BUREAU OF EDUCATIONAL AND CULTURAL AFFAIRS

MONITORING, EVALUATION, LEARNING, AND INNOVATION UNIT

MELI UNIT DATA GOVERNANCE POLICY

FEBRUARY 2025

TABLE OF CONTENTS

DATA GOVERNANCE FRAMEWORK

"Data is a critical instrument of Diplomacy"
Department of State Enterprise Data Strategy 2021[1]

In line with the Department's recently released Enterprise Data Strategy's Goal 3 to Establish Mission Driven Data Management and Goal 4 to Enhance Enterprise Data Governance, the following Data Policy outlines the Bureau of Educational and Cultural Affairs' (ECA) Monitoring, Evaluation, Learning and Innovation (MELI) Unit's commitment to responsible data stewardship and approach to ensuring effective data management. For the MELI Unit, using data responsibly in public diplomacy monitoring & evaluation (M&E) requires balancing three overarching goals:

Supporting our ECA Colleagues:
The MELI Unit sees itself as a service provider to its ECA colleagues. In that role, we seek to ensure offices have the data necessary to make informed decisions about their programs and other bureau activities. Any data we collect should meet the purpose of supporting ECA's programmatic mission and the Federal Government for adequate data management.

Transparency with the Public:
In line with the Department's commitment to "operational excellence and... [to] leverage data to appropriately assess program effectiveness, pinpoint and mitigate areas of risk, and provide transparency to the public," ECA's MELI Unit works to promote transparency, accountability, and value creation by making government data (excluding Personally Identifiable Information [PII] pursuant to the Privacy Act of 1974) available to both internal and external stakeholders.[2] As a steward of public funds, the MELI Unit seeks to be transparent with its evaluation and research findings, maintain accountability to the U.S. taxpayer, and uphold the norms and scientific rigor in the research community of the

1. U.S. Department of State, Enterprise Data Strategy, 2021. Accessed September 20, 2021, https://www.state.gov/wp-content/uploads/2021/09/Reference-EDS-Accessible.pdf
2. U.S. Department of State, Enterprise Data Strategy, 2021. Accessed September 20, 2021, https://www.state.gov/wp-content/uploads/2021/09/Reference-EDS-Accessible.pdf

replicability of published results. The MELI Unit seeks to ensure that both internal and external stakeholders within the public diplomacy community[3], including researchers, policymakers, other agencies, or the general public, are able to analyze the same data used for ECA evaluation and research activities and reach the same results/conclusions. By expanding access to data and providing opportunities for re-analysis or even new avenues of research from our data collection, the MELI Unit can add value to policy-relevant discussions.

Protecting the Confidentiality of our Respondents:

The MELI Unit seeks to uphold the ethical guiding principle of the Department's Enterprise Data Strategy of responsibly collecting, securely storing, and utilizing data. The MELI Unit recognizes the need to reinforce the first two objectives with an obligation to protect the confidentiality and privacy of respondents who have participated in data collection efforts. We seek to ensure that:

- The privacy of respondents is protected, including securing safeguarding data in our possession and limiting what information is made public or utilized with artificial intelligence (AI) platforms, per Department of State's FAM policies on Data and AI.

- Respondents have a choice in the collection process through strict and clear informed consent procedures that make respondents fully aware of how their information will be used (including the potential use of AI platforms), stored, shared, and destroyed.

- Use of AI platforms will be limited to Department of State - approved AI platforms for analyzing data collected from respondents, which will be de-identified of any personally identifiable information (PII) before any AI use.

Underlying these objectives are the responsibilities the MELI Unit has:

- Meeting our legal and ethical commitments
- Managing our reputational risk (privacy breaches, etc.)
- Ensuring that adequate funding is available for data collection, analysis, and use
- Being good resource stewards through accountability, transparency, and using data to inform and improve our programs and bureau activities.

3. One of the five 'SAGES' (Sharing, Applied, Governed, Ethical, Secure) guiding principles in the Department's Enterprise Data Strategy includes the ethical collection, utilization and storage of data collected by the Department and observation of scientific rigor and integrity standards: "Data is responsibly collected, stored, and utilized to provide accountability to the U.S. taxpayer and uphold the highest levels of scientific and data integrity. Implementing leading industry standards in ethical data capabilities minimizes bias, fulfills the Department's obligations to the U.S. people, and models the importance of incorporating democratic values in technology on the world stage."

In balancing these objectives and responsibilities, the MELI Unit's data governance policies and procedures are guided by the following seven principles:

People first. All evaluation and research projects in which data are collected must apply American values as a fundamental right.

Beneficial purpose. There must be a clear purpose and value to the data collection.

Informed consent. Projects must always inform individuals of how and why their information is being collected and used, and do so in a way that is proactive, clear, and easy to understand. If a person opts-in to data collection that uses individual identification, that person must have a meaningful understanding of how the information is used. Any respondent must be granted the ability to opt-out of data collection at any point.

Data Transparency. Data collected is solely used to gain insights into how ECA's programs meet the objectives of public diplomacy priorities determined by the Department of State. Data analysis methods always include the MELI Unit and its approved contractors and could at times include use of Department of State approved AI tools, which will always include validation and review by a member of the MELI Unit.

Limiting personally identifiable information collection. If PII and/or other sensitive information are not needed, then they should not be included in the data collection.

De-identify[4] by default. Data collected that includes personal information must be "de-identified" by default, meaning designed to not be able to trace back to any individual. Once de-identified, a data set is considered to present a low risk of re-identification.

Open by default. De-identified data will be made available upon request to encourage innovation and reflect the role of MELI as a steward of public funds.

The ECA MELI Unit plans to revisit this policy at a minimum of every three years or as needed to ensure its alignment and compliance with Administration and Department-wide policies as well as federal regulation as they develop.

4. De-identified: A record in which identifying information such as names, address, email address, phone numbers, etc. are removed.

AUTHORITIES

This Data Governance Policy adheres to current available system security protection policies governed by the following acts, guidance, and Department of State Policies and handbooks, including:

- *The Privacy Act of 1974*
- *Memoranda 99-05 Attachment B, Privacy and Personal Information in Records Management*
- *5 FAM Information Management*
- *5 FAM 100 Information Technology Management*
- *5 FAM-400 Records Management*
- *5 FAH-400 Records Management Handbook5 FAH-3 H-210 Personal Names*
- *5 FAM 770, Federal Web Sites, 5 FAM 772 Privacy Principles for Federal Websites*
- *20 FAM 100, Data and Artificial Intelligence*
- *20 FAM 101, Guiding Principles, Scope, and Business Drivers*
- *20 FAM 102, Roles and Responsibilities (Data and AI)*
- *E-Government Act of 2002 (Public Law 107-347)*
- *Federal Information Security Management Act (FISMA) 2014*
- *Federal Information Processing Standards (FIPS) 199*
- *Federal Information Processing Standards (FIPS) 200*
- *5 FAM 1066 Office of Information Technology Security Compliance*
- *Security Authorization of Information Systems in Cloud Computing Environment (FedRAMP)*
- *Circular No. A-130*
- *Information Technology Reform Act (ITRA) / Clinger-Cohen Act*
- *NIST 800-53 Rev 5*
- *NIST 800-53rev5, Appendix J - Privacy Control Catalog*
- *12 FAM Diplomatic Security*

Additionally, to the extent possible, the MELI Unit will follow the special publications, guidance and best practices for federal data information management provided by the National Institution of Standards and Technology (NIST). These may include but are not limited to:

- *NIST 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- *NISTIR 8053, De-Identification of Personal Information*

SCOPE

This policy is intended to govern the MELI Unit's evaluation and research work, including the work conducted by external contactors on behalf of the MELI Unit. The Monitoring Data for ECA (MODE) Framework data is collected by ECA's implementing partners and therefore is not covered under the scope of this policy.

1 DATA COLLECTION

1.1 INFORMED CONSENT

Any data collection efforts undertaken by the MELI Unit or its contractors should include an informed consent process through which respondents are made aware of the data collection purpose, who will have access to this information, and confidentiality. Contractors may use their own informed consent statement; however, it must meet the following minimum requirements set out by the MELI Unit (see Annex A for an example that contractors may use):

- Explain the purpose of the data collection;
- State how long the data collection is expected to take;
- Explain how data will be used, shared, and stored (this is especially important for data collection efforts involving the collection of PII);
- Explain how data may be used with Department of State-approved AI platforms solely for data analysis purposes.
- Specify that participation in data collection is voluntary and/or outline associated risks or direct benefits of participating to the respondent;
- Provide contact information for questions or technical support; and
- Be written in language that can be easily understood by individuals for whom English is a second language or be translated into their native language.

1.2 PRIVACY ACT STATEMENT

Surveys or other data collection tools that collect PII or can otherwise be attributed to specific individuals using a unique identifier require the inclusion of a Privacy Act Statement. The Privacy Act applies to U.S. citizens and lawful permanent residents admitted for legal permanent residence. Therefore, a survey or any other data collection tool that

collects information from both U.S. and non-U.S. persons requires a Privacy Act Statement.[5] When a Privacy Act Statement is required, it should replace and incorporate relevant elements of the informed consent statement.

A Privacy Act Statement should include the following elements and, along with the tools, should be cleared by the Privacy Office (Privacy@state.gov). A sample Privacy Act Statement is available in Annex B. Privacy Act Statements must include:[6]

- Authority: The legal authority for collecting the information – statute, executive order, regulation.
- Purpose: The purpose(s) for collecting the information and how it will be used.
- Routine Uses: To whom the information may be disclosed and for what purposes.
- Disclosure (Mandatory or Voluntary): Whether providing the information is mandatory or voluntary. The effects, if any, of a respondent not providing the information – for example, the loss or denial of a privilege, benefit, or entitlement sought as a consequence of not furnishing the requested information.

1.3 DATA COLLECTION FROM MINORS

When collecting data from minors (under the age of 18 at the time of data collection), regardless of their nationality, consent must be obtained from the respondents' legal guardians. While ECA programs primarily target adults (over age 18), individuals under 13 should be excluded from ECA data collection efforts.[7]

1.4 PERSONALLY IDENTIFIABLE INFORMATION AND SENSITIVE INFORMATION MINIMIZATION

PII and/or sensitive information should not be included in data collection if not needed. The collection, storage, and duplication of PII and sensitive information should be limited to the minimum business need.

5. Please seek guidance from the MELI Unit on the use of Privacy Act Statements when collecting data from non-U.S. persons.
6. See Department Notice dated September 29, 2021 on Privacy Act Requirements: https://departmentnoticesprod-usdos.msappproxy.net/TodaysNotices/88461?origin=email.
7. While the age of consent varies by country, the MELI Unit's policy that legal guardians must provide consent for individuals under the age of 18 supersedes local regulations when the age of consent is younger than 18.

PII is any information that can be used, on its own or when combined with other information that is linked or can be linked to a specific individual, to identify, locate, or contact the individual. It includes:[5]

Direct Identifiers: such as the individual's full name, a mailing or home address, city of residence, dates relating to the individual such as date of birth, disability status, email address, telephone number, passport number, physical/biological identifiers[6] (physical appearance, through photo or video data collection, fingerprints, DNA, etc.).

Indirect Identifiers: Information that can be combined with other information to potentially re-identify a specific individual even when direct identifiers have been removed. For ECA, indirect identifiers include unique, observable or other characteristics such as program track, cohort year, age, and/or country of citizenship. The possibility of an indirect identifier being used to re-identify an individual increases when the respondent pool is small, for example collecting information on city and state of an exchange participant.

Sensitive data includes information that poses a risk to the individual or entity if it is collected or released in a way that it can be linked to a specific individual. This could include income, assets, or health status, the public release of which could harm survey respondents. Storage and management of PII is addressed in Section 5.

1.5 DATA SUBMISSIONS TO ECA'S MELI UNIT

Quantitative Data

Quantitative data collected by external contractors working on MELI-funded projects are required to be submitted to the MELI Unit upon project completion, per the terms of each project's contract. Quantitative data are not required to be collected anonymously; however, contractors are required to provide the MELI Unit with a de-identified dataset as a deliverable. This includes both data collected and supporting documentation, as listed below:

- Full de-identified survey datasets.
- Data dictionaries, including:
  - Codebooks
  - Data collection tools (questionnaires, interview guides, etc.)
  - Notes on data quality, data limitations, or data context
  - Data gathering methodologies
- Data de-identification process document

Qualitative Data

Given the resources involved in de-identifying qualitative data[8] and the limitations of de-identified qualitative data, in most instances the ECA MELI Unit does not require contractors to submit any focus group, interview transcripts, and open-ended survey responses collected outside of the MELI Unit's Qualtrics platform.

Furthermore, the Evaluation Manager, in concert with the Program Officer and the MELI Unit Chief, may in some cases make the determination that ECA has a legitimate business need for the raw qualitative data collected outside of our Qualtrics platform. In such cases, the contractor will be expected to include the necessary language in their informed consent form to permit sharing of the raw qualitative data with the MELI Unit in a de-identified format.

Social Media Data

Data collected via social media and/or open platforms on the worldwide web such as Twitter, Instagram, Facebook, blogs, forums, news outlets, and Tumblr will focus only on publicly available information. As these data are already in the public domain, contractors are not required to submit these data to ECA and are not subject to the de-identification requirements outlined above.

Data Collected through Qualtrics

In some cases, contractors may be asked to administer surveys through the MELI Unit's Qualtrics platform. When such cases occur, the contractor will be expected to include necessary language in their informed consent to allow the sharing of de-identified and/or anonymized survey data (both quantitative and qualitative) between the MELI Unit and the contractor.

8. https://www.reliasmedia.com/articles/141738-de-identifying-data-in-qualitative-research-is-complex-time-consuming

1.6 PUBLIC ACCESS TO ECA-COLLECTED DATA

In accordance with the Department's Enterprise Development Strategy SAGES' (Sharing, Applied, Governed, Ethical, Secure) first guiding principle on data stewardship and sharing and Objective 3.1, the ECA MELI Unit provides tiered access to its data both internally and externally to both enable additional and supplemental analysis and enhance the data's value. ECA MELI Unit-collected data and relevant supporting documentation will either be made publicly available or available upon request (see further details below). Prior to being shared either internally (other offices within the Department) or externally (entities outside the Department), data must undergo a review by the MELI Unit to ensure there is low risk of re-identification. The following rules to access data apply to all stakeholders both internal and external to the Department. Exceptions will be made for reports classified at the SBU level or higher in that these will not be released to the public.

10. The 'SAGES' (Sharing, Applied, Governed, Ethical, Secure) Guiding Principles support the overall data strategy by providing a clear value framework for prioritizing implementation activities and addressing challenges
that arise. These Guiding Principles were informed and validated by stakeholders across the Department.

Public Access (available on the MELI Unit website)

- Aggregate Data Summaries
- Final Evaluation Report
- General Research Reports
- Summary of Findings
- Infographic Reports
- Evaluation Statement of Work
- Questionnaires
- Interview Guides

Non-Public (currently available upon request)

- Evaluation Plans
- De-identified datasets (with accompanying codebooks and/or data dictionaries)
- Documentation on data quality, data limitations, or data context (should they not be included in any publicly available documentation)

No Access

This constitutes data that cannot be sufficiently de-identified, nor be made accessible through either public use or request-only access. This includes internal and external stakeholders.

- Qualitative data collected through Focus Group Discussions (FGDs) and/or Key Informant Interviews (KIIs).
- Qualitative data collected through open-ended survey questions.
- Quantitative datasets containing PII.
- Quantitative data tables with fewer than five respondents.
- MODE data, which is not covered under the scope of this policy. (This policy governs data collection activities undertaken directly by MELI and our contractors, and therefore the MELI Unit cannot provide access to MODE data collected by ECA's implementing partners.)

2 DATA QUALITY ASSURANCE AND REVIEW

All data submitted to the MELI Unit from contractors must meet the minimum standards, which are outlined below.

2.1 DATA QUALITY ASSURANCE

The MELI Unit maintains a continuous quality assurance process of its own data collection efforts as well as for all data collected by MELI Unit contractors. This includes reviewing contractors' sampling methodology, data collection instruments, and data collection procedures for soundness and rigor.

Each evaluation is assigned an Evaluation Manager who is responsible for ensuring that data are collected according to industry best practices and federal system compliance requirements. Internal data collection efforts are subject to a peer-review process as well as a final review by the MELI Unit Chief. Through these processes, the MELI Unit ensures that data collected under its purview meet the data quality standards of Validity, Reliability, Completeness, Timeliness, and Integrity.[11]

Data Quality Standard	How the MELI Unit Meets this Standard
Validity: the data mean what they are supposed to mean	Reviews data collection tools and methods to ensure that data collection tools ask the correct questions to gather data in line with the evaluation questions and that the data collection method is the best way to collect this information. Data collection instruments are pilot tested to ensure they are robust.
Reliability: the data are collected using the same procedures and definitions across collectors and sites.	In the case of multiple fieldwork sites, the MELI Unit ensures that evaluators use the same tools and processes for identifying respondents.

11. USAID TIPS: Data Quality Standards. 2009. Accessed February 20, 2020, https://www.fsnnetwork.org/sites/default/files/tips-dataqualitystandards.pdf

Data Quality Standard	How the MELI Unit Meets this Standard
Completeness: the data are sufficient to represent the activity, population and/or sample	Reviews data collection sampling methods and response rates. Data collection efforts undertaken on MELI's behalf are required to meet the minimum response rates outlined in the SOW.
Timeliness: the data are available at a useful frequency and are available when needed for management decisions	The MELI Unit ensures that data are used within a designated period of time so that it will still be relevant and of value.
Integrity: data are protected from transcription errors or data manipulation	The MELI Unit requires that evaluation contractors submit de-identified quantitative data files and raw qualitative data files (when there is a legitimate business need), codebooks for cleaning and analysis. Additionally, fieldwork by contractors is overseen by the Evaluation Manager for quality assurance.

The MELI Unit strives to ensure the highest quality of data given its available resources. In some cases, simpler, lower-cost approaches may be more appropriate. In other cases, where data measure performance in major areas of investment, higher data quality is required.

2.2 DATA DISPOSISTION

ECA evaluation contractors are required to destroy any datasets (quantitative, qualitative, and/or contact information) containing PII data within two years of evaluation project completion (or based on bureau policy) and send a confirmation email to both the Evaluation Manager and the MELI Unit Chief confirming deletion/destruction of the data. Note: De-identified datasets are exempt from this requirement. The MELI Unit will maintain data collected via discrete research projects and evaluations indefinitely, in line with the General Records Schedule. The MELI Unit will also maintain a catalog of its available data, its provenance, variables, etc. This does not apply to MODE Framework data collected by award recipients.

3 GUIDELINES FOR DE-IDENTIFICATION

Any data shared outside of ECA is required to be de-identified. In some cases, datasets will be de-identified by the MELI Unit, in others by the contractor directly responsible for the data collection. Below are guidelines for data handlers to help ensure that all datasets are anonymized based on the same standards. The MELI Unit will not share data collected by award recipients requested as part of the background information for an evaluation. To obtain award recipient data, data requestors should contact the award recipient directly.

3.1 STRIPPING DIRECT IDENTIFIERS AND SENSITIVE INFORMATION

As a first step in anonymizing data, data handlers should identify any data that can or cannot be released publicly due to privacy concerns. At a minimum, data should be stripped of any direct and sensitive information (de-identification). This includes the following information:

- Name
- Email Address
- Physical Address
- Date of Birth
- Photos
- Driver's License and/or Passport Number
- SEVIS number, if applicable

Information such as program track and year, home country/state, and age are not considered direct identifiers or sensitive information and thus are acceptable to keep in a dataset in most cases. However, the possibility of an indirect identifier being used to re-identify an individual increases when the survey sample is small. Prior to any data being released/shared externally data shall be reviewed by the ECA MELI Unit to determine whether any indirect identifiers should be removed or recoded (see section 3.2 on de-identification and recoding data).

Additionally, any open-ended survey responses will be removed if sharing externally; when sharing internally (i.e., outside the MELI Unit, but within the Department of State), identifiable information from open-ended responses such as names, places, and organizations shall be removed.

3.2 DE-IDENTIFICATION OF INDIRECT IDENTIFIERS

Data handlers are encouraged to document a de-identification strategy early, keeping in mind that data from which PII have been removed can be "re-identified" by combining them with other data sources. For example, administrative program records could be combined with survey data, which contains program location to re-identify specific individuals. Data handlers should consider the following approaches, in addition to data de-identification, in order to minimize respondent re-identification risk.

- Generalization: reporting values within a range or as a member of a set, rather than the exact value.
- Perturbation: replacing all values in a manner that is consistent for each data subject, within a defined level of generalization.
- Swapping: exchanging values among records, with a defined level of generalization
- Recoding: reduces the number of unique combinations, by combining or grouping categories and groups.
- Aggregate or reduce the precision of variables
- Top-/bottom-code outliers
- Removal of individual variables and local suppression (only when absolutely necessary): data handlers should consider the removal of any specific data points or variables (for example, open-ended text responses) that could permit re-identification.

3.3 BALANCING ANONYMIZATION AND DATA INTEGRITY

In some cases, anonymizing the data would require steps that jeopardize data integrity and validity, the MELI Unit reserves the right not to make the data publicly available in such cases.

4 DATA REQUESTS

4.1 SUBMITTING DATA REQUESTS

Evaluation and research dataset requests can be made directly to the MELI Unit by emailing ECAevaluation@state.gov. See section 4.2 for details on what these requests should include and Annex C and the MELI Unit's website for a Data Request Form. The MELI Unit prohibits recipients from any attempts to re-identify data subjects.

4.2 REQUESTING ACCESS TO ECA DATA

The MELI Unit will review each data request to ensure the rights and privacy of respondents are protected. Only de-identified data may be shared with external public and private sector institutions (e.g., outside ECA and DoS). The request should detail:

- The project title
- The researchers and their affiliations
- The requested dataset(s)
- The research purpose (including whether the researcher intends to attempt to publish) and plan
- Anticipated duration of project and timeline
- A data security plan (i.e., how the requestor plans to safeguard the data)

Data shared externally will be de-identified and sensitive information will be removed.

While any party can request datasets from the MELI Unit, all requests will be assessed based on the following:

- Risk of re-identification
- Request scope
- Intended data use
- Data security policies and data protection precautions outlined in the request
- Commitment not to use data for financial gain

ECA requires that Data Request Forms (see Annex C) be signed by the data requestor. In some cases, which are outlined below, countersignatures will be required:

- Student researchers: an advisor and/or an employee of the university will be required to countersign.
- Researchers: The chair of the IRB that approved the research will be required to countersign (as applicable).
- Journalists: an organizational representative will be required to countersign.

The Data Request Form should be reviewed by a member of the MELI Unit to determine risk of re-identification and safety precautions. The request should be cleared by:

1. A member of the MELI Unit
2. The MELI Unit Chief
3. The relevant Program Office Director

4.3 DATA SECURITY BY DATA REQUESTORS

The Data Requestor will not in any manner, directly or indirectly, make known, disclose, publish or communicate the dataset itself, or any part thereof to any person, firm, or organization without the express written consent of the MELI Unit.

Any summary results, however, can be shared. Summary results are those items which cannot be used to identify an individual. It should be noted that the stripping of an individual's name or individual identification number does not preclude the identification of that individual, and therefore stripping of the limited information does not constitute "sufficient protection" to protect the confidentiality of an individual's data, additional security measures must be taken to protect the information dataset(s).

4.4 PERMISSIBLE USE OF DATA

Recipient organizations may use data in the following ways:

- Data may not be released by a recipient organization without permission from the MELI Unit.
- Recipient organizations will be required to meet basic security requirements as outlined in Section 5.
- Any analysis/reports written using the shared data may be published without express permission of ECA; however, it is requested that analyses and published reports be shared back with ECA.

5 SECURITY

This section outlines security controls used by the MELI Unit to protect the data it manages. "Management" refers to both storage and processing of data by the MELI Unit.

5.1 LOCAL STORAGE

Department Computers
Most data held by the MELI Unit are managed on U.S. Department of State (DOS) computers, on which team members are permitted to manage both anonymized datasets and those containing PII or sensitive information.

Personal Computers
Team members may manage anonymized datasets on their personal computers. However, datasets containing PII or sensitive information may not be downloaded to personal computers. In alignment with Department Foreign Affairs Manual (FAM) 12 FAM 544.3 Electronic Transmission Via the Internet:
All users who process SBU information on personally owned computers must ensure that these computers will provide adequate and appropriate security for that information. This includes:
(1) Disabling unencrypted wireless access;
(2) The maintenance of adequate physical security;
(3) The use of anti-virus and spyware software; and
(4) Ensuring that all operating system and other software security patches, virus definitions, firewall version updates, and spyware definitions are current.

5.2 CLOUD STORAGE AUTHORIZATION

While most data are managed locally, the MELI Unit utilizes some online platforms.

Per Office of Management and Budget (OMB) regulations, any online platform used by the Federal Government must be authorized by the U.S. Federal Risk and Authorization Management Program (FedRAMP) authorized. FedRAMP was established to provide a standardized approach for assessing, monitoring, and authorizing cloud computing services under the Federal Information Security Management Act (FISMA) and to accelerate the adoption of secure cloud solutions. The FISMA process, but not the underlying standards themselves, was replaced by FedRAMP in 2011. The National Institute of

Standards and Technology (NIST) 800 – 53 sets the standard and FedRAMP is the program that certifies that a cloud service provider meets the standard.

FedRAMP-authorized platforms currently in use by the MELI Unit include:

- MS Teams/Sharepoint: The MELI Unit utilizes these platforms for internal collaboration, which may include sharing datasets between team members (Note: these are not platforms used to share datasets with external stakeholders)
- Qualtrics: The MELI Unit's survey platform, which collects and stores survey data.
- Foreign Affairs Network (FAN) Google Workspace: The Department of State's enterprise implementation of Google Workspace for Government, which allows the MELI Unit to share documents with external contractors, including datasets which may contain PII or sensitive information. Members of the MELI Unit can request a FAN.gov account by completing this form: https://seirmprod.servicenowservices.com/dos?id=sc_cat_item&sys_id=3b27cba71bde5450b38a10ad9c4bcb77

Additionally, FISMA mandates Agency Authority to Operate (ATOs) for all systems wherein Federal Data is managed. ATOs are required of FedRAMP systems. FedRAMP is a critical requirement in the selection of cloud systems to ensure minimum federal security controls outlined within FIPS 199, 200, and NIST 800-53. However, FedRAMP is not the exclusive security authorization requirement, through the selection of a FedRAMP vendor, agency efficiencies are gained supporting the processing times of ATOs. Agency ATOs are supported initially through Bureau Information System Security Officers (ISSOs). ECA's Executive (EX) Office, Information Technology (IT), Security and Governance (SG) Branch ISSOs are the authorized personnel supporting the Department IRM Cyber Operations (CO) Agency ATO process. Additional details aligned to Agency vs FedRAMP responsibilities can be found at the following link in general terms: https://www.fedramp.gov/assets/resources/documents/Agency_Authorization_Roles_and_Responsibilities_for_FedRAMP_CSPs_and_Agencies.pdf

5.3 PASSWORD PROTECTIONS

Per department regulations, the MELI Unit has safeguards in place to protect the confidentiality of stored data. These include:

- Password protections on all data management systems
- All data files are saved on the ECA MELI shared drive, which is accessible only through a DoS password-protected computer and/or remote access (also password and keycard protected). The ECA MELI shared drive is only accessible to members of the MELI Unit.
- Data files containing sensitive information and requiring an additional layer of security should be password protected by the Evaluation Manager. The password should be shared with the MELI Unit Chief.

5.4 RESTRICTIVE ACCESS

Per Privacy Act requirements, access to any PII or sensitive information held by the MELI Unit is restricted to those with a business need-to-know. Those who have a need-to-know include the members of the MELI Unit and the MELI Unit Chief.

5.5 REQUIREMENTS FOR EXTERNAL CONTRACTORS

Data Policies
External contractors working on MELI-funded projects are required to have organizational data management policies. The MELI Unit reserves the right to request and review these policies to ensure they meet MELI's standards.

6 SPECIAL CONSIDERATIONS

6.1 GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR is a regulation in European Union (EU) law on data protection and privacy, whose primary aim is to give control to individuals over their personal data and to simplify the regulatory environment for international businesses by unifying the regulation within the EU. ECA grantees operating in the EUR region have occasionally noted that, because of GDPR, most of the countries have strict laws about maintaining databases of personal information and even more so in supplying that contact information to "third parties" (the evaluation firms) without the consent of each person.

