24 April 2019
EBF_036657

EBF comments on the DG TRADE Consultation on EU-U.S. regulatory cooperation – financial regulatory cooperation, data flows and cybersecurity chapters

Key points:

- **Financial regulatory cooperation:** the EBF believes that the existing framework for EU-U.S. financial regulatory cooperation, the EU-U.S. Financial Regulatory Forum (the Forum), while important and improved in comparison to its predecessor (the Financial Markets Regulatory Dialog), could be further enhanced. We believe that dialogue between regulators, while crucial, should be complemented by a binding obligation to act jointly towards uniform implementation of internationally agreed standards, leading to globally integrated, safer and more resilient financial markets.
- **Data flows:** as the free movement of data is a vital component of the modern economy and international trade, further steps should be taken in order to ensure legal certainty with regards to transatlantic data flows. The EU/U.S. trade agreement represents a perfect opportunity to provide certainty for market participants that flow of data will not be hampered.
- **Cybersecurity:** the EU and the U.S. share key priorities in cybersecurity, such as protecting critical infrastructures and developing cyber protection and resilience measures. Therefore, it is paramount that they develop a closer cooperation on these issues.

1. Financial regulatory cooperation

The EBF believes that, in order to be meaningful, the financial regulatory cooperation should be incorporated as a separate chapter into a trade and investment agreement negotiated between the EU and the U.S. Such chapter should be underpinned by effective institutional arrangements and should allow regulators from both sides of the Atlantic to meet on a regular basis to discuss planned and ongoing regulatory initiatives. These arrangements should help to prevent that the U.S. or the EU resorts either to regulatory unilateralism instead of aiming for the consistent implementation of internationally agreed

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

standards or to the extraterritorial application of national rules, resulting, eventually, in regulatory fragmentation, protectionism and retaliatory measures.

In particular we believe that:

- The Parties should ensure better cooperation on the international fora and should also work together to ensure the consistent implementation and application of internationally agreed standards.
- The Parties should consult each other in advance on proposed financial regulations and other measures which may significantly affect markets of the other Party.
- The Parties should cooperate towards achieving equivalence of both regulatory systems based on the objectives sought and agreed between them.
- These commitments should be underpinned by a robust institutional framework to ensure that the necessary expertise of financial regulators is available and represented.
- Finally the processes of regulatory cooperation should be transparent and should allow participation of affected stakeholders in the EU and the U.S.

In order to preserve regulatory agencies' independence, they should retain an "opt-out" option on grounds of national regulatory principles if they cannot find agreement with their transatlantic counterparts. But such rejection of regulatory cooperation should be made transparent and explained to both political leadership and the broader public in the U.S. and the EU.

The envisaged regulatory cooperation framework should be forward looking and should not be used to undermine already implemented regulations or to weaken the existing high standards of protection of the markets and market participants. Moreover, it should allow regulators to tackle all future issues affecting financial markets as they arise while preventing the re-appearance of the regulatory divergence which may lead to balkanization of the markets and regulatory arbitrage.

2. Data flows

Further steps should be taken in order to ensure legal certainty with regards to transatlantic data flows. Currently, the EU-U.S. Privacy Shield acts as a mechanism through which European companies can transfer data of European data subjects to certified US companies. However, although the Privacy Shield provides a more robust framework for the exchange of data and imposes stronger obligations on U.S. companies to protect European's personal data, the fate of its predecessor leads to concern and uncertainty as its robustness.

The free movement of data is a vital component of international trade. It has become an everyday necessity for firms in a wide range of industries to perform everyday tasks and access technology provided abroad such as Cloud Computing or Artificial Intelligence. Financial services firms store and process personal data to operate retail and corporate accounts, provide lending, execute securities operations, make and execute investments, undertake research and development, and prevent financial crime. Effectively managing a multinational workforce, whether by a financial services firm or a firm in another sector, also requires the transfer of personal data among jurisdictions.

At the same time, ensuring strong privacy and data protection rules are vital. These protect data subject's fundamental rights and help underpin consumers' confidence in digital and data-based services.

The latest developments with regards to data protection and privacy in the U.S. are encouraging. The debate on data protection and privacy is taking speed in Washington DC, with several hearings having taken place in both the U.S. Chamber of Representatives and the U.S. Senate. Furthermore, several U.S. congressmen and women have expressed their will to establish a data protection framework at federal level in the U.S., with the framework established by the General Data Protection Regulation in the European Union having been referenced. An adequacy decision or a data exchange framework incorporated in a binding trade agreement would go a long way in ensuring legal certainty for both EU and U.S. players and ensuring a high level of protection for both EU and U.S. citizens alike.

3. Cybersecurity

Cyber-attacks are rapidly increasing, they have an international impact, and are a threat not only to customers and businesses on both sides of the Atlantic, but also to digital and physical trade flows, in which the financial sector plays an important part. For the purposes of fostering transatlantic trade and customer protection against cyber risks, the EBF supports the creation of a more harmonised European and international regulatory environment. By agreeing on internationally recognised rules and standards, businesses, financial institutions and customers would benefit from a safer, faster and more guaranteed trade of products and services at global level.

The EU and the U.S. share key priorities in cybersecurity, such as protecting critical infrastructures and developing cyber protection and resilience measures. In this context, specific areas of interest for EU-U.S. cooperation would include:

- A common taxonomy: by strengthening the existing cybersecurity dialogue and increasing collaboration between the U.S. and EU agencies in charge of the implementation of the main cybersecurity-related legal frameworks (e.g. NIST framework in the U.S., NIS Directive in the EU), a common taxonomy across the two regulations and jurisdictions could be achieved. On one hand, this would help better understand the characteristics and impact of multi-sector and cross-border cyber-attacks and would, therefore, improve the quality of cyber responses. One the other hand, this could also be the basis for an effective information sharing on cyber incidents between the EU and the U.S.
- Cybersecurity certification standards: in light of the new EU framework for cybersecurity certification established by the Cybersecurity Act for ICT products and services, the mutual recognition of cybersecurity certificates and/or the alignment between existing cybersecurity certification schemes, could also lead to international accepted technical requirements, standards and procedures. Such alignment will facilitate the movement and use of such products and services in both the EU and the U.S.
- Resilience testing frameworks: fragmentation in the testing field between the EU and the U.S. as well as between EU Member States themselves is adding to the compliance burden of cross-border financial institutions and financial market infrastructures. Regulators on both sides of the Atlantic could work closer together to develop compatible and mutually accepted testing frameworks to facilitate compliance and enhance the cyber maturity of the financial sector actors.

- Cybercrime prosecution: U.S. and EU should collaborate in prosecuting cyber-criminals acting within their borders as well as in preventing and prosecuting attacks on data confidentiality, integrity and availability of critical infrastructures.

About EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.1 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu

For more information contact:

Blazej Blasikiewicz
Senior Policy Adviser
b.blasikiewicz@ebf.eu
+32 2 508 37 32