October 2020

Frequently Asked Questions: Cross Border Data Transfers as Part of AT&T's Global Privacy Program

AT&T has a longstanding commitment to data protection and transparency, and we want you to know about our safeguards for transferring data outside of the European Economic Area (EEA), Switzerland, and the United Kingdom. In addition, we believe it's important to understand the rigorous process we have in place for responding to government and legal demands made to our company, which we publish in our Transparency Report. Our comprehensive AT&T Privacy Center provides General Data Protection Regulation (GDPR) notices, details about our global and U.S. approach to privacy, and privacy protecting tips and tools, and our answers to the frequently asked questions below provide additional details about our data transfer practices and compliance with government regulations. Our approach to compliance, transparency, and responsibility make AT&T a trusted steward of personal data.

COMPLIANCE

- *What did the Court of Justice of the European Union (CJEU) decide in the Schrems II case?*

The CJEU considered whether transfers of European personal data to the United States comply with European privacy rights and the General Data Protection Regulation (GDPR). The specific complaint was that US law provides US national security and law enforcement agencies too much access to personal data and without sufficient right of redress, particularly for persons in the EU. The CJEU determined that one cross border transfer mechanism, the EU-US Privacy Shield Framework, did not provide adequate protection and was, therefore, invalid. The CJEU determined another cross border transfer mechanism, the standard contractual clauses (SCCs), remain valid. EU Member State regulators and the parties using SCCs must assess on a case-by-case basis if the SCCs may be validly used for transfers to particular countries, including to the US, and whether supplementary safeguarding measures additional to the SCCs should be applied.

- *What are the impacts of this decision for AT&T?*

AT&T made very limited use of the Privacy Shield, including with suppliers. These transfers will be now made pursuant to SCCs. AT&T makes broad use of SCCs – both for internal transfers and for transfers involving personal data of customers, as well as onward transfers to suppliers that support our services. These agreements using SCCs remain valid, but AT&T is taking further steps to support ongoing validity. AT&T will use appropriate transfer mechanisms in a responsible manner to securely process personal data.

- *May companies in Europe continue to work with AT&T?*

Yes. The CJEU opinion does not prohibit transfers to the US using SCCs. AT&T is committed to fulfilling our responsibilities in relation to collection, retention, use, and other processing of personal data that is within the scope of the GDPR and other applicable data protection laws. Such personal data will be processed only for lawful and appropriate purposes. AT&T has implemented measures designed to keep personal data secure against unauthorized or accidental access, erasure, or other misuse of personal data. AT&T will facilitate the exercise of data subject rights under the GDPR in an effective and transparent manner.

TRANSPARENCY

- *What will AT&T do to supplement use of the standard contractual clauses?*

AT&T has taken and will continue to take additional steps so that we and our customers are able to demonstrate adequate levels of data protection. Specifically, AT&T will provide greater access to information about our safeguards, as well as to how individuals can exercise applicable rights. We will work with our customers to strengthen data protection procedures and support, including providing guidance on how our customers can enhance security when using AT&T products and services.

AT&T is also committed to working with governments in Europe and the US to support secure and stable mechanisms to transfer personal data. The U.S. Department of Commerce issued a white paper on the use of SCCs to explain both the types of data actually of interest to the US Government as well as the many safeguards the US Government has in place to limit data collection and protect data acquired.

- *Where does AT&T provide more information about its Privacy Program?*

AT&T's Privacy Center provides a wealth of information and resources about how AT&T protects customer privacy and offers customers choices. The Privacy Center explains our privacy program, as well as a link to our Transparency Reports (see below). On the Global Approach page, we offer our regional privacy notices that detail how AT&T complies with data protection laws around the world. AT&T's privacy program is premised on the fact that privacy is fundamental to our business. We're committed to:

  - Transparency - We're open and honest about how we use your data.
  - Choice and Control - We give you choices about how we use your data.
  - Security - We use strong safeguards to keep your data confidential and secure.
  - Integrity - We do what we say.

AT&T also makes available – on the internet and through our sales and support teams – information about how our products operate, including data protection. Additional information is made directly available to customers.

- *Does AT&T publish a Transparency Report?*

Yes. AT&T publishes a biannual Transparency Report, in English, Spanish, and Portuguese. But in any language, the fundamental commitment of AT&T is that "We pledge to protect your privacy and to comply with applicable law."

RESPONSIBILITY

- *Does AT&T respond to demands for information from government entities inside the US?*

Yes. Like all companies, AT&T is required by law to provide information to government and law enforcement entities, as well as parties to civil lawsuits, by complying with court orders, subpoenas, lawful discovery requests and other legal demands.

- *Does AT&T have a process to review demands for appropriateness?*

Yes. Before AT&T responds to any legal demand, we determine that we have received the correct type of demand based on the applicable law for the type of information sought. If the requesting agency has failed to send the correct type of demand, AT&T rejects the demand. The number of demands we reject is stated in our Transparency Report. Where appropriate, AT&T will seek clarification or modification of a request or object to a government demand or court order in the appropriate forum. For more information, see our Transparency Report and Human Rights Policy.

- *Does AT&T respond to demands for information from government entities outside the US?*

Yes. When AT&T in the US receives a non-US demand for information we refer the requester to that country's Mutual Legal Assistance Treaty (MLAT) process. The US Federal Bureau of Investigation (FBI) ensures that we receive the proper form of U.S. process and that cross-border data flows are handled appropriately. Thus, any such international originated demands that follow an MLAT procedure are reported in our Total Demands category of our Transparency Report because we can't separate them from any other FBI legal demand we may receive. AT&T does report uniquely in our Transparency Report on countries that have made demands of AT&T to produce historic subscriber information or for IP/URL blocking.

If you have any questions about AT&T's privacy program or cross border transfers, please contact the AT&T Chief Privacy Office at Askprivacy@att.com or the AT&T Data Protection Officer at AT&TDPO@att.com.