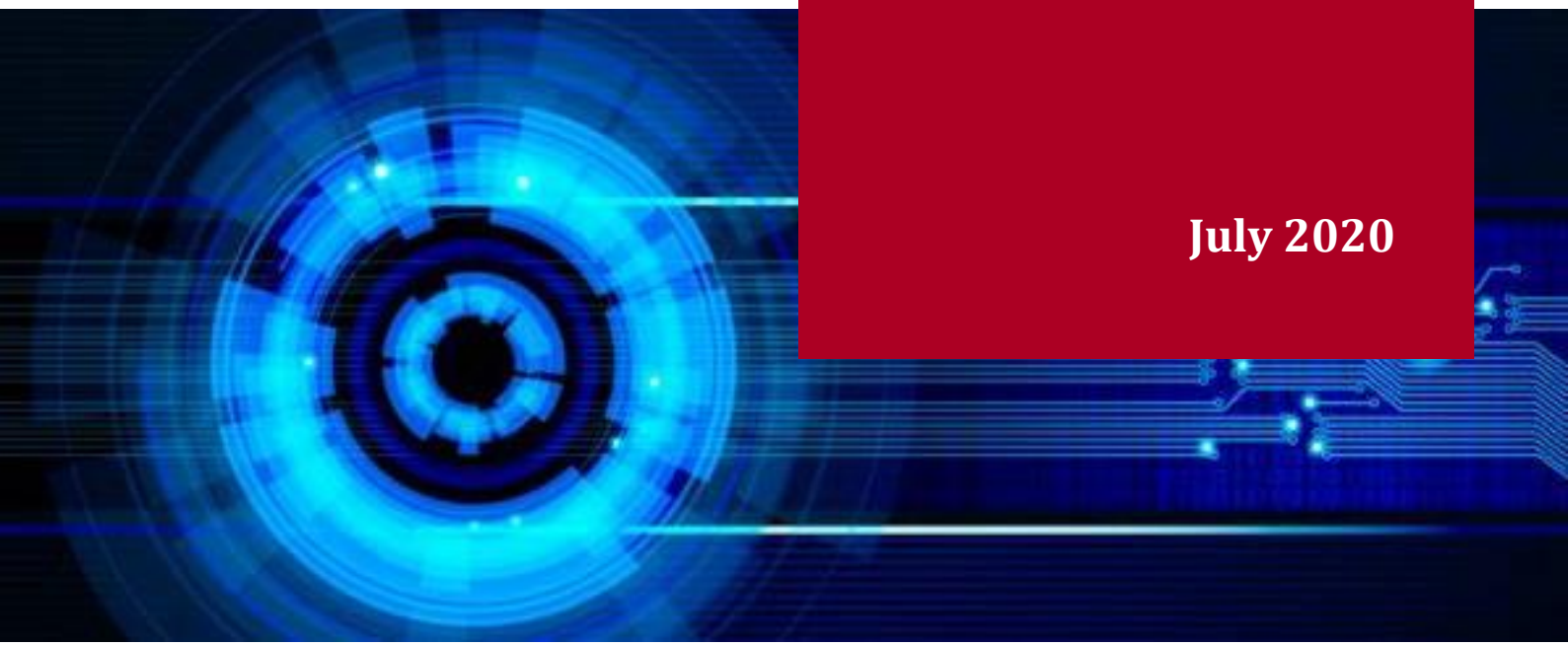
KREAB

DIGITAL FINANCIAL SERVICES

BRUSSELS BULLETIN



July 2020

IN THIS ISSUE

THIS MONTH'S FOCUS:

GDPR
Is the EU's "trademark" data protection framework a success story?

Cybersecurity
Commission publishes Security Union Strategy

Blockchain
Blockchain Observatory issues 2018-2020 report

Interchange Fees
No legislative review proposed

DIGITAL FINANCIAL SERVICES TIMELINE

CONSULTATIONS

ESMA:
"Draft Guidelines on Outsourcing to Cloud Service Providers"
Closes 1 September

IOSCO:
"Principles on Outsourcing"
Closes 1 October

European Commission
"Revision of the NIS Directive"
Closes 2 October

European Commission
"Roadmap on the eIDAS Regulation"
Closes 2 October

IOSCO:
"The use of Artificial Intelligence and Machine Learning by market Intermediaries and asset managers"
Closes 26 October

FOR MORE INFORMATION PLEASE CONTACT
Kelsey Paulding
kelsey.paulding@kreab.com

GDPR:

Is the EU's "trademark" data protection framework a success story?

