COVID-19 KEY EU DEVELOPMENTS POLICY & REGULATORY UPDATE

No. 91 | 9 November 2022

This regular alert covers key regulatory EU developments related to the COVID-19 situation. It does not purport to provide an exhaustive overview of developments and contains no analysis or opinion.

LATEST KEY DEVELOPMENTS

Competition & State Aid

- European Commission releases draft revised Market Definition Notice and opens public consultation
- Second meeting of EU-US Joint Technology Competition Policy Dialogue
- European Commission approves further schemes under Ukraine Temporary Crisis Framework

Trade / Export Controls

- European Commission adopts proposed Regulation to increase the availability and use of instant payments in euro
- European Commission publishes third Report on assessment of risk of money laundering and terrorist financing

Medicines and Medical Devices

- European Commission reaches agreement with BioNTech-Pfizer on improving Member State management of vaccine needs

Cybersecurity, Privacy & Data Protection

- European Commission publishes proposed Regulation on data collection and sharing relating to short-term accommodation rental services
- European Commission, EU Member States and ENISA simulate large-scale cyber-attacks in “Blueprint Operational Level Exercise”
- ENISA publishes Threat Landscape 2022 Report

COMPETITION & STATE AID

Competition

European Commission releases draft revised Market Definition Notice and opens public consultation (see here and here)

On 8 November 2022, the Commission made public the draft revised Market Definition Notice and opened a public consultation on the draft Notice.

This is the first revision of the 1997 Market Definition Notice, which provides guidance on the principles and best practices of how the Commission applies the concept of relevant product and geographic market in enforcing EU competition law. The revision process seeks to take into account significant market developments over the years, and the draft Notice reflects the extensive review process launched in April 2020, including views gathered from over 100 stakeholders on the current Notice.

The draft Notice, in particular, reflects digitalization, globalization, and new ways of offering goods and services. As noted by the Commission, the role of online platforms is ever-increasing due to the growth in e-commerce, which was further strengthened due to the COVID-19 pandemic, which incentivized consumers to more heavily rely on their use of search engines, social media and online entertainment media (*see Commission Evaluation of the Commission Notice on the definition of relevant market for the purposes of Community competition law of 9 December 1997 (here)*).

The draft Notice's main objective is to boost guidance, transparency and legal certainty for businesses to facilitate compliance. The proposed changes provide new or additional guidance on various key market definition issues, such as:

- Explanations on the principles of market definition and how market definition is used for the purpose of applying competition rules.
- Greater emphasis on non-price elements such as innovation and quality of products and services.
- Clarifications on the forward-looking application of market definition, especially in markets expected to undergo structural transitions, such as technological or regulatory changes.
- New guidance on market definition in digital markets, for example multi-sided markets and "digital eco-systems" (e.g. products built around a mobile operating system).
- New principles on innovation-intensive markets, clarifying how to assess markets where companies compete on innovation, including through pipeline products.
- Expanded guidance on geographic market definition, such as the conditions for defining global markets and the approach to assessing imports.

Comments on the draft Notice may be submitted until 13 January 2023. On the basis of evidence gathered during the review process, including

