Office of Government Ethics

Reasonable Accommodation Request Application
Privacy Impact Assessment

July 2023

Compliance Division

U.S. Office of Government Ethics (OGE)
Privacy Impact Assessment (PIA) for the
Reasonable Accommodation Request Application

Name of Project/System: Reasonable Accommodation Request Application (RARA)
Office: Compliance Division

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Jennifer Matis
Privacy Officer & Associate Counsel
Legal, External Affairs and Performance Branch
jmatis@oge.gov
202-482-9214

2) Who is the system owner?

Chip Christopher
Deputy Director
Compliance Division
dachrist@oge.gov
202-482-9224

3) Who is the system manager?

Sidney Williams
HR Attorney-Advisor
Administrative Operations Branch
Compliance Division
SWilliam@oge.gov
202 482-9209

4) Who is the Chief Information Security Officer (CISO) who reviewed this document?

Ty Cooper
Chief Information & Cybersecurity Officer
IT Division
jtcooper@oge.gov
(202) 482-9226

5) Who is the Senior Agency Official for Privacy who reviewed this document?

Diana J. Veilleux
Senior Agency Official for Privacy and
Chief, Legal, External Affairs and Performance Branch
Diana.veilleux@oge.gov
202-482-9203

6) Who is the Reviewing Official?

Ty Cooper
Chief Information & Cybersecurity Officer
IT Division
jtcooper@oge.gov
202-482-9226

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes. This system will include information about any OGE employee who submits a request for a reasonable accommodation based on disability or religion. It may also contain information about potential employees (i.e. applicants), who may also request reasonable accommodations. The information will include information about their work responsibilities, their disability (if seeking a disability accommodation), their religious practices (if seeking a religious accommodation), and any accommodations requested and/or granted.

a. Is this information identifiable to the individual?

Yes.

b. Is the information about individual members of the public?

Potentially, see above.

c. Is the information about employees?

Yes, see above.

2) What is the purpose of the system/application?

The purpose is to collect and maintain information regarding employee reasonable accommodation requests and to track the status of these requests.

3) What legal authority authorizes the purchase or development of this system/application?

The Rehabilitation Act of 1973 (29 U.S.C. § 701 et seq.), as amended by the Americans with Disabilities Act Amendments Act of 2008 (ADAAA), and Title VII of the Civil Rights Act of 1964 (42 U.S.C. §2000e et seq.).

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

OGE employees and potential employees (i.e. applicants). These individuals' records may remain in the application after their employment or potential employment is over.

2) What are the sources of the information in the system?

The source of the information about the employees' disability or religious practices and requested accommodation is provided by the employees' supervisor or manager, based on their discussion regarding the employees' accommodation request. See OGE Revised Reasonable Accommodation Policy, page 6; OGE's Policy on Religious Accommodations, page 2. OGE's Human Resources Attorney-Advisor and/or the Deputy Director may add additional information regarding the granting or denial of the request.

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

See above.

b. What federal agencies provide data for use in the system?

None.

c. What State and local agencies are providing data for use in the system?

None.

d. From what other third party sources will data be collected?

None.

e. What information will be collected from the employee and the public?

- The employee's name, division, title, and official government address/email/phone number

- The employee's personal address/email/phone number
- Medical information regarding the employee's disability
- Information on the employee's religious practices
- Information on accommodations requested and provided
- Documents, such as documentation from medical providers, may be uploaded into the application

Dates of birth and Social Security numbers will not be collected. Supervisors, who will be the individuals entering information into the system, will be directed not to enter such information.

3) Accuracy, Timeliness, Reliability, and Completeness

a. How will data collected from sources other than OGE records be verified for accuracy?

No data is collected from sources other than OGE records. OGE relies on the supervisor or manager entering the request to collect and provide accurate information.

b. How will data be checked for completeness?

The supervisor or manager entering the request is responsible for ensuring the data is complete.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

The information is not intended to be continuously updated, rather it is record documenting a particular request and determination.

d. Are the data elements described in detail and documented?

The data elements contained in the application are not documented but are simple and self-explanatory.

D. ATTRIBUTES OF THE DATA:

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No. The information collected by the application was previously maintained by individual supervisors.

3) Will the new data be placed in the individual's record?

The application maintains individual records for each employee or potential employee who requests an accommodation. However, these records are not linked to any other records on that individual.

4) Can the system make determinations about employees/the public that would not be possible without the new data?

No.