Joyce Kolman, Executive Associate at Kreab, looks at the road ahead

On 25 May 2020, the EU celebrated the 2-year anniversary of its General Data Protection Regulation (GDPR); one month later, the European Commission published an evaluation report concluding that a review would be premature at this stage. Although adopted only by the EU, the GDPR imposes obligations onto any international firm if it collects personal data connected to EU citizens. The GDPR has also become a global reference point, with similar rules having emerged in Singapore, South Korea, Japan, Australia, and California. Commission Vice-President Věra Jourová called the GDPR "a European trademark", contrasting it with the approaches in America and China.

However, while the EU champions itself as the leading data protection regime, the evaluation report shows that many obstacles remain in the effective enforcement of the GDPR. Experiences on the ground have shown that enforcement is at risk due to a variety of reasons: a lack of resources for national Data Protection Authorities (DPAs), inaction against BigTech's data protection violations, SMEs' lack of regulatory clarity, Member States' fragmented (or even lack of) implementation of the rules, and ongoing court cases questioning the validity of international data transfer mechanisms.

Looking forward, there are many areas which can be addressed. Firstly, it is key that national DPAs have sufficient technical and financial resources. The Commission's report and a recent study by digital rights NGO *Access Now* shows that most DPAs are still unequipped to effectively enforce the GDPR. Under the one-stop-shop mechanism, it is especially the Irish and Luxembourgish DPAs who have been overwhelmed with cases involving large online platforms headquartered in their territories. While their inquiries continue to stack up, many cross-border investigations still are unresolved.

Secondly, for the effective functioning of the Single Market and to avoid unnecessary burden on companies, it is essential that national legislation does not go beyond the margins set by the GDPR or introduce any additional requirements. The Commission's report indicates that current fragmentation is caused by the extensive use of specification clauses and derogations from the general prohibition to process special categories of personal data. On the other extreme, some Member States have disregarded the new rules. Hungary, for instance, has decided to suspend GDPR data subject rights to respond to the COVID-19 crisis, while Slovenia has not implemented the GDPR yet.

Thirdly, for the GDPR to be applied consistently across industry, it is essential that SMEs receive sufficient support and guidance from their DPAs. A 2019 GDPR Small Business Survey showed that around half of small businesses were not sure whether they comply with the following two key requirements: i) describing data processing activities in clear, plain language to data subjects, and ii) identifying a lawful basis for processing data. Many SMEs were also unfamiliar with basic data security concepts, such as encryption.

Fourth, the availability of trustworthy international data transfer mechanisms is crucial for the continuous protection of EU citizens' data when their data is transferred outside of the EU. The GDPR provides several such mechanisms, including adequacy decisions (e.g. Privacy Shield), Standard Contractual Clauses (SCCs), and Binding Corporate Rules (BCRs). However, the existing SCCs concluded under the 1995 Data Protection Directive do not consider the new GDPR requirements for data controllers and processors and are not adapted to all transfer scenarios. The CJEU has recently ruled against the validity of the Privacy Shield. Responding to this ruling will be a key next step for Vice-President Jourová given its impact on transatlantic data flows.

The 'fitness' of the GDPR is further challenged by COVID-19-related surveillance measures and emerging technologies such as blockchain, the Internet of Things (IoT) and facial recognition. Although the GDPR is intended to be technology neutral, France's DPA (CNIL) has observed that when data is registered on a blockchain, it is technically impossible for companies to grant a request for erasure (Art. 17 GDPR).

Promising initiatives to foster GDPR enforcement are in the Commission's pipeline. Yet, the EU will need to remain vigilant about new data protection threats posed by emerging technologies, whilst ensuring that the GDPR does not hinder innovation.

