DIGITALEUROPE

22 DECEMBER 2023

European Health Data Space (EHDS): key issues to address in trilogues

Executive summary

While the EHDS is essential for digital transformation in healthcare and to advance health R&I in the EU, the interinstitutional negotiations must address outstanding issues in the positions of both co-legislators. This paper highlights the most significant legislative risks in the EHDS that require attention and recommends solutions to fix those shortcomings:

- The vague definitions of 'electronic health data' and 'data holder' could undermine the interpretation of the entire legislation.
- The ambiguously defined electronic health data categories for secondary use may generate more risks than potential benefits.
- The proposed IP framework would be in conflict with existing legal safeguards aimed at protecting the scientific and technological potential and interests of researchers and innovators. In addition, the EHDS would fall much lower in its standard of trade secrets protection compared to the Data Act.
- The introduction of excessive and unclear data localisation and international health data transfer requirements, on top of the GDPR, may block essential data flows and lead to inconsistent implementation of rules across the EU.
- The proposed rules on EHR systems and wellness applications lack clarity and clear interaction with other legislation, and may lead to a fragmented legal landscape across the EU.

Table of contents

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Electronic health data

Legislative problems

'Personal electronic health data'

One of the fundamental questions of the EHDS is how it defines the contours of 'electronic health data', and how it delineates its subsets. Regarding the definition of '**personal electronic health data**', there is alignment between the legislative positions of Council and EP that it should include 'data concerning health' and 'genetic data', as defined under Articles 4(13) and 4(15) of Regulation (EU) 2016/679 ('GDPR'), that are processed in electronic form. From a healthcare perspective, it is important to include 'genetic data' under the definition of 'electronic health data', as its legitimate processing has huge potential in health R&I and personalised medicine. However, from a data protection perspective, there are uncertainties and growing 'grey areas' where it is not obvious whether data falls under the scope of 'data concerning health' or 'genetic data'. For this reason, it would be useful to provide more clarity about the application of these notions in the context of the EHDS.

The set of electronic health data that does not qualify as 'personal electronic health data'

Another problem under the EHDS (with far-reaching implications) is how it defines the set of data that would fall under the larger scope of 'electronic health data' without qualifying as 'personal electronic health data'.

- If that scope of data were defined along the lines of the Commission's proposal (and EP's position) as '**non-personal electronic health data**' meaning *"data concerning health and (aggregated) genetic data in electronic format that falls outside the definition of personal data"*, then that would be self-contradictory, because 'data concerning health' and 'genetic data' are 'personal data' per se. It is also questionable what '*aggregated* genetic data' would imply considering that aggregation does not have an established definition and there are other generalisation and randomisation techniques that can also guarantee anonymisation.[1]
- Council's position is that the abovementioned scope of data should be defined as '**anonymous electronic health data**' meaning *"data related to health, processed in an electronic form, which does not relate to an identified or identifiable natural person or personal data concerning health processed in such a manner that the data subject is not or no longer identifiable"*. The problem is that this definition simply

[1] See Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (10 April 2014).

paraphrases the description of 'anonymous information' under Recital (26) of the GDPR without considering the possible implications under the EHDS:

- It would lead to a situation of uncertainty that the first part of the definition relies on the assumption that there is a threshold where 'anonymous' data may become 'related to health' without falling under the scope of 'personal electronic health data'.
- In the context of connected products and related services, it would be unclear under what condition would product data or related services data, as described under Recital (15) and Articles 2(5)–(6) of the Data Act,[2] become 'related to health'. Connected products (e.g. connected medical devices, wellness applications, sensors in ambient assisted living systems, or certain product components of hospital information systems) and related services (e.g. algorithms/software or AI systems enabling the functioning of those connected products) may generate or obtain data (such as data relating to hardware status, battery levels, malfunctions, data transmissions, version control, security functions or the location of the product) where there is arguably no clear 'demonstrable relationship' between the data and the capacity to determine the health aspect of a natural person. However, a legal requirement under the EHDS for data holders to make available all such data for secondary use purposes would pose huge security risks for all parties concerned, as it would make digital health systems basically an 'open book'.

