

United States Department of Justice



Administrative Privacy Impact Assessment for Eventbrite

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [November 28, 2017] |

[Administrative Edits Made July 6, 2018]

(May 2015 DOJ Admin PIA)

Blank Page

EXECUTIVE SUMMARY

Eventbrite is a third-party event management and registration platform that enables the United States Department of Justice (DOJ or the Department) and its components¹ to facilitate event registration in their official capacities on behalf of the Department.² Eventbrite allows the Department and its components: to create event registration, speaker profiles, organizer profiles, and other webpages related to Department events; to promote those pages and events to visitors or browsers on Eventbrite services; and to facilitate event registration for registrants.

The Department conducted this Administrative Privacy Impact Assessment (Admin PIA) because the Department and its components may utilize Eventbrite to collect and retain personally identifiable information (PII), including an event registrant's name, address, email address, and other information that enable the Department and/or Eventbrite to identify individuals. Eventbrite's Terms of Service and Privacy Policy govern Eventbrite's collection, use, maintenance, and disclosure of information.³ 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 Department events utilizing Eventbrite's services.

Section 1: The Type and Purpose of System and Information Collected and Stored within the System:

1.1 What is the purpose for which the records and/or system were designed to serve for the agency?

Eventbrite is a third-party web service that automates certain tasks associated with managing event registration. The Department and its components frequently host training and events for federal employees and members of the public that require advanced registration. The Department and its components generally publicize these events on Department websites or by email. Registrants respond to the training/event announcements and receive automated registration confirmation messages or waitlist messages through Eventbrite. Eventbrite alleviates the need for the Department to manually track and individually respond to registrants.

¹ Prior to using Eventbrite, Department components must certify that they have read this Admin PIA and will utilize Eventbrite in a manner consistent with the activities described herein. Department components that wish to use Eventbrite in a manner that is beyond the scope of this Admin PIA must complete a separate PIA, or provide an addendum to this Admin PIA, that the Department, where practicable, will publish on the DOJ PIA webpage: <https://www.justice.gov/opcl/doj-privacy-impact-assessments>.

² More information on Eventbrite can be found at: <https://www.eventbrite.com>.

³ The Eventbrite "Amendment to its Terms of Service that Apply to Federal Agencies Using Eventbrite" can be found at: <https://www.eventbrite.com/1/federaltos/>. The Eventbrite Privacy Policy can be found at: https://www.eventbrite.com/support/articles/en_US/Troubleshooting/eventbrite-privacy-policy?lg=en_US.

1.2 What information in identifiable form (IIF) is made available or is to be collected, maintained, used or disseminated by the system (e.g., identifying numbers, general personal data, work-related data, distinguishing features/biometrics, system admin and user data)?

[The Department utilizes Eventbrite to collect a registrant's name, address, and/or email address to facilitate training and event registration. Depending on the event, Department organizers can set up event registration pages to collect additional information from registrants (for example, requests for accommodations) in connection with the Department's event registration process and to facilitate event registration. Event pages may also include speaker biographic information (e.g., name, academic history, employment history). Components will only provide this information with the consent of the speaker. Overall, the Department will collect only information necessary for the proper performance of agency functions and that has practical utility.

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 the Department to facilitate event registration in its official capacity.⁴]

1.2 About whom (e.g., government employees, members of the public, individuals associated with investigations) and from whom is the IIF collected (e.g., directly from individual about whom the information pertains, government or non-government sources)?

[Information is about and collected directly from government employees and members of the public who choose to attend Department-hosted trainings and events that utilize Eventbrite to manage registration.]

⁴ Note that information a user provides or submits to a Department event registration page, including information that may have been provided during the Eventbrite registration process, such as the user's name, may be collected, maintained, or disseminated, consistent with the practices described in this Admin PIA.

Section 2: The Uses and Sharing of Information Collected and Stored within the System:

2.1 What are all the Department's intended uses of the IIF collected (e.g., criminal law enforcement, intelligence matters, civil enforcement, administrative matters, public affairs, or human resources)?

[The Department uses the information to communicate with event attendees about training materials, for event logistics purposes, to request for event feedback, and to otherwise facilitate Department events.

