DIGITALEUROPE

16 OCTOBER 2023

How to Design a Successful European Payments Market? DIGITALEUROPE's position on the Payment Services Regulation (PSR) and Payment Services Directive 3 (PSD3) Proposals

Executive summary

Valued at €240 trillion in Europe in 2021,[1] electronic payments are essential to Europe's economy. Their importance and value will only increase. As the legislative framework governing electronic payments, **the Payment Services Regulation must deliver logical and common-sense rules that make EU citizens' lives simpler**. Payment security can be achieved without undermining user-friendliness. The two are not mutually exclusive. To achieve this, the EU needs to:

1. **Allow industry flexibility in providing Strong Customer Authentication (SCA),** including by exempting electric vehicle charging stations from the SCA's scope.[2]
2. **Remove Art. 59 from the text, as it unjustifiably makes industry accountable for fraudsters' impersonation scams.** The focus must instead be on raising consumer awareness and detecting criminals through public-private collaboration.[3]
3. **Maintain alignment between data permission dashboards** in this regulation and with those in the Financial Data Access Regulation (FIDA). This is vital to ensure proper data consent monitoring by the customer.

[1] European Commission, *Electronic Payments in the EU, Review of the Payment Services Directive 2* (June 2023): https://finance.ec.europa.eu/system/files/2023-06/230628-payments-fida-factsheet_en.pdf.

[2] For more on this point, see DIGITALEUROPE, *Contactless Payments: An Enabler for e-Mobility in the EU*, (April 2022): https://www.digitaleurope.org/resources/contactless-payments-an-enabler-for-e-mobility-in-the-eu/.

[3] The EU can take cues from successful models like the European Union Agency for Cybersecurity (ENISA)'s Information Sharing and Analysis Centres (ISACs), a leading example of effective cooperation in cyber threat intelligence gathering: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

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

Table of contents

Scope (Art.2)

- **Include payment account data within FIDA:** Payment data currently in scope of this regulation should be included within the scope of the FIDA once it has been set up, is functioning well, and once its data-sharing schemes are available. **The establishment of two different frameworks and sets of rules for what falls under the umbrella of financial data will lead to compliance and regulatory complexity.**
- **Amend definition of AISP to include ability to transmit data to a third party:** The definition of an Account Information Service Provider (AISP) must be modified to clarify that the information they aggregate may be transmitted to a third party to enable that third party to provide another service to the end-user, with the end-user's permission (as opposed to only having the possibility to show this aggregated data to the user). While we welcome that Recital 26 calls for this, it must be included in the Regulation itself. We suggest this wording:

> *"'Account Information Service' means an online service of collecting, either directly or through a technical service provider, and consolidating information held on one or more payment accounts of a payment service user with one or several ASPSPs, at the request of the PSU, with a view to either presenting this information, in a consolidated format, to the PSU, or to transmitting it to another party to enable that party, on the basis of that information, to provide another service to the PSU".*

- **Align the definitions of 'technical service provider' (TSP) under the EU PSR and PSD3 for greater clarity:** A sufficiently broad definition of TSPs (which includes ancillary/supporting services) is needed to ensure TSPs can continue to provide their services and help innovate and modernise the payment infrastructure. Whilst in the PSR a TSP is defined as a provider of services which **support** the provision of payment services, in the PSD3, the same TSP is defined as a provider that is **necessary** to support the provision of payment services. The latter definition thus implies that TSPs that are **not necessary** for the provision of payment services may instead be included in the definition of Payment Services. This is concerning, as TSPs – **necessary or not** - do not constitute payment services as they do not enter at any time into possession of funds to be transferred. We recommend this definition under the PSD3:

> *"'Technical Service Provider' means a provider of services which support the provision of payment services, without entering at any time into possession of the funds to be transferred".*

Strong Customer Authentication (SCA) (Art. 85 – 89)

We recognise that industry innovation and the SCA requirements introduced by the Payment Services Directive 2 (PSD2) helped to considerably reduce the value of fraudulent e-commerce transactions by 50%[4]. We also recognise and welcome the improvements around the SCA framework in PSR, and in particular the recognition that the European Banking Authority should **follow the principle of technology neutrality** when developing upcoming Regulatory Technical Standards (RTSs) **to allow for the development of user-friendly solutions.**