Recommended solution

The definition of 'electronic health data' could be reworded as follows:

'electronic health data' means:

(a) personal electronic health data, including **personal electronic health data in pseudonymised format; or**

(b) anonymised electronic health data; or

(c) anonymous statistical electronic health data.

In connection with the notion of '**personal electronic health data**', it would be useful to clarify (in a Recital) that there has to be a **demonstrable relationship** between the data and the capacity to determine (infer, derive or predict

[2] European Parliament legislative resolution of 9 November 2023 on the proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).

information about) the health aspect (health status or health risk) or genetic characteristic of an identified or identifiable natural person based on the data itself or on the data in combination with data from other sources.[3]

'**Personal electronic health data in pseudonymised format**' could be defined as **personal electronic health data that has undergone pseudonymisation in accordance with Article 4(5) of the GDPR**. Pseudonymisation reduces the linkability of a dataset with the original identification of a data subject. It would bring further clarity if the EHDS explicitly stated that those datasets have distinct characteristics.

'Anonymised electronic health data' could be defined as **data obtained as the result of processing (anonymising) personal electronic health data in such a manner that natural persons are not identifiable and cannot be re-identified by any means reasonably likely to be used by the (electronic health) data holder or to whom the data is made available, in particular the (electronic health) data user.**

'Anonymous statistical electronic health data' could be defined as **data obtained as the result of any operation of data collection, processed in electronic form, that is related to the health status, health risk or genetic characteristics of natural persons for statistical purposes in such a manner that natural persons are not identifiable and cannot be re-identified by any means reasonably likely to be used by the (electronic health) data holder or to whom the data is made available, in particular the (electronic health) data user.**

Data holder

Legislative problems

In addition to the shortcomings that stem from the inadequate definition of 'electronic health data', the definitions of '(health) data holder' provided under the legislative positions of Council and EP remain ambiguous, lack consistency with other Union legislations and could lead to implementation problems:

- There is no need to extend the definition of 'data holder' to cover the processing of personal electronic health data in the context of primary use, because it is the controller, in accordance with the GDPR, that bears responsibilities to ensure the rights of natural persons in relation to the processing of personal electronic health data concerning them.

[3] See Article 29 Data Protection Working Party, Letter from the ART 29 WP to the European Commission, DG CONNECT on mHealth, Annex – health data in apps and devices (5 February 2015), 3–5.

- The requirement to make available so-called non-personal/anonymous electronic health data 'through control of the technical design of a product and related services' could lead to implementation problems. An entity that produces such a dataset (e.g. healthcare provider) is often not the entity that controls the technical design of a product and related services (e.g. SaaS provider). The definition of 'data holder' under the Data Act proposal had the very same wording, but it was refined in the legislative procedure. By contrast to the EHDS, it is important to point out that the Data Act also accounts for 'contractually agreed' cases.
- It is not clear what would be the legal basis for determining whether a person/body functions in a specific (e.g. health, care, social security or reimbursement services) sector, or performs research in relation to that sector. Under Council's position, it is also unclear what subjective and objective conditions would the requirement of 'developing products or services intended for the health, healthcare or care sectors' entail.

Recommended solution

The definition of 'data holder' could be reworded as follows:

'electronic health data holder' means a natural or legal person, including public sector bodies, which has an obligation, in accordance with Chapter IV of this Regulation, to make available:

(a) personal electronic health data for secondary use in its capacity as controller or joint controller under Regulation (EU) 2016/679; or

(b) anonymised electronic health data or anonymous statistical electronic health data in its capacity as a database maker under Directive 96/9/EC, alone or jointly with any other rights holder pursuant to a contractual agreement.

