PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

August 29, 2017

Control Number: PGLD-10-0817-0002
Expiration Date: 08-29-2019
Affected IRM: 10.5.1

MEMORANDUM FOR DISTRIBUTION

FROM: Frances W. Kleckley */s/ Frances W. Kleckley*
Director, Privacy Policy and Compliance

SUBJECT: **1. Digital Assistants and Other Devices**
2. Chief Privacy Officer Title Change

This memorandum issues privacy policy in IG# PGLD-10-0817-0002, guidance on **1. Digital Assistants and Other Devices and 2. Chief Privacy Officer Title Change** until IRM 10.5.1 is published. Please ensure that this information is distributed to all personnel responsible for protecting SBU data, including tax information and PII. The policy applies to all employees, contractors, and vendors of the Service.

Purpose:

1. The interim guidance (IG) provides specific policy regarding methods for protecting privacy when working around digital assistants and other devices that can record and/or transmit sensitive audio or visual information in the work/telework environment. Many such devices and applications can record and/or transmit data when activated. This IG memo is meant to help personnel be aware of the risks and how to protect SBU data.

2. The IG Memo is updating the title **Director, PGLD** to **Chief Privacy Officer (CPO).**

Background/Source(s) of Authority: IRM 10.5.1 is issued under the authority of the Privacy Act of 1974, the Internal Revenue Code, the Taxpayer Browsing Protection Act of 1997, the E-Government Act of 2002 (to include accompanying guidance outlined in OMB memoranda), the Consolidated Appropriations Act of 2005, §522, Treasury Directives and other federal guidance. For a full listing of privacy laws relevant to this IRM section, refer to Exhibit 10.5.1-2, *References*.

Effect on Other Documents: This guidance will be incorporated into IRM 10.5.1, *Privacy Policy*, by August 29, 2019.

Effective Date: August 29, 2017

Contact: If you have any questions, please contact me, or a member of your staff may contact Greg Ricketts, Associate Director, Privacy Policy and Knowledge Management, at 901-546-3078, or Gregory.T.Ricketts@irs.gov.

Distribution:
Commissioner of Internal Revenue
Deputy Commissioner for Operations Support Deputy Commissioner for Services & Enforcement Commissioner, Large Business and International Division Commissioner, Small Business/Self-Employed Division Commissioner, Tax-Exempt and Government Entities Division Commissioner, Wage and Investment Division
Chief of Staff
Chief, Agency-Wide Shared Services
Chief, Appeals
Chief, Communications and Liaison
Chief Counsel
Chief, Criminal Investigation
Chief Financial Officer
Chief, Planning, Programming & Audit Oversight
Chief, Risk Officer
Chief Technology Officer
Director, Affordable Care Act Office Director, Office of Compliance Analytics Director, Office of Online Services
Director, Office of Professional Responsibility Director, Office of Research, Analysis and Statistics Director, Privacy, Governmental Liaison and Disclosure Director, Return Preparer Office
Director, Whistleblower Office
Executive Director, Equity, Diversity and Inclusion
IRS Human Capital Officer
National Taxpayer Advocate
Treasury Inspector General for Tax Administration (TIGTA) Associate Chief Information Officer, Cybersecurity
www.IRS.gov

Attachment Interim Guidance: PGLD-10-0817-0002

The following changes are hereby effective August 29, 2017, for IRM 10.5.1:

1. For the Digital Assistant and Other Devices update:

10.5.1.6.10
(08-29-2017)
Telework

(8) Digital assistants and other devices that can record or transmit sensitive audio or visual information must not be allowed to compromise privacy in the work or telework environment. These devices typically contain sensors, microphones, cameras, data storage components, speech recognition, GPS options, and other multimedia capabilities. These features could put the privacy of employees and/or taxpayers at risk due to the personal information that might be unwittingly disclosed. When working on any form of SBU data, especially PII or FTI, follow these rules:

a. Treat the device as if it were another person in the room because many such devices and applications can record and/or transmit data when activated. To protect privacy, the employees must mute or disable the listening/detecting features of the device so that SBU data is not sent to the device or anything to which it is connected.
b. If the device or application can take photos or record video or sound, then the employee must not do sensitive work within visual or audio range.

These devices/applications include (but are not limited to the examples provided):

- Digital assistants (such as Dot or Echo hardware using Alexa software, HomePod using Siri, etc.).
- Voice-activated devices and smartphone applications (such as Siri, Google Now ("Okay Google"), or Alexa on phones, tablets, etc.).
- Internet-connected toys (Cloud Pet, Smart Toy, Hello Barbie, etc.) that might record and transmit.
- Security systems and webcams in the telework environment.
- Smart TVs or auxiliary equipment (if includes voice activation).
- Operating systems/applications (such as Windows 10, Cortana, etc.) that allow voice commands.
- Home surveillance, security, and video/audio: Webcams on personal devices in the home, security cameras/microphones.

Note: For more information about privacy risks of Internet-connected toys, refer to the FBI's Public Service Announcement, "Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children:" https://www.ic3.gov/media/2017/170717.aspx

10.5.1.6.12.2
(08-29-2017)
Recordings in the Workplace

(4) Employees may use their smartphones (or other devices with recording capabilities) in the workplace. However, they should take reasonable precautions that no unauthorized recordings or disclosures occur. When working on any form of SBU, especially PII or FTI, such precautions include muting or disabling voice-activated devices and smartphone applications (such as Siri or Google Now (“Okay Google”) on phones, tablets, etc.). For more information about precautions, see the Telework section of this IRM about digital assistants and other devices that can record or transmit sensitive audio or visual information.

2. For the Director, PGLD title change to Chief Privacy Officer (CPO):

10.5.1.5.2
(08-29-2017)
Senior Management/Executives
(1) Senior Management/Executives must:
a. Work with the ~~Director, PGLD~~**Chief Privacy Officer (CPO)** to develop, implement, maintain, and enforce a program to protect all SBU data for which they are responsible in accordance with IRS privacy policies and procedures.

And:
10.5.1.7.1
(08-29-2017)
Privacy Council
(2) The purpose of the Privacy Council is to:
c. Centralize the ~~Director, PGLD~~**Chief Privacy Officer's (CPO)** policy-making role in the development and evaluation of legislative, regulatory, and other policy proposals, which implicate information privacy issues. In so doing, the Council takes a central role in ensuring the IRS is fully compliant with federal laws, regulations, and policies relating to information privacy while enabling continued progress and innovation.

(3) To accomplish these objectives, the Privacy Council members will:
c. Generate policy guidance to be issued from the ~~Director, PGLD~~**CPO**.