August 2021

Frequently Asked Questions: Cross Border Data Transfers as Part of AT&T's 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. We also believe it is important to understand the rigorous processes we have in place for responding to governmental and legal demands made to our company, which we publish in our biannual Transparency Report.

On our comprehensive AT&T Privacy Center, you can find:

- Our Most of World (MOW) data protection notices, which explain AT&T's processing activities in support of serving our customers;
- Details about our global and U.S. approaches to privacy;
- Links for exercising individual rights and contact information for asking questions;
- Privacy-protecting tips and tools.

Below, we have addressed frequently asked questions 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 are the requirements to transfer personal data for processing outside the European Union?*

Under the European Union's (EU) General Data Protection Regulation (GDPR), personal data that is transferred for processing outside the EU must receive "essentially equivalent" protection as the personal data would receive in the EU under GDPR. In 2020, the Court of Justice of the EU (CJEU) considered whether transfers of European personal data to the United States comply with European privacy rights and GDPR. 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 that another cross border transfer mechanism, the standard contractual clauses (SCCs), remain valid but may need supplementary safeguards so that personal data transferred receives an "essentially equivalent" level of protection as it would directly under GDPR. SCCs are used between an exporting party in the EU and an importing party not in the EU and add data protection requirements to the relationship. Since the CJEU's decision, the European Commission (EC) has adopted updated SCCs to address the Court's findings, and the European Data Protection Board (EDPB) has offered recommendations for how use of the SCCs may be further supplemented, as necessary.

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

Yes. AT&T makes broad use of the SCCs – for internal transfers and for transfers involving personal data of customers, as well as transfers to suppliers that support our services. These agreements using SCCs remain valid under the CJEU decision and AT&T is working with customers and suppliers to update our contracts and further supplement our data protection measures. AT&T is making these updates as to personal data within the scope of GDPR (EU and European Economic Area (EEA) countries) as well as personal data within the scope of the similar laws in Switzerland and the United Kingdom.

AT&T is committed to fulfilling our responsibilities for the 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. 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. We are updating our contracts with customers and suppliers to address the requirements of the updated SCCs and supplementing our relationships with customers and suppliers to further protect

personal data. Specifically, AT&T will provide more information about our safeguards, as well as to how individuals can exercise applicable rights. We will work with our customers and suppliers to strengthen data protection procedures and support, including providing guidance on how our customers can enhance security when using AT&T products and services. Whether personal data is processed in Europe or elsewhere around the world, AT&T is committed to using appropriate security measures to protect that data.

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.

- *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 choices to customers. The Privacy Center explains our privacy program, as well as a link to our Transparency Report. On the Global Approach page, we offer our Most of World (MOW) privacy notices that detail how AT&T complies with data protection laws. AT&T's privacy program is built on the principle that privacy is fundamental to our business. We're committed to:

  - Transparency - We're open and honest about how we use your data.
  - Choices and Controls - 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 and services operate. 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 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.

- *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.

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.