



January 2022

# DIGITALEUROPE comments on the proposed General Product Safety Regulation

## Executive summary

DIGITALEUROPE welcomes the Commission's proposal to review and update the General Product Safety Directive and make it fit for the digital era and modern-day market conditions. We in particular appreciate the effort to harmonise the rules and their implementation, such as through the use of a Regulation as the legal instrument.

In this paper, we develop and explain our position and proposals to further improve the Commission's text, to ensure the continued functionality of the General Product Safety Regulation (GPSR) as a cornerstone of the New Legislative Framework (NLF).

This includes:

- ▶▶ Alignment with existing or new and upcoming legislation, such as the AI Act, the Machinery Regulation, sectoral rules and developments on Cybersecurity.
- ▶▶ Ensure that GPSR is still functional as the baseline legislation for *all* products. Products presenting a higher safety risk are addressed in their respective existing/new legislation.
- ▶▶ Alignment with the NLF on standards and economic operator obligations, as well as regarding the responsible person, keeping the obligations proportionate and avoiding overlap or duplications.
- ▶▶ Support and suggest how to use various digital tools for product compliance information and sharing, tracing, etc.
- ▶▶ Consider more manageable timelines and procedures for recalls/remedies, as well as dependency on proper notifications.



## Content

### New technologies & Risks

The General Product Safety Regulation (GPSR) proposal introduces various changes and new provisions related to new technologies and perceived risks, such as related to AI, cybersecurity and IoT.

DIGITALEUROPE welcomes the forward-looking approach taken by the Commission, while noting that several of these aspects would need further clarification and detail to be effective in practice and to keep them aligned with other pieces of existing or upcoming legislation.

#### Definitions (art. 3, rec. 21)

The GPSR expands existing definitions and introduces new ones. Recital 21 seems to imply that ‘health’ for the purposes of the GPSR includes mental and societal health, referring to the terminology of the WHO. While useful for broader discussions on health risks in general, the WHO definition is less useful as a clear legal term, as it has been controversial for a number of years and lacks the required technical standards and specificity to define such risks.

The GPSR needs also to clearly distinguish between potential health risks and risks for health and safety caused by products. Health issues like depression, for example, are not necessarily caused by a product itself, but rather by inter-social behaviour or the content that was accessed or ‘consumed’ through the product.

DIGITALEUROPE therefore believes that the WHO definition of health and the subsequent reference to mental health should not be used within the proposal and should be removed.

In addition, it is unclear how ‘misuse’ (as referenced in the definition of “safe product”) is to be understood in the context of the GPSR. Manufacturers can, and should, only be held accountable for normal or reasonably foreseeable use of their products, as under the existing GPSD, not its misuse. The term ‘misuse’ should be removed from the proposal in order to avoid confusion, mistaken expectations and potential excessive liability for manufacturers.

Similarly, while the manufacturer can provide warnings and recommendations to the user about extended use, he cannot generally control the actual duration of use by the end users, and this cannot be a basis for considering a product to be ‘dangerous’ within the meaning of the Regulation. Thus, we recommend that the words ‘including the actual duration of use’ be removed from the definition of ‘safe product’.

## Cybersecurity and AI risks (art. 7)

The GPSR puts in place new obligations that, when assessing a product's safety, manufacturers and authorities must now consider, among other new risks:

- ▶▶ If a product has “appropriate cybersecurity features necessary to protect the product”, and;
- ▶▶ A product's “evolving, learning, or predictive functionalities.”

There are however not yet agreed standards on what ‘appropriate cybersecurity’ entails, and how importers/distributors can check/confirm this. Next to current pieces of legislation focusing on cybersecurity, many cybersecurity requirements for products are also being dealt with under newly proposed instruments related to the Radio Equipment Directive (RED). The same goes for AI software embedded in products, which will also need to be assessed as part of the proposed AI Act.

DIGITALEUROPE therefore cautions policymakers to not introduce these new and unspecified safety assessment requirements which will be better addressed in their own legislative proposals, to avoid duplication and inconsistencies.

DIGITALEUROPE consequently suggests to delete, article 7, (h) and (i), because of this aforementioned inconsistency risk, as well as other unclarities on the wording and scope. For example, vague wording such as ‘take into account’ shouldn't be used if the practical and legal implication isn't made clear.

## IoT risks (art. 7)

Similarly, the draft GPSR also places new obligations on manufacturers to ‘take account’ of connectivity/IoT risks when assessing a product's safety (see draft Art 7 (b) and (c)). While DIGITALEUROPE members do not oppose the inclusion of these new provisions per se, it's disproportionate to express them so widely by reference to all products that may reasonably foreseeable be used with or connected to the product under assessment.

DIGITALEUROPE recommends therefore that the duties in these subparagraphs be limited to assessment of the impact of products that are *intended* to be used together or connected.

## New obligations on market actors

Following changes in market, technology and how consumers and businesses access product information online, the GPSR introduces several changes to the

obligations of different types of market actors (including manufacturers, distributors, marketplaces).

### **Obligations of manufacturers (art. 8)**

The GPSR proposal requires manufacturers to display certain pieces of contact information, including both postal and electronic addresses. DIGITALEUROPE proposes to maintain a better alignment and coherence with the NLF, which does not have such a mandatory requirement, by dealing with the electronic address in a similar way of what it is described in the Blue Guide. In such scenario, we suggest that the electronic address is either an email or a web address which is not mandatory in case a postal address is already provided.

We strongly believe that the GPSR should not impose an address requirement that is more restrictive than the other NLF legislations. The proposed article could further create confusion about which address is correct for harmonized products that fall under the NLF legislation.

We would also like to underline the need for consistent and coherent goal setting within the various legislative instruments. The ICT sector is certainly an enabler of customer empowerment, green transition and enhanced consumer safety, while facilitating operations for businesses. Several articles within the GPSR also seem to relate, although not explicitly, to for example, the Sustainable Products Initiative (SPI) and its Digital Product Passport (DPP) components, which do not particularly relate to product safety.

The GPSR should deal exclusively with product safety in order to maintain coherence within the EU product safety framework, namely the NLF. While we see no obstacle in clarifying conceptual intentions within the Recitals, the aim of aligning the GPSR with legislation beyond the NLF should not influence its primary objectives.

### **Obligations of importers (art.10)**

Under the New Legislative Framework, there is a obligation on importers to ensure that the technical documentation can be made available to authorities on request. Importers can meet this obligation through contractual arrangements with manufacturers. This is a proportionate approach since the technical documentation usually includes confidential and commercially sensitive information which the manufacturer would not normally distribute to 3<sup>rd</sup> parties.

Unfortunately, Article 10(9) of the proposed Regulation introduces a disproportionate requirement on importers to keep the technical documentation. This can only lead to undue burden on both importers and manufacturers whereby they will be obliged to enter into complex legal agreements to protect

the confidentiality of the documentation. It may even lead to some importers being excluded or facing barriers to trade. There is no apparent reason why this aspect of the Regulation should be stricter than that in the harmonised legislation where the arrangements between authorities, manufactures and importers has worked well for some years.

DIGITALEUROPE consequently recommends that the importer obligations of the Regulation should be aligned with that of the harmonised legislation.

### **Obligations of distributors (art.11)**

DIGITALEUROPE considers that the current formulation of the proposed article 11 places an unduly heavy burden on distributors. This provision would oblige distributors of double-checking the conformity of products put on the market, in a sense almost duplicating the work of the manufacturer as under the New Legislative Framework.

The current General Product Safety Directive require distributors to do so, but “*within the limits of their respective activities.*” Consistent with this, it is considered that the imposition of no more than a due care standard on distributors would reflect a fair and proportionate allocation of responsibility compared to that of a manufacturer or importer.

DIGITALEUROPE therefore proposes for the article to be amended and text to be inserted to the effect that “*When making a product available on the market, distributors shall act with due care in relation to the requirements applicable to them*”, as a more proportionate solution.

### **Display of compliance information for distance sales (art. 18)**

The GPSR introduces the obligation for online marketplaces and other distance sellers to display at a minimum:

- ▶▶ The manufacturer’s name and contact details;
- ▶▶ If the manufacturer is not based in the EU, then the name and contact details of the EU ‘responsible person’ for compliance (RSP);
- ▶▶ The product’s batch/serial number, and;
- ▶▶ All safety warnings/information in the consumer’s language.

While DIGITALEUROPE members commit to communicate relevant product information to consumers as much as possible, some of the newly required data on safety information or batch and serial numbers are however not always readily available or exist in a structured form for online display.

The General Product Safety Directive (and proposed GPSR) is applicable to any and all products, not just those subject to specialised or harmonised safety legislation. Consequently, also very 'simple' and harmless products such as pens or birthday cards fall in scope. These are not product categories where the required information exists or is available in a structured manner.

Further, various types of safety information may only be mentioned on the booklets or manuals accompanying the product, inside the box. This type of information is consequently not visible or easily accessible to the consumer and trader at physical retail store either. Requiring this information online, while not requiring it offline, is a disproportionate discrepancy.

The online/distance sale requirements should mimic what it is like for a consumer to go into a store. In practice today, online storefronts and marketplaces normally already showcase the 'six-sided product images'. This makes it equivalent to offline stores, where the consumer can check and read the information on the product packaging. Additional information can be supplied if available, but should not be a mandatory requirement.

Moreover, the Responsible Person information is not required to be on the product or packaging. It may be on an accompanying document that is inside the box. Further, the Responsible Person has no obligations vis-à-vis consumers, so it is not clear why this would need to be displayed to consumers.

DIGITALEUROPE recommends that the new requirements should be channel neutral, applying in principle the same rules for offline and online, to avoid imposing higher costs on certain channels and ensure these costs will not become barriers to innovation, preventing new market entrants or smaller players from launching new initiatives. They should also not impose disproportionate burdens, for example the duty to appoint an EU responsible person, on low risk products (see next section).

### **Responsible person (art. 15)**

The proposed GPSR expands the application of the Responsible Person (RSP) from article 4 of Regulation (EU) 2019/1020 on market surveillance and compliance of products (MSR) to all products and adds responsibilities such as sample testing. Adding new obligations on RSPs, before MSR article 4 has been given time to be applied and experienced in practice seems premature and unnecessarily burdensome. The current form of the RSP obligation is weak as it is not a professional entity and risks creating a framework that makes it easier for unsafe products to be made available on the market. The RSP alone cannot and should not be the solution to all product safety challenges.

A general RSP requirement for all products, including those typically considered as very low risk (books, cards, etc.) will be too costly and present very few

benefits, especially when balancing the perspectives of enforcement capacity, resources available to smaller economic actors, the need for high product safety standards and evaluated risk.

DIGITALEUROPE recommends a proportionate, rather than blanket application of this obligation to high risk products only. DIGITALEUROPE would support limiting the scope to the products categories under the MSR, with the possibility for the Commission to conduct an impact assessment and adopt delegated acts for further categories if there is a proven need.

Article 15(2) further introduces the responsibility on the RSP to sample test randomly chosen products. There are however no cited harmonised standards for most products in the scope of GPSR. This raises the question of the criteria against which sample testing might be carried out and it is therefore unclear what tests would be required and how there will be consistency.

The testing requirement also effectively puts manufacturer obligations on the RSP. Manufacturers generally prefer to maintain the ability to test their own products, as opposed to third party testing, in order to have visibility on the information from testing reports which will help maintaining and enhancing the integrity of their products.

Next to duplicating manufacturers obligations, the RSPs may not have the stock levels to test products in a way that does not put them at an economic disadvantage or allows them to test at the required scale (for instance, testing may represent 10% of their stock rather than 1% of the manufacturer, etc.).

DIGITALEUROPE therefore recommends removing the sample testing obligation for RSPs under article 15(2).

## **Market Surveillance**

### **Presumption of conformity (art. 6)**

DIGITALEUROPE is strongly in favour of the use of harmonised standards, cited in the Official Journal, as the cornerstone for product compliance and market access. In the absence of such standards, consideration should first be given to other European or International Standards that could be considered to support the objectives of the Regulation.

Therefore article 6(1)(b), which relies only on national legislation, should be amended, to avoid fragmentation of the Single Market and national divergences instead of making use of harmonised, EU rules and standards. Additional national requirements should be a last resort as these could lead to an increase

in the effort and costs of development processes due to the need for country-specific product solutions.

In addition, to maintain consistency throughout the product safety framework and avoid misconceptions, DIGITALEUROPE recommends amending the title of article 6 '*Presumption of safety*' to '*Presumption of conformity*'.

### **Traceability of products (art. 17)**

DIGITALEUROPE stresses that electronic identification function on products should ideally be an identification method that can be used worldwide.

We would also remind the Commission that such traceability systems can only be effective with cooperation and commitment of manufacturers and other economic operators. Scrupulous and well-intentioned manufacturers will of course always cooperate but invariably such manufacturers will also act in good faith even without such a system. Less scrupulous manufacturers who have not applied due diligence or operated within the spirit or intent of the Regulation can usually not be trusted to cooperate within the framework of even the best traceability system.

It is in this context that the Commission should consider the likely benefits and efficacy of any traceability system implemented under Article 17.

### **Authority data scraping (art. 20)**

The GPSR introduces the requirement for economic operators to consent to data scraping by authorities and allow authorities to access the economic operator interface so that 'online tools' can be deployed to detect compliance issues.

Giving direct access however to authorities, on a general basis, would be a very concerning development. Access to such infrastructure and data would most likely expose business sensitive information and may impact the integrity of the systems and degrade the user experience.

DIGITALEUROPE calls on the legislators to consider alternative approaches to this proposal, encouraging enhanced cooperation with market surveillance authorities and the development of mechanisms and communication channels building on the EU Product Safety Pledge<sup>1</sup>, such as through periodic reports.

### **Targeting (art. 4)**

---

<sup>1</sup> [https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/product-safety-pledge\\_en](https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/product-safety-pledge_en)



Following case law and jurisprudence (Alpenhof<sup>2</sup>), the concept of ‘targeting’ is currently too broad to ensure legal certainty. The legislators should aim to clarify this concept first, before using it as a legal criterion.

The GPSR might not be the suitable framework for this broader concept of international private law, as the framework on applicable law and jurisdiction have been in discussions for many years and the lack of clarity in that space is generally acknowledged by experts.

## Recalls & Remedies

Various changes are made to the existing recall and remedies framework, including very strict deadlines and other measures. DIGITALEUROPE offers some amendments to keep these proposals manageable and implementable in practice, for all market actors.

### Two days notification (art 19)

Article 19 proposes that the manufacturer of a product shall ensure that, through the Safety Business Gateway referred to in article 25, an accident caused by a product placed or made available on the market is notified, *within two working days* from the moment it knows about the accident.

DIGITALEUROPE members are very concerned that in its present form this article is likely to result in economic operators and market surveillance authorities becoming overburdened with unnecessary notifications. The Safety Business Gateway could be overpopulated with reports that are misleading to consumers and unfairly damaging to the business and reputation of economic operators.

It is noted that article 8(10) (manufacturers) and the corresponding article 10(8) (importers) require notification separately from article 19 – and also through the Safety Business Gateway – where the economic operator *considers or have reason to believe, on the basis of the information in their possession, that a product which they have placed on the market is not safe* (i.e. is a dangerous product, as defined). Similarly, recital (54) envisages notifications in relation to ‘dangerous products’ (products that are not ‘safe’ as defined).

This approach makes sense. Accidents and incidents can, and indeed frequently do, occur even though the product is entirely safe, for example through unforeseeable misuse of the product by the customer. It is also not unknown for

---

<sup>2</sup> <https://curia.europa.eu/juris/liste.jsf?num=C-585/08&language=en>

economic operators to receive mischievous reports of entirely spurious ‘accidents, that quickly prove to be false upon investigation.

It is not however in the interests of economic operators, market surveillance authorities or consumers for companies to be required to notify any and all accidents, unless there is reason to believe the accident has been caused by an unsafe product (consistent with the approach in article 8(10)).

It is clear from article 32 that the Commission intends for consumers to have access to information on the Safety Business Gateway. It would be misleading to consumers and potentially unfairly damaging to the reputation of economic operators for accidents that do not actually relate to any lack of safety in the related product to be reported there.

Economic operators must of course act with urgency to investigate reported accidents. However, a blanket two working day deadline may be insufficient time in which to obtain even basic information to establish that there is reason to believe a safety issue exists.

Businesses may well be reliant on information being provided by consumers, and if there are any delays in receiving information, there is a risk that businesses will miss this deadline for reasons beyond their control or make precautionary notifications, possibly containing factual inaccuracies due to the paucity of information then available, that quickly prove to have been unnecessary but in the meantime create churn for authorities who inevitably have to make requests for further information that the economic operator is likely already pursuing as quickly as it can.

DIGITALEUROPE therefore recommends that an ‘accident’ is clearly defined and that economic operators should report verified or plausible reports of accidents ‘without undue delay’ rather than within a general two days deadline for all. This, while still strict, would allow operators a limited degree of latitude in appropriate cases to conduct sufficient urgent inquiries and to establish if there is genuine reason to believe there may be a causal connection between a lack of safety in a product and the reported accident. It also still allows an authority to later determine whether or not the notification was in fact made with undue delay and act against the economic operator accordingly.

As a way forward, the term ‘accident’ should be removed throughout the legislation and, where necessary, replaced instead with the wording of ‘unsafe product’. If it’s decided to still retain the term ‘accident’, then the definition should be changed to mean “*serious personal injury or damage to personal property that has objectively been shown to have been caused by a product and is indicative of a systemically unsafe product.*”

## Two/five days product removal (art. 20)

The GPSR introduces a more stringent obligation for product removal. In practice, this will only be feasible if the obligation and removal requests are supported by clear and unambiguous information to help identify the products. The quality of the notice is crucial for effective and timely removal.<sup>3</sup>

With respect to the two- and five-days' timeframe, these might be especially difficult for smaller online marketplaces. We therefore suggest that the timeframe should only start once the online marketplace has processed the notice.

DIGITALEUROPE recommends aligning product removal obligations with the existing obligations under the Product Safety Pledge<sup>4</sup>, effectively what is set out in article 20 GPSR.

## Recalls (arts. 34 and 35, rec. 30-64)

The new GPSR provision in article 35 mandates that product recalls must provide consumers with one of three costless remedies: repair of the product, replacement or a refund. The non-binding recitals further specify that sustainability and reducing waste should be considered, in practice giving a preference for the product repair option.

In order to make this more effective in practice, DIGITALEUROPE supports the notion that regulators should follow consistent practices to notify manufacturers and request details in a uniform way.

## Right to remedy (art. 35)

The 'right to remedy' is a new concept in the context of the GPSR. While this addition is understandable from a content point of view, our members believe that its stipulation in the GPSR is not reasonable nor feasible in this context.

Usually a right to remedy is not linked to product safety. The 'right to remedy' is already regulated in the EU Member States and relates to warranty and liability obligations rather than actual product safety requirements. We would also caution policy makers against the risk for fragmentation of the Single Market through national legislation.

A prime example of this would be article 35(2), which states that "*repair, disposal and destruction of products by consumers shall only be considered when easy and safe for consumers*". While DIGITALEUROPE members generally agree with

---

<sup>3</sup> <https://ecipe.org/publications/combating-unsafe-products/>

<sup>4</sup> [https://ec.europa.eu/info/files/product-safety-pledge\\_en](https://ec.europa.eu/info/files/product-safety-pledge_en)

this, we already see potential contradictions with national legislation. France's repairability score, for example, seeks to promote self-repair of electronics (including TVs) and producers are encouraged to facilitate this to gain points.

Additionally, when talking about recalls, there are various large and small phenomena and causes for said recall. Prescribing too detailed decisions here could hinder entirely satisfactory, low environmental impact recall activities by industry players. For example, it is possible that a safety risk can be adequately addressed through the provision of revised installation instructions without any change to or replacement of the product, or the supplying of a missing part. We believe that it is desirable to only specify the minimum requirements for consumer protection and, with the approval of the authorities, determine the appropriate recall content and method.

## **Penalties & Entry into force**

### **Penalties (art. 40)**

Article 40 provides for very severe financial penalties on economic operators. Such measures may be appropriate in extreme cases where consumers have been exposed to very high risk due to reckless and highly negligent activities by economic operators who subsequently act in contempt of the Regulation. Clear Guidance will help ensure that this is applied in a proportionate manner.

The GPSR draft requires country penalty law to have a maximum fine that is at least 4% of the company's Member State (or if multiple Member States, then all such states') turnover. This room for national divergence will lead to fragmentation. It must be avoided that any Member State would act in a disproportionate manner and ensured that fines – if any – are in proportion to the nature of the issue and that any mitigating actions taken by the manufacturer before or after the event are taken in to account.

DIGITALEUROPE believes in the importance of building up the resources and expertise within market surveillance authorities so as to improve both their enforcement capacity and their options for preventive action, rather than focusing or relying only on penalties.

### **Transition of 6 months (art. 47)**

The GPSR is currently proposed to go into force after 6 months. DIGITALEUROPE argues that at least 36 months should be allowed for businesses to plan, budget and develop the solutions needed for compliance with the GPSR and its many new requirements and obligations. Some of the

requirements will require updated labelling, packaging, websites, and IT systems. The time needed to design, verify and implement such changes without disruption to high volume manufacturing processes must not be underestimated and a realistic transition period will help to ensure the success of the Regulation from the outset.

Further, there is an important educational and awareness aspect. As a comparison, the MSR had a transition period of two years, and even here businesses struggled to be properly informed and ready in time. The new requirements under the GPSR are even considerably more burdensome to comply with, including due to the fact that these obligations will apply to all products instead of specific product categories or subsets.

Economic operators of all sizes will require the time to understand the rules and implement the necessary measures. Authorities as well will require time to prepare and ensure the necessary resources are deployed.

FOR MORE INFORMATION, PLEASE CONTACT:



Jochen Mistiaen

**Senior Policy Manager**

[jochen.mistiaen@digitaleurope.org](mailto:jochen.mistiaen@digitaleurope.org) / +32 496 20 54 11

---

## 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, Assent, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, 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, 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

**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, numeum

**Germany:** bitkom, ZVEI

**Greece:** SEPE

**Hungary:** IVSZ

**Ireland:** Technology Ireland

**Italy:** Anitec-Assinform

**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:** AMETIC

**Sweden:** TechSverige, Teknikföretagen

**Switzerland:** SWICO

**Turkey:** Digital Turkey Platform, ECID

**United Kingdom:** techUK