ReedSmith

Driving progress
through partnership

Trans-Atlantic Data Privacy Framework: What To Do Now

2022-04-11T04:00:14000-04:00 – The European Commission and U.S. government's important new agreement governing the transfer of data between the EU and the U.S., the Trans-Atlantic Data Privacy Framework, should help rebuild and strengthen trust and resulting data flows between the two parties.

The framework addresses both sides' concerns over the necessity and proportionality of U.S. national security-related data collection. It is intended to ensure sufficient means of redress are provided to EU citizens whose data has been collected and processed in the U.S. These concerns contributed to the invalidation of the prior Privacy Shield Framework.

The Trans-Atlantic Data Privacy Framework attempts to address the concerns of the Court of Justice of the European Union which in 2020 invalidated the original Privacy Shield Framework. As a legal matter, it will be critical to the success of the framework that EU courts and members of civil society concur that the new framework contains sufficient fundamental privacy protections. The new framework will have a similar adherence structure as the invalidated Privacy Shield.

Developments in the EU-U.S. Framework

The new framework addresses two concerns of the Court of Justice related to U.S. surveillance laws:(1) the scope and proportionality of permissible U.S. national security surveillance activities; and (2) the availability of redress mechanisms for Europeans whose personal data is determined to have been collected improperly by U.S. intelligence agencies.

The new framework affirms that U.S. surveillance practices must be necessary and proportionate. Additionally, it will require an independent data protection review court to provide review and redress for Europeans impacted by allegedly improper surveillance.

Steps Businesses Should Consider

Building resilient privacy and data protection practices represents an important step for companies as they scale. Embracing the new framework by meeting or exceeding its requirements may help companies avoid litigation and investigation in the EU.

Some companies are anticipating the framework's unannounced specifics by enhancing management of legal requests for customer data and providing legal support for individuals concerned about their rights. These efforts may improve business confidence in vendors and providers and may reduce the likelihood of pursuit by activists.

In light of the new framework, businesses that have not recently done so may consider:

- Conducting gap analyses of existing compliance programs against the new framework and other laws;
- Creating or updating data inventories;
- Reassessing security and privacy practices and agreements with third-party partners vendors and suppliers;
- Ensuring privacy policies address international data transfers;
- Developing internal protocols to address new or modified data subject rights; and
- Evaluating the best means for international data transfers from the EU such as using the GDPR Standard Contractual Clauses.

Business Policy Measures Being Taken

Concerns with—and the invalidation of—the Privacy Shield Framework rested on the necessity and proportionality of U.S. national security surveillance activities. Invalidation of the Privacy Shield raised concerns on the sufficiency of redress mechanisms for Europeans whose personal data is collected by U.S. intelligence agencies.

The extraterritorial application of privacy and data protection law remains a thorny legal issue which will continue to be problematic for global enterprises. These issues have devolved into an implicit guerrilla trade war where an individual company's (and country's) ability to do business globally is increasingly subject to the vagaries of foreign regimes.

Government Information Demand Management

Businesses seeking to rely upon the new framework may seek to confirm that demands for personal data from the U.S. government complies with the Trans-Atlantic Data Privacy and Security Framework. Where an organization believes the demand is not compliant, it may challenge such demands as a matter of policy.

While such a commitment cannot ensure that the framework itself will survive challenge, it may inoculate or reduce the risk of the particular company being targeted.

Redress Remedies

While the details of the new framework relating to redress have not been finalized, some businesses are already committing to actively participate in the judicial review of an individual's claim of harm. Where the alleged harm is in connection with the collection and processing of data relating to that individual in connection with the business' service offerings, some businesses may pledge to use legal means to resist collection.

Considerations

Data protection issues and privacy concerns between nation states are not disappearing. The volume and velocity of prescriptive regulatory requirements relating to personal data remains challenging for information-centric companies, in addition to the use of data for the public good.

In areas such as health care, financial services, consumer credit markets, and emerging technologies, defensible data management is emerging for many as a mission critical capability for businesses.

Emerging trends for successful enterprises include:

- **Early and Strategic Approach**. Successful companies increasingly devote resources early and frequently to data-related issues embedding expertise at the concept stage for new offerings and throughout their lifecycle.
- **Data Lifecycle Management**. Existing enterprises frequently commit material resources to examining the lifecycle of data collected and shared. Third-party risk management represents a fast growing area of governance, risk, and compliance work.
- **Leadership Focus**. In digital transformation, senior leaders may require education and training to drive successful transformation aligned with governance of mission critical regulatory risks.

While these trends may be beginning for many organizations, less mature organizations may be forced to be more reactive in keeping track of ever-changing legal requirements. Organizations are considering these issues earlier and often doing more than what the law demands to address anticipated requirements.

The Trans-Atlantic Data Privacy Framework represents the latest continuation of a growing global trend of action and reaction by regulators and businesses to changing circumstances.

This article does not necessarily reflect the opinion of The Bureau of National Affairs, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners.

Author Information

Gerry Stegmaier is a partner in Reed Smith's Tech & Data group, focusing on corporate governance, intellectual property, and internet issues especially as they relate to privacy, information security, and consumer protection. He advises companies facing multi-jurisdictional global data protection challenges and disputes.

Lauren Weaver is an associate in Reed Smith's Global Regulatory Enforcement group. Her practice involves data privacy, cybersecurity, and information governance, advising clients on compliance with state, federal, and international privacy and security regimes.