadvertent failures to issue written notices at the right time.

Documentation that required steps have been taken – For example, POM will document the fact that an employee has seen and had an opportunity to comment on a performance plan or adverse action.

Individual’s right to correct or supplement the record – POM provides a ready means for the individual to respond to adverse or inaccurate information, as required by the Privacy Act. Such responses also become immediately available to those with a need to know. The system can even automatically notify appropriate persons when a file has been updated.

ELECTRONIC GOVERNMENT

Is use of ADS consistent with Government management policy? ADS users are at the forefront in implementing the President’s Management Agenda objective of improving effectiveness and cutting costs through e-government. Congress has mandated that Federal agencies move expeditiously to adopt electronic processes. Under the Government Paperwork Elimination Act (GPEA), Federal agencies are required by October 21, 2003 to provide the public with “the option of electronic maintenance, submission, or disclosure of information, when practicable, as a substitute for paper.” GPEA recognizes that paper-based systems have significant limitations: storage of paper documents consumes vast amounts of space; single documents may easily be lost or become irretrievable; transportation of paper is time consuming; access is limited to those having physical possession of the document or a copy; extracting information from multiple paper sources is difficult and time-consuming; and

search capabilities are often very limited. As stated in recent General Accounting Office testimony provided to Congress:

"With the speed and ease of massive interconnectivity offered by the Internet, improvements in operational efficiencies, lower costs, and improved customer service delivery truly can be dramatic." GAO testimony on "Electronic Government" dated May 22, 2000.

ADS addresses these objectives by providing a dynamic, automated solution with embedded logic that significantly streamlines Federal Government HR management processes.

FREEDOM OF INFORMATION ACT (FOIA)

What is FOIA? Enacted in 1966, FOIA established for the first time an effective statutory right of access to government records. FOIA generally provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from disclosure by one of nine exemptions or by one of three special law enforcement record exclusions. "The basic purpose of [the] FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed."

Which are the FOIA Exemptions that are most relevant to records produced using ADS? Several of the FOIA Exemptions may be relevant to FOIA requests for records that may be produced using ADS.

Exemption 2. Exemption 2 exempts records from disclosure that relate to internal personnel rules and practices. Exemption 2 may be applicable to records such as interview guidelines, rating and ranking criteria, and internal personnel policies.

Exemption 5. Exemption 5 exempts records from disclosure that are inter-agency and intra-agency memoranda or letters that are protected by legal privileges. One of the most common categories of legal privileges is the so-called "deliberative process privilege" that applies to records that are predecisional and "deliberative" (in the sense that they contain recommendations or express opinions on legal or policy matters). Exemption 5 may be applied to disciplinary and other decisional documents that do not represent final decisions.

Exemption 6. Exemption 6 exempts records for which disclosure would clearly constitute an unwarranted invasion of privacy. The determination of whether this exemption applies to a record involves balancing the potential embarrassment or harm to an individual versus the public interest in disclosure of the record. Exemption 6 covers a broader scope of information than the Privacy Act (discussed below) in that Exemption 6 potentially is applicable to any agency record pertaining to personal information regardless of whether such information is retrieved by personal identifier. Exemption 6 has been applied to records such as applications and resumes of unsuccessful job applicants, job performance evaluations, and reasons for termination.

Electronic and paper documents are treated alike under the exemptions.

Are employee disciplinary records or job performance ratings subject to disclosure under FOIA? These types of records containing highly personal information generally may be withheld under FOIA Exemption 6. However, disclosure may be required when there is a strong public interest in the disclosure of information contained in the record. As indicated above, this exemption involves a balancing test regarding the potential embarrassment or harm to an individual versus the public interest in disclosure of the record.

Are electronic resumes that are submitted through the ADS PMRS Module exempt from disclosure under FOIA? In general, information submitted by unsuccessful job

applicants may be withheld under Exemption 6, but certain information submitted by successful job applicants may be released under FOIA. Even for successful candidates, however, the agency might be justified in withholding information such as home addresses, telephone numbers, references, etc. See *Barvick v. Cisneros*, 941 F. Supp. 1015 (D. Kan. 1996). The ultimate determination depends on the application of Exemption 6's balancing test to the specific facts.

Are Internet Protocol (IP) logs maintained at the ADS Data Center exempt from disclosure? We do not consider the IP logs to be "agency records" for purposes of FOIA, since they are not maintained by the agency, although Avue does provide access to the IP logs to agency officials on a "need to know" basis, such as in the event of a hacker attack. Even if the logs were deemed to be "agency records" under FOIA, the logs may be withholdable under Exemption 6, although we are aware of no court opinions addressing this issue. Although IP addresses do not identify a particular individual, they may be used by a private sector organization to send advertisements and other "spam" to the IP addresses, and such information will ultimately reach individuals. In contrast, the public's interest in disclosure appears to be minimal—disclosure of the logs would shed very little, if any, light on Government operations.

MONITORING OF WEBSITE VISITS

Much public interest has focused on the fact that many websites automatically collect data on site visits that is not knowingly supplied by the site visitors.

What are "cookies"? "Cookies" are a web technology that places small bits of software on a web user's hard drive to personalize the web site when the user returns. Guidance issued by OMB distinguishes between two kinds of cookies, so-called "session cookies" and "persistent cookies." Session cookies are used only for a single session or transition and are erased when users close their browsers.

Persistent cookies specify expiration dates, remain stored on the user's computer until the expiration date, and can be used to track users' browsing behavior. Pursuant to OMB instruction on this subject, persistent cookies should not be used unless (1) the web page gives clear and conspicuous notice to users; (2) there is a compelling need to gather the data on the web page; (3) appropriate and publicly disclosed privacy safeguards exist; and (4) your agency head approves their use.

Does Avue use cookies? No, Avue does not use cookies in any ADS module. Avue does use "URL encoding", which is used to create a session space on the ADS servers (not on the web user's hard drive) and monitors use during the web user's session on ADS. The URL encoding is only used during the ADS session.

FOR FURTHER INFORMATION ON ADS PRIVACY AND SECURITY

Contact Gary Frank, Chief Technology Officer at big.guy@avuetech.com.

This white paper contains facts and Avue's views on the application of legal standards. It does not constitute legal advice to any agency, company, or individual and it is not the subject of any warranty.