Yet, specific SCA provisions still need a more **flexible approach in order to strike the right balance between security and convenience.** Overly prescriptive SCA provisions will make it disproportionately difficult for customers to complete legitimate transactions. **We recommend setting rules on targeted outcomes for fraud or authentication rates that reflect the complex, multi-party structure behind today's commerce and payment transactions while keeping flexibility on SCA models.**

Preserve independence of SCA elements belonging to same categories (Art.85(12)):

We welcome the addition that the two or more elements on which SCA authentication shall be based *(knowledge – something only the user knows; possession – something only the user possesses; and inherence – something the user is)* **do not necessarily need to belong to different categories as long as their independence is preserved**. This change opens the door to innovative combinations of authentication.

However, **this provision should incorporate two elements:**

- **Art.85(12) must include a concrete definition of independence** to avoid misinterpretation. We propose one that draws on Art.3(35). Namely: ***'By being independent from each other, it should be understood that the breach of one element does not compromise the reliability of the others,*** *and is designed in such a way as to protect the confidentiality of the authentication data'.*
- **The provision must specify that SCA solutions based on the use of two knowledge factors (e.g. two passwords) should not be allowed** as they are not sufficiently secure. Conversely, two possession or inherence factors should be allowed, again provided

[4] European Commission, *Electronic Payments in the EU, Review of the Payment Services Directive 2* (June 2023): https://finance.ec.europa.eu/system/files/2023-06/230628-payments-fida-factsheet_en.pdf.

their independence is sufficiently preserved through the use of different devices.

Merchant Initiated Transactions (MITs) and Mail Orders or Telephone Orders (MOTOs)

- **MOTOs: We welcome the clarification that MOTO transactions are not subject to SCA.** The emphasis that only the initiation – and not the execution – of a payment transaction needs to be non-digital in order for that transaction to be considered as a MOTO and thus not be covered by the SCA obligations is important as without this exception, only cash payments would fall outside the scope of SCA.
- **MIT: We also welcome the clarification that as payee-initiated transactions, there is a need to apply SCA at the set-up of the mandate, but without any need to apply it for subsequent MITs.**
- **MIT refund right: We do not agree with the extension of unconditional refund rights to all payee-initiated transactions from Art.62.1(4).** In cases where there is adequate proof that the intended goods or services have been delivered or, if a good or service was delivered before the consumer cancelled their subscription or, if SCA was done at the mandate set up with clear conditions of the mandate being displayed to the user, then the unconditional refund right should not apply. While we support consumer protection, MITs already offer a high level of protection in comparison with direct debits. **The extension of this unconditional refund rights to MITs would risk having a substantial increase of first party fraud** and would have a negative impact in the entire ecosystem, putting unproportional pressure on merchants.

Liability of TSPs and of operators of payment schemes (Art.58)

Art.58 on the liability of TSPs and of operators of payment schemes **should be revisited to:**

- **Take into account existing liability frameworks** in commercial law (TSPs and operators of payment schemes do not offer SCA services without contracts, and thus are already liable under existing contracts).
- **Reflect the variety of actors that are involved in the payment chain that also play a part in the SCA authentication process** (beyond TSPs and scheme operators) and which TSPs and scheme operators have no control of.

Finetuning Exemptions

The EU PSR requires that the EBA develops Regulatory Technical Standards (RTS) on exemptions from SCA requirements *inter alia*. Our industry experience with SCA and exemptions suggests that the current exemptions regime should be fine-tuned for greater efficiency, user experience, and balance. To this end, **we suggest that further exemptions are envisaged for low-risk and low-value use cases:**

- **Extend the transport and parking exemption** under Article 12 RTS on SCA[5] to transactions for electric vehicle (EV) charging, alternative fuel filling and vending machines. Donations should also be included under this exemption but for up to EUR 50 only. Exempting transactions for EV charging and alternative fuel filling from SCA requirements would help the EU meet its Green Deal goals and contribute to plugging the investment gap in EV infrastructure. Estimates say the EU would need to install 150.000 new electric vehicle charging points each year, or roughly 3.000 per week, to reach its 2025 target).[6]
- **Deferred authorisation:** Introduce a new exemption for airline in-flight transactions taking place in an offline environment. We have seen issues in the case that transactions are performed when no connection is available to authenticate and authorise and are therefore processed later. However, we recommend that a specific floor limit be put in place for this exemption/type of transaction.
- **Extend the secure corporate payments exemption** under Article 17 RTS on SCA[7] to all forms of access to corporate accounts apart from transactions with Travel & Entertainment cards.
- **Fraud calculation for TRA exemption:** We welcome the references in Recital 115 of the PSR acknowledging industry feedback on the need to assess the potential benefits of allowing PSPs to report fraudulent transactions for which they are solely liable. We believe that it will encourage all parties to continue innovating and investing on risk

