DIGITALEUROPE

20 OCTOBER

DIGITALEUROPE priorities for the digitalisation of financial services

Executive Summary

Finance is the largest ICT user in the world with about 20% of all ICT expenditure.[1] An industry-friendly fintech regulatory framework is the precondition for any effort to put the sector at the centre of digital transformation in Europe. Technologies like artificial intelligence can help to identify fraud and improve efficiency in finance processes for the customer's benefit. Contactless payments emerged as a key ally in addressing hygiene and social distancing concerns during the pandemic.

For EU finance policy-makers, preserving the role of digital as an enabler of innovation must be the top priority. We should proceed with caution on legislation where existing rules already guarantee oversight and ensure technology-neutrality stays at the core of any activity. New e-payment means for consumers, cloud services for financial institutions and other emerging applications will be a defining element of the industry moving forward. Citizens and society will be the first to reap their benefits.

We strongly recommend the EU the following:

- **EC legislative proposal on the Digital Operational Resilience of Financial Services (DORA)**: the EU should harmonise ICT and security incident reporting requirements across the EU. The final framework should facilitate the adoption of new technology by EU financial services organisations. Crucially, it should also align with the ongoing review of the NIS Directive and seek to strengthen the existing outsourcing framework, not introduce unjustified new direct oversight requirements for ICT third-party providers.
- **Retail Payment Strategy for the EU:** the EC should uphold the importance of economic openness, a level-playing field for all industry players and technology-neutrality. Consumer choice and market-based solutions, rather than legislation, should be the driver for payment solution adoption in Europe. The mid-2021 review of the PSD2 should emphasise

[1] European Commission, Public consultation on a digital operational resilience framework for financial services, 2019

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

how industry players are still adapting to the complex regulatory changes this Directive has brought. Reopening it prematurely would be unhelpful.

As the EU institutions work to elaborate on the announced initiatives, we are ready to discuss and share our expertise and experiences.

Table of Contents

1. Digital Operational Resilience Act (DORA)

1.1 ICT and security requirements

Any ICT and security risk management framework for financial entities should be based on common principles. These include:

- **Use of existing ICT standards**. The use of global standards such as ISO 27001, ISO 9001, ISAE 3402 and EU standards such as TIBER-EU for testing requirements. This is key to prevent fragmentation in this space and promote best practices.
- **Definition of Recovery Time Objective (RTO) and Recovery Point Objective (RPO) based on agreements between financial institutions and their service providers.** Legislation cannot contemplate all ICT uses so as to prescribe universally adequate or appropriate RTOs and RPOs. Authorities should rather promote non-regulatory guidance and share best practices to define risk assessments that look at the criticality of the system, process or function for the financial institution and its clients.
- **Promotion of voluntary information-sharing among cybersecurity vendors.** A relevant example to consider is the Cyber Threat Alliance (CTA).[2] It has signed a cooperative working agreement in early 2020 with the Financial Services Information Sharing and Analysis Center (FS-ISAC) to cooperate on threat intelligence.[3] The Cyber Information and Intelligence Sharing Initiative (CIISI-EU) promoted by the ECB is, too, a useful information-sharing platform bringing together a community of public and private entities.

1.2 ICT and security incident reporting requirements

The EU must design a more harmonised ICT and security incident reporting framework. Actors in the digital space such as banks and cloud service providers would greatly benefit from it. There are unnecessary costs today stemming from fragmented and inconsistent provisions among Member States, which in the case of multi-tenant public cloud services are even higher.

DIGITALEUROPE urges EU policy-makers to:

[2] The CTA includes 26 cybersecurity member companies from around the world that share threat intelligence with each other to better protect their customers and increase the impact across the ecosystem.

