19 MAY 2021

The importance of international data flows in the European financial ecosystem

Executive summary

Data flows are essential to a thriving European digital economy and will be a key driver in making the 2020s the 'Digital Decade'. This is especially relevant in data-rich sector like finance. Studies show data analytics can reduce payments' fraud by between 3 and 30%.[1] Allowing financial data to flow globally is key to improve the security, resilience and innovation of the EU financial ecosystem.

We call on EU policy-makers to boost the international position of EU financial players through adherence to global standards and dialogue with global partners, not by restricting the sector's ability to move data.

International financial data flows are already subject to robust provisions under the General Data Protection Regulation (GDPR). They protect payment and other types of financial data while and after it is transferred and stored outside the EU, by subjecting data transfers to stringent legal mechanisms. We highlight in particular the following transfer mechanisms under the GDPR:

- Standard contractual clauses (SCCs) for transferring personal data to non-EU countries. They require companies to undertake case-by-case assessments of their cross-border data transfers and implement additional safeguards when needed. The new draft set of SCCs aimed to reinforce further safeguards in place.
- Binding corporate rules (BCRs). They set out how companies assess the validity of requests they receive from foreign governments and indicate processes to resolve remaining conflicts.

Below we elaborate in more detail on the importance of global data flows in the financial sector and the validity of existing rules to effectively protect EU businesses and consumers.

[1] McKinsey, 'Combating payments fraud and enhancing customer experience', avaialble at https://www.mckinsey.com/industries/financial-services/our-insights/combating-payments-fraud-and-enhancing-customer-experience

Table of contents

Benefits of international data flows for European consumers and financial entities

Anti-money laundering

We acknowledge the importance of addressing emerging money laundering (ML) risks in the financial ecosystem and support the EU's goal to establish a comprehensive Anti-Money Laundering (AML) policy framework at European level. Such efforts should be coupled with a strong emphasis on ML risk awareness in the industry as well as the further development of a culture of ML risk analysis in the sector. This will help to generate cutting-edge AML solutions able to constantly adapt to ever-evolving threats.

In such an endeavour, **data transfers between EU and non-EU countries are part of the solution to address ML risks**. Erecting barriers to data and information flows hinders companies' ability to successfully identify malicious actors by making use of innovative applications.

Fight against fraud and financial crime

Safeguarding the international free flow of data is a powerful weapon in preventing the consequences of financial crime, which materially affects the wellbeing of businesses and consumers.

The scale, sophistication and complexity of fraud and other financial crime is rising. Estimates put its cost for the global economy at almost €2 trillion a year.[2] Data is the most powerful tool to tackle this problem. That is because effective fraud mitigation depends on:

- *Real-time data analysis*. Fraud detection models demand sophisticated monitoring of transactions and rapid detection at the point of interaction to interpret and weigh the risk of fraud for each payment transaction, whether domestic or cross-border.
- *Training data***.** The volume, quality and variety of data is of primary importance to build effective fraud detection models. Excluding data inputs generated from intra-EU transactions, or limiting the analysis to a single country or region, deprives the fraud model of the training it needs. It makes it blind to patterns of fraud which originate or spread across the EU. Innovative and effective global fraud, AML, counterterrorism financing models must capture transaction data in and across regions. Fraud and other financial crime are borderless.

[2] World Economic Forum, 'Why we need to talk about financial crime,' available at https://www.weforum.org/agenda/2018/01/we-need-to-talk-about-financial-crime

Security and resilience of financial services

A global technological footprint and the ability to rely on geographically distributed infrastructure are key factors to ensure security and operational resilience of financial services.

Global data transfers allow financial services firms to shift operations from one region to another. As COVID-19 shows, this is essential to address local challenges to business continuity. Businesses would have not been able to cope with local lockdowns had cross-border transfers of the underlying data not been in place.

