14 November 2022

Transatlantic Business Associations Join in Strong Support of EU-U.S. Data Privacy Framework

The undersigned associations, representing the transatlantic business community, appreciate the U.S. Administration's recently published Executive Order (EO) and accompanying Department of Justice (DOJ) regulations that set out the significant legal changes the U.S. has instituted to implement its commitments under the EU-U.S. Data Privacy Framework.

The unprecedented legal changes adopted by the U.S. to establish a comprehensive and credible solution that builds on the political agreement reached in March 2022 reflect the EU and U.S.'s shared ambition and commitment to upholding fundamental values. We thank EU and U.S. negotiators for their tireless work over two years to achieve that goal.

As a cross-sectoral, international industry coalition that values the importance of privacy and fundamental rights, as well as the geopolitical and economic importance of the transatlantic relationship, our goal is to provide a helpful initial analysis of these changes to U.S. law, with the aim of informing and supporting the important work ahead by EU Institutions towards making the EU-U.S. Data Privacy Framework operational through the EU adequacy decision process.

The EO and DOJ regulations signify a critical step towards building a comprehensive, durable framework that protects the fundamental rights of citizens and facilitates the data flows that underpin the $7.1 trillion economic relationship between the EU and U.S. Transatlantic businesses across all sectors of the economy, such as health care, media and entertainment, financial services, education, and e-commerce, rely on strong privacy protections which are foundational to consumer confidence and trust, as do

businesses of all sizes (indeed, 70% of companies certified to Privacy Shield are small and medium-sized enterprises). Equally, as trusted allies and partners, the EU and U.S. require a data sharing framework that upholds citizens' fundamental privacy rights, while providing national security authorities with the necessary and proportionate tools to protect citizens' public safety interests at a time when shared democratic values are increasingly under threat.

The significance of a new framework

Following the invalidation of the EU-U.S. Privacy Shield agreement in 2020, the transatlantic business community called on EU and U.S. negotiators to develop and conclude a new agreement to address the issues presented by the Court of Justice of the European Union (CJEU). The 2020 *Schrems II* ruling has created significant uncertainty for businesses of all sizes on both sides of the Atlantic. New barriers to data transfers have undermined economic growth and stifled competition. At the same time, the instability caused by the invalidation of the Privacy Shield Framework has been counterproductive to improving the protection of personal data.

While our industries have a clear and important interest in this debate for all the reasons stated above, we are also fully conscious of the importance of the fundamental issues at stake, and of moving forward with a solid, reliable mechanism that can stand the test of time, including future legal challenge. Further, we are encouraged by the work of independent academic experts from Europe and the U.S. who have carefully and objectively reviewed the EO and DOJ regulations and maintain that the thorough and creative solution strikes the right balance to achieve these multiple aims.

Key elements introduced by the EO and DOJ regulations

The EO and DOJ regulations represent significant and meaningful changes to U.S. law that properly address both the "necessity and proportionality" and "redress" requirements set out by the CJEU.

First, the EO places robust and binding safeguards on U.S. signals intelligence activities and deals directly with the CJEU's requirement that personal data collection be limited only to what is **necessary** and **proportionate** under these circumstances. Some of the most notable safeguards in this area include:

- U.S. signals intelligence authorities must consider the legitimate privacy interests of all persons, regardless of their nationality or country in which they reside and ensure that privacy and civil liberties are "integral considerations" when planning and implementing such activity.
- Signals intelligence activities shall only be conducted where "necessary to advance a validated intelligence priority" to meet an authorized national security objective and "only to the extent and in a manner that is proportionate to [that] priority." Further, explicit guardrails are established around both permissible and impermissible collection activities, and there are additional safeguards around how the signals intelligence can be collected, how long it can be maintained, and how it can be used and shared.
- Multiple oversight layers ensure adherence to these core principles and related data handling obligations. Each element of the Intelligence Community is itself accountable for upholding the EO; the Civil Liberties Protection Officer of the Director of National Intelligence (CLPO) is ultimately responsible for overall compliance; and the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency with information access and review authority, provides an external audit and check function.

Significantly, these measures are immediately binding on U.S. intelligence agencies.

Second, the EO establishes an **independent** and **binding** redress mechanism that affords EU citizens (as well as nationals of other qualifying states or regional economic integration organizations) a meaningful

way to defend their fundamental right to privacy, while respecting the unique requirements of the Intelligence Community under U.S. law.

- The two-layer complaints review process provides an efficient and pragmatic means for non-U.S. citizens to obtain effective redress, and avoids the significant legal pitfalls associated with the difficulty of establishing sufficient legal "standing" necessary to access U.S. federal courts.
- The Data Protection Review Court (DPRC) provides a clear judicial function with independent review as a matter of right, and investigatory powers and decision-making authority with binding effect on U.S. intelligence agencies. Covered violations that can be submitted to the DPRC include violations of the U.S. Constitution, the Foreign Intelligence Surveillance Act ("FISA"), and Executive Order 12333, among other policies and statutes.
- Along with the role of the Special Advocate to facilitate and manage complaints, the system provides robust avenues for redress that break new ground and go far beyond the safeguards provided by the former Privacy Shield Ombudsperson.

The need for fair and balanced assessment

We urge all stakeholders to consider deliberately but fairly the substance of these new U.S. legal requirements, which establish unprecedented restrictions on U.S. surveillance activities as well as a meaningful redress mechanism for EU citizens. We are heartened that these new safeguards serve to strengthen all existing transfer mechanisms available to companies, including standard contractual clauses, and should be relevant considerations in the context of EU supervisory authority investigations. Furthermore, we recognize that this is not only a matter of facilitating economic stability and growth. The efforts to reach agreement on a new framework embody a statement of common purpose from the EU and U.S., and a willingness to work together to find new ways to uphold the joint values we share as democratic societies. These developments also send a strong message on the importance of privacy globally, and in establishing robust and secure frameworks for cross-border data transfers.

The EO and accompanying regulations reflect the U.S. government's implementation of the EU-U.S. political agreement. It is our assessment that the implementation credibly complies with the demands of the CJEU's 2020 ruling, both the EU and U.S. legal systems, and, importantly, reflects our shared values and interests.

On behalf of the business community, we support the swift conclusion of the EU adequacy decision process, so that businesses can confidently rely on the new EU-U.S. Data Privacy Framework. We stand ready to assist in any way that is helpful.

Sincerely,

ACT | The App Association
Alliance Française des Industries du Numérique (AFNUM)
Alliance for Automotive Innovation
Allied for Startups
AmCham EU
AmCham Ireland
American Council of Life Insurers
Asia Internet Coalition (AIC)
Biotechnology Innovation Organization (BIO)
Bitkom
Business Roundtable
Coalition of Services Industries (CSI)
Computer & Communications Industry Association (CCIA)

Confederation of Danish Industry (DI)
Confederation of Industry of the Czech Republic (SPCR)
Consumer Technology Association® (CTA)
Danish Entrepreneurs
Dansk Erhverv / The Danish Chamber of Commerce
Developers Alliance
Digital Future for Europe
Digital Poland ZIPSEE
Ecommerce Europe
Engine
Entertainment Software Association
European Games Developer Federation (EGDF)
European Publishers Council
FEDMA
IAB
INFOBALT
Interactive Software Federation of Europe (ISFE)
Internet Infrastructure Coalition
ITI – The Information Technology Industry Council
National Retail Federation
NLdigital
Software & Information Industry Association (SIIA)
Swedish Enterprise (SN)
TechNet
techUK
Trans-Atlantic Business Council
U.S. Chamber of Commerce
U.S. Council of International Business (USCIB)