



PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

Date of Issuance: 04-25-2024

Control Number: PGLD-10-0424-0011
Expiration Date: 04-26-2026
Affected IRM(s): 10.5.1; 10.8.1; 1.15.6

MEMORANDUM FOR ALL OPERATING DIVISIONS AND FUNCTIONS

FROM: John J. Walker /s/ *John J. Walker*
Acting Director, Privacy Policy and Compliance

SUBJECT: Text Messaging Privacy

This memorandum issues emergency interim guidance on text messaging privacy and is effective as of April 26, 2024. This supersedes Interim Guidance Memorandum PGLD-10-0224-0006, Text Messaging Privacy, dated 02-26-2024, to add a clarifying note from stakeholder feedback of that emergency guidance. Please distribute this information to all affected personnel within your organization.

Purpose: This emergency interim guidance allows for limited automated, system-generated one-way text messaging with generic, non-sensitive information and clarifies privacy requirements for phone conversations about sensitive information. It requires immediate issuance to prevent work stoppage for implementing systemic messaging provisions of the IRS Inflation Reduction Act Strategic Operating Plan during the current filing season.

Background/Source(s) of Authority: This interim guidance falls under the authorities listed in the Authority section of IRM 10.5.1, Privacy Policy.

Procedural Change: The procedural changes in the attached interim guidance apply.

Effect on Other Documents: This supersedes Interim Guidance Memorandum PGLD-10-0224-0006, Text Messaging Privacy, dated 02-26-2024, to add a clarifying note from stakeholder feedback of that emergency guidance. We will incorporate this interim guidance into IRM 10.5.1, by April 26, 2026.

Effective Date: April 26, 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-10-0424-0011

The following changes take effect April 26, 2024, for [IRM 10.5.1](#).

10.5.1.6.7

(04-26-2024)

Phone

- (1) When talking about SBU data (including PII and tax information) via phone call, IRS personnel must:
 - a. Authenticate the individual. See [IRM 10.5.1.2.9](#), Authentication.
 - b. Confirm you're talking to an authorized person before discussing the information. See [IRM 10.5.1.2.10](#), Authorization.
 - c. Inform them you'll be talking about sensitive information.
 - d. Make sure no one else can overhear the conversation. See [IRM 10.5.1.6.7.1](#), Cell Phone or Cordless Device.

Note: It is understood you might not be able to avoid other IRS employees when in an IRS office.

- (2) This subsection applies to talking on phone calls (including internet-based calls). For texting restrictions, see [IRM 10.5.1.6.9.6](#), Text Messaging (Texting).
- (3) For security information on phones, refer to [IRM 10.8.1.4.1.18.1](#), Telecommunication Devices.

10.5.1.6.9.6

(04-26-2024)

Text Messaging (Texting)

- (1) The IRS may use limited automated, system-generated (or system user-initiated), one-way text messaging to send generic, non-sensitive information with prior consent. The messages must not include SBU data (such as personnel information or taxpayer case data).

NOTE: Do not include SBU data in texts because any transmission of SBU data must meet encryption requirements in [IRM 10.8.1.4.18.7](#), SC-08 Transmission Confidentiality and Integrity.
- (2) Automated, system-generated short one-way event or time-based text messages sent on behalf of the IRS must follow the policy for emails generated to taxpayers or representatives by approved online applications in [IRM 10.5.1.6.8.5](#), Limited Exceptions to Email SBU Data Encryption.
- (3) Any other text messaging for official business remains prohibited.
- (4) Privacy policy must review and approve system-generated message content. For questions and approval, email [*Privacy](#).
- (5) These messages must follow records retention requirements in [IRM 1.15.6.14.2](#), Preserving Electronic Messages. They must also follow IT Security Policy in [IRM 10.8.1.4.1.18.1](#), Telecommunication Devices.