DIGITALEUROPE

DIGITALEUROPE response to public consultation on Article 29 Data Protection Working Party draft guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679

Brussels, 28 November 2017

INTRODUCTION

We welcome the fact that Article 29 Working Party (WP29) is aiming to adopt guidelines on automated individual decision-making and profiling. These types of processing are covered by complex provisions in the General Data Protection Regulation (GDPR) and raise challenges in various sectors.

Many issues are being addressed in the draft guidelines with helpful recommendations. We focus here on points that we believe require further attention in view of the finalization and adoption of the guidelines.

As a general point, we are concerned by the fact that these WP29 guidelines, like previous ones, go beyond the scope of the GDPR. Given the GDPR has changed the nature of previous WP29 opinions to binding guidelines, WP29 needs to ensure the guidelines remain within the scope of what the law foresees providing clarifications and interpretations but not creating new legal requirements. The democratic legislative process is otherwise undermined and the guidelines do not ultimately serve the purpose of providing legal certainty.

DEFINITION OF PROFILING

In relation to the definition of profiling (page 6), the reference to the Council of Europe Recommendation CM/Rec (2010)13 is not helpful. This definition omits one important stage of profiling: the "decision". The third stage of profiling described in the Recommendation, i.e. "applying the correlation to an individual to identify characteristics of present or future behaviour", does not necessarily include a "decision" by a controller or processor in relation to a specific individual. For example, through the use of profiling techniques, a retailer, for instance, may identify that a customer is interested in specific products using profiling techniques. All three stages of profiling in the recommendation will have taken place in order to come to this conclusion. However, that retailer may choose to not present offers to the profiled specific customer based on this profiling (therefore no "decision", i.e. "action" has been taken in regard to the specific profiled customer). The retailer may, for instance, use this information for product selection in a specific geographic area based on buying preferences of a wider customer sample in that area.

WP29 seems to acknowledge the distinction in the example included at the end of page 9 which differentiates a "recommendation" -which the guidelines here define as the "product" of an automated process- from the "final decision" that may be taken by a human or may remain part of the automated process.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

SCOPE OF ARTICLE 22 - "DECISION"

Section II "Specific provisions on automated decision-making as defined in Article 2" of the guidelines (p. 9) analyses the wording of Article 22§1 to help define its scope. We think it is crucially important to include here an analysis of the word "decision" and would strongly recommend that this is added to the guidelines. During the legislative process, there were extensive discussions on the term "decision", including discussions on whether the wider term "measures" should be used instead. A "decision" requires an 'action' from the data controller or data processor, which relates to a specific individual as indicated above. This excludes from the scope of Article 22 (but not from the GDPR general provisions of course) all types of analytics that take place in order to, for example, improve a service without a decision being taken in relation to a specific individual.

Based on this analysis, the following statement on page 6 of the guidelines would not apply: "The GDPR does not just focus on the decisions made as a result of automated processing or profiling. It applies to the collection of data for the creation of profiles, as well as the application of those profiles to individuals". The GDPR does focus on the "decisions" resulting from the automated decision processing, both in Article 22 and all other provisions that relate to automated decision-making as indicated above because the "decision" is the part of the technical process that carries the greater risk for the individual. All other parts of the technical process starting with the collection of data for the creation of profiles remain regulated under the general provisions of the GDPR.

SIMILARLY SIGNIFICANT EFFECT

We welcome the effort to clarify the threshold of Article 22 in relation to the wording "similarly significantly affects him or her". This is definitely a point that creates legal uncertainty in practice. The guidelines (page 10) however focus more on the interpretation of the word "significant" i.e. the "degree" of the impact on the individual and not on the word "similarly", i.e. the "type" of impact on the individual which is required to have similar significance to a legal effect. The latter wording in the threshold is indeed what is harder to interpret in practice given that, as the guidelines state, the word 'similarly' was not present in Article 15 of Directive 95/46/EC and is introduced by the GDPR.

This uncertainty remains also in the example related to online advertising. But the guidelines do not address the more complex and crucial question of whether these potential significant effects of online advertising could ever qualify as being "similar" to legal effects.

Furthermore, also as regards the "significance", i.e. the degree of impact, the guidelines do not provide sufficient guidance. The phrase "effects of the processing must be more than trivial and must be sufficiently great or important to be worthy of attention" (page 10) is too vague to be meaningful in organisations' compliance efforts. Also, the following sentence is not helpful: "the decision must have the potential to significantly influence the circumstances, behaviour or choices of the individuals concerned". We need more guidance around the term "significantly" and this term as used in the explanation.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

We would also ask for more clarity in regard to the following points in this section of the guidelines:

- We are concerned by the following statement on page 11: "Automated decision-making that results in differential pricing could also have a significant effect if, for example, prohibitively high prices effectively bar someone from certain goods or services". It is too generic and seems to imply that differential pricing may always fall within the scope of this article. We note that when differential pricing is based on illegitimate factors and is discriminatory, it is prohibited under different rules. However, there may be a legitimate basis for differential pricing, for instance, in relation to proximity for shipping or bulk pricing. Other factors that are important in this assessment may include how big the differential is, and what constitutes a "prohibitive" price (which is different from person to person), or someone being "barred" from buying because of a differential.

- We furthermore would like to note that up-sell and cross-sell activities should not be considered as automated decision-making with legal effect or similar as legal effects because the client still has the choice to accept or not the proposal made by the operator. The decision to send the offer to client X and not to client Y should not constitute a "decision" in the meaning of Article 22. Because proposing offers does not entail a legal effect as long as the client does not accept the offer.

- "Positive" similarly significant effects should not be included in the threshold, and their inclusion results in confusion. Not only because such an interpretation would not be in line with the risk-based approach of the GDPR but also because it was clear during the legislative process that the intention of the legislators was to protect the individual from negative effects (alternative wording considered throughout the legislative process included "discriminatory" or "adverse" effects).

- Possible effects that "may also be triggered by the actions of individuals other than the one to which the automated decision relates" are practically impossible to assess. How do we define who those other individuals may be, how do we estimate the possible actions of each of those individuals and how do we assess the possible effects of those possible actions on the individual being profiled? This cannot serve as a criterion to determine whether a practice meets the threshold in question.

THE "PROHIBITION" OF ARTICLE 22§1

In relation to the analysis included on page 12 of the guidelines and followed throughout the document regarding Article 22§1, we question whether this provision sets out a prohibition. Article 22§1 establishes a right for the data subjects. In practice, because this right is defined with negation "not to be subject", organisations may indeed establish that the required level of legal certainty can safely be achieved by only relying on the three legal bases provided in what the guidelines refer to as "exceptions". We would welcome an interpretation of the structure of this article that is based on the letter of the law and recognizes that the article establishes a right and not a prohibition. Consequently, paragraph 2 does not include "exceptions" but rather sets out cases when paragraph 1 does not apply.

This interpretation is not only in line with the letter of the law but also the intention of the legislature; many legislative amendments considered throughout the legislative procedure would have established a clear prohibition (notably tied with wording related to "adverse" or "discriminatory" effects as described above), but these were rejected, and the legislature finally adopted a different approach.

NETWORK AND INFORMATION SECURITY

The processing of personal data for the purposes of ensuring network and information