[3] More info here

- Make coordination with the ongoing review of the NIS Directive[4] a key priority of any ICT and security incident reporting policy effort for financial services.
- Focus on principles and risk-based regulation and alignment with internationally recognised standards such as ISO and NIST to increase harmonisation and avoid overly-prescriptive requirements. These efforts should especially be centred on:
    - Taxonomy of reportable incidents, including the distinction between an actual or suspected/potential/unsuccessful incident
    - Reporting templates, including phased reporting and a common definition of each reporting phase. Requirements should be generic in the early phases, and progressively more detailed later
    - Reporting timeframe, including the start of the reporting window
    - Materiality thresholds:
        - confirmed vs unconfirmed incidents. Reporting should be limited only to confirmed incidents. This is crucial notably in the context of multi-tenant public cloud services, where there is a vast number of potential threats and unsuccessful attacks. Informing of an incident all potentially impacted customers, only to find later that it actually impacted just a sub-set of them, plays only in the hands of malicious actors. It also gives insufficient and non-actionable information to the regulators when there is an obligation to report incidents under investigation.
        - the meaning of “detection”, i.e. what triggers reporting
        - Simple vs complex thresholds. In an incident situation, organisations must focus on resolving the incident rather than making complex calculations.
        - Minor vs. impactful incidents. The added value of reporting minor incidents (e.g. incidents that have no impact on individuals or that were resolved quickly) may not be clear and/or in proportion with the resources required to address the reporting, both from an organization and a regulator’s standpoint. This does not mean that organizations should

[4] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

not track and record all incidents and remain accountable for how they resolve those.

- Number of reports and competent authority. There should be one unified report to a single competent authority, or at the very least, to multiple authorities closely cooperating.

1.3 Oversight of third-party providers (including outsourcing)

1.3.1 Oversight framework

In the effort to develop a new direct oversight framework for critical ICT third-party providers, it is important the EU adheres to the principles of technological neutrality and proportionality, as well as aligns with the established international solutions. Given the global nature of both the financial and ICT sectors, it is critical the EU framework maintains a level playing field to ensure EU financial services organisations remain competitive. Moreover, whatever approach Europe is going to take will set a new, unprecedented example for cloud governance and outsourcing in other parts of the world. It is therefore absolutely critical to consider its proportionality and effectiveness, as well as a principles-based and risk-based foundation.
DIGITALEUROPE, which is uniquely positioned to represent financial services firms, cloud services providers (CSPs) and other service providers, firmly believes the EU oversight framework for third-party providers should observe the following principles:

- *Harmonisation and strengthening of the existing requirements, rather than introducing conflicting obligations for the firms and their ICT third-party providers.* The outsourcing guidelines, such as those produced by the EBA[5] and the EIOPA[6] as well as the draft ESMA guidelines under consultation[7] - represent a welcome effort to harmonise requirements for cloud outsourcing across Europe and provide additional regulatory certainty to firms and their providers. The new oversight framework needs to build on this valuable work and share the same principles. A global approach to outsourcing will be further defined in the new IOSCO Principles on Outsourcing,[8] which need to be taken into consideration by

[5] European Banking Authority (EBA), Guidelines on outsourcing arrangements, 2019
[6] European Insurance and Occupational Pensions Authority (EIOPA), Guidelines on outsourcing to cloud service providers, 2020
[7] ESMA, ESMA consults cloud outsourcing guidelines, 2020

[8] ISOSCO, Principles on outsourcing: consultation report, 2020

the European policymakers to ensure consistency with the international benchmarks. We urge policymakers to avoid regulatory and market fragmentation with the introduction of the DORA. At the very least, for outsourcing to 'Critical Third-Party Providers' (CTPPs), DORA should supersede the current outsourcing regime.

- *It is key to establish trust and a clear passport to operate for the CTPPs in scope and for their financial services customers.* Similarly, once the direct oversight framework over CTPPs is adopted, **it should replace the existing requirements for financial services customers to notify or seek regulatory approval** when implementing cloud deployments with CTPPs. This will help to **streamline the compliance process**. Outsourcing to CTPPs should be exempt from this notification process in the EU, as their security and operational practices would be independently verified by the competent overseeing authorities - regardless of the specific customer deployments. As part of this process, it will be important for overseeing authorities to ensure that National Competent Authorities are sufficiently informed of deployments and developments, in order for them to satisfy their supervisory mandates.

- *The proposal needs to stimulate cloud adoption, not impede innovation.* Cloud technology has become an important driver of innovation for the financial services sector across Europe and globally. It provides significant benefits to raise productivity, reduce costs and enable firms to augment their security capabilities. At the same time, cloud platforms have become an accelerator to the adoption of AI and machine learning technologies, allowing financial institutions to improve consumer experiences, increase accuracy and efficiency of internal compliance, risk assessment processes and regulatory reporting, as well as innovate their financial products. Today, we are seeing an increased trust and confidence in the safety and security of public cloud technology across the globe, both from the industry and regulatory community. A recent report commissioned by the Bank of England recommends the Bank to ''embrace cloud technologies, which have matured to the point they can meet the high expectations of regulators and financial services''.[9] The Financial Stability Board (FSB) has recently ''determined that there are no immediate financial stability risks stemming from the use of cloud services by financial institutions''.[10] We urge EU policymakers to support and champion this approach. Introducing a new **oversight regime should**

[9] Future of Finance, Review on the outlook of the UK financial system: What it means for the Bank of England, 2019

[10] Financial Stability Board (FSB), Third-party dependencies in cloud services: Considerations on financial stability implications, 2019

grant additional assurances and incentives for the European financial services sector to move to the public cloud at scale. A burdensome supervisory framework, non-compatible with the fast-paced technological innovation in this space, could significantly slow down the adoption of new technologies across Europe, directly impacting on their ability to address customers' demand and competitiveness.

- *Scope of the oversight*: it is imperative to assess the criticality of services and functions outsourced by financial organisations to evaluate the potential level of systemic risk. Not all outsourced tasks have the same level of risk. Such assessment must treat all outsourcing providers in the same way, regardless of whether they are active in the public cloud, private cloud, or some variant. It must also duly acknowledge influential studies[11] concluding there is no immediate financial stability risk for financial institutions from the use of cloud services. Ultimately, **the oversight needs to be performed based on the materiality and importance of the outsourced services, not the type or scale of the outsourcing provider**, and be principles and risk-based.

- *Competent authority***:** It is crucial that the supervisory power leverages an effective mechanism which allows for the relevant expertise and inter-agency collaboration. The EU framework will be the first of its kind globally, hence we strongly believe this demands an effective and well-coordinated effort to ensure its success. We agree with the current proposal granting core oversight powers to the ESAs which will help ensure the effectiveness of this approach. To avoid fragmentation, National Competent Authorities (NCAs) should not have additional oversight powers at the national level.

- *Avoidance of regulatory overlaps:* while we appreciate that Article 1 (2) of DORA foresees a clear hierarchy between DORA and the NIS Directive (NISD) for financial services qualifying as Operators of Essential Services (OESs) under NISD, the proposal does not foresee such hierarchy or delineation between DORA and NISD for ICT providers (or CTPPs), who may qualify as Digital Service Providers (DSPs) under the NISD. We ask the Commission to duly consider this aspect and avoid regulatory overlaps between different pieces of EU legislation, especially as the NIS Directive is currently being reviewed.

[11] Financial Stability Board (FSB), Third-party dependencies in cloud services: Considerations on financial stability implications', 2019

With these principles in mind, the oversight framework needs to acknowledge that not all traditional prudential regulatory and enforcement measures would be proportionate and effective in the context of ICT regulation:

- *Mandatory remediation by supervisors*: any findings by regulators as a result of the oversight process should be subject to discussion with the relevant third-party provider to ensure effective implementation and balance the twin desires of robust regulation and high levels of innovation - in line with the existing audit procedures. The US Bank Service Company Act[12] could present a constructive example of an existing international practice in this area, where financial services regulators have a direct audit right over technology providers as part of the oversight but the audit does not include remediation measures impeding providers' ability to maintain appropriate controls. We also caution against potential supervisory action to mandate **changes or termination to the firms' relationship with their providers.** This ultimately needs to be a business decision of the financial services institutions based on their thorough risk assessment and exit strategies. Unilateral regulatory action could be harmful to the integrity and security of the firms' outsourced services. There are also considerations around complexity, costs and timings of migration issues to take into account in such unilateral regulatory action. We strongly recommend that the EU adopts a proportionate approach where the regulatory observations and findings resulting from the oversight regime should form ***recommendations*** for technology providers to **implement changes in a risk-based, proportionate way, tailored to the nature of their services and over a reasonable amount of time**.

- A clear *appeal process* should also be introduced for the technology providers to address potential gaps in the identified recommendations. Any further considerations to sanctions and penalties as part of remediation should equally be proportionate and well-measured.

- *Approach to sub-outsourcing*: it needs to be consistent with the current EBA and EIOPA outsourcing guidelines and consider the nature of cloud one-to-many multitenant services. We believe that today's outsourcing frameworks already grant supervisors sufficient control over providers' sub-outsourcing arrangements which is equally reflected in customer contractual commitments. A similar approach was taken in the U.S., where regulators have the authority to request information about the sub-outsourcing arrangements of technology service providers, but they do

[12] Section 7 of the US Bank Service Company Act

not have the authority to place restrictions on these relationships which would disrupt the secure provision of technology services.

- *Testing:* any requirement for operational resilience and penetration testing by financial institutions that include third-party providers need to be assessed against the technological reality of these processes, potential risks and trade-offs. Whilst we agree that cooperation between firms and their providers for testing purposes is important, as recognised for example in the FSB Effective Practices for Cyber Incident Response and Recovery Consultation,[13] it needs to take into account that cloud services are a one-to-many multi-tenant environment. From this perspective, a public cloud provider cannot simulate a disruption of its service to support a single customer's testing because this could impact the integrity and security of the operations of other customers. At the same time, cloud service providers offer tools to customers to perform independent testing and simulate disruptions of their own cloud resources. If collaborative testing is required, it is critically important that such exercises remain voluntary, risk-based and bilaterally agreed upon between the customers and their providers. Recognising this view, the U.S. authorities agreed that mandatory, regulator-led penetration testing presents more security risks and vulnerabilities than it reduces.

- *Data residence:* the global footprint of technology operators and reliance on a geographically distributed infrastructure are key factors to ensure security and operational resilience of cloud services. Similarly, global financial institutions with customers across the world may choose to locate and transfer their data internationally for latency and other business purposes, maintaining the appropriate legal and security safeguards. For these reasons, any forced data localisation requirement, as suggested by some Member States, are overall incompatible with the security and resilience of cloud services. We welcome the EC approach confirming that no additional data localisation requirements should be introduced as part of DORA and the oversight practice. **Data location should remain the customer choice based on risk assessment**, and their providers need to offer technological capabilities and contractual commitments to support these choices.

- *Multi-vendor and interoperability requirements*: we understand regulator concerns over the perceived market concentration risk, and believe that those need to be addressed in conjunction with the recognition of the security and operational resilience of cloud systems. At a micro level, hyperscale cloud providers have security and operational resilience

[13] More info here

capabilities that benefit financial services customers and surpass those features that are available on-premise. The overall threat of a single point of failure is, in our view, unjustified. With this in mind, principles of flexibility and industry-led best practices in approaching portability and interoperability need to be maintained, consistent with the multi-stakeholder efforts under SWIPO. Equally, whilst it is a sensible business practice, a multi-vendor strategy needs to remain the customer choice, based on their risk assessment and business priorities, not a regulatory provision. Policymakers should further support and endorse principles of openness and interoperability in the industry, but it is too early to formulate any of those in prescriptive regulatory requirements which would slow down the adoption of cloud as a whole. We agree with the approach taken by the DORA proposal on these issues.

- *Customer data privacy and security*: we note in the proposal the regulators' broad powers to request customer data from the CTTPs as part of the oversight and general investigations. We caution policymakers against an overreaching approach and urge them to institute appropriate safe harbours to guarantee that privacy and security of the financial institutions' and their customer data are not compromised in the course of the audits.
- *Third-country regime*: we note unhelpful language in the proposal to dissuade firms from using third-country providers. These provisions need to be clarified as they would ultimately deter European firms against global technology players, despite the quality and commercial benefits of their services, and would create competitive challenges for the EU market denying its financial firms access to the benefits of global technology innovation.

1.3.2 Standard Contractual Clauses for cloud arrangements with financial sector entities

Both the EBA "Guidelines on Outsourcing" and the EIOPA's "Guidelines on Outsourcing to Cloud Service Providers" provide a valid, principle-based template for the standardisation of contractual clauses. Whilst setting a high bar in terms of audit rights and sub-outsourcing, the EBA and EIOPA's approach provides the flexibility needed to meet specific requirements for the services being used. This is fundamental given the differences across providers and to avoid a race to the bottom amongst them, a factor which could potentially hinder security and innovation.

We recommend the EBA and EIOPA approach is taken as a foundation to define the scope of standardisation in the first place.

Separately, we urge policymakers to adopt a fully transparent and collaborative process to further design the applicable Standard Contractual Clauses in dynamic consultation with the industry, cloud service providers and financial firms included, to allow for their expertise to be taken into consideration in the definition of the scope and language of such Clauses.

Finally, we believe these Standard Contractual Clauses need to remain voluntary, principles-based and not excessively detailed or prescriptive. This is key to allow innovation in this space and avoid hindering the benefits of public cloud.

2. A retail payments strategy for the EU

The best way for the EU to encourage the emergence of European retail players is by supporting a wide variety of payment options for consumers. Additional regulations will only make it more difficult for new actors to grow. It will also reduce the variety of payment options to the detriment of Europe's consumers and society. Thanks to digital technology, European citizens have never had access to so many payment options at one of the lowest costs globally. The announced EU's retail payment strategy will turn into a success if it pays close attention to two main principles:

- **Economy openness**: Europe has developed a robust payment system and has led the way on many payment technologies (chip & pin, contactless). It has been able to do so thanks to an open economy that fosters innovation.
- **Technology-neutrality**: The EU should promote greater choices for consumers without any bias for any specific solution based on technology or provider headquarters. Competition is the best tool for the emergence of a variety of solutions for consumers.

2.1 Payment innovation

Europe's payment market has traditionally been very fragmented, with strong national preferences and differences in the payment means used by EU citizens. Consumer preference, not legislation, should drive its harmonisation. E-commerce and mobile payments are growing because they are convenient for citizens. Mandating the adherence to the SEPA Instant Credit Transfer (SCT Inst.) scheme, the replacement of regular SEPA Credit Transfer (SCT) with SCT

Inst. or other similar binding provisions would stifle Europe's payment innovation. All digital payment solutions are relevant for merchants as long as they guarantee safe, secure, simple and efficient transactions. We strongly recommend policy-makers to:

- **Focus on supporting global, non-proprietary technology standards** like EMVCo, rather than favoring via legislation one digital payment option over another or through adopting regional standards. Any European standard may come at the cost of global payment acceptance.
- **Avoid mandating the adherence to SCT Inst. for payment service providers (PSPs).** If the Commission were still to support a mandate, 2023 should be the end-date for implementation as industry players need time to adapt.
- **Recognise shifting consumer preferences from cash towards e-payments.** Although cash is still relevant for vulnerable people, its hegemony is waning. It is also a cause of the shadow economy. Existing e-payment solutions are safer and more secure.
- **Identify relevant existing international standards or foster the development of new ones by Standard Development Organisations (SDOs), so to facilitate cross-border interoperability for customer on-boarding and payments authentication.** The review of the eIDAS Regulation can foster this process of harmonisation, allowing enough room for market actors to propose interoperable solutions.
- **Boost digital literacy across society.** Basic digital skills are a must for everyone to be an active citizen of society and benefit from digital payment innovation.

2.1.1 Technical infrastructure in payments

The EU must foster competition, innovation and consumer protection in the Single Market, not prescribe technology solutions. There are examples of Member States, such as Germany, that adopted legislation obliging technical service providers in payments to give access to such technical services to all PSPs. As no PSP has made use of this law, its benefits remain unclear.
We ask policy-makers to refrain from replicating this type of regulatory approaches elsewhere, as they do not enhance competition, financial security, data protection, user autonomy or privacy. They rather create a disincentive to innovate, add a security risk and interfere with the integrity of proprietary technology solutions, which are open to all payment service providers and card issuers without exclusivity or discrimination so to maintain intact the level playing field. Such type of measures are examples of regulatory actions that undermine

the integrity of the Single Market. Indeed, technology in the payments sector, including Near Field Communication (NFC), must ensure users' privacy and data protection as well as functional and payment security. To foster competition, it must facilitate user autonomy and choice, e.g. by allowing for an easy switch of services.

2.1.2 Instant Payments

Instant payments are a promising opportunity to further develop the payments market. Experience in countries like Sweden and Denmark shows that its features (ease of use, faster payments) provide a real added value for citizens.

Yet, the technology also faces challenges:

- Risks to Anti-Money Laundering (AML) goals: fraudsters could exploit the real-time processing capability of the technology to quickly distribute money on different accounts, thereby hindering the detection of financial crime. There are industry solutions to tackle this threat.
- No chargeback process: instant payments do not have a dispute resolution system like cards have, since the system does not rely on a centralised authority.
- Viable business model: instant payments demand a profitable business model so that providers (i.e. banks) can offer new features.

Instant payments are not to be perceived as alternative to other payment means, but rather complementary to them. Just like for other payment means, the industry will find solutions for the technology to reach a high-level of safety and security while remaining convenient for citizens.

2.2 PSD2 implementation and market developments

We oppose reopening of the PSD2[14] at this stage. Industry players are still adapting to highly complex changes PSD2 introduced in aspects such as Strong Customer Authentication (SCA). We cannot yet see the full impact of the Directive on the European retail payments sector, but we do see already some encouraging signs, for instance in facilitating access to the market for PSPs other than banks.

[14] Directive 2015/2366/EU on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

We urge policy-makers to:

- **Refrain from introducing additional measures on top of SCA.** Industry invested to prepare for SCA migration. New measures would be very premature today, especially as SCA has not been fully implemented yet.
- **Review the current regulatory SCA limits for contactless transactions to better reflect consumer average spending, while keeping fraud rates low.** Contactless payments emerged as a key ally in fighting COVID-19. They allowed to reduce the checkout time for consumers and process more sales for retailers, hence increasing the latter's revenues.
- **Introduce a precise and targeted exemption from SCA for unconnected and remote environments** to make sure consumers can continue to make payments onboard aircraft and ships. This follows the EBA's rationale of establishing an exemption where the use of SCA cannot or may not always be applied for operational reasons.

2.2.1 Open Banking under PSD2

DIGITALEUROPE supports the continuation of the Euro Retail Payments Board (ERPB) Working Group on a SEPA Application Programming Interface (API) Access Scheme to advance discussions on open banking. Such work should forge a Scheme operating within the legal and regulatory framework of PSD2. As stated, we are against any possible revision of this Directive today.

The SEPA API Access Scheme should include:

- **delegation of SCA to third-party providers**: this is important to facilitate payment innovation and help ensure a good customer experience.
- **consent dashboards** allowing payment service users to manage the consent to access their data via a single interface.

We are instead against any change to current provisions around authentication methods. PSD2 allows for redirection-only based customer journeys as long as they do not pose an obstacle to third-party providers, which is an assessment made by each national competent authority. Changing this provision would fundamentally disrupt work around SCA's implementation.

2.3 Cross-border payments between the EU and other jurisdictions

The EU should play a role in providing further guidance on a core set of activities that remain blurry at this stage for cross-border payments on a global level. This is the case for AML, Know Your Customer (KYC) or Financial Action Task Force (FATF) guidelines. It can further support the development of competitive and innovative payments in Europe through adherence to global standards, dialogue with global partners and setting of interoperability end-goals for the industry. We identify four main policy goals the EU can achieve with its global partners:

- Secure and harmonised digital identity systems for efficient user experience in payments.
- Global interoperability and international standards to guarantee world-wide acceptance of payment products and services.
- Streamlined licensing and approvals for greater market innovation.
- Consistent and harmonised compliance requirements to introduce new services.

3. Data sharing in finance

Creating Common European data spaces would make more data available for AI applications to thrive. It is however important to ensure that the development of such data space schemes is based on a robust and market-friendly governance framework, ensuring voluntary participation to the schemes.

Enabling and facilitating data sharing is a key element for the digitalisation of the financial sector. It will bring innovative, convenient, more efficient services for consumers, who should be at the centre of such a data sharing ecosystem. It will enable the creation of new data-driven solutions in areas like AI, which is finding its way in applications like fraud identification, anti-money laundering (transaction monitoring, sanction screening, etc.), as well as risk models & risk mitigation measures. It will enhance access to credit for SMEs.

Any effort to advance an open finance policy at EU level should focus on:

- Common data formats

- Clarity on the entities covered, including potential thresholds
- Interoperability across sectors and standardised APIs

We welcome the Commission's announcement of the creation of EU infrastructure to ensure publicly disclosed information relevant to capital markets is available in standardised and machine-readable formats and an EU-funded infrastructure will be set up for public disclosure.

Finally, any open finance policy at EU level should rely on the principle of the free flow of data. It has proved essential in allowing relevant actors in open finance (as well as their providers, including cloud service players) to transfer and store data both across the EU and outside it in line with the strong guarantees of the GDPR and valid data transfer mechanisms. Europe's citizens and digital players are ultimately those that reap the biggest benefits from the free flow of data in open finance. The Commission has been so far supportive of this principle. Together with Member States, it should uphold its criticality in any new open finance initiative.

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.eu / +32 490 11 42 15

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, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

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, 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, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK