



11 June 2021

Making the most of the GDPR to advance health research

Executive summary

Research has rightfully been granted prominence under the General Data Protection Regulation (GDPR),¹ making it possible to construct many legal provisions in a more favourable way given the significant role research plays in our economy and society. This is especially true of health research, as the COVID-19 pandemic has made painstakingly evident.

However, there is still too much uncertainty around how health research can be conducted in accordance with data protection rules, and upcoming Guidelines from the European Data Protection Board (EDPB) should aim to remove as much of this uncertainty as possible. Resolving these issues is also necessary to make the future European Health Data Space (EHDS) possible and successful.

This paper provides an analysis of some of the main concepts that have proved central to health research, building on existing opinions from data protection authorities and on industry experience.

Our analysis shows that:

- ▶▶ Fragmentation in Member States' interpretation and approaches is a key challenge that the upcoming Guidelines should aim to tackle, not shy away from.
- ▶▶ Both the compatibility presumption and broad consent have been clear and conscious choices in the design of the GDPR. They should be promoted and not restricted in their correct application.
- ▶▶ Full use of all applicable legal bases, such as public interest or legal obligation, should be promoted given the inherent challenges that consent represents in a research context.

¹ Regulation (EU) 2016/679.

- ▶ Best practice in appropriate safeguards, such as established research frameworks and federated models, should be promoted.
- ▶ Ethical assessments, solutions for controlling data access, and alternative information methods can help ensure transparency and control for data subjects under the real-world conditions of health research.

With our contribution we hope to help the drafting process for the EDPB Guidelines, and to support an enabling data protection framework for the crucial economic and social mission of health research.

Table of contents

• Executive summary	1
• Table of contents	2
• Harmonising requirements	3
Defining research	3
Role of codes of conduct	4
Role of a European Health Data Space	4
• Compatibility presumption	5
Further processing and legal bases	6
Further processing for research and ‘balancing test’	6
• Broad consent	7
• Consent and other legal bases	8
Case example: Medical Device Regulation.....	8
Case example: COVID vaccines research.....	9
• Appropriate safeguards	10
Research frameworks	11
Federated research model	11
Agreements between controllers and processors	12
Data provider is data controller, all other parties are processors.....	12
Joint controller agreements.....	12
• Transparency and control	12

Harmonising requirements

Different interpretations of the provisions pertaining to research to date have been shaped and compounded by disparate Member State rules governing health, and the continued leeway the GDPR has provided for national derogations. For example, myriad legal bases are used across Member States to process health data for research across both public and private sector.

This fragmented landscape limits Europe's capability to share health data across Member States for research purposes, thus preventing important research in the field of health from taking place at scale.

While this state of affairs is unfortunate and largely stems from the legislature's choice not to achieve fuller harmonisation, we disagree with the EDPB's position that this 'lack of homogeneity cannot be solved in the EDPB guidelines or by means of Codes of conduct.'²

While certainly Member State laws cannot be circumvented, the upcoming Guidelines should seek, to the fullest extent possible, to conciliate different approaches in order to facilitate compliance and coherence.³

In particular, the upcoming Guidelines should seek to overcome constraints due to Member States' use of Art. 9(4) GDPR. For example, divergences in the concept of public interest of the research, the impossibility or the disproportionate effort to obtain consent or the concept of research institute or body.

Defining research

Recital 159 GDPR provides that the definition of what can be considered as research 'should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.' By reference to Art. 179(1) TFEU, this definition includes not only academic researchers but also industry, including SMEs.

Such explicit preference for a broad interpretation is present in the GDPR in only three other circumstances,⁴ and is therefore notable. This broad interpretation can conflict, in particular, with more restrictive provisions in Member State law,

² Para. 15, *EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research* (February 2021), available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaire_research_final.pdf.

³ See 'Consent and other legal bases' section at p. 8 below.

⁴ In relation to the broader scope of data protection impact assessments (Recital 92), damages (Recital 146) and freedom of expression (Recital 153).

for example regarding the classification of public interest. For this reason, the Guidelines should recognise that the development of technologies that have wider public and societal benefits – for example, to help detect or treat diseases – even in a commercial context, as a rule should benefit from the scientific research provisions.

In order to duly take into account the GDPR's broad definition of research, the Guidelines could focus on what criteria should be used to determine what *cannot* be considered as scientific research. For example, they could include cases of commercial interests that do not coincide with the objective in Art. 179(1) TFEU 'of strengthening [the Union's] scientific and technological bases by ... encouraging it to become more competitive, including in its industry.'

Role of codes of conduct

Similar to the upcoming Guidelines, CoCs should be seen as a tool to harmonise interpretations and requirements, to the fullest extent allowed under the GDPR.⁵ From this perspective, the EDPB should work collaboratively with CoC proponents to address harmonisation issues stemming from national laws.

Drafting and approving CoCs has proved challenging considering the national character of the approval process. The cross-border nature of most research requires a CoC review process that considers processing activities in several Member States and can reach general validity within the Union. Work at EDPB level and open collaboration with the research community are quintessential to the success of CoCs that can provide scalable solutions across Europe, minimising the negative impact of any remaining national divergences.

The cross-border nature of research also requires international data transfers to be tackled as an essential element of successful CoCs for health research. The safeguards adopted for transfers in CoCs must reflect the purposes and nature of health research, and it is paramount for the EDPB to allow for a realistic assessment of what supplementary measures are appropriate in a research context.⁶

Role of a European Health Data Space

⁵ For more on CoCs, see our *Response to public consultation on draft EDPB Guidelines on codes of conduct and monitoring bodies*, available at <https://www.digitaleurope.org/wp/wp-content/uploads/2019/04/DIGITALEUROPE-response-to-draft-EDPB-guidelines-on-codes-of-conduct-and-monitoring-bodies.pdf>.

⁶ For more on supplementary measures for data transfers, see our paper *Data transfers and effectiveness of supplementary measures*, available at <https://www.digitaleurope.org/wp/wp-content/uploads/2021/05/Data-transfers-and-effectiveness-of-supplementary-measures.pdf>.

We wholeheartedly support the EDPB's call 'on the Commission to explore whether in the forthcoming legislative proposal on the EHDS ... a common legal basis and/or scientific research regime for the processing of personal health data could be provided.'⁷

A truly connected, interoperable and sustainable EHDS is a precondition to unlocking the potential of health data in the EU, and solving these issues is central to breaking any remaining barriers to data sharing between Member States.

The harmonisation of conditions within the EHDS, however, will not achieve the same results for data outside the EHDS, including for health research, which will continue to be processed in a variety of research environments.

In addition, if and to what extent the EHDS will explore these issues and specify them in relation to the GDPR is not yet known at present.

For these reasons, we urge the EDPB to use the upcoming Guidelines to provide as much harmonised interpretation as possible. Clarifying the issues we identify in this paper will both bolster the success of the EHDS and support health data processing and sharing outside it, based on appropriate safeguards.

Compatibility presumption

Art. 5(1)(b) GDPR sets out a general principle relating to the further processing of health data for research, establishing that such further processing shall 'not be considered to be incompatible with the initial purposes' for which the data was collected.

This is an explicit articulation of the purpose limitation principle, which is laid down in the same article, as applied to research. This articulation was a conscious and explicit choice from the legislature, and as such there is no need to 'reconcile' this presumption with the purpose limitation principle, because it is part and parcel of it.⁸

The GDPR hence establishes a general presumption of compatibility⁹ for the processing of data for research, which must in any event comply with the conditions laid down in Art. 89(1). Such article always applies when data is

⁷ Para. 18, *EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*.

⁸ As argued instead at p. 2, *Discussion points document* (April 2021) circulated by the EDPB in preparation for the stakeholder event on the application of the GDPR to the processing of personal data for scientific research purposes.

⁹ Note, in particular, the use of the verb 'shall' in Art. 5(1)(b) GDPR.

processed for scientific or historical research, which obviously includes further processing to this end of data initially collected for other purposes.

Rather than restricting the legislative choice behind this presumption, which is apparent from the letter of the text, the future Guidelines should focus on what elements might contravene it.¹⁰

Further processing and legal bases

We are puzzled by the EDPB's statement that the upcoming Guidelines 'will provide further clarification on the requirement of a legal basis for further processing for scientific research purposes by the original or a subsequent controller.'¹¹

Recital 50 GDPR clearly provides that in case of compatible further processing 'no legal basis separate from that which allowed the collection of the personal data is required.' In cases where a different controller processes the data at hand for research purposes, processing by such controller would not qualify as further processing but as processing for such controller's own primary research purposes, which is subject to all applicable conditions, including notably the establishment of both a legal basis and an exemption under Arts 6 and 9, respectively.¹²

Further processing for research and 'balancing test'

The EDPB has sought feedback on the application of the 'balancing test' under Art. 6(4) GDPR when relying on further processing for scientific or historical research.

¹⁰ This reflects the approach taken, correctly, at para. 31 of the EDPB *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR)*, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_en.pdf.

¹¹ Para. 21, *EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*. We note that the EDPB position might result from the WP29 *Opinion 03/2013 on purpose limitation*, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. This Opinion argued that in Directive 95/46/EC compatibility and legal bases were 'cumulative.' However, as recognised with regret by that Opinion with reference to the then proposed Regulation (see p. 33), the GDPR has introduced crucial differences that explicitly contradict this position. This also applies to the EDPB's position relating to compatibility, the balancing test, broad consent and appropriate safeguards, as we argue separately.

¹² Our interpretation is also supported by the European Commission's GDPR Q&A website, available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_en, which correctly characterises the letter of the law.

However, we submit that the assessment mandated for further processing in general is not required for scientific or historical research, precisely because it is the GDPR itself that has established a presumption of compatibility for this specific purpose in Art. 5(1)(b).¹³

This does not mean that the elements included in Art. 6(4) GDPR do not play a role, notably in the consideration of appropriate safeguards under Art. 89(1) GDPR. This, however, is a different determination compared to establishing whether further processing is compatible in the first place.

Broad consent

Recital 33 GDPR recognises there may be difficulties in precisely identifying purposes at the time the data is collected for research. In such cases, it allows data subjects to provide consent for ‘certain areas of scientific research,’ as opposed to more specified and explicit purposes, so long as the research activity complies with recognised ethical standards.

This calls for an ad hoc interpretation of Art. 5(1)(b) GDPR, which runs in parallel with the same preference given to further processing for research in the same article. Again, this does not create a need to ‘reconcile’ this interpretation with the purpose limitation principle, because it is an explicit choice made by the legislature as to how the principle should be interpreted.

We therefore strongly disagree with the EDPB’s stated position that, contrary to the letter and spirit of the GDPR, ‘applying the flexible approach of Recital 33 will be subject to a stricter interpretation and requires a high degree of scrutiny.’¹⁴

On the contrary, any interpretation of Recital 33 GDPR must take note of the explicit preference given to research under the law. In this context, it is important to stress that Recital 33 conditions reliance on so-called broad consent to adherence to ‘recognised ethical standards for scientific research.’ This aims to ensure a proper balance that takes into account ‘the impact of [“broad consent”] on the protection of the rights and interests of data subjects,’¹⁵ which should be explicitly recognised by the future Guidelines.

¹³ We take issue, in particular, with the EDPS interpretation that this presumption is merely ‘advisory’ because Recital 50 uses the term ‘should’ and has no equivalent provision in an article. On the contrary, this recital is reflected in the use of ‘shall’ in Art. 5(1)(b). See EDPS, *A Preliminary Opinion on data protection and scientific research* (January 2020), available at https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

¹⁴ Para. 28, *EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*.

¹⁵ P. 2, *Discussion points* document.

Again, our considerations regarding Recital 33 GDPR obviously do not at all imply that the appropriate safeguards under Art. 89(1) GDPR do not apply. The existence of appropriate safeguards is a requirement relating to all processing for research – indeed, all processing more broadly – and has no bearing on the general principles described in Art. 5 GDPR, to which purpose limitation – and specific interpretations thereof for research pursuant to Art. 5(1)(b) – pertains.

Consent and other legal bases

We welcome the EDPB's clarification that consent, even when required for participation in a scientific research project, cannot be interpreted as the only legal basis to legitimise the processing of health data for scientific research purposes. In particular:

“ Article 6 and Article 9 GDPR contain other options for a legal basis and an exemption, that can be relied on for processing health data for scientific research purposes. The requirement of informed consent can and must be distinguished from explicit consent as a possibility to legitimise the processing of personal data for scientific research purposes.¹⁶

In light of this – although Member State laws can differ with respect to how they specify, prescribe or exclude legal bases as well as the exemptions pursuant to Arts 9(2)(g)–(j) GDPR – the upcoming Guidelines should aim to provide a more detailed overview of the available legal bases and exemptions, and to harmonise interpretation as much as possible based on these. This will help in allowing for a more sustainable use of the available legal bases and in overcoming the difficulties associated with consent in a health research context.

Case example: Medical Device Regulation

A clearer articulation of public interest or legal obligation – pursuant to Arts 6(1)(c), (e) and 9(2)(i) – would help overcome situations where reliance on such legal bases stems from EU legal acts that are binding in their entirety and directly applicable in all Member States, but would conflict with incompatible Member State rules.

For example, Germany requires consent for the processing of personal data for any clinical evaluation and research. This is at odds with the possibility of

¹⁶ Para. 5, *EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research.*

relying on public interest or legal obligation flowing from the Medical Device Regulation (MDR) to guarantee the safety and efficacy of medical devices.¹⁷

In such cases, the upcoming Guidelines should recognise that national requirements cannot override directly applicable EU law and the corresponding implications in terms of GDPR legal bases and exemptions, and that as a consequence reliance on public interest or legal obligation should be possible in these cases.¹⁸

In the current context, several reasons exist for avoiding reliance on consent. For instance, consent withdrawal can contradict scientific principles, which require that results be verifiable and traceable. Relying on consent would make it necessary to identify an alternative legal basis for processing operations for such purposes, while identifying an equally applicable legal basis upfront would obviate such need and increase transparency for the data subject.¹⁹

Using a consent-based model may limit possibilities in areas where there is no direct relationship with the patient or in case of a specific need, such as in areas where patients may have a very limited time to live. In these circumstances, it could become impossible to obtain consent from the population required for the research.

Case example: COVID vaccines research

Using a consent-based model can prevent innovation and better insight into new discoveries. Consent forms a barrier to obtaining necessary new knowledge on the efficacy and safety of products, which is essential to limiting risks. A pertinent example can be found in the continuously evolving needs for the development of COVID vaccines. For instance:

- ▶▶ When rare safety-related concerns arise after the marketing of a COVID vaccine, the pseudonymised data collected during safety and efficacy trials needs to be further analysed, which would require data reuse that was not foreseen during the initial studies.
- ▶▶ There might be a need to develop more precise diagnostic methods to ensure that individuals with certain biomarkers, which can indicate

¹⁷ Regulation (EU) 2017/745.

¹⁸ This reflects the approach taken by the EDPB with respect to reliability and safety purposes under the Clinical Trials Regulation. See Section 2.1, *Opinion 3/2019*.

¹⁹ See paras 22–24, *Opinion 3/2019*.

higher risk for safety-related issues concerning the specific vaccine, can be identified and offered another treatment.

- ▶ When the virus mutates, in order to speed up the time needed to develop a new vaccine, using data from the original research is necessary, as that data contains information that would be essential for the modified vaccine.

Appropriate safeguards

The EDPB states that '[r]eliance on most “research exemptions” in the GDPR is conditional on the provision of additional and/or compensatory safeguards.’²⁰ The GDPR, however, always refers to measures that are ‘proportionate,’ or ‘suitable and specific’ when it comes to research.²¹

Importantly, Art. 89(1) GDPR provides that processing for research ‘shall be subject to *appropriate* safeguards, *in accordance with this Regulation*, for the rights and freedoms of the data subject.’²² Put differently, this article merely states that, although special interpretations exist for research, beyond such specific provisions the other GDPR safeguards still apply.²³ It does not require anything *additional*, and this term should therefore not be used.

From this perspective, the future Guidelines could expand on what safeguards might be appropriate in the context of the specific research processing activity at hand. They should not mandate any specific measures but should instead collect best practice.

As with any technical and organisational measure required by the GDPR, such determination is contextual and depends on the specifics of the research activity, as well as the likelihood and severity of risk to individuals’ rights and freedoms. Any safeguards must start from an understanding that the purpose of scientific research is to test hypotheses, not to reach conclusions about individuals or to make decisions affecting them personally such as their access to healthcare or social benefits.

Particularly, recourse to functional separation (such as partial or full anonymisation, pseudonymisation and aggregation of data) should not be seen as all-purpose solution for research. On the other hand, the Guidelines could provide concrete references to practical scenarios of when data can be

²⁰ P. 3, *Discussion points* document.

²¹ See, for example, Art. 9(2)(j) GDPR.

²² Emphasis added.

²³ This reflects the approach taken, correctly, at para. 32, *Opinion 3/2019*.

considered anonymous, as well as to adequate anonymisation techniques, based on internationally recognised approaches to anonymisation.²⁴

We highlight below some of the most promising models that have emerged in the field of health research that the Guidelines could expand on. These models are also relevant for medicine approvals, as well as for monitoring the safety of medicines.

Research frameworks

Scientific research is a process that adheres to sound scientific principles and follows a clear methodology. With this in mind, the upcoming Guidelines should as much as possible aim to reconcile sound scientific principles, as developed under relevant research frameworks, with data protection rules.

This is particularly important given our considerations above regarding Recital 33 GDPR, which allows ‘broad consent’ in light of the fact that the research activity should comply with recognised ethical standards. The GDPR therefore assigns a special role to recognised ethical standards as safeguards, and this role should be more prominently recognised in the upcoming Guidelines.

For example, there are many established research frameworks such as the European Medicines Agency’s (EMA) ICH Good Clinical Practice Guideline²⁵ and the ENCePP Code of Conduct.²⁶

Such established frameworks provide reliable international ethical and scientific quality standards for designing, conducting, recording and reporting research. They permit a high level of public scrutiny and assurance that individuals’ rights, safety and wellbeing are protected as part of research activities.

Federated research model

The federated research model enables the processing of personal data to remain local. Only aggregated information leaves the hospital/institution. This is an efficient method of reducing data protection–related risks.

The potential downside of a federated research model is that there is less robustness in terms of being able to fully verify the correctness of the scientific results, largely due to the limited possibilities to perform source data verification,

²⁴ For an overview, see the EMA workshop report *Data anonymisation: A key enabler for clinical data sharing* (December 2018), available at https://www.ema.europa.eu/en/documents/report/report-data-anonymisation-key-enabler-clinical-data-sharing_en.pdf.

²⁵ Available at <https://www.ema.europa.eu/en/ich-e6-r2-good-clinical-practice>.

²⁶ Available at http://www.encepp.eu/code_of_conduct/documents/ENCEPPCodeofConduct.pdf.

which is a common way of ensuring the validity of the results in a traditional clinical research scenario.

Agreements between controllers and processors

Data processing agreements provide a central venue to define clear roles as well as appropriate technical and organisational measures so that processing for research can meet the GDPR requirements and protect individuals.²⁷

For example, some large research consortia have opted for two models, depending on the organisation of the research activity.

Data provider is data controller, all other parties are processors

This model provides sufficient control by the data provider to ensure that data is only processed as instructed.

Given the specific nature of research, these arrangements should be reconciled as much as possible with the GDPR definitions of controller and processor. While the consortium may at times have to make joint decisions as to how the data will be used, for example as a part of a working group, the data provider still sets the boundaries for processing and exercises the necessary oversight.

Joint controller agreements

This model details the responsibilities of a research consortium by classifying each party as a joint controller.

As the detailed setup of the research consortium may not yet be settled when the data is first collected, it should be possible to provide the data subject with information about the arrangement, as required by Art. 26(2) GDPR, at a subsequent point in time as opposed to upfront.

Transparency and control

The research community is particularly challenged by the legal aspects of ensuring transparency and control.

The information obligations contained in Arts 13-14 GDPR do not always generate more effective protection for the average data subject, resulting in long

²⁷ For more on the controller-processor relationship, please see our *Response to EDPB consultation on draft Guidelines on the concepts of controller and processor*, available at <https://www.digitaleurope.org/wp/wp-content/uploads/2020/10/DIGITALEUROPEs-response-to-EDPB-guidelines-concepts-of-controller-and-processor.pdf>.

and complex data protection declarations that at best serve to fulfil a legal obligation.

The upcoming Guidelines should build on existing best practice concerning appropriate safeguards that can compensate for any loss of transparency and control generated by the real-world conditions of health research.

Such best practice includes:

- ▶ Technological solutions for controlling access to data. It is already possible to create privacy-preserving and highly secure research environments, where data does not leave the data controller.
- ▶ Ethical assessment. An ethical assessment of the individual case at hand can help in considering the relevance of specific transparency requirements, e.g. if individuals may have potentially passed away due to the disease and contacting a close relative may be upsetting.
- ▶ Alternative methods for informing. In case of compatible further processing of data not specified in the initial notice, for example, information could be made available through other channels such as a website. This may also provide a mechanism for individuals to exercise their rights.

FOR MORE INFORMATION, PLEASE CONTACT:



Alberto Di Felice

Director for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25



Ray Pinto

Director for Digital Transformation

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



Thomas Hellebrand

Policy Officer, Digital Transformation

thomas.hellebrand@digitaleurope.org / +32 492 46 78 17

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

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, SECIMAVI, 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

Slovakia: ITAS

Slovenia: ICT Association of Slovenia at CCIS

Spain: AMETIC

Sweden: Teknikföretagen, IT&Telekomföretagen

Switzerland: SWICO

Turkey: Digital Turkey Platform, ECID

United Kingdom: techUK