Additionally, information may be necessary to maintain the security of the personnel and locations at which the DOJ operates, and to determine eligibility and/or the status of individuals who have applied for, sought, been considered for, attempted and/or obtained access to such locations.]

2.2 Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the intended uses described above and to further the component's and/or the Department's mission. Indicate legal authorities, policies, or agreements that authorize collection of the information in the system.

[Collecting the names and email addresses is necessary to communicate with attendees to provide them with logistical information and materials in advance of each training or event. In order to ensure that room capacity, event registration, and other event preparation activities are properly considered, the Department must have a reliable way to review registrants for its events. Biographical information about event speakers will allow participants to understand event specifics and the expertise of the trainers.

Additionally, security personnel may require certain information about registrants in advance for the purpose of physical security and to determine eligibility and/or the status of individuals who have applied for, sought, been considered for, attempted, and/or obtained access to locations at which the DOJ operates.]

2.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. Reference the applicable retention schedule approved by the National Archives and Records Administration, if available or necessary.

The information collected and retained on Eventbrite is not an agency record. To the extent that the Department creates and maintains training rosters separately from Eventbrite, these records will be retained for 6 years in accordance with the Department-wide records schedule for Training Records, DAA-0060-2017-0009-0004.

2.4 With whom does the component intend to share the information in the system (e.g., within the component, other Department components, foreign/federal/state/local authorities, public, etc.) and how will the information be shared (e.g., case-by-case basis, bulk transfer, or direct access)?

Information will be shared within the Department with personnel who have a need to know, including component staff responsible for event logistics and Department security staff. Only component staff managing event registration will have direct access to Eventbrite. Additionally, components may make a full list of event participants available to the participants at the event. If components use Eventbrite to facilitate registration for an event that requires the Department to make public a list of attendees, the component will publically release the names of individuals registered through Eventbrite.

By providing information through Eventbrite for a Department event, Eventbrite will also collect, use, maintain, and disclose user information in accordance with its Terms of Service and Privacy Policy.⁵ 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 Department events utilizing Eventbrite's services.

2.5 Are there any potential threats to privacy that exist in light of the information collected or shared? Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy.

The Department has taken appropriate steps to mitigate any potential threats to privacy that exist in light of the event registration information collected and shared. For the purposes of event registration, the Department will collect only information necessary for the proper performance of agency functions and that has practical utility, minimizing the risks of collecting unnecessary information. Additionally, DOJ employs a robust physical security system to protect its servers and access terminals to minimize the unauthorized access or misuse of registration information maintained by the Department. The Department has examined Eventbrite's Privacy Policy to evaluate the

⁵ See *supra* note 3.

risks, and is developing a process in which it will monitor any changes to the Eventbrite's Privacy Policy that would require a reassessment of those risks. Finally, information is entered directly by the registrant to minimize the possibility of the Department entering inaccurate information. |

Section 3: The Security of the Information Collected and Stored within the System:

3.1 What controls has the component put into place to ensure that the information is handled, retained, and disposed of appropriately (e.g., access/security controls, monitoring/testing/evaluation, auditing, privacy training, automatic purging of information, MOUs)?

|Prior to utilizing Eventbrite, the Department and its components must coordinate with the DOJ Office of the Chief Information Officer, or a component's Chief Information Officer, to issue a risk certification memorandum that affirms an acceptable residual risk associated with the component's use of Eventbrite for event management purposes. Each component's use of Eventbrite will be different depending on the information necessary for facilitating event registration; however, the security risk assessment will review, among other things, access/security controls in place, monitoring auditing activities, privacy training and awareness, and the automatic purging of information. The component must obtain this certification memorandum prior to utilizing Eventbrite. |

3.2 Has a Certification and Accreditation (C&A) been completed for this system?

|A full C&A is not required for the Department's use of Eventbrite, consistent with the practices outlined in this Admin PIA. Prior to utilizing Eventbrite, however, Department components must coordinate with the DOJ Office of the Chief Information Officer, or the component's Chief Information Officer, to issue a risk certification memorandum that affirms an acceptable residual risk associated with the component's use of Eventbrite for event management purposes. The component must obtain this certification memorandum prior to utilizing Eventbrite. |

3.3 Has security risk assessment been completed for this system?

|Prior to utilizing Eventbrite, Department components must coordinate with the DOJ Office of the Chief Information Officer, or the component's Chief Information Officer, to issue a risk certification memorandum that affirms an acceptable residual risk associated with the component's use of Eventbrite for event management. Each

component's use of Eventbrite will be different depending on the information necessary for facilitating event registration; however, the security risk assessment will review, among other things, the access/security controls, monitoring auditing activities, privacy training and awareness, and the automatic purging of information. The component must obtain this certification memorandum prior to utilizing Eventbrite.

3.4 Do contractors have access to the system, and if yes, can you confirm that there are (a) provisions in their contract binding them under the Privacy Act; and (b) information security provisions in their contracts required by DOJ policy?

[To the extent that the Department or its components host an event in which DOJ contractors have a need to access the event registration information, they are required to comply with all privacy and information security requirements applicable to Department employees, including the practices outlined in this Admin PIA.]

Section 4: Notice, Consent, and Redress:

4.1 Will individuals be notified if their information is collected, maintained, or disseminated by the system (e.g., system of records notice, Privacy Act 552a(e)(3) notice)? Please specify.

[The Department will set up official event registration pages that clearly establish that DOJ is hosting the event. For example, the Department will, where feasible, use the DOJ seal on event registration pages. The Department also manages its Website Privacy Policy that informs visitors of the Department's use of pages on third-party websites and applications.⁶

The Department and its components will, where feasible, provide a privacy notice on any Eventbrite event page requesting information. The notice will explain that Eventbrite is not a Department website, that it is controlled and operated by a third party, and that the Department's Website Privacy Policy does not apply to the third party. The notice will also describe how the component will maintain, use, or share PII, and explain that individuals may be providing information to third parties by using Eventbrite.

⁶ The Department's Website Privacy Policy can be viewed at: <https://www.justice.gov/doj/privacy-policy>.

4.2 Do individuals have the opportunity to decline to provide information? Please specify.

[To the extent that the Department requires its employees to participate in a training that utilizes Eventbrite to facilitate registration, individuals do not have the opportunity to decline to provide event registration information. The Department and its components, however, may choose to make accommodations for those who wish to provide registration information through other means. To the extent that participating in a Department event is voluntary, individuals have the opportunity to decline to provide information to the Department, however, failure to provide information may delay or prohibit event registration.]

4.3 Do individuals have the opportunity to consent to particular uses of the information? Please specify.

[Implicit in DOJ notifying registrants of the particular uses of their information, individuals have the opportunity to consent to the uses of their information provided to the Department through Eventbrite. Individuals do not otherwise have the opportunity to consent to the particular uses of the information. The minimal information collected is required to facilitate event and training registration and communication.]

Section 5: Privacy Act:

5.1 Is a system of records being created, or has one been created, under the Privacy Act, 5 U.S.C. § 552a? If yes, indicate the existing system of records notice or whether one is being developed.

[The intended use of Eventbrite to facilitate event registration, as a matter of practice, will not result in the Department maintaining records about an individual and retrieving an individual's record by the individual's name or other identifying particular. As a result, a component's maintenance of event registration information alone to facilitate Department event registration does not constitute a system of records, and a System of Records Notice (SORN) is not required.

The Department, however, may be required to disclose particular event registration information to other components within the Department, on a need-to-know basis, to facilitate other mission essential functions. For example, a component may be required to submit event registration information to Department building security personnel for the purpose of maintaining the security of the personnel and locations at which the DOJ operates. Such disclosures may result in the Department maintaining an individual's information in a system of records (for example, JUSTICE/DOJ-011 Access Control

System (ACS), last published in full at 69 Fed. Reg. 70279 (Dec. 03, 2004)). At such point, information will be maintained consistent with the Privacy Act of 1974, including but not limited to, maintaining information in a system of records with an appropriately published SORN.]

5.2 Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved (e.g., name or other personal identifier).

[N/A – A components maintenance of registrant names and email addresses to facilitate Department event registration, as a matter of practice, does not constitute a system of records and a System of Records Notice is not required. For more information, please see section 5.1, above.]