5) How will the new data be verified for relevance and accuracy?

OGE will rely on the employees' supervisor or manager to collect and provide accurate information.

6) If the data is being aggregated, what controls are in place to protect the data from unauthorized access or use?

Not applicable, the system is not capable of aggregating information on individuals.

7) If data is being aggregated, are the proper controls remaining in place to protect the data and prevent unauthorized access?

Not applicable.

8) How will the data be retrieved? Does a personal identifier retrieve the data?

The data will be retrieved by the employees' or potential employees' name, as well as other data points such as request status, date, etc.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

No reports are produced on individuals. Although reports will be produced out of this application, they will not contain names or positions.

10) What opportunities do individuals have to decline/refuse to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses)?

Individuals must provide the information in order to request a reasonable accommodation pursuant to the Rehabilitation Act or Title VII.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

Not applicable.

2) Is the data in the system covered by existing records disposition authority? If yes, what are the retention periods of data in this system?

These records are maintained in accordance with the National Archives and Records Administration (NARA) General Records Schedule 2.3 Employee Relations Records.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Pursuant to the General Records Schedule, the records are destroyed when three years old or longer if required for business use. OGE's records management policies document the procedures for disposition.

4) Is the system using technologies in ways that the OGE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

5) How does the use of this technology affect public/employee privacy?

The application has a minimal effect on employee privacy compared to the prior method of maintaining these records. Previously, each supervisor maintained the records for their own subordinates, generally on OGE's network drives or in hard copy. The application is more secure. Supervisors and managers have access only to the entries they create. Only the Deputy Director, the HR Attorney-Advisor, and LEAP Branch Chief have unrestricted access to the application.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

No.

7) What kinds of information are collected as a function of the monitoring of individuals?

Not applicable.

8) What controls will be used to prevent unauthorized monitoring?

The system does not have the capability to monitor individuals.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

OGE/INTERNAL-1, Employee Leave, Travel, Reasonable Accommodation, and Payment Records. A Privacy Act statement is included in OGE's Reasonable Accommodation Policy and Procedures for Individuals with Disabilities and OGE's Policy on Religious Accommodations. Employees will be directed to review the appropriate policy and Privacy Act statement before seeking a reasonable accommodation.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

It does not require amendment.

F. ACCESS TO DATA:

1) Who will have access to the data in the system?

See section E.5., above.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access to OGE applications is governed by the Account Access Request Form (AARF) process, which authorizes the Information Technology Division (ITD) to create, modify, and disable network accounts, including providing access to OGE applications. AARF requests must be signed by the employee, his/her supervisor, and the Chief Information & Cybersecurity Officer before a request is approved to be implemented by ITD staff.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

See section E.5., above.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

Users cannot access records that they are not authorized to access, thus preventing unauthorized browsing. In addition, authorized users have been advised that agency policy prohibits them from unauthorized browsing of data and have been instructed not to engage in such activities.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

   No.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

   No.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

   Not applicable.

8) **Will other agencies share data or have access to the data in this system (Federal, State, or Local)?**

   No.

9) **How will the data be used by the other agency?**

   Not applicable.

10) **Who is responsible for assuring proper use of the data?**

    Each authorized user is responsible for assuring proper use of the data.

The Following Officials Have Approved the PIA for the Reasonable Accommodations Request Application:

1) **System Manager**

Electronic Signature: SIDNEY WILLIAMS Digitally signed by SIDNEY WILLIAMS Date: 2023.08.07 15:02:23 -04'00'

Name: Sidney Williams
Title: HR Attorney-Advisor, Administrative Operations Branch

2) **System Owner**

Electronic Signature: DALE CHRISTOPHER Digitally signed by DALE CHRISTOPHER Date: 2023.08.07 13:50:55 -04'00'

Name: Chip Christopher
Title: Deputy Director, Compliance Division

3) **Chief Information & Cybersecurity Officer**

Electronic Signature: JAMES COOPER Digitally signed by JAMES COOPER Date: 2023.08.01 16:46:38 -04'00'

Name: Ty Cooper
Title: Chief Information & Cybersecurity Officer

4) **Senior Agency Official for Privacy**

Electronic Signature: DIANA VEILLEUX Digitally signed by DIANA VEILLEUX Date: 2023.08.07 15:24:24 -04'00'

Name: Diana J. Veilleux
Title: Chief, Legal, External Affairs and Performance Branch and Senior Agency Official for Privacy