	comments received in the present public consultation, the Commission will revise and finalize the draft Notice in view of having a new Market Definition Notice in place in Q3 2023.
Second meeting of EU-US Joint Technology Competition Policy Dialogue (see here)	On 13 October 2022, the second meeting of the EU-US Joint Technology Competition Policy Dialogue (TCPD) took place between European Commission Executive Vice-President and Competition Commissioner Margrethe Vestager, US Federal Trade Commission Chair Lina Khan, and Assistant Attorney General for Antitrust of the US Department of Justice Jonathan Kanter. To recall, the EU-US TCPD seeks to help the EU and US to address common perceived challenges in technology and digital markets. Its first meeting was on 7 December 2021 (see here). Commissioner Vestager has earlier commented on the prominence of technology, both in serving to recover from the COVID-19 pandemic and in raising complexities in safeguarding competition, individuals, and democratic values. This includes shared EU and US ambitions for unprecedented levels of funding on innovation from 5G and fibre rollout to advanced digital skills (*see Jones Day COVID-19 Update No. 71 of 13 December 2021*). This second TCPD meeting took stock on the progress made on EU-US cooperation efforts to ensure and promote fair competition in the digital sector. Among others, the discussion focused on the: – importance of forward-looking analysis in the field of technology to identify future key markets and potential issues in the digital sector; – adoption of effective remedies in digital cases; and – need to keep merger regulations suited to a digitalized economy. The TCPD will continue with high-level meetings, in addition to regular discussions at technical level. The TCPD was created alongside the EU-US Trade and Technology Council (TTC), which focuses on coordinated EU-US approaches to global trade, economic, and technology issues and the strengthening of transatlantic trade and economic relations. (*see Jones Day COVID-19 Update No. 84 of 17 May 2022*).
State Aid	
European Commission approves further schemes under Ukraine Temporary Crisis Framework (see here)	The Commission continues to approve additional measures under the State aid Temporary Crisis Framework for State Aid measures in the context of Russia's invasion of Ukraine. To recall, in adopting this Crisis Framework, the Commission noted that the conflict had significantly impacted the energy market, and steep rises in energy prices had affected various economic sectors, including some of those particularly affected by the COVID-19 pandemic, such as transport and tourism. The conflict has also disrupted supply chains for both EU imports from Ukraine (in particular, cereals and vegetable oils) and EU exports to Ukraine.

The Commission recently prolonged (until 31 December 2023 (instead of 31 December 2022)) and expanded the Crisis Framework (*see Jones Day COVID-19 Update No. 90 of 28 October 2022*).

Among the latest schemes under the Crisis Framework (until 9 November 2022):

- €16.8 billion Danish guarantee scheme to support energy companies in the context of Russia's war against Ukraine
- €1.34 billion Danish scheme to support energy intensive companies in the context of Russia's war against Ukraine
- €16.8 billion Danish guarantee scheme to support energy companies in the context of Russia's war against Ukraine
- €3.4 billion Danish scheme to support energy intensive companies in the context of Russia's war against Ukraine
- €1.5 billion Belgian scheme to support energy suppliers in the context of Russia's war against Ukraine

Notably, the Crisis Framework complements the various possibilities for Member States to design measures in line with existing EU State aid rules. For instance, State aid measures under the Crisis Framework may be cumulated with aid granted under the COVID-19 Temporary Framework, provided that their respective cumulation rules are respected.

The Crisis Framework, applicable since 1 February 2022, will be in place until 31 December 2023. During its period of application, the Commission will keep the Framework under review in light of developments regarding the energy markets, other input markets, and the general economic situation. Prior to the Crisis Framework's end date, and in view of maintaining legal certainty, the Commission will assess whether it should be prolonged.

TRADE / EXPORT CONTROLS

European Commission adopts proposed Regulation to increase the availability and use of instant payments in euro (see here)

On 26 October 2022, the European Commission adopted a proposed Regulation regulating instant credit transfers in euro,* in view of making instant payments (IPs) in euro available to all businesses and individuals holding a bank account in the EU and in EEA countries.

The proposed Regulation responds to the Commission's Retail Payment Strategy of 2020 (see here), which noted that the COVID-19 pandemic further reinforced the shift to digital payments and included a call for an initiative aimed at the prompt, full uptake of IPs in the EU.

The broad-scale adoption of IPs, according to the Commission, can also serve to support a quicker post-pandemic recovery of the European economy, as money is reinjected into the economy at a faster pace (i.e., IPs' very nature induces a higher velocity of money circulation in the economy) (*see Commission's Impact Assessment Report accompanying the proposed Regulation (see here)*).

The proposed Regulation addresses four key requirements regarding euro IPs:

- Universal availability: All payment services providers (PSPs) that offer credit transfers in euro (with very targeted exceptions), must offer euro IPs to all of their customers.
- Affordability: Charges for euro IPs must be equal to or lower than the charges for traditional, non-instant euro credit transfers.
- Increased trust: Providers of euro IPs will be required to verify the match between the bank account number (IBAN) and the payment beneficiary's name in order to alert the payer of a possible error or fraud before the payment is made.
- Greater efficiency in screening persons subject to sanctions: Towards facilitating the processing of euro IPs while preserving the effective screening of persons subject to EU sanctions, each PSP that offers euro IPs will be responsible for screening its own clients, both:
  - when a payment account is opened; and
  - via at least, daily updates, of its customer records in relation to the latest EU sanctions lists. This new daily procedure will replace PSPs' current and inefficient use of transaction-by-transaction screening methods, which are not adapted to IPs. PSPs cannot verify, within short time limits, inaccurately flagged transactions, which are then rejected on the side of caution (up to 9.4% of cross-border IPs are rejected due to a suspected breach of EU sanctions, but such rejections are erroneous in 99.8% of cases).