KREAB

Cybersecurity

Commission publishes Security Union Strategy

The Commission's new Security Union Strategy for 2020-2025 brings together the full range of security needs, such as protection and resilience of critical infrastructure, protection against cyber-attacks, hybrid threats, cybercrime, terrorism and organized crime, including identity theft. The Strategy defines key priorities and actions to address digital and physical risks, taking into consideration the need for strategic autonomy for EU supply chains and risks stemming from new technologies and their use for malicious purposes. Overall, the Strategy aims at creating a future-proof security environment in all sectors from financial, energy, healthcare, transport to judiciary and law enforcement through the following common objectives:

- Building capabilities and capacities for early detection, prevention, and rapid response to crises
- Focusing on results based around careful threat and risk assessment
- Linking all players in the public and private sectors in a common effort.

Most of the concrete actions identified in this Strategy were already presented in the Commission's Work Programme for 2020. For instance, the revision of the NIS directive, the upcoming Cybersecurity Strategy, the review of legislation on freezing and confiscation and on Asset Recovery Offices, and legislation on the protection and resilience of critical infrastructure. The Strategy emphasises the need to address increased interconnectedness and interdependency in critical infrastructures and to have in place protection and resilience measures, both cyber and physical. Given the high dependence of the financial sector on IT services and its high vulnerability to cyber-attacks, a first step will be the upcoming initiative on the digital operational resilience for financial sectors. The Strategy also focuses on proper implementation and enforcement of existing and future legislation and will be monitored through regular Security Union reports.

Next steps: The Commission invites the European Parliament and the Council to endorse this Security Union Strategy as the basis for cooperation and joint action on security in the next five years.

Blockchain

Blockchain Observatory issues 2018-2020 report

On 26 June, the European Blockchain Observatory and Forum published it 2018-2020 Conclusions and Reflections Report. The report outlines the Observatory's work over the past two years on the relationship between blockchain and a wide variety of topics including financial services, smart contracts, digital identity, healthcare, education, sustainability, and artificial intelligence. To recall, the Observatory was set up by the European Commission to bring together stakeholders and policymakers to analyse and report on a wide range or cross sectoral blockchain themes. With respect to financial services, the report highlights work done around digital assets, private vs public blockchains for financial market infrastructure, stablecoins, and regulatory action. Specifically, the report notes that regulators have been more focused on the risks of digital assets. The group recommends authorities should continue efforts to ensure healthy growth of digital asset use in an innovation friendly environment which is safe for consumers. Any regulation is recommended to be technologically neutral, should anticipate innovation and should avoid fragmentation across Member States.

Next steps: The Commission is expected to publish its Blockchain Strategy in Q3 2020

Interchange Fees

No legislative review proposed

On 29 June, DG COMP published a report on the impact of the Interchange Fees Regulation (IFR) for card-based payment transactions. The Commission's report builds on a comprehensive study commissioned to EY and published on 11 March. According to the report, the main objectives of the Regulation have been achieved, as interchange fees for consumer cards have decreased, leading to reduced merchants' charges for card payments, and ultimately resulting in improved services to consumers and lower consumer prices. Furthermore, market integration has improved through the increased use by merchants of acquirers (banks servicing merchants) located in other Member States (cross-border acquiring services) and more cross-border card transactions. However, further monitoring and reinforced data gathering are necessary in some areas, including those where only limited time has elapsed since the Regulation entered into force. Given the positive impact of the IFR and the need for more time to see the full effects of the Regulation, the report is not accompanied by a revision legislative proposal.

KREAB FINANCIAL SERVICES AND TECHNOLOGY FORUM

Kreab's Financial Services and Technology Forum (FSTF) allows stakeholders to engage in high-level discussions on the most pertinent technological and regulatory topics. Launched in 2014, the Forum has addressed a broad spectrum of topics, such as security tokens, crowdfunding, blockchain, payments, data protection, and Artificial Intelligence. This year the FSTF will host quarterly events on issues likely to take centre-stage in 2020, including crypto-assets, Artificial Intelligence in FS, Instant payments, and cybersecurity in FS.

DIGITAL FINANCIAL SERVICES TIMELINE 2020