Institute of Museum and Library Services

Privacy Impact Assessment

for

CONSTANT CONTACT

9/27/2023

Institute of Museum and Library Services Privacy Impact Assessment

CONSTANT CONTACT

Under the E-Government Act of 2002, the Institute of Museum and Library Services ("IMLS") must perform a Privacy Impact Assessment (PIA) (i) before initiating a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government); or (ii) before developing or procuring information technology systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public.

Section 1. Description of the system/project

Please provide a description of the information system or project in plain language. If it would enhance the public's understanding of the system or project, please provide a system diagram.

Constant Contact is a web-based email marketing software (Software as a Service) that primarily helps businesses create branded emails, websites, online stores and more in one online marketing platform. IMLS uses this platform to (1) maintain a subscribed user list for news releases, blogs, research announcements, and monthly newsletters; (2) distribute event invitations; and (3) connect with past, present, and potential grantees about panels, reviewer opportunities, and webinar information via email distribution lists.

Names and email addresses are stored on the platform. Subscribers are sorted into lists of their choosing. Professional contacts for invitations or targeted communications are uploaded from contacts in IMLS's electronic Grants Management System (eGMS) system and maintained in specifically labeled, limited-use distribution lists.

Constant Contact does not sell or rent email addresses. Users are not permitted to upload or use purchased, traded, shared, or borrowed lists to their Constant Contact account. Similarly, IMLS does not sell or share its email lists from Constant Contact.

In your description, please be sure to address the following:

a. *The purpose that the system/project is designed to serve.*
b. *Whether it is a general support system, major application, or other type of system/project.*
c. *System/project location (e.g., within Microsoft Azure, Qualtrics, Drupal, etc.).*
d. *How information in the system/project is retrieved by the user.*
e. *Any information sharing.*

Section 2. Information Collected

2.1 Indicate below what personally identifiable information (PII) is collected, maintained, and/or disseminated by your system/project (check all that apply).

Identifying numbers (IN)					
a. Social security number (full or truncated form)*		b. Driver's License		c. Financial Account	
d. Taxpayer ID		e. Passport		f. Financial Transaction	
g. Employer/Employee ID		h. Credit Card		i. U.S. Citizenship and Immigration Services	
j. File/Grant ID					
k. Other identifying numbers:					
* Explanation for the need to collect, maintain, or disseminate the Social Security Number:					

General Personal Data (GPD)					
a. Name	X[1]	b. Maiden Name		c. Email Address	X
d. Date of Birth		e. Home Address		f. Age	
g. Gender		h. Personal Telephone Number		i. Education	
j. Marital Status		k. Race/Ethnicity			
l. Other general personal data:					

Work-related data[1]					
a. Occupation	X	b. Job Title	X	c. Work Email Address	X
d. Work Address		e. Work Telephone Number		f. Salary	
g. Employment History		h. Procurement/Contracting Records		i. Employment Performance Rating	
j. Other work-related data:					

System Administration/Audit Data					
a. IP Address	X	b. User ID/Username		c. Date/Time of Access	X
d. Queries Run		e. ID of Files Accessed		f. Personal Identity Verification (PIV) Card	

[1] This information is optional to provide.

Other system administration/audit data: Emails sent from the Constant Contact platform include single pixel gifs, also known as web beacons, which contain unique identifiers that enable Constant Contact and IMLS to recognize when their contacts have opened an email or clicked certain links. These technologies record each contact's email address, IP address, date, and time associated with each open and click for an email campaign.

2.2 Indicate sources of the information in the system/project and explain how the information is received.

Source of Information	**Explanation**
Directly From the Individual About Whom the Information Pertains:	Individuals sign up for emails from IMLS via Constant Contact through www.imls.gov/news/subscribe
Government Sources:	Professional Contacts are often retrieved from the electronic Grants Management System (eGMS) where information is uploaded from official grant applications, and they have consented to being contacted by IMLS.
Non-Government Sources:	
Other:	

2.3 Whose data is collected, disseminated, disclosed, used, or maintained by the system/project? Please also provide an estimate of the number of individuals and minors within each category whose PII is contained within the system/project.

Members of the public	26,000 *(includes professional contacts)* (There is no data on minors collected, disseminated, disclosed, used, or maintained.)
IMLS employees/ contractors	65
Other (explain)	

2.4 Provide the legal authority that permits the collection, dissemination, disclosure, use, and/or maintenance of the PII mentioned in Section 2.1 (e.g., Section 9141 of the Museum and Library Services Act of 2018 (20 U.S.C. Ch. 72), OMB Circular A-130, etc.).

Section 9103(c) of the Museum and Library Services Act of 2018 (20 USC Ch. 72)

2.5 Describe how the accuracy of the information in the system/project is ensured.

Individuals can update their own information in the system. IMLS occasionally receives requests to update email addresses from individuals. Professional association lists are reviewed to ensure returned emails are accurate or determine if they need to be revised or removed. Individuals are also able to remove themselves from the distribution lists. Due to the nature of the platform, IMLS cannot resubscribe users without their permission.

2.6 Is the information covered by the Paperwork Reduction Act?

Yes? Please include the OMB control number and the agency number for the collection.	No?
	X

2.7 What is the records retention schedule approved by the National Archives and Records Administration (NARA) for the records contained in this system/project?

These are temporary files. The information is deleted when superseded, obsolete, or the customer requests the agency to remove the records.

2.8 Is the PII within this system/project disposed of according to the records disposition schedule?

Yes

Section 3. Purpose and Use

3.1 Indicate why the PII in the system/project is being collected, maintained, or disseminated (e.g., for administrative purposes, to improve our services, etc.).

Information collected is expressly used for the distribution of news and other communications relevant to the public and our professional audiences.

3.2 Indicate whether the system collects only the minimum amount required to achieve the purpose stated in response to Question 3.1.

The system collects the minimum required information (email address). Optional information can be provided by the individual (name, organization, title). The system also collects information for administrative purposes (IP address, date and time of access).

3.3 Indicate how you intend to use the information in order to achieve the purpose stated in Question 3.1 (e.g., to verify existing data, to verify identification, to administer grant aid, etc.).

IMLS uses the information collected to distribute official communications from the agency to improve understanding of the organization, its activities, and potential opportunities for professionals.

3.4 Does the system use or interconnect with any of the following technologies? (Check all that apply.)

Social Media	
Web-based Application (e.g., SharePoint)	
Data Aggregation/Analytics	
Artificial Intelligence/Machine Learning	
Persistent Tracking Technology	
Cloud Computing	
Personal Identity Verification (PIV) Cards	
None of these	x

Section 4. Information Security and Safeguards

4.1 Does this system/project connect, obtain data from, or share PII with any other IMLS systems or projects?

Yes? Explain.	Some contacts are manually pulled from the electronic Grants Management System (eGMS).
No, this system/project does not connect with, obtain data from, or share PII with any other IMLS system or project.	

4.2 Does this system/project connect, obtain data from, or share PII with any external (non-IMLS) systems or projects?

Yes? Explain. (Please also describe the type of PII shared, the purpose for sharing it, the name of the information sharing agreement, and how the PII will be shared.)	
No, this system/project does not connect with, obtain data from, or share PII with any external system or project.	X

4.3 Describe any de-identification methods used to manage privacy risks, if applicable.

4.4 Identify who will have access to the system/project and the PII.

Members of the public	
IMLS employees/contractors	X
Other (explain)	

4.5 Does the system/project maintain an audit or access log?

Yes? Explain. (Including what information is compiled in the log)	
No, this system/project does not compile an audit or access log.	X

4.6 What administrative, technical, and physical safeguards are in place to protect the PII in the system/project?

Physical Security: Physical access to Constant Contact machines is restricted to specific individuals and uses multiple levels of security.

Network Security: Constant Contact's hosting environment is protected from the public Internet via multiple and distinct firewalls and monitored with a network-based commercial intrusion detection system.

Host Security: Constant Contact undergoes industry-standard security hardening efforts on all systems. In accordance with security and change management policies, unused services are disabled, and software updates are applied on a regular basis. Servers are monitored 24x7 for malicious activity. Administrative access to Constant Contact infrastructure is limited strictly to authorized users. Individual usernames and passwords are required for all machine and data access.

User Account Security: User-level access to Constant Contact services is provided via a username and an encrypted password selected by the end user. User account setup, maintenance, and termination are under the control of the end user.

4.7 What are the privacy risks associated with the system/project and how are those risks mitigated (e.g., automated privacy controls, privacy training, etc.)? Please include a description of the technology used to protect PII in the system/project.

Constant Contact regularly undergoes security reviews, including external and internal scanning for vulnerabilities on an ongoing basis by a 3rd-party vendor. All vulnerabilities discovered are reviewed by internal security and addressed according to severity.

IMLS staff undergo federally required annual training on ethics and privacy.

4.8 Under NIST FIPS Publication 199, what is the security categorization of the system/ project? Low, Moderate, or High?[2] (Please contact OCIO if you do not know.)

[2] Federal Information Processing Standards Publication 199 defines three levels of potential impact on organizations and/or individuals should there be a breach of security. The potential impact is defined as low if "[t]he loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals." Nat'l Inst. of Standards and Tech., *Fed. Info. Processing Standards Publ'n 199, Standards for Security Categorization of Federal Information and Information Systems* 2 (2004), https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

Low	X (However, Constant Contact is not FedRAMP certified)
Moderate	
High	

4.9 Please describe any monitoring, testing, or evaluation conducted on a regular basis to ensure the security controls continue to work as intended to safeguard the PII within the system/project.

Refer to section 4.7.

(emphasis omitted). The potential impact is defined as moderate if "[t]he loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals." *Id.* (emphasis omitted). The potential impact is high if "[t]he loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals." *Id.* at 3 (emphasis omitted).

Section 5. Notice and Consent

5.1 Indicate whether individuals will be notified that their PII is being collected, maintained, or disseminated. (Check the box or expand on the response that applies.)

Yes, notice is provided through a system of records notice (SORN) that was published in the Federal Register and is discussed in the next section.	
Yes, notice is provided through a Privacy Act statement, privacy policy, PIA, or privacy notice. The Privacy Act statement, privacy policy, and/or the privacy notice can be found at (provide text of the notice if a link isn't available):	X Constant Contact has a privacy policy available on their website at https://www.constantcontact.com/legal/privacy-center and also includes a consent notification during the subscription process
Yes, notice is provided by other means:	
No, notice is not provided. Please explain why:	

5.2 Please describe whether individuals are given the opportunity to consent to uses of their PII, decline to provide PII, or opt out of the system/project. Specify how below.

Consent	Yes, individuals have the opportunity to consent to uses of their PII:	X	
	No, individuals do not have the opportunity to consent to uses of their PII.		
Decline	Yes, individuals have the opportunity to decline to provide their PII:	X	
	No, individuals do not have the opportunity to decline to provide their PII.		
Opt out of	Yes, individuals have the opportunity to opt out of the system/project:	X	
	No, individuals do not have the opportunity to opt out of the system/project.		

5.3 Please describe what, if any, procedures exist to allow individuals the opportunity to review or request amendment or correction of the PII maintained about them in the system/project.

Individuals can update their own information in the system. IMLS occasionally receives requests to update email addresses from individuals. Professional association lists are reviewed to ensure returned emails are accurate or determine if they need to be revised or removed.

Section 6. Privacy Act

6.1 Is a "system of records" being created under the Privacy Act?

The Privacy Act of 1974 defines a "system of records" as "a group of any records . . . 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."[3]

Yes, a "system of records" is created by this system/project.	
No, a "system of records" is not created by this system/project.	X

6.2 If you answered Yes to the previous question, please include a link to the system of records notice for this system/project. Or please indicate that we will need to create a new systems of records notice for this system/project.

[3] *See* Privacy Act of 1974, 5 U.S.C. § 552a(a)(5), https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf.

Section 7. Assessment Analysis

Constant Contact is a Software as a Service. While it is not FedRAMP certified the system does not contain information that is highly sensitive. The information contained within Constant Contact is the minimum PII required, an email address, for the agency to maintain connection with our constituents and professional audiences. IMLS has established appropriate security controls to protect the information contained within the system.