Timing: Obligations under the proposed Regulation are expected to be introduced in steps, as the Commission seeks to allow payment service providers to spread their internal resources over a longer period of time and to optimize implementation costs. For instance, the proposal foresees that the obligation to offer the service of receiving euro IPs will apply 6 months after the Regulation's entry into force, followed by the obligation to offer the service of sending euro IPs, which will apply 12 months after the Regulation's entry into force for payment service providers located in Euro Area Member States.

* *The proposed Regulation amends the 2012 Regulation 260/2012 on the Single Euro Payments Area (SEPA) and the 2021 Regulation 2021/1230 on cross-border payments.*

European Commission publishes third Report on assessment of risk of money laundering and terrorist financing (see here)

On 28 October 2022, the European Commission released its third Report on the assessment of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.

The Report seeks to assist Member States in identifying and addressing money laundering and terrorist financing (ML/TF) risks. It highlights two key impacts in assessing these risks:

- The COVID-19 crisis led to unprecedented global challenges and economic disruption. The new circumstances have enhanced the money laundering risk in many economic sectors and business activities; and

- With Russia's war against Ukraine, the EU broadly expanded sanctions imposed by the EU and U.S. following Russia's illegal annexation of Crimea in 2014, which had already led to, in particular, a surge in Russian applications for investor citizenship schemes and the increased risk of sanctions evasion and potential laundering of illicit funds.

The Report analyzed the ML/TF risks of 43 products and services (grouped within 8 categories) that threaten the EU internal market, such as the following:

- Financial sector (e.g., deposit on accounts, retail and institutional investment, transfers of funds, virtual assets). For example, crypto-assets carry a significant ML/TF risk, due to the ease of transferring crypto-assets to different countries as well as the absence of uniform controls and prevention measures at a global level. In this respect, the Report notes that the proposed AML/CFT Regulation (see here), intended as the EU's "single rulebook" on AML/CFT would, in particular, address the misuse of anonymous instruments (such as crypto-assets) by extending the list of obliged entities to include all crypto-asset service providers;

- Gambling sector: The gambling sector reflects rapid economic expansion and technological development, with a strong growth of the online sector during and after the COVID-19 pandemic. Competent authorities have reported a further increase in risks stemming from online gambling since the publication of the Commission's second Report in 2019. The Report recommends, in particular, that competent authorities build programs to raise awareness among online gambling operators of the emerging risk factors impacting the sector's vulnerabilities, including the use of anonymous e-money and virtual currencies; and

- Free-trade zones (FTZs or "free zones"). This sector continues to present high ML/TF risks, as FTZs seek to facilitate trade by offering various advantages from a customs and taxation perspective and are conducive to secrecy. These features may make FTZs more likely to facilitate offences or abuse, such as tax avoidance, as well as the export of counterfeit and pirated products. The Report indicates that the Commission is currently undertaking, in particular, an evaluation of the costs/benefits of EU free zones, including the risk of possible misuse, both in the customs and taxation area.

Also on 28 October 2022, the Commission released new guidance on the use of public-private partnerships (PPPs) to more efficiently combat ML/TF (see here). Such PPPs generally imply establishing a framework for sharing information between Member State financial intelligence units, law enforcement authorities, and the private sector. In recent years, the Commission reports that PPPs have developed to exchange strategic information (e.g., trends in criminal activities and ML/TF risk indicators) and operational information (e.g., concerning specific cases, transactions, known persons).

MEDICINES AND MEDICAL DEVICES

European Commission reaches agreement with BioNTech-Pfizer on improving Member State management of vaccine needs (see here)

On 9 November 2022, the Commission agreed to an amendment of the purchase agreement with BioNTech-Pfizer for COVID-19 vaccines in view of facilitating Member State management of their vaccine supply and delivery needs.

The amendment ensures that Member States may request the delivery of vaccine doses to a designated central storage facility, rather than directly to the Member State. This arrangement will enable Member States to better oversee the storage of ordered doses and to receive additional storage capacity.

In announcing the amendment, European Commissioner for Health, Stella Kyriakides, stated: "*At the request of our Member States, we have worked tirelessly with vaccine manufacturers to find flexible arrangements for the delivery of safe and effective COVID-19 vaccines to ensure that demand is met and that they have access to the doses when they need them most.*" (*free translation*)

The Commission further noted that Member States currently receive the adapted BioNTech-Pfizer BA. 4/5, ensuring better protection against dominant variants.

CYBERSECURITY, PRIVACY & DATA PROTECTION

European Commission publishes proposed Regulation on data collection and sharing relating to short-term accommodation rental services (see here)

On 7 November 2022, the Commission published the proposed Regulation on data collection and sharing relating to short-term accommodation rental services (STRs).

STRs have become critical to the EU tourism sector, with fast-paced growth largely boosted by the platform economy. The COVID-19 crisis confirmed this trend, with STR bookings during the summers of 2020 and 2021 exceeding those in the summer of 2018.

The Proposal seeks to enhance transparency in the field of STRs and to enable public authorities across the EU to promote a balanced tourism ecosystem. The Commission notes that public authorities require quality data on STRs to develop policies and rules to improve services to travellers and local communities (e.g., better waste, water supply management or transport services, and addressing affordable housing issues).

The Proposal would replace currently disparate Member State rules by a single framework for data sharing by online short-term rental platforms with public authorities, which would increase legal certainty and ensure that the exchanged data is standardized and interoperable.

On data protection, the Proposal indicates, in particular, that it lays down the grounds for lawful processing of personal data that is necessary in view of increasing the STR sector's transparency and provides for data protection safeguards to ensure full compliance with the GDPR.

The Proposal provides for measures such as:

	• Harmonized registration procedures *(required only where Member States wish to obtain data from platforms)*. Harmonized registration procedures, which must be fully online and user-friendly, will enable competent authorities to collect information on hosts and units relating to STRs. Public authorities will receive this data through newly created national "single digital entry points." When completing registration, hosts should receive a unique registration number. Hosts must register and display the correct numbers. Public authorities may suspend registration numbers and ask platforms to delist non-compliant hosts. • Streamlined data sharing between online platforms and public authorities (*required only if authorities have registration systems)*. Online platforms shall report data to public authorities once a month concerning the number of rented nights and guests. Lighter reporting possibilities are foreseen for small and micro platforms. • Re-use of data, in aggregate form, for the purposes of compiling national and European statistics. • Rules on implementation. Member States shall monitor the implementation of this transparency framework and establish the relevant penalties for non-compliance with the Regulation. The Proposal would also complement existing instruments, such as the Digital Services Act (*see also Jones Day COVID-19 Update No. 90 of 28 October 2022*) and the 2020 Directive on administrative cooperation in the field of taxation to address the urgent need to defer certain time limits for the filing and exchange of information in the field of taxation because of the COVID-19 pandemic (see here). The Proposal will now undergo discussion by the European Parliament and the Council of the European Union. If adopted, upon entry into force, Member States will have a two-year period to establish the necessary mechanisms for data exchanges.
European Commission, EU Member States and ENISA simulate large-scale cyber-attacks in "Blueprint Operational Level Exercise" (see here)	On 7 November 2022, the Commission, senior cybersecurity representatives of the Member States, and the EU Agency for Cybersecurity (ENISA) took part in a two-day "Blueprint Operational Level Exercise" (Blue OLEx) to test crisis management procedures. The annual Blue OLEx event forms part of the EU Cybersecurity Strategy (see here). The exercise, hosted in Vilnius, Lithuania, took place physically for the first time since the COVID-19 outbreak. This large-scale cybersecurity exercise aims at enhancing common coordination, situation awareness and decision-making process, while fostering trust-building and information sharing, including between Member States and the Commission. It was undertaken particularly in light of the upcoming implementation of the Network and Information Systems Directive (NIS2 Directive) (*see also Jones Day COVID-19 Update No. 84 of 17 May 2022*), The exercise was organized by the Lithuanian Authorities with the support of ENISA within the framework of the European Cyber Crisis Liaison Organization Network (CyCLONe), which will be formally established with the

