



Tennessee Valley Authority Privacy Impact Assessment (PIA)

Calendly

This PIA is a tool used by the TVA Privacy Office to identify privacy risks at the planning/initiation phase of the system development lifecycle (SDLC) or early stages of project/program development. The PIA should be reviewed and updated on an annual basis, or sooner, if the system undergoes a major change. Questions regarding this document should be directed to privacy@tva.gov.

PIA should be submitted to:

TVA Privacy Office

privacy@tva.gov

Version 3.0
September 2018



PROGRAM MANAGEMENT

Author Name

[Redacted]

Date of Submission

09/22/2023

Responsible TVA Business Unit

Human Resources

Name of System

Calendly

System Owner Details

Reason for Completing PIA

Name

[Redacted]

Title

Phone

Email

- New system
- Significant modification to an existing system
- To update existing PIA for a security authorization

PRIVACY DETERMINATION

(To be completed by the TVA Privacy Program)

Privacy Office Comments

[Empty box for comments]

The signatures below certify that the information in this document has been reviewed and approved:

	Name	Signature	Date
System Owner	[Redacted]	[Redacted]	09/25/2023
Senior Privacy Program Manager	Chris Marsalis	Chris Marsalis (E-Signature)	09/22/2023



SYSTEM OVERVIEW

1. Please describe the purpose of the system/collection:

Calendly is an app for scheduling applicant appointments and meetings. Its goal is to eliminate the problematic back-and-forth when trying to nail down times. Rather than email chains and phone tag, you can send your availability with a Calendly link

2. About whom does the system collect, maintain, use and/or disseminate information? Check all that apply:

- TVA employees
- TVA contractor
- Members of the public

3. Is the information collected directly from the individual?

- Yes
- No

4. What type of personally identifiable information (PII) can be/is collected, maintained, used, and/or disseminated?

Check all that apply: (Per the Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.)

- | | | |
|-------------------------------------------------|--------------------------------------------------------|----------------------------------------------------------|
| <input checked="" type="checkbox"/> Home Phone | <input type="checkbox"/> Financial Information | <input type="checkbox"/> Biometric Information |
| <input type="checkbox"/> Home Address | <input type="checkbox"/> Clearance Information | <input type="checkbox"/> Citizenship |
| <input checked="" type="checkbox"/> Home Email | <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Driver's License Number |
| <input type="checkbox"/> Employment Information | <input type="checkbox"/> Date of Birth | <input type="checkbox"/> Username/Password |
| <input type="checkbox"/> Work Address | <input type="checkbox"/> Place of Birth | <input type="checkbox"/> Passport Number |
| <input checked="" type="checkbox"/> Work Phone | <input type="checkbox"/> Criminal History | <input type="checkbox"/> Other: |
| <input checked="" type="checkbox"/> Work Email | <input type="checkbox"/> Social Security number (SSN) | <input style="width: 150px; height: 15px;" type="text"/> |
| <input type="checkbox"/> Name | <input type="checkbox"/> Medical or Health Information | |

If none of the above data elements are checked, stop and submit this PTA as-is to TVA Privacy Office at privacy@tva.gov. Otherwise, please continue completing the remaining questions in the document.

Privacy Notice and Transparency

5. Legal authority to collect, use, maintain, and share data in the system:

Tennessee Valley Authority Act of 1933, 16 U.S.C. 831-831ee; Executive Order 10577; Executive Order 10450; Executive Order 11478; Executive Order 11222; Equal Employment Opportunity Act of 1972, Public Law 92-261, 86 Stat. 103; Veterans' Preference Act of 1944, 58 Stat. 387, as amended; various sections of title 5 of the United States Code related to employment by TVA.

6. Does the system have a SORN? (If PII in the system is retrieved using one or more of the identifiers listed in Question 4, a System of Records Notice (SORN) is required.)

- Yes
- No

List name(s) of applicable SORN(s):

7. How are individuals notified as to how their information will be collected, maintained, used, and/or disseminated within this system?

8. What consent options do individuals have regarding specific uses or sharing of their information?

Applicants have consented to this use by already applying for the position.

DATA MINIMIZATION

9. Are only the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose collected, used and retained?

Yes No

10. What are the retention periods for the information in the system?

Calendly shall return or securely destroy Personal Data, in accordance with Customer's instructions, upon Customer's request or upon termination of Customer's account(s) unless Personal Data must be retained to comply with applicable law.

DATA QUALITY

11. How is data quality (i.e., accuracy, relevance, timeliness, and completeness) ensured throughout the data lifecycle and business processes associated with the use of the information? Check all that apply.

Information is collected directly from individuals (preferred method of collection, whenever possible)
If collected via a form, please list form(s) name and number here:

Cross referencing information enties with other systems Third party information verification

Character limits on text submissions Numerical restrictions in text boxes

Other:

12. How is inaccurate or outdated information checked for and corrected?

The individual provides their own data directly.

Access and Redress

13. How can an individual access their information and have it corrected, amended, or deleted?

The individual will log into the system to correct information, or have it deleted.

Internal and External Sharing

14. Explain how the information in the system is limited to the uses specified in the notices discussed above.

Information in the system will only be used for scheduling appointments and meetings

15. With which (if any) internal TVA systems is the information shared?

Information will not be shared with any other internal systems

16. With which (if any) organizations external to TVA is information shared?

Information will not be shared with any other external systems

17. Does the system have any associated websites/applications including an external TVA website or third-party owned or managed website or application (e.g., Facebook, YouTube, Twitter, Flickr, etc.)?

- Yes
- No

SECURITY

18. What privacy orientation or training is provided to authorized users of the system or individuals with access to the system?

[Redacted]

19. Has a FIPS 199 determination been made?

[Redacted]

20. What is the FIPS 199 determination? Check one for each.

[Redacted]

21. What types of technical safeguards are in place to protect the information?

[Redacted]

22. What types of physical safeguards exist to protect the information?

[Redacted]



23. What types of administrative safeguards exist to protect the information?

24. What monitoring, recording, and auditing safeguards are in place to prevent or detect unauthorized access or inappropriate usage?

All users must sign in through Azure AD. All monitoring, recording, and auditing safeguards are in place to prevent or detect unauthorized access or inappropriate usage by TVA Cybersecurity.

25. Discuss any other potential privacy risks to the information within the system and safeguards that are in place to mitigate those risks.

None

Please submit completed form to: **TVA Privacy Office**
privacy@tva.gov