GDPR's Applicability

- **DOES** apply when American organizations based in the EU are sharing personal data of EU participants with the USG (either Embassies or ECA). Example: An American implementing partner operating in the Ukraine cannot provide contact information of Ukrainian participants to ECA without prior consent from the participants.
- **DOES** apply when a U.S. Embassy based in the EU provides information to an external party. Example: The U.S. Embassy in Germany cannot provide contact information of German program alumni to a MELI contractor without prior consent from the alumni.
- **DOES** apply when American organizations (on behalf of the USG) are collecting data on participants within the EU. Meaning that a MELI Contractor collecting data within the EU (either in-person or remotely) must follow all GDPR regulations related to data privacy and protection.
- Does **NOT** apply if a U.S. Embassy within the EU provides information to ECA (USG to USG). Example: The U.S. Embassy in Serbia can provide contact information for ECA alumni to the MELI Unit without prior consent of the alumni. MELI can then use that contact information for evaluation purposes.
- Does **NOT** apply if ECA provides data for EU participants to US-based entities (such as external evaluation firms). Example: The MELI Unit provides contact information for Belgian participants from an internal ECA source.

Data Collection Considerations [12]

For ECA evaluations and research projects, this means that data collection occurring within the EU will require alumni to opt-into any data collection efforts, either by:

- Asking for Program Officers/Embassy to send emails to participants to request they opt-in to the evaluation by providing their contact information back to the Program Officer/Embassy; or
- [Preferably] Collecting opt-in consent and contact information via a survey (so as to reduce the burden on embassies if the number of participants is large).

12. Please consult the MELI Unit to discuss data collection in the EU further.

When collecting opt-in consent via survey, the evaluation firm should request that the Program Office/Embassy email the survey to alumni with the following language appended to any general consent language used for the survey: By filling in this form and clicking the option "DONE", I hereby give my consent to XX, a private research firm based in the United States, to process my personal data, provided in this form, for the purposes of [EVALUATION]. I am aware of my rights under the European Union's General Data Protection Regulation, including the right to withdraw my consent to the processing of my personal data by emailing [EMAIL].

It is also an option to ask the U.S. Embassy to distribute any surveys or other electronic data collection tools directly to their contacts. This can be done in-lieu of having alumni opt-into data collection efforts.

6.2 COLLABORATING WITH INTERNS

Interns working with MELI from their personal device (i.e. virtual interns) are only permitted to work with anonymized datasets. They may not access PII or other sensitive information. Interns working with MELI from a government-issued device (i.e. in-person interns) must follow the security measures outlined in this document and Department policy when accessing PII data or sensitive information.

ANNEXES

ANNEX A: CONSENT LANGUAGE

The below consent language is a starting point for you to work from. We have indicated places where you can make adjustments to this language and where you must include the language as written. All adjustments must be cleared by your evaluation manger.

[CONTRACTOR], an independent third-party evaluation firm, has been contracted by the U.S. Department of State to conduct an evaluation of the [PROGRAM] to assess the effectiveness of the program to date and to provide recommendations to strengthen the program in the future. As [STAKEHOLDER TYPE] of the program, your unique perspectives will assist us in understanding the impact of [PROGRAM].

The survey contains [XX] questions and should take [XX] minutes (average) to complete.

Please note that your participation in this survey is voluntary, and you are free to end the survey at any time. By clicking the "Consent and enter survey" button below, you are consenting to the following terms:

- Your participation in this evaluation is voluntary. We do not anticipate that participating in this evaluation will result in any risks or direct benefit to you. However, your inputs may lead to recommendations that benefit the [PROGRAM]—and, thereby, the general public. You may skip any questions you are not comfortable answering.
- The information that you provide in the survey will be used to write a report. This report will be shared with the U.S. Department of State and other stakeholders for comment and will eventually be made public. Any responses you provide may be reported in the final report as part of the anonymized aggregated quantitative analysis or the qualitative analysis from open-ended responses, with all personal identifying information removed.
- The U.S. government and its contractors will take reasonable measures to protect privacy data, personally identifiable information, and other sensitive data obtained from the survey.
- Responses to questions other than those about your connections with others may be reported by demographic category (i.e., field of study, employment status), country, or cohort year. The only identifying information used will be the demographic information collected in [section number or set of questions] of the survey.

- As this evaluation requires us to speak with a broad range of program alumni, we may ask you to share contact information for the connections that you mention in the cases where we do not already have updated or valid contact information for these parties. As with all other questions, you may skip or decline to answer any questions you are not comfortable answering.
- Updated contact information may be shared with the U.S. Department of State and [IMPLEMENTING PARTNER(S)] upon completion of this survey.
- The data you provide may be reanalyzed at a later date for a follow-up study or other purpose approved by the U.S. Department of State. The data may be made available to third parties as required by law.
- You may withdraw your consent at any time by contacting ECAEvaluation@state.gov.

ANNEX B: SAMPLE PRIVACY ACT LANGUAGE

AUTHORITY: The information on this form is requested under the authority of 22 U.S.C. 2451 et seq (Mutual Educational and Cultural Exchange Act of 1961), P.L. 103-62 (Government Performance and Results Act of 1993), and P.L. 111-352 (Government Performance and Results Modernization Act of 2010).

PURPOSE: The purpose of gathering this information is to track the networks and relationships built as a result of participation in the [PROGRAM].

ROUTINE USES: The information on this form may be shared with members of Congress, and the Office of Management and Budget (OMB). De-identified data files may be shared (without Personally Identifiable Information such as names or contact information) with ECA implementing partners and external researchers who are assisting ECA in measuring its impact. More information on the Routine Uses for the system can be found in the System of Records Notice State-08, Educational and Cultural Exchange Program Records.

DISCLOSURE: Responding to this survey is voluntary. The answers you provide on the survey will have no bearing on your participation in future program activities or any future applications you may submit for U.S. State Department programs.

If you have any questions about this survey or the [PROGRAM] evaluation more broadly, you can contact [INDIVIDUAL] at [EMAIL].

CONSENT TO PARTICIPATE

By clicking the button to begin the survey below, you are giving your consent to participate in this evaluation. If you do not wish to participate, please click the exit survey link below.

- Consent and enter survey
- Decline and end survey now

ANNEX C: DATA REQUEST FORM

MELI Unit Data Request Form
Draft, [INSERT DATE HERE]

This form should not exceed 10 pages once complete.

[PROJECT TITLE]

Data Requestors
List all individuals who will have access to these data. Please also list their affiliation, contact information, and their role on the project.

Requested Datasets
List all requested datasets here.

Project Purpose and Plan
This section should provide an understanding of the research questions, why these questions are of importance to the Bureau of Educational and Cultural Affairs' MELI Unit, the methodology that will be used, and how the requested data will be used for the project. This section can be used as a form of proposal, explaining the research, how it will be conducted, and its importance.

Anticipated Duration of Project and Timeline
The proposed duration of the project is [X] months.
Use the table below to further detail the timeline. The timeline should include activities such as cleaning data, merging data, conducting specific analyses, and estimated timeframe for dissemination, such as publications, presentations, or any public use products. You are encouraged to attached additional documentation of needed.

Data Security Plan
This section should provide an understanding of how the data requestor plans to manage the data upon receipt, how the data will be stored, who will have access to the data, and what (if any) data will be included in any publications, presentations or any public use products.

Institutional Review Board

Will your project plan be reviewed by an Institutional Review Board (IRB)? YES ___NO ___

Data Protection Statement

I, [Name(s) of Data Requestor(s)] will not in any manner, directly or indirectly, make known, disclose, publish or communicate the dataset itself, or any part thereof to any person, firm, or corporation without the express written consent of the MELI Unit.

I [Name(s) of Data Requestor(s)], will not attempt to re-identify data subjects, including linking this dataset to external data and sharing data without permission.

I, [Name(s) of Data Requestor(s)] shall not retain any copies of such data, or any part thereof (such as subsets).

I hereby certify that, to the best of my knowledge, the provided information in this Data Request form is true and accurate. By signing below, I agree to the terms of the above outlined data protection statement.

Data Requestor(s) Signature

Additional signature lines may be added as needed.

_____	_____
Name	*Date*
_____	_____
Name	*Date*
_____	_____
Name	*Date*

Signature of Academic Advisor

If one or more Data Requestor(s) is a student at an Academic Institution

Name	*Date*

Signature of Institutional Review Board Chair

If project was submitted to an IRB review

Name	*Date*

Signature of Organizational Representative

If requestor is from a non-academic organization

Name	*Date*

To be completed by ECA:

- Who "owns" the data? Was the data collection purely ECA-financed? Or was it done in partnership with another entity (government, implementing partner, other researchers)?
- Was the data collected under any IRB review/clearance? (If applicable) Does the original IRB review/clearance provide for data sharing?
- Does the informed consent language place any limitations on sharing this data?
- What harm (if any) could arise to respondents if these data were to be released?

ECA Decision: **Approved** _____ **Not Approved** _____

ECA Signature

_____ _____

Name *Date*

ABOUT THE MONITORING, EVALUATION, LEARNING, AND INNOVATION UNIT

The Bureau of Educational and Cultural Affairs' (ECA) Monitoring Evaluation Learning and Innovation (MELI) Unit has been at the forefront of the Department of State's monitoring and evaluation (M&E) efforts since its creation in 1999. Throughout its 20 years, the MELI Unit has built a robust M&E system to ensure that ECA program staff and senior leadership benefit from timely performance data that they can utilize for evidence-based decision-making.

For a complete listing of ongoing evaluation projects, an archive of completed reports, and resources for conducting evaluations, visit the MELI Unit's website: https://eca.state.gov/impact/eca-evaluation-division

If you would like additional information or have any questions, please contact us at ECAevaluation@state.gov

MELI
Monitoring. Evaluation.
Learning. Innovation.