	adoption of NIS2 Directive. CyCLONe shall ensure the regular exchange of information among Member States and EU entities and contributes to implementing the European Commission Blueprint (see here) for a rapid emergency response in case of a large-scale cross-border cyber incident.
ENISA publishes Threat Landscape 2022 Report (see here)	On 3 November 2022, the European Union Agency for Cybersecurity (ENISA) published the 10th edition of the annual ENISA Threat Landscape Report covering the period July 2021 to July 2022 (*see 9th Report in Jones Day COVID-19 Update No. 66 of 2 November 2021*). In setting out the cybersecurity threat landscape, the Report identifies the top threats, major threat-related trends, threat actors and attack techniques, as well mitigation measures. The Report emphasizes the impact of the Ukraine-Russia conflict and the COVID-19 pandemic on the cybersecurity threat landscape: – The conflict between Russia-Ukraine reshaped the threat landscape during the reporting period, with significant increases in hacktivist activity, cyber actors conducting operations in concert with military action, cybercrime, and aid by nation-state groups during this conflict. – On cybersecurity trends specifically driven by the COVID-19 pandemic, the Report identifies, e.g.: • Accelerated widespread adoption of cloud-based services supporting the business processes of organizations, which provides attack opportunities for cybercriminals; • A global decrease in malware in 2020 and early 2021, which was linked to the COVID-19 pandemic and the fact that employees worked from home, thus limiting the visibility of malware infections typically found on corporate infrastructures. By end-2021, when more people started returning to the office, a heavy increase in malware was notified and is mainly attributed to crypto-jacking and IoT malware; and • Ransom denial of service (RDoS) or extortion by distributed denial of service (DDoS) mostly targeting businesses in the e-commerce, finance and travel sectors on a global scale. The Report notes, for instance, that sites used to combat COVID-19 remain a primary target of DDoS. For example, Italian and Bulgarian COVID-19 related services were hit by DDoS attacks. The Report also sets out proposed high-level mitigation measures in light of identified threats, attack techniques, and trends, such as the following recommendations for organizations: – Concerning malware, e.g., performing regular vulnerability scanning to identify and address vulnerabilities; and periodic security awareness and training are critical, as ransomware often relies on social engineering to lure users into clicking a link; – On threats against availability, e.g., building a team of specialists capable of responding to DDoS attacks, which is critically important to maintain system availability and operation; and ensuring a “plan B” to quickly restore business-critical services and reduce the mean time to

recovery; and

- On ransomware, e.g., implementing a secure and redundant backup strategy, including maintaining offline, encrypted data backups that are regularly tested, following the organization's backup procedures.

The Report notes that its key findings in this assessment are based on multiple and publicly available resources, as provided in the references used for developing the document.

LAWYER CONTACTS

Kaarli H. Eichhorn
Partner, Antitrust & Competition Law; Government Regulation; Technology
Brussels
keichhorn@jonesday.com
+32.2.645.14.41

Cristiana Spontoni
Partner, Health Care & Life Sciences; Government Regulation
Brussels
cspontoni@jonesday.com
+32.2.645.14.48

Dr. Jörg Hladjk
Partner, Cybersecurity, Privacy & Data Protection; Government Regulation; Technology
Brussels
jhladjk@jonesday.com
+32.2.645.15.30

Rick van 't Hullenaar
Partner, Government Regulation; Investigations & White Collar Defense
Amsterdam
rvanthullenaar@jonesday.com
+31.20.305.4223

Nadiya Nychay
Partner, Government Regulation; Antitrust & Competition Law
Brussels
nnychay@jonesday.com
+32.2.645.14.46

Lucie Fournier *(Associate),* ***Cecelia Kye*** *(Consultant), and* ***Justine Naessens*** *(Associate) in the Brussels Office contributed to this Update.*