Making available electronic health data for secondary use

Legislative problems

The scaling up of the secondary use of electronic health data under a harmonised data governance framework could bring wide-ranging benefits to healthcare-related activities and research in the EU. If the electronic health data categories for secondary use are specified appropriately, then the EHDS could lead to better individual and population health outcomes by facilitating improved resource efficiency, evidence-based practices (real-world evidence), risk stratification, personalised medicine, or by optimising patient pathways.

However, the legislative positions of Council and EP on the **electronic (health) data categories for secondary use** suffer from significant shortcomings. It is vital to address the associated risks to avoid serious consequences. In general, it would lead to uncertainty if the various data categories apply to 'data', 'aggregated data', 'electronic data', 'health data', 'healthcare-related data', 'determinants of health' or 'electronic health data' without there being any clear indication about what some of these data categories would entail.[4] Regarding the specific provisions, major problems include:

- The requirement to make available (electronic) health data directly from medical devices (under both Council's and EP's position) would generate significant security risks. It is important that (only personal) electronic health data obtained or generated by the use of a medical device can be made available only from data repositories/platforms, such as registries for medical devices or from EHRs. Similar risks and solutions need to be considered with respect to the requirement of making available 'data from wellness applications'.
- It is unclear what 'person-generated electronic health data' (Council's position) would entail and whether this category would also cover machine- or sensor-generated data. In the absence of a legal definition, it is also unclear what data from 'other digital health applications' (Council's position) would encompass.
- The requirement to make available 'electronic health data from clinical trials or clinical investigations' as soon as they end would seriously undermine clinical developments in the EU, if data holders are not provided adequate and effective safeguards in the EHDS. In connection with this requirement, it is unclear why EP's position does not make a distinction between clinical trials and clinical investigations, whereas the two are regulated by different regulations.
- The requirement to make available an overly broad category of 'data from research cohorts, questionnaires and surveys related to health' (EP's position) without validation and publication may run counter to scientific considerations and harm the interests of research.
- The protection of the scientific or technological potential of basic or early phase/preclinical research can only be guaranteed through the significant refinement of the rules on IP governance (see below).
- It is unclear (under both Council's and EP's position) whether the requirement to make available 'data from biobanks and dedicated/associated databases' refers solely to poly-user biobanks established for the purpose of data sharing, or also to collections of

[4] See Stakeholder coalition calls for legislative refinement of the EHDS (4 December 2023).

biological samples by other entities (e.g. research companies, universities).

If an '**opt-out**' (and '**opt-in**') mechanism would be added in this context, it would lead to implementation problems due to overlapping electronic health data categories (i.e. the same dataset could fall into multiple data categories) and potentially overlapping secondary use purposes (e.g. 'scientific research' to 'ensure high levels of quality and safety of healthcare'). Furthermore:

- There would be the risk that data bias would become systematic within the EHDS from its inception and thus undermine its principal value for secondary use purposes.[5] The costs involved with putting the EHDS in place would be a waste if it leads to health data disparities, inequalities and health systems cannot meet the needs of everybody.
- A fragmented EHDS would prevent the understanding of geographic disparities and undermine scientific considerations to ensure data representativeness for evidence-based decision-making.
- When datasets are used to develop and validate digital health technologies, a possible extreme scenario could be that data-driven interventions are safe and effective for some people, but dangerous and ineffective for others.
- When personal electronic health data is processed in a pseudonymised format, an opt-out mechanism would increase data protection risks due to the necessity to reidentify data subjects and the requirement to cross-check whether a natural person is included in opt-out registries.

In addition, it is important that it remains clear that the common legal mechanism for secondary use of electronic health data established under the EHDS should not hinder or replace **contractual or other voluntary mechanisms** pursued between relevant parties (in line with Council's legislative position), albeit with a clarification that this should comprise both existing and future initiatives.

Recommended solution

The EHDS should set forth electronic health data categories for secondary use, in alignment with the definition of 'electronic health data'. The electronic health data categories need to be specified by clearly defining the registries/databases from which electronic health data shall be made available and/or the original processing purposes of (personal) electronic health data. Device-related provisions should be specified in a manner that eliminates/mitigates security risks. When electronic health data is made

[5] See Joint Statement: health organisations define EHDS' opt-out required for life-saving research (8 June 2023).

available from research/clinical contexts, it is important to ensure the scientific/clinical validation of datasets before they are made available for secondary use. Respect should also be given to existing legal safeguards aimed at protecting the scientific or technological potential or interests of researchers and innovators (see section on IP governance below).

IP governance

Legislative problems

Significance of IP protection for healthcare and health R&I

Making available 'electronic health data entailing IP rights and trade secrets' under the EHDS without adequate and effective control and safeguards granted to data holders would undermine existing legal protection and incentives that are vital for researchers and innovators. The proposed rules would set back health R&I in the EU, weaken the global competitiveness and resilience of the EU's health and life sciences sector, and disrupt European health ecosystems:

- The protection of IP is an essential incentive that compensates researchers and innovators in their trial-and-error efforts while attempting to advance health R&I over time. In addition, trade secrets protection is crucial to protect scientific, technological and business information and know-how where there is both a legitimate interest in keeping them confidential and a legitimate expectation that such confidentiality will be preserved.
- The proposed rules under the EHDS make it too easy to identify and scrape information about competitors' trade secrets and protected databases. This would do irreversible and lasting damages to the EU's health and life sciences sector.
- The lack of safeguards would hinder access for patients and providers to state-of-the-art healthcare innovations.
- Increased risks and uncertainty would drive up costs not only for researchers and innovators in the EU, but also for Member States that need to procure innovative healthcare solutions.

Conflicts between the EHDS, international treaties and EU acquis

The proposed governance of IP rights and trade secrets under the EHDS is arguably in conflict with **international treaties** (cf. Agreement on Trade-Related Aspects of Intellectual Property (TRIPS), Articles 10(2) and 39(2)–(3); Paris Convention for the Protection of Industrial Property, Article 10bis; WIPO

Copyright Treaty (WCT), Article 5). In certain cases, the proposed rules under the EHDS may even constitute an unnecessary and disproportionate limitation of the 'right to property' of data holders, violating generally recognised legal principles under EU law and the constitutions of Member States.

The proposed rules would also lead to uncertainties about the proper interaction between IP and trade secrets governance under the EHDS and related rules under **other EU legal acts**, such as the protection of undisclosed know-how and business information (trade secrets) provided under the Trade Secrets Directive (Recitals 1, 9, 14 and Art. 2(1)), the *sui generis* database right provided under the Database Directive (Article 7(1)), or the regulatory data protection proposed under the Proposal for a Directive on the Union code relating to medicinal products for human use (Article 81).

Conflicts between the EHDS and the Data Act

Although the Data Act will have a different data governance framework and scope than the EHDS, it is not clear what the policy benefits of lowering the level of control and safeguards granted for data holders could be under the EHDS, and why health data access bodies should be responsible for managing and processing the protected assets of data holders. The EHDS should not fall lower in its standard of trade secrets protection compared to the Data Act. It is important to recall that under the Data Act the co-legislators:

- enabled the data holder (as a trade secret holder) to **refuse, withhold or suspend the sharing of data**. Article 4(7) of the Data Act specifies that: *"[w]here there is no agreement on the necessary measures referred to in [Article 4(6)], or if the user fails to implement the measures agreed pursuant to [Article 4(6)] or undermines the confidentiality of the trade secrets, the data holder may withhold or, as the case may be, suspend the sharing of data identified as trade secrets."* Article 4(8) adds that: *"[i]n exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets, despite the technical and organisational measures taken by the user pursuant to [Article 4(6)], that data holder may refuse on a case-by-case basis a request for access to the specific data in question."*
- set forth **additional prohibited purposes** compared to the EHDS, including prohibitions to use data to develop competing products; to derive insights about the economic situation, assets and production methods of or use by the data holder; or to use data in a manner that adversely impacts the security of the product or related service(s) (see Article 6(2) of the Data Act).

Recommended solution

The addition of the following IP governance rules to the EHDS would respect the abovementioned legal frameworks and ensure appropriate balancing of rights and legitimate interests:

The [electronic health] data holder shall not be obliged to make available electronic health data for secondary use, if it demonstrates to the health data access body any of the following:

(a) the electronic health data is subject to the protection of international, Union or national legislation or a judicial or administrative decision providing an intellectual property right, a *sui generis* database right or commercial confidentiality, including trade secret protection or regulatory data protection, or

(b) making available electronic health data for secondary use would likely harm the right or legitimate interest of the data holder due to risks undermining its scientific or technological potential, security measures, strategic market position or ability to compete, or

(c) making available electronic health data may lead to an act of competition by the data user that is contrary to honest practices in industrial or commercial matters, or to a marketing authorisation or reimbursement for a similar product to a product of the data holder.

If the data holder decides to make available electronic health data for secondary use subject to the protection referred to under paragraph (a), the health data access body shall support the data holder in implementing and maintaining appropriate legal, technical and organisational measures necessary for the protection of the acquired rights and related legitimate interests of the data holder.

Data localisation and international health data transfers

Legislative problems

The EHDS should avoid excessive data localisation and international health data transfer requirements.[6] While storage of personal electronic health data by health data access bodies and secure processing environments (Council's legislative position) might be a reasonable safeguard to implement, broader **data storage requirements** (EP's legislative position) would pose significant risks, for example, in terms of their potential adverse effects on life-saving

[6] See Stakeholder coalition calls for legislative refinement of the EHDS (4 December 2023).

international health R&I collaborations, the functioning of pan-European medical registries, or the provision of ubiquitous digital health services through anytime-anywhere connectivity. The lack of understanding of what constitutes 'data storage' in technical terms would amplify implementation problems. Moreover, the requirement (in EP's position) to oblige controllers or processors of personal electronic health data to prove that they are not subject to third country law conflicting with Union data protection rules would not only go beyond the requirements of GDPR, but would subject those entities to a practically impossible burden of proof.

The provisions on **international transfers of non-personal/anonymous electronic health data** suffer from the shortcomings that stem from the inadequate definition of 'electronic health data'. These provisions could lead to inconsistent implementation of rules across the EU (under both Council's and EP's position). For example, Council's legislative position concerning 'anonymous electronic health data' 'based on a natural person's electronic health data' 'provided that their transfer to third countries presents a risk of becoming personal electronic health data' is self-contradictory.

The legal avenues provided by Chapter V of the GDPR set the legal bases for **international transfers of personal data**. If the EHDS were to allow Member States to maintain or introduce further conditions, including limitations for international transfers and access of personal electronic health data, then this would contradict the objective of the EHDS 'to harmonise data flows to support natural persons in benefiting from protection and free movement of electronic health data', both internally in the EU as well as with trusted third countries, and may even contradict the GDPR. It is essential to avoid an inconsistent and fragmented approach to data transfer throughout the EU that would lead to different degrees of protection of data subjects.[7]

Electronic health record (systems) and wellness applications

Legislative problems

The definitions of '**EHR (electronic health record)**' provided under the legislative positions of Council and EP are too broad. Not every 'collection' of personal electronic health data constitutes an 'EHR', but only a 'repository' that integrates personal electronic health data related to a natural person collected in the health system (longitudinally and from various sources).[8]

[7] See EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, para. 110.

[8] See ISO/TR 20514:2005(en) Health informatics — Electronic health record — Definition, scope and context.

By re-defining an '**EHR system**' as a 'product', the legislative position of EP would ensure alignment with the NLF. With regard to the complex systems architectures of EHR systems, it is also clearer in EP's position that the 'primary intention' of the manufacturer would necessitate that the product components are manufactured specifically to be used as an EHR system. However, there would be uncertainty about what could be 'reasonably expected by the manufacturer to be used for [specific] purposes'.