Global data transfers also help reduce network latency, which is the time it takes for data or a request to go from source to destination. Global financial institutions routinely make use of such transfers while maintaining the appropriate legal and security safeguards. Customers benefit from quicker response times in online banking and next-generation customer-facing banking services.

Cost reduction

Banks and merchants rely on data centres and around-the-clock support services accessible from multiple locations. Sharing such resources amongst banks and across borders provides for flexibility, scalability and cost savings.

A report indicates that data localisation measures deter companies from investing in cloud networking and accessing innovative tech solutions, resulting in companies paying 30-60% more for their computing needs.[3] Building local infrastructure beyond the needs of the market would make such services more expensive and less flexible, and likely prevent SMEs' access to some of these services altogether. Data localisation of payment-related services create other types of extra costs, such as those for (re)localising back-office for technical support, call centres, customer service, dispute resolution and all other core functions that require access to payment data in order to operate.

Innovation

Access to data is at the core of fintech innovations based on AI and blockchain. Data localisation requirements would erect barriers for European fintech start-ups to leverage these technologies.

[3] Leviathan Security Group, *Quantifying the Cost of Forced Localisation*, available at https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf

The top 50 fintech start-ups in Europe are valued, collectively, at over €78 billion. Fintech adoption among digitally active consumers is rapidly growing in Europe[4] and in key non-EU markets, where it has jumped from 30% to 60%.[5] These trends offer significant opportunities for Europe's fintech industry to expand at home and internationally.

It is key to maintain the international free flow of data in place. It provides incentives for companies to keep investing in data science in Europe and introduce new data-driven products and services on the market with better customer experiences overall.

Validity of existing rules to effectively protect EU businesses and consumers

International data flows are subject to robust provisions under the General Data Protection Regulation (GDPR), which requires companies to implement accountability and privacy by design programmes aiming to:

- Assess and mitigate potential risks when processing payment data of EU citizens and keep a record of such impact assessments.
- Be transparent towards individuals with respect to how their data is handled and shared with third parties, including with foreign governments.
- Provide training and awareness to all staff handling personal data, including on how to effectively protect EU payment and other personal data at all times.

The GDPR protects payment and other types of financial data while and after it is transferred and stored outside the EU.

In particular, the GDPR subjects data transfers to stringent legal mechanisms that require in-depth assessments and safeguards from companies, along with enforcement powers from data protection authorities (DPAs).

Standard contractual clauses (SCCs) approved by the European Commission require companies to undertake case-by-case assessments of their cross-border data transfers, considering the level of protection offered under the data protection law and the surveillance practices of the destination country, and to implement additional safeguards when needed. The new draft set of SCCs adopted by the European Commission have

[4] EY, 'How FinTech is fuelling an ecosystem future in Europe,' available at How FinTech https://www.ey.com/en_us/banking-capital-markets/how-fintech-is fuelling -fueling-an -ecosystem -future -in Europe-europe, 2019

[5] EY, 'Global FinTech Adoption Index 2019' available at https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/financial-services/ey-global-fintech-adoption-index-2019.pdf

been reinforced through more detailed indications on how to address conflicts of law and clearer procedures to handle government requests to data.[6]

Binding corporate rules (BCRs) approved by competent DPAs set out how companies assess the validity of the requests they receive from foreign governments and indicate processes to resolve remaining conflicts. These may include a DPA referral.

FOR MORE INFORMATION, PLEASE CONTACT:

Ray Pinto

Digital Transformation Policy Director

ray.pinto@digitaleurope.org / +32 472 55 84 02

Vincenzo Renda

Senior Policy Manager for Digital Industrial Transformation

vincenzo.renda@digitaleurope.org / +32 490 11 42 15

Thomas Hellebrand

Policy Officer Digital Transformation

thomas.hellebrand@digitaleurope.org / +32 492 46 78 17

[6] European Commission, 'Data protection - standard contractual clauses for transferring personal data to non-EU countries (implementing act)', available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Cothefmmission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, ESET, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK