Events Management System

Privacy Impact Assessment (PIA)

April 2024

POINT of CONTACT

privacy.office@gsa.gov

GSA Stakeholders

The GSA representatives listed below have reviewed the information provided by the vendor for completeness.

Name of GSA Program Manager: Kelsey Gustin

X DocuSigned by:
Kelsey Gustin
55FB6934FF7B40C...

GSA Program Manager

Name GSA Chief Privacy Officer (CPO): Richard Speidel

X DocuSigned by:
Richard Speidel
171D5411183F40A...

GSA Chief Privacy Officer

Table of Contents

Document purpose

This document contains guidance for vendors that maintain and operate nonfederal systems. To provide the requested service, the vendor collects, maintains and/or disseminates personally identifiable information (PII) about the people who use such products and services. PII is any information[1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

Vendors should use this PIA guidance to explain how and why they collect, maintain, disseminate, use, secure, and destroy information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals.

Overview

A. System, Application, or Project Name:

Events Management System

B. GSA Client:

Public Buildings Service, General Services Administration (GSA)

C. System, application, or project includes information about:

1. Members of the public who register for in-person building tours and online public programming offered by GSA staff;

2. Federal employees who register for in-person building tours and online public programming offered by GSA staff; and

3. GSA employees and contractors who use the system.

D. System, application, or project includes these data elements:

[1] OMB Memorandum Preparing for and Responding to the Breach of Personally Identifiable Information (OMB M-17-12) defines PII as: "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." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

The General Services Administration (GSA) collects the first name, last name, affiliation, country of citizenship, and minor status (whether or not a visitor is under 13 years of age or between the ages of 13 and 17 years) from members of the public, federal employees, and contractors through the Events Management System). Depending on the event, GSA organizers might collect additional information from registrants, such as requests for special accommodations, to facilitate event attendance. Such accommodations may include assistive technologies or other means of providing access to the subject of the tour and, depending on the requested accommodation, GSA may receive information from individuals that includes, but is not limited to, health information.

Virtual or in-person events may also include speaker biographic information (e.g. name, academic history, employment history, etc.). Speaker information will only be provided with the consent of the speaker.

For example, users may choose to create an Eventbrite account, although this is not required to register for an event. To create an Eventbrite account, users provide their email address, create a password, and provide additional information as required by Eventbrite. Eventbrite does not provide this account information to GSA to facilitate event registration in its official capacity.

Eventbrite will also collect, use, maintain, and disclose user information in accordance with its Terms of Service and Privacy Policy. Users may wish to review the Eventbrite Privacy Policy before using its services to understand how and when Eventbrite collects, uses, and shares the information submitted for GSA events utilizing Eventbrite's services.

E. The purpose of the system, application, or project is:

The Events Management System is a third-party web service that allows members of the public, federal employees, and contractors to register for free in-person building tours and online public programming offered by the General Services Administration (GSA). A critical aspect of GSA's mission is to connect members of the public, federal employees, and contractors to the art and architecture of government buildings managed by GSA, including buildings that are in use by other federal agencies. An online event registration system enables users to register to attend building tours, trainings, and other public programming. GSA staff require the tools offered by an Events Management System to manage the attendance of large groups of people registering for virtual and in-person events. While some online event management systems provide tools for planning both free and paid events, GSA will never organize paid events through these services.

When users register through the Events Management System, GSA staff collects only the necessary information that is required by building security for in-person access. This includes the first name, last name, affiliation, country of citizenship, and minor status (whether or not a visitor is under 13 years of age or between the ages of 13 and 17 years). Minors under the age of 13 years old will not be allowed to register independently. A parent or legal guardian must register any minor under 13 years old and will only need to supply that minor's name and country of citizenship. Minors between the ages of 13 and 17 years old can register for events but will need to identify their minor status when doing so.

Email addresses are also collected to communicate information about the tour, its location, and instructions for security screening in advance of the event. If the event is online, GSA staff send users a link to a video conferencing platform such as Zoom or Google Meet where the online event will be hosted. After the event, GSA staff send an anonymous feedback form by email, and users are also given the opportunity to sign up for an email mailing list to receive future information about free virtual and in-person events offered by GSA that they can opt out of at any time.

Before an event takes place, GSA staff export the name, email address, affiliation, country of citizenship, and minor status from the Events Management System as a spreadsheet. GSA staff provide this information to building security personnel via encrypted email. The email addresses are used by GSA staff to communicate pertinent information before and after the event, and for users who opt to join a mailing list, GSA staff will retain those email addresses and add them to a mailing list where users can receive future information about GSA events. Users can opt out of the mailing list at any time. All information gathered by GSA is handled electronically and archived in accordance with the appropriate records retention schedule.

SECTION 1.0 OPENNESS AND TRANSPARENCY

1.1 Are individuals given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

GSA sets up official event registration pages that clearly establish that GSA is hosting the event. GSA provides, where feasible, a Privacy Notice or Privacy Act Statement on any event page requesting information. The Notice or Statement explains if the online Events Management System is not a GSA website and if it is controlled and operated by a third party. The Notice or Statement also describes how GSA maintains, uses, or shares personal identifiable information (PII) and explains that individuals may be providing information to a third party.

SECTION 2.0 DATA MINIMIZATION

2.1 Why is the collection and use of PII necessary to the system, application, or project?

The information that GSA requests on the Events Management System is required for facilitating access to secure government buildings and communicating pertinent information about virtual and in-person events.

2.2 Will the system monitor the public, GSA employees, or contractors?

While a third-party Events Management System may collect information that can facilitate the monitoring of an individual, this information is not shared with GSA staff, nor would it be used or accessed by GSA staff if made available to locate or monitor members of the public, federal employees, or contractors.

2.3 What kinds of report(s) can be produced on individuals?

The Events Management System allows GSA staff to export a list of names, email addresses, affiliations, countries of citizenship, and minor status of attendees. No other information or reports are accessible or used by GSA staff.

2.4 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

The information collected and retained on the third-party Events Management System is not an agency record. Only a subset of the information provided by the registrant is passed on to GSA. After GSA staff export this information and use it for building security access and the communication of event information, GSA staff archive the report in accordance with the appropriate records retention schedule. Users are given the option of joining an email mailing list to learn about future virtual or in-person events and may opt out of the mailing list at any time.

SECTION 3.0 LIMITS ON USING AND SHARING INFORMATION

3.1 Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?

GSA staff will only communicate the names, countries of citizenship, affiliations, and minor status to building security for a specific event. If the building's security does not require information on the country of citizenship, for example, GSA will not collect this information within the Events Management System. If the event is virtual, GSA staff will only collect pertinent information such as email addresses or special accommodations for users with disabilities. When at all possible, GSA will limit the scope of information it requests on the Events Management System and will only collect the information that is required for each specific event.

3.2 Will the information be shared with other individuals, federal and/or state agencies, private-sector organizations, foreign governments and/ other entities (e.g., nonprofits, trade associations)? If so, how will the vendor share the information?

Information is shared within GSA with personnel who have a lawful government purpose to access the information. Only GSA staff managing event registration have direct access to the Events Management System. GSA staff will only communicate the names, countries of citizenship, affiliations, and minor status to building security of tenant agencies for a specific event. This information will be communicated via encrypted email to the appropriate security staff of the tenant agency where the tour will take place.

A third-party Events Management System, such as Eventbrite, will also collect, use, maintain, and disclose user information in accordance with its Terms of Service and Privacy Policy. Users may wish to review the Eventbrite Privacy Policy before using its services to understand how and when the third-party Events Management System collects, uses, and shares the information submitted for GSA events utilizing its services.

3.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

GSA will collect information directly from individuals who are voluntarily registering to attend a virtual or in-person event, with the exception of minors under the age of 13 years old. A parent or legal guardian can register a minor under 13 years old and provide information on the minor’s name and country of citizenship.

SECTION 4.0 DATA QUALITY AND INTEGRITY

4.1 How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?

The information provided to the Events Management System will be verified by confirmation emails with individuals. It is up to the individual to verify that the information is accurate.

SECTION 5.0 SECURITY

5.1 Who or what will have access to the data in the system, application, or project? What is the authorization process to gain access?

GSA staff that assist in organizing the event and have a lawful government purpose have access to the information voluntarily submitted by each registrant. GSA staff that assist with events and registration activities may be contractors. These contractors are subject to confidentiality requirements. Only GSA staff managing event registration have direct access to the Events Management System.

5.2 Has a System Security and Privacy Plan (SSPP) been completed for the information system(s) or application?

This system relies upon a third-party system to collect and provide the information solicited from individuals. PII is transmitted in accordance with federal and GSA policies and procedures. As this system is based on a process that spans multiple third-party and FISMA systems, the SSPPs of those individual systems can be consulted.

5.3 How will the system or application be secured from a physical, technical, and managerial perspective?

Records in the system are protected from unauthorized access and misuse through a combination of administrative and technical security measures. Administrative measures include but are not limited to policies that limit system access to individuals within the agency with a legitimate business need and regular review of security procedures and best practices to enhance security. Technical measures include but are not limited to system design that allows authorized system users access only to data for which they are responsible; and use of encryption for certain data transfers. Sensitive data is encrypted in transit and at rest.

5.4 What mechanisms are in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

Third-party Events Management Systems, such as Eventbrite, employ a full-time legal and security team focused on privacy and security issues. All applications are regularly scanned for common security vulnerabilities. Use of encryption for the storage and transmission of sensitive information is regularly audited by its Security Team. Third-party providers have taken appropriate measures to vet its employees and maintain a stringent information security training program. In the event of a breach of the information system, the service has a detailed Incident Response plan in place.

SECTION 6.0 INDIVIDUAL PARTICIPATION

6.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

GSA may make accommodations for those who wish to provide registration information through alternative means outside of the Events Management System. However, when it comes to accessing a building with security protocols, a user will need to provide first and last name, minor status, and country of citizenship to attend.

To the extent that participating in a GSA event is voluntary, individuals have the opportunity to decline to provide information to GSA, however, failure to provide information may delay or prohibit event registration.

6.2 What procedures allow individuals to access their information?

Users can access their own account information and event registration from the Events Management System website provided by a third-party vendor.

6.3 Can individuals amend information about themselves? If so, how?

Individuals are allowed to change submitted information through the Events Management System and will also have the ability to correct any information when GSA staff email a confirmation of their registration.

SECTION 7.0 AWARENESS AND TRAINING

7.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.

All GSA personnel are subject to GSA agency-wide procedures for safeguarding PII and receive annual privacy and security training.

All GSA staff must report any compromise of their accounts or related records to the appropriate GSA officials in accordance with established procedures. Access to the GSA network is restricted to authorized users with password authentication controls, servers are located in secured facilities behind restrictive firewalls, and access to databases and files is controlled by the system administrator and restricted to authorized personnel based on the need-to-know principle. Other security controls include continuously monitoring threats, rapid response to incidents, and mandatory security and privacy training.

SECTION 8.0 ACCOUNTABILITY AND AUDITING

8.1 How does the system owner ensure that the information is only being used according to the stated practices in this PIA?

GSA event organizers must use their official email address to create an account with a third-party Events Management System and will have access only to the account they use to create and manage event pages and event-related communications. GSA users must access their account while using GSA-approved devices, not personal devices.

All GSA employees and contractors must coordinate with their supervisor and other appropriate officials to ensure that physical, technical, and administrative safeguards are in place to protect the records in their custody. GSA employees and contractors can help protect PII collected through the Events Management System by safeguarding their user credentials and avoiding the storage of records on shared networks or folders accessible to individuals who do not have an official need-to-know. GSA employees and contractors are responsible for safeguarding all information they remove from their official duty station and information they create at any alternative workplace in accordance with the Federal Records Act, Privacy Act, Freedom of Information Act, and other federal laws, regulations, and GSA policies. GSA employees and contractors may share event-related records only with authorized officials using approved sharing methods.