On the other side, the legislative position of Council provides an overly broad definition of what an 'EHR system' constitutes. The (unintended) consequence of this would be that a wide range of medical device software and applications used in digital health would fall under the definition. Council's position would also cause implementation problems, as it is not clear how manufacturers could perform self-conformity assessment of 'discrete parts of software'. By focusing merely on the interoperability and logging functionalities of EHR systems and by allowing Member States to introduce national requirements for EHR systems on conformity assessment in relation to aspects other than the so-called harmonised components of EHR systems, Council's position would undermine the original goal of the EHDS to harmonise the safety/security, quality and interoperability requirements of EHR systems at an EU level. This could lead to fragmentation and would be a major set back to the development of a single market for digital health products and services.

Both legislative texts lack clarifications about how the manufacturer of an EHR system or 'product claiming interoperability with EHR systems' would have to demonstrate conformity with the EHDS and the MDR/IVDR, Cyber Resilience Act and/or AI Act. There is also significant uncertainty about the conditions under which a manufacturer may/should claim that its product is 'interoperable' with (one or more) EHR systems, and about the obligations that Annex II would entail for manufacturers of those products.

It would be important to make the borderline between medical devices and **wellness applications** clearer, and clarify the technical use configurations of a wellness application to reflect technological reality.

Recommended solution

The key definitions of Chapter III of the EHDS could be defined as follows:

'EHR' (electronic health record) could be defined as **an integrated repository of personal electronic health data related to a natural person and collected in the health system, processed for healthcare purposes**.

'EHR system' (electronic health record system) could be defined as **any product (hardware or software) primarily intended by its manufacturer to be used for accessing, editing or sharing electronic health records or data contained in electronic health records**.

'Wellness application' could be defined as **any software intended by its manufacturer to be used, alone or in combination with a physical accessory, by a natural person for a non-medical purpose to monitor fitness, lifestyle or well-being, or provide educational or reference information thereof**.

In relation to Chapter III, it would be important to clarify its scope of application (by excluding enabling products and services) and its interaction with other legislation (to address regulatory duplications) along the following lines:

Chapter III shall not apply to general software or hardware used in a healthcare environment setting, or to cloud or scalable distributed computing services or web-hosting services providing underlying infrastructural storage, or hosting or computing services of an internet-based application, website or online platform infrastructure that is primarily not intended by its manufacturer to be used as an EHR system.

Software, including module(s) of or accessory to software, which qualifies as an EHR system and also falls within the definition of a medical device, *in vitro* diagnostic medical device or high-risk artificial intelligence (AI) system should only be subject to the essential requirements on interoperability of the EHDS to the extent that the manufacturer of the medical device, *in vitro* diagnostic medical device or high-risk AI system, which is providing electronic health data to be processed as part of the EHR system, claims interoperability with such EHR system. Such software should be certified in accordance with Regulation (EU) 2017/745, Regulation (EU) 2017/746 and [Artificial Intelligence Act]. In such case, only the provisions on common specifications for EHR systems should be applicable to those medical devices, *in vitro* diagnostic medical devices and high-risk AI systems.

Conclusions

This paper demonstrates that there remain significant number and severity of legislative risks in the EHDS. With regard to the sensitivity of the data concerned, the complexity of the proposed data governance mechanisms as well as the interplay with other legal acts (some not yet even finalised or in force), the interinstitutional negotiations should take the appropriate amount of time to thoroughly examine these problems and similar concerns raised by healthcare stakeholders in a careful manner. The issues of the EHDS at stake are simply too high for patients/citizens, health systems and the future health research and innovation capacity of the EU, to favor legislative speed over substance.

FOR MORE INFORMATION, PLEASE CONTACT:

Ray Pinto

Senior Director for Digital Transformation Policy

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

Dr. Richard Rak

Manager for Digital Health Policy

richard.rak@digitaleurope.org / +32 492 46 78 17

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 106 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, LSEG, 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 Energy, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Tesla, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Vantiva, 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, Digital Poland Association
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