PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

Date of Issuance: 09-30-2024

Control Number: PGLD-10-0924-0020
Expiration Date: 09-30-2026
Affected IRM(s): 10.5.1

MEMORANDUM FOR ALL OPERATING DIVISIONS AND FUNCTIONS

FROM: Gregory T. Ricketts */s/ Gregory T. Ricketts*
Acting Director, Privacy Policy and Compliance

SUBJECT: Privacy Policy for Artificial Intelligence

This memorandum issues privacy policy interim guidance on artificial intelligence and is effective as of September 30, 2024. Please distribute this information to all affected personnel within your organization.

**Purpose:** This interim guidance implements privacy policy related to IRS use of Artificial Intelligence (AI). This guidance adds a new subsection that provides context for applying the existing IRS Privacy Principles when using AI. For an overarching IRS AI policy and definition, refer to IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles (and related interim guidance), published as Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles.

**Background/Source(s) of Authority**: This interim guidance falls under the authorities listed in the Authority subsection of IRM 10.5.1, Privacy Policy. It implements privacy application of Executive Order (EO) 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, EO 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, and OMB M-24-10, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence.

**Procedural Change:** The procedural changes in the attached interim guidance apply.
**Effect on Other Documents**: We will incorporate this interim guidance into IRM 10.5.1, by September 30, 2026.

**Effective Date:** September 30, 2024

**Contact:** If you have any questions, please email the Associate Director, Privacy Policy, at *Privacy.

**Distribution:** FOIA Library (external) on IRS.gov.

**Attachment Interim Guidance:** PGLD-10-0924-0020

**Interim Guidance:** PGLD-10-0924-0020

**The following changes take effect** September 30, 2024**, for** IRM 10.5.1.

**10.5.1.6.22**
**(09-30-2024)**
**Artificial Intelligence**

(1) This policy outlines privacy requirements and considerations for IRS use of artificial intelligence (AI) and applies to IRS users, developers, and providers of AI. It links the IRS Privacy Principles, from IRM 10.5.1.3.2, to key AI policy and requirements based on Executive Orders, Treasury Directives, and related IRMs.
**Note**: For an overarching IRS AI policy and definition, see IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles, published as Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles.
(2) As EO 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, points out, "Artificial intelligence (AI) holds extraordinary potential for both promise and peril." All IRS personnel must follow the IRS Privacy Principles to manage the promises and perils of AI use.
(3) IRS privacy policy is technology neutral, meaning that these principles apply to any technology. This policy is for any design, development, acquisition, or use of AI (hereafter referred to as AI use), whether a web-based online form, commercial-off-the-shelf (COTS) product or service, custom built IRS tool, or any other use case. This policy applies to associated technology that may not meet the IRS definition of AI. Examples of AI or associated technology include, but are not limited to:
    - Generative AI
    - Predictive AI
    - Machine Learning (ML)
    - Large Language Models (LLM)
    - Voicebots and chatbots
    - Robotic Process Automation (RPA)

    **CAUTION**: AI capabilities often appear as part of many other tools, applications or commercial, off the shelf (COTS) products, without expressly being identified as an AI.
(4) Use of AI may create new privacy risks or exacerbate privacy risks present in other systems. When using AI, you must consider the relationship between AI and privacy risks, such as collecting more data than is necessary, improper disclosure, misuse, and even aspects of bias that may impact privacy and civil liberties. Use privacy enhancing technologies (PETs), where possible, to protect privacy. [EO 14110]
(5) Use only IRS-approved AI that adhere to AI risk management, privacy, and security. Refer to IRM 10.24.1.10, Privacy and Security Requirements, published in Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles.

(6) You are responsible for the information you share when using AI, just as you are responsible for the information you share in a conversation or email. This includes considering how the AI might use the information later. Treat AI as another person and follow authentication, authorization, and need to know. Do you know who they are? Are they authorized to see the information? Do they have a need to know? If not, don't share it. Refer to paragraph (3) of IRM 10.24.1.6, AI Sharing and Collaboration, published in Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles.
(7) IRS personnel who manage contracts must make sure that contractors follow this policy. Contractors that use AI must meet all applicable privacy, security, and AI risk management requirements and pass them on to subcontractors.
(8) System owners and authorizing officials must have written documentation concerning how their use of AI meets all IRS Privacy Principles. The required Privacy Threshold Assessment (PTA) and Privacy and Civil Liberties Impact Assessment (PCLIA), as well as other OneSDLC artifacts, address this documentation. For more information on PCLIAs, refer to IRM 10.5.2; and for more information on AI risk assessments, refer to IRM 10.24.1, published in Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles.
(9) The protections required by IRM 10.5.1.8, NIST 800-53 Security and Privacy Controls, also apply to uses of AI.

**10.5.1.6.22.1**
**(09-30-2024)**
**Accountability for AI**

(1) IRS users, developers, and providers of AI are responsible for the effective implementation of privacy protections. Whether you are buying or developing a new AI or are the end-user of an application or web service, you must understand how to use the AI so that you protect the information it uses.
(2) IRS personnel who manage contracts must make sure that contractors follow this policy. Contractors that use AI must meet all applicable privacy, security, and AI risk management requirements and pass them on to subcontractors.
(3) The AI principle from EO 13960 of "Responsible and traceable" aligns to the IRS privacy principle of accountability by requiring agencies to clearly define, understand, and assign human roles and responsibilities for AI use. These roles, responsibilities and system use plans should be well documented and traceable.
(4) See IRM 10.5.1.3.2.1, Accountability. Also refer to IRM 10.24.1.8.1, AI Impact Assessment, published in Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles.

**10.5.1.6.22.2**
**(09-30-2024)**
**Purpose Limitation for AI**

(1) IRS may only use data for the purpose we originally collected it. IRS may only use AI to analyze data when the analysis supports the need originally described at the time of collection. The purpose may be broad, such as “tax administration,” which means the use must align to a defined tax administration purpose.
    Example: The IRS can use line-item values to process a tax return (tax administration), but we may also use that data (along with other taxpayers' data) to detect potential noncompliance or fraud (also a tax administration purpose).
(2) Do not use sensitive but unclassified (SBU) data (including PII and tax information) to train public AI models. Refer to IRM 10.24.1.6, AI Sharing and Collaboration and its subsections, published in Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles.
(3) The EO 13960 AI principle “Purposeful and performance-driven” tells agencies to carefully consider the risks when looking for opportunities for AI use. Before AI use, the IRS assessment of the risks, described in IRM 10.24.1.8.1, AI Impact Assessment (published in Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles), should include a complete description of the purpose for which we will use the AI and what data the AI uses. By doing a proper risk assessment for your AI, you will limit the use to a legitimate business purpose that can increase the performance of your programs without jeopardizing privacy.
(4) See IRM 10.5.1.3.2.2, Purpose Limitation.

**10.5.1.6.22.3**
**(09-30-2024)**
**Minimizing Collection, Use, Retention, and Disclosure for AI**

(1) Many AI models have the capability to intake, keep, and reuse data. Minimize the collection, use, retention, and disclosure of data in AI to what is specifically relevant and necessary. Take steps to understand how AI might redisclose data and share only what is necessary for your task. When developing an AI model, build in safeguards that guide users how to minimize data and to prevent its improper disclosure.
(2) Do not allow use SBU data (including PII and tax information) to train public AI models. Refer to IRM 10.24.1.6.5, Unintended Disclosure of Data from AI Models, published in Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles.
(3) For more information about disclosure policy, refer to the IRM 11.3 series. For more information about reporting incidents, refer to IRM 10.5.4.
(4) The EO 13960 AI principle “Lawful and respectful of our Nation's values” tells agencies to use AI in a way that is consistent with our values and the Constitution, and that addresses privacy.
(5) See IRM 10.5.1.3.2.3, Minimizing Collection, Use, Retention, and Disclosure.

**10.5.1.6.22.4**
**(09-30-2024)**
**Openness and Consent for AI**

(1) In the context of AI, the IRS privacy principle of openness includes the ability to understand how the AI made the decision. As much as practical, without unduly exposing sensitive information, describe the AI decision-making process in the privacy documentation, such as a PCLIA or AI risk assessment. This documentation informs individuals about the uses to which they consent when they provide data.
(2) For more information on the AI risk assessments, refer to IRM 10.24.1.8.1, AI Impact Assessment, published in Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles.
(3) The EO 13960 AI principle “Transparent” requires agencies to be transparent in showing relevant information about their use of AI. When AI use is appropriately transparent, it protects privacy.
(4) During the development of AI, consider allowing users to opt out of having their information included in the AI, where practical.
(5) See IRM 10.5.1.3.2.4, Openness and Consent. Also refer to IRM 10.24.1.8.14, Opt Out Options, published in Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles.

**10.5.1.6.22.5**
**(09-30-2024)**
**Strict Confidentiality for AI**

(1) IRS users, developers, and providers of AI must protect data and share it only with authorized individuals and systems.
(2) EO 14110 says AI’s capabilities can increase the risk of personal data exploitation and exposure. To combat this risk, the agencies must make sure that the AI use is lawful, secure, and mitigates privacy and confidentiality risks.
(3) With AI use, make sure the data you share is only accessible by those with a need to know (including other systems). Make sure safeguards are in place to purge data or otherwise prevent re-disclosure after the authorized AI use.
(4) You are responsible for the information you share when using AI, which includes considering how the AI might use the information later.
(5) See IRM 10.5.1.3.2.5, Strict Confidentiality.

**10.5.1.6.22.6**
**(09-30-2024)**
**Security for AI**

(1) AI requires special attention to make sure that developers build it to protect the administrative, technical, and physical access to the system and its data. Use only IRS-approved AI that adhere to AI risk management, privacy, and security policies.

(2) AI use cases must follow all relevant IRS privacy and security policies, such as those in IRM 10.24.1 (published in Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles), and the IRM 10.8 series.
(3) The EO 13960 principle “Safe, secure, and resilient” requires agencies to ensure the safety, security, and resiliency of their AI applications.
(4) For AI use, take steps to ensure the security of the system and the data it uses. For more information, refer to National Institute of Standards and Technology (NIST) AI 100-1, Artificial Intelligence Risk Management Framework (NIST AI 100-1), with further details in IRM 10.8.1 and IRM 10.5.1.8, NIST 800-53 Security and Privacy Controls.
(5) See IRM 10.5.1.3.2.6, Security.

**10.5.1.6.22.7**
**(09-30-2024)**
**Data Quality for AI**

(1) Because many types of AI keep data for future uses, make sure that the data used by AI is accurate, complete, and current. As much as possible, use data collected directly from the individual to whom it relates.
(2) To help ensure data quality, review the results for improper biases that impact rights, such as civil liberties, whether the result of human inputs or generated from the AI’s misunderstanding of the data or directives given to it.
(3) The EO 13960 principle “Accurate, reliable, and effective” instructs agencies to make sure that their application of AI is consistent with the use cases for which that AI was trained, and such use is accurate, reliable, and effective.
(4) See IRM 10.5.1.3.2.7, Data Quality. Also refer to IRM 10.24.1.8.2, Real-World Performance Testing, published in Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles.

**10.5.1.6.22.8**
**(09-30-2024)**
**Verification and Notification for AI**

(1) Verify and validate data with AI use as much as possible, including the source of the data. Verification includes leveraging a human review process before taking adverse action based on that data. Where practical, let individuals know about AI use when you collect their data and how to contest inaccurate information. [OMB M 24-10]
(2) The EO 13960 principle “Regularly monitored” expects agencies to make sure they regularly test their AI applications against these principles and stop the use of any AI that does not perform as intended.
(3) See IRM 10.5.1.3.2.8, Verification and Notification. Also refer to IRM 10.24.1.8.8, Public Notice and Plain Language Documentation and IRM 10.24.1.8.13, Human Consideration and Remedy Processes, published in Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles.

**10.5.1.6.22.9**
**(09-30-2024)**
**Access, Correction, and Redress for AI**

(1) With AI use, you must be able to give individuals access to and the ability to correct their PII upon request where practical. Programs and processes that use AI must make sure individuals can contest determinations made based on allegedly incomplete, inaccurate, or out-of-date information.
(2) The OMB M-24-10 practice of “Maintain human consideration and remedy processes” tells agencies to include a human in the correction and redress process for uses of rights-impacting AI. Refer to IRM 10.24.1.8.13, Human Consideration and Remedy Processes, published in Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles.
(3) See IRM 10.5.1.3.2.9, Access, Correction, and Redress.

**10.5.1.6.22.10**
**(09-30-2024)**
**Privacy Awareness and Training for AI**

(1) IRS users, developers, and providers of AI must remain current with IRS privacy and awareness training requirements. IRS personnel who use AI should make sure they have current guidance and training on how to effectively apply the privacy principles when using AI. As such, you are responsible for protecting the privacy of individuals whose data the AI uses.
(2) Likewise, the IRS must make sure that AI training follows the privacy principles in its analysis, storage, and use of data. A best practice includes using privacy enhancing technologies and techniques to train AI to follow IRS Privacy Principles. [NIST AI 100-1]
(3) The EO 13960 principle “Accountable” states that agencies must provide training to all agency personnel responsible for AI use.
(4) See IRM 10.5.1.3.2.10, Privacy Awareness and Training. Also refer to IRM 10.24.1.8.6, Human Training and Assessment, published in Interim Guidance for New IRM 10.24.1, Artificial Intelligence (AI) Governance and Principles.