[5] Article.12, Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

[6] DIGITALEUROPE, *Contactless Payments: An Enabler for e-Mobility in the EU*, (April 2022): https://www.digitaleurope.org/resources/contactless-payments-an-enabler-for-e-mobility-in-the-eu/.

[7] Article.17, Delegated Regulation (EU) 2018/389 *(see footnote 5).*

management technology and we encourage the EBA to take this into consideration when developing the RTS.

- **Limited network exclusion and hybrid cards:** We welcome the fact that this exclusion is maintained and is now included in the Regulation. This will hopefully bring further harmonisation as we still see divergent interpretations as to what it is considered a limited range of good and services. **The future RTS outlining the conditions for this exclusion will need to clearly define what constitutes a limited range of goods and a limited network.** This will provide clear guidance for member states, enabling them to adopt a harmonised approach that avoids creating competitive disadvantages. We would like to point out that the EUR 1 million total value threshold for notification and annual audit opinion, as stipulated in Article 39 of the proposed PSD3, is too low and we would recommend increasing it, in order to enable smaller programs to operate without incurring disproportionate costs associated with these notifications and audited reports.

SCA solutions for vulnerable customers (Art.88)

Whilst we welcome the new requirement to make SCA solutions accessible for vulnerable customers (e.g. the elderly, people with disabilities, non-digitally savvy consumers), we believe that **PSPs should be required to provide non-smartphone-based SCA solutions only to vulnerable customers who do not have access to app-based solutions.**

SCA in relation to Account Information Service Providers (AISP) (Art.86)

The rationale and benefit of requiring AISPs to apply SCA after the ASPSP has applied SCA on initial access to payment account data remain unclear. Instead, the requirement under PSD2, wherein ASPSPs are exclusively responsible for implementing SCA, is more logical.

Maintaining the requirement for ASPSPs to implement SCA would safeguard business continuity and compatibility with existing SCA solutions as well as ensure that small AISPs are not disproportionately affected by being required to make substantial investments to support SCA application. Additionally, there is a potential risk of unauthorised access to customers' data if ASPSPs are unaware of whether the AISP has applied their own SCA within the set timeframe (every 180 days after the initial application of the ASPSP's SCA).

Intervention by the European Banking Authority (EBA) and National Competent Authorities

- **EBA intervention powers:** To encourage dialogue between the EBA and industry, and to prevent rushed decisions, there should be an **explicit right for the relevant PSP or TSP to be consulted before the EBA imposes a temporary prohibition or restriction on a payment or e-money service in the EU.** A prohibition or ban by the EBA should constitute a last recourse, following due consultation with the relevant parties, given the potential severe ramifications for a PSP's or TSP's business operations in the EU.
- **National Competent Authorities: Penalties should be limited to proportionate and adequate measures.** Under the PSR, national competent authorities have been given extensive investigation powers and the ability to impose fines up to 10% of annual turnover (including on both PSPs and TSPs) for specified breaches which given the small size of most PSPs and TSPs, seems disproportionate.

Open Banking & Data Access: Permission Dashboards (Art.43)

- **Consistency of dashboards between FIDA and the PSR is crucial:** This includes allowing data holders to manage data permissions stemming from both FIDA and PSR through a single payment dashboard. **The establishment of two different frameworks and different rules for financial data sharing (FIDA and PSR/PSD3) would hinder customer permission management and entail higher costs and operational difficulties for industry as the dashboards will require significant resources to implement** (as mentioned above under 'Scope', by eventually including payment account data within FIDA, all financial data could be shared through a single dashboard more easily). **Seamless alignments across both regulations is of the utmost importance to avoid confusion on the consumer side, and unnecessary complexity for industry.**
- **Industry principles for dashboard development:** The requirements for configuring the permission dashboards must be **high-level, establishing general principles and leaving flexibility to the data holder in configuring the details.** Permission dashboards can become complex and challenging to manage, especially when dealing with multiple stakeholders across various organisations. The absence of an industry standardised approach to permission dashboards poses

a significant barrier to enhancing transparency and trust and would ultimately lead to confusion for customers.

- **Real-time challenge:** The **obligation on the data holder to manage permissions and access in real-time poses several challenges including ensuring data security,** collecting the appropriate data, integrating distributed data sources, analysing the data using costly resources, ensuring scalability and performance of the infrastructure, and maintaining data quality.
- **Re-establishing permissions: The requirement for dashboards (operated by ASPSPs) to enable payment service users (PSU) to re-establish a permission, which they have previously withdrawn, should be removed (Art.43(2)(c)).** When PSUs re-establish their permissions for specific AIS/PIS services, this should only be done with agreement and in accordance with the applicable terms and procedures of the relevant AISP/PISP.

Payment Service Provider's liability for impersonation fraud (Art.59)

We suggest removing this article. **A pure shift of liability to the PSP for impersonation scams is akin to putting a band aid over a gaping wound: it will not fix the underlying problem long-term.**

Instead, we suggest:

- **Focus on preventing and detecting fraudsters:** Impersonation scams are a major problem that require addressing. However, **by requiring PSPs to cover the costs of impersonation of a PSP employee, we are ignoring the need to focus on preventing and detecting the criminals carrying out the fraud.** Impersonation scam levels and number of victims will not reduce if we do not target those carrying them out.
- **Encourage consumers to be diligent themselves:** Similarly, **shifting the liability entirely to the PSP discourages consumers from being diligent themselves.** EU consumer-related laws should be consistent: **to imply consumer unaccountability in the field of payment services is contradictory to other fields of consumer law** that are based on an average consumer who is reasonably well informed and observant. Erasing gross negligence from the payment services legal framework would entail an unreasonable discrimination

to the payment services industry in comparison to other industries (e.g. insurance, household supplies etc).

- **Raise consumer awareness via third parties:** Another crucial ingredient – to encourage consumers to be diligent themselves - is raising consumer awareness. **Systems and campaigns should be put in place to help them to better recognise, avoid and report scams.**
- **Encourage other actors involved in the payment journey to take scam-mitigating measures:** An Article placing the onus entirely on the PSP for impersonation scams will discourage other actors from taking scam mitigating measures. The collaboration between communication operators must be specified and detailed to be effective in reducing this type of fraud.

Refunds in the case of scams should be limited to unauthorised payments

- **Refunds to payers should remain constrained to *un*authorised payments.** Doing otherwise would have unintended consequences, such as **moral hazard, criminals taking advantages of reimbursement, and PSPs not offering services to reduce their financial liability risk.**
- **This Regulation could also establish certain situations in which the PSP should not be obliged to make reimbursements.** These could take into account: fraudulent activities through channels and means other than those usually used by the PSP; the PSP's efforts to educate and raise consumer awareness about this type of fraud through accessible and standardised channels; the PSP's provision of an online mechanism for verifying communications that the consumer receives etc.
- **The exchange of information between PSPs to prevent fraud via transaction monitoring mechanisms (Art.83) must be stipulated under Art.6(1)c (legal obligation) of the GDPR** and ensure the coherence and compliance of said regulation.
- **The regulation should lay out specific use cases and instances of gross negligence where consumers should partially or entirely bear the responsibility for the fraudulent payment transaction** (Art.59(2)(b)). As examples, we suggest:

- Sharing payment credentials including OTP with third parties and allowing others to use one's device with their biometrics (e.g., fingerprint) enabled and stored in the device.
- Carrying out payments where the amount and merchant name displayed to consumers do not (fully) reflect the intended payment. This may for example be because the merchant's name resembles known entities (e.g., tax office or police). If in doubt, consumers should check with the impersonated entity whether they actually requested the payment.
- Carrying out high risk investments that were clearly indicated as such (with promised returns much higher than market rates), which were delivered but then lost their value.

Authorisation of Payment Transactions (Art.55)

The Commission considers that, with impersonation scams, the difference between authorised and non-authorised transactions is becoming more blurred and complex to apply in practice. We disagree as even in the case of authorised push scams, there is no ambiguity surrounding the fact that the payer **intends** to carry out the transaction at that moment (it is only afterwards that they realise they have been misled and subjected to a scam).

- **Article 55 PSR must refer to "authentication" rather than "authorisation"** as the "authentication" of a payment transaction is something that PSPs are able to demonstrate. "Authorisation" means the payer's consent to carry out the payment transaction as outlined in the contract, encompassing the customer's expression of will. Typically, this 'will' is expressed through the authentication process.

  On the other hand, "authentication" relates to the procedure enabling the PSP to verify the identity of a payment service user.

  Whilst PSPs lack the means to demonstrate whether a payment transaction has been authorised (as they are not able to analyse the customer's state of mind and prove the 'client's will'), they **are** able to demonstrate whether the payment transaction has been authenticated or not.

- **As a second option, we suggest that a clear definition of "authorisation" in the regulation would avoid ambiguities:** It is important to have legal certainty about the authorisation and thus the finality of the transaction. Under PSD2, a payment transaction is considered unauthorised in the absence of consent. Whilst Art.49 states that payment transactions shall be authorised only if the payer

has given its permission for the execution of said transaction, it should also include a definition of authorisation. Such a definition could look like: *"The expression of the permission given by the payer to his PSP to execute a transaction, through the process and in the form agreed between the payer and his PSP. Permission can be given by the payer by using the personalised security credentials."*

Extension of IBAN Verification Services to all credit transfers (Art. 50)

The new service referred to as the "confirmation of payee"[8] (CoP) - likely to be mandated by the future Instant Payments Regulation - has been extended to encompass regular credit transfers within the PSR Proposal. Although the rationale in both cases is consistent - an effort to contribute to the reduction of payer fraud or errors (PSR Recital (70) and Article 50) – **we are concerned that given the fast-evolving nature of fraud, a static IBAN-name check will have a limited contribution to fraud prevention,** covering only fraud scenarios such as scam and whaling, while leaving out other fraud types such as phishing, malware and swap IBAN.

In the event that the obligation to offer the "confirmation of payee" service is extended to regular credit transfers within the PSR, **we urge the co-legislators to take into account that building such a service would be an extensive project requiring significant time** and resources and thus we urge that they take into consideration the same issues raised by industry as in the Instant Payments framework:

- **Flexibility:** Regulators should allow for flexibility in the technical provision of the CoP service in order to ensure the effectiveness of the service in relation to the intended purpose, while providing a good UX and guaranteeing that resources are not allocated needlessly. It would be worth considering whether the European Payments Council may be best suited to develop the design of the service, to ensure its homogeneity.
- **Customer presence:** This service should be implemented only on electronic/digital interfaces with real-time interaction with the Payment User, excluding ATMs, branches, paper-based and phone banking

[8] Article 50(1) PSR Proposal: "In case of credit transfers, the payment service provider of the payee shall, free of charge, at the request of the payment service provider of the payer, verify whether or not the unique identifier and the name of the payee as provided by the payer match, and shall communicate the outcome of this verification to the payment service provider of the payer".

interfaces (CoP will not be feasible in the latter examples, as customers may not be present).

- **Payer filling in payee details:** The CoP provision should only be mandated in situations when the payers themselves fill in the payee details. This therefore excludes Payments at the Point of Sale, e-commerce payments, direct debits or other payee-initiated payment orders, because the risk of misdirected or fraudulent payments is considerably lower and the obligation to offer the CoP service would only add friction.
- **Corporate bulk payments:** These should also be excluded from the CoP provision as: i) this would be a disproportionate requirement compared to the objectives of the Regulation ii) it is it is not feasible since the payer is not present to return the answer and accept or refuse the payment order depending on the matching result and iii) companies have usually made this check before initiating the payment.
- **Fees:** PSPs should be entitled to charge a fee for this service because any new service should be based on an adequate business case for its providers. Additionally, the level of the fee should be left to the market.
- **Liability:** The PSR should include a provision to clarify that PSPs shall not be liable for the execution of a payment to an unintended payee when the Payment User has authorised the payment despite a detected discrepancy via the CoP service.

PSPs should remain free to determine the opt-out possibility of their customers. However, we support the Commission's and Council's approach in the Instant Payments Regulation to leave the possibility to charge for the payee verification service for corporate clients.

Surcharging

Under the EU PSR, the payee cannot request changes for the use of consumer payment cards that are subject to the interchange fee caps set out in Regulation (EU) 2015/751 (the so-called 'Interchange Fee Regulation' or 'IFR'), and credit transfers and direct debits in EUR (e.g. SEPA Credit Transfers and SEPA direct debits) and non-EU currencies.

Surcharging is instead allowed within the limit of the costs borne by the merchant for the following categories of payment cards that are not subject to the interchange fee caps under the IFR (Art. 28(5) EU PSR): commercial payment cards, card issued by 'three-party schemes'.

Member states are, however, allowed to provide a total ban on surcharge at national level also for these 'unregulated' cards (Art.28(4) EU PSR).

Conversely, unregulated three-party payment cards that are not subject to the IFR caps can have higher costs for acceptance. **National approaches to surcharging should aim to ensure a level playing field, for example by allowing merchants to benefit from surcharge to recover the extra costs for accepting those cards.**

New measures for fraud prevention

The PSR should clarify that PSPs remain free to terminate their relationship with a payment service user (PSU) based on the PSPs own determination of fraud risk. The PSR requires PSPs to maintain a TMM (transaction monitoring mechanism) beyond the sole purpose of implementing SCA and SCA exemptions (which was the case under PSD2). This requirement also extends to TPPs. Furthermore, PSPs will enter into 'data sharing arrangements' to share certain information related to instances of detected fraud. However, the proposal also contains certain safeguards that aim at protecting the PSU against potential termination of the contractual relationship (Article 83(6) PSR). **This creates uncertainty as to whether PSPs are allowed to terminate the contractual relationship on their own determination** and for reasons that are not related to the processing of data under Article 83(6) PSR.

Payment Services Directive 3 (PSD3)

- **Licensing of payment institutions:** The PSD3 includes a new requirement for existing Payment institutions (PIs) and Electronic Money Institutions (EMIs) to seek a new authorisation as Payment Institutions (PIs) under the PSD3. Member States can provide mechanisms to automatically grant this new authorisation to existing PIs and EMIs. **We believe that existing PIs and EMIs should be allowed to continue to provide their services under their current PSD2/EMD2 licenses without the need to seek a new PSD3 license.** Nonetheless, **if organisations must reauthorise, this process should be seamless and not provide any additional regulatory or administrative burden.** This is important to ensure business continuity of existing PIs and EMIs and avoid increased costs and regulatory arbitrage.
- **Alignments of Recitals and Regulation:** Recital (25) PSD3 refers to the possibility left to PISPs and AISPs to have initial capital instead of a PII (professional indemnity insurance), yet in the body of PSD3 this option only appears to exist for AISPs (but not PISPs who are apparently always required to have initial capital). PSD3 does not

seem to give PISPs any kind of flexibility regarding the PII that they must hold and arguably, PISPs may have the same difficulties in practice as AISPs when it comes to subscribe to the PII during the authorisation process.

- **Buy Now Pay Later Services:** We welcome the clarification that 'Buy Now Pay Later' (BNPL) services are not a payment service under the PSD3. **For the sake of clarity, the PSD3 should expressly indicate that entities providing BNPL services are nonetheless subject to the PSD3 requirements if they provide payment services in combination with such BNPL services.**
- **Access to payment systems and interplay with SFD:** We welcome the new requirement introduced by the PSD3 to allow Payment Institutions (PIs) and E-money Institutions (EMIs) to directly participate in payment systems that are designated under the Settlement Finality Directive (SFD).

FOR MORE INFORMATION, PLEASE CONTACT:

Vincenzo Renda

Associate Director for Digital Transformation Policy

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

Laura Chaney

Officer for Digital Transformation Policy

laura.chaney@digitaleurope.org / +32 493 09 87 42

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 102 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Applied Materials, Amazon, AMD, Apple, Arçelik, Arm, Assent, Autodesk, Avery Dennison, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, CaixaBank, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, Honeywell, HP Inc., Huawei, ING, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe, NEC, Nemetschek, NetApp, Nintendo, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Pearson, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK