Resources for Providers Receiving Legal Process Subject to a CLOUD Act Agreement

The Clarifying Lawful Overseas Use of Data Act, or "CLOUD Act," authorizes the United States to enter into executive agreements with other countries that remove restrictions under each country's laws so that communication service providers in one country can comply with qualifying, lawful orders for electronic data issued by the other country. For providers subject to U.S. law, the CLOUD Act amended the Stored Communications Act, the Wiretap Act, and the Pen Register Trap and Trace Act to permit the disclosure to a foreign government of the contents and metadata of wire or electronic communications pursuant to an order subject to a CLOUD Act agreement (hereinafter, "a CLOUD Agreement"). Any legal effect of an order subject to a CLOUD Agreement derives solely from the law of the Issuing Party; the Act did not create any new legal rights or obligations.

On October 3, 2019, the United States and the United Kingdom signed the first agreement under the CLOUD Act, the *Agreement Between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime* ("the U.S.-UK Agreement"). The U.S.-UK Agreement came into force on October 3, 2022.

Definitions

Covered Providers are defined in CLOUD Agreements as private entities to the extent they are: (1) providing to the public the ability to communicate, or to process or store computer data, by means of a computer system or a telecommunications system or (2) processing or storing Covered Data on behalf of an entity defined in (1).

Covered Data is data in the possession or control of a Covered Provider that constitutes (a) the content of an electronic or wire communication, (b) computer data stored or processed for a user, (c) traffic data or metadata pertaining to an electronic or wire communication or the storage or processing of computer data for a user, and (d) subscriber information relating to users when sought pursuant to an order that also seeks the data referenced in (a), (b), or (c).

Foreign country, as used in this document, refers to any country other than the United States that is a signatory to a CLOUD Agreement.

Issuing Party, as used in this document, is the country that issues and serves an order subject to a CLOUD Agreement on a Covered Provider.

Effect of a CLOUD Agreement for Covered Providers

Covered Providers in the United States that receive an order subject to a CLOUD Agreement are permitted under U.S. law to comply with the order.

Covered Providers in a foreign country that receive an order subject to such CLOUD Agreement are permitted under that country's law to comply with the order.

A CLOUD Agreement does not create new, legal rights or obligations for Covered Providers. Any legal effect of an order subject to a CLOUD Agreement derives solely from the law of the

Issuing Party. That is, for orders from the foreign country, the legal effect of the order comes only from the foreign country's law; for orders from the United States, the legal effect of the order comes only from U.S. law.

CLOUD Agreement Designated Authorities and Orders

Covered Providers will receive orders subject to a CLOUD Agreement only from the Designated Authority of the Issuing Party. Orders from the United States will come from the U.S. Designated Authority: **the Office of International Affairs in the Criminal Division of the U.S. Department of Justice**. Orders from the foreign country will come from its Designated Authority, which for the purposes of the existing CLOUD Agreement(s) are the following:

United Kingdom: **Investigatory Powers Unit of the UK Home Office**.

Australia: **International Production Order Section, Cybercrime and Cross Border Data Branch, of the Attorney-General's Department of Australia.**

Along with each order, Covered Providers will receive a certificate from the Designated Authority certifying that the order meets the requirements of the particular CLOUD Agreement. It is the responsibility of the Designated Authority to ensure that each order transmitted satisfies the requirements under the CLOUD Agreement, including the serious crime threshold and targeting restrictions. The certificate and order will direct Covered Providers on how to respond to the relevant authorities in compliance with the order.

Covered Providers located in the United States that receive this certificate from the foreign country's Designated Authority are not precluded from complying with the order by the Stored Communications Act, the Wiretap Act, and/or the Pen Register Trap and Trace Act.

For Covered Providers located in the following foreign countries, receipt of this certificate from the U.S. Designated Authority permits disclosure pursuant to the following laws:

United Kingdom: **Investigatory Powers Act 2016 and the Data Protection Act 2018**.

Australia: **Telecommunications (Interception and Access) Act 1979**.

Objections

A Covered Provider that receives an order subject to a CLOUD Agreement may raise specific objections when it has a reasonable belief that the CLOUD Agreement may not be properly invoked with regard to the specific order. The certificate from the Designated Authority of the Issuing Party will include a point of contact at that Authority that can provide information on legal or practical issues relating to the order.

A Covered Provider located in the United States wishing to object to an order from the foreign country's Designated Authority should first raise any concerns about the order with the foreign country's Designated Authority. The Covered Provider should raise any such objections within a reasonable amount of time after receipt of the order. To raise such concerns, the provider should contact the foreign country's Designated Authority as instructed in the certificate accompanying

the relevant order. If the concerns are not resolved, the Covered Provider may then raise the concerns with the U.S. Designated Authority, which has the power to conclude that the foreign country's Designated Authority may not properly invoke the CLOUD Agreement as to the particular order.

A Covered Provider located in the foreign country wishing to object to an order received from the U.S. Designated Authority should first raise any concerns about the order with the U.S. Designated Authority. The Covered Provider should raise any concerns within a reasonable amount of time after receipt of the order. To raise such concerns, the provider should contact the U.S. Designated Authority as instructed in the certificate accompanying the relevant order. If the concerns are not resolved, the Covered Provider may then raise the concerns with the foreign country's Designated Authority, which has the power to conclude that the U.S. Designated Authority may not properly invoke the CLOUD Agreement as to the particular order and therefore the order is not subject to it.

In addition, Covered Providers retain any existing rights to raise legal objections to an order subject to a CLOUD Agreement pursuant to the law of the Issuing Party.

Covered Providers located in the United States needing legal assistance regarding foreign law with respect to an order under a CLOUD Agreement may find information on obtaining such assistance on the website of the U.S. Embassy in the relevant country, under U.S. Citizen Services.

Requests for Preservation of Data and Subscriber Information

For information regarding requests seeking preservation of data and disclosure of just subscriber information, please visit **here**.

Frequently Asked Questions

Q: We received an order with a certificate invoking a CLOUD Agreement that does not specify the crime under investigation. How can we be sure that the order is for the purpose of the prevention, detection, investigation, and prosecution of serious crime under the particular CLOUD Agreement if we don't know the potential penalty of the crime under investigation?

A: It is the responsibility of the Designated Authority of the Issuing Party to assess whether an order is properly issued under the particular CLOUD Agreement, including whether the order is for the purpose of obtaining information related to the prevention, detection, investigation, or prosecution of serious crime as defined in the CLOUD Agreement. Prior to submitting an order to the Covered Provider, the Designated Authority will review the relevant offense and penalty to confirm that they meet the definition of serious crime. When the serious crime requirement is satisfied, the Designated Authority will so certify in the certificate that accompanies the order.

Q: As a Covered Provider in the United States, we received a certificate from a foreign country's Designated Authority invoking a CLOUD Agreement for an order targeting an account that we have reason to believe belongs to a U.S. resident. What should we do?

A: It is the responsibility of the Designated Authority of the Issuing Party to assess whether an order is properly issued under a particular CLOUD Agreement, including whether the targeting restrictions have been met. However, if a Covered Provider has information creating a reasonable belief that the CLOUD Agreement may not be invoked for an order, such as information relating to the targeting restrictions of the CLOUD Agreement, the Covered Provider can raise that specific concern with the foreign country's Designated Authority. If the Covered Provider is not able to resolve the concerns with the foreign country's Designated Authority, the Covered Provider may raise the concern with the U.S. Designated Authority, which has the power to conclude that the CLOUD Agreement may not be invoked with respect to a particular order. To raise such concerns, the U.S. Designated Authority may be reached by e-mail at CLOUD.RESPONSE.TEAM@usdoj.gov.

Q: Does a CLOUD Agreement provide for compensation for the costs of compliance with an order subject to the Agreement?

A: CLOUD Agreements do not create any legal rights for Covered Providers. The domestic law of the Issuing Party governs the legal effect of orders subject to a particular CLOUD Agreement, including any right to compensation available to Covered Providers.

Q: We received an order subject to a CLOUD Agreement, including an order prohibiting notification of the account holder. Must we comply with that order?

A: CLOUD Agreements do not create new legal obligations for Covered Providers. The domestic law of the Issuing Party governs the legal effect of orders subject to a CLOUD Agreement, including any prohibition on notification to an accountholder.

Q: We received an order subject to a CLOUD Agreement for an account that belongs to a third-party national whom we believe is not in the United States nor in the territory of the Issuing Party, but is in a third country. Will the government of the third country be notified of the order?

A: If it is appropriate in specific cases to provide third country notifications, the Designated Authority of the Issuing Party shall notify the appropriate government of orders issued for individuals located in that country. The Designated Authority shall notify the third country unless such notification would be detrimental to operational or national security, impede the conduct of an investigation, or imperil human rights.

Q: As a Covered Provider located in both the United States and in a foreign country subject to a CLOUD Agreement, should we expect every order we receive from a U.S. or foreign country authority going forward to invoke the particular CLOUD Agreement?

A: No. On the contrary, existing processes and procedures pertaining to domestic court orders will continue unchanged. CLOUD Agreements are not the exclusive mechanism for seeking Covered Data from Covered Providers. The parties will continue to obtain electronic data through other available mechanisms, such as mutual legal assistance or domestic court orders served on local providers outside the CLOUD Agreement.

Q: If a Covered Provider has questions about executing an order it has received that invokes a CLOUD Agreement, who should it contact?

A: The certificate will include a point of contact at the Designated Authority of the Issuing Party who can provide information on legal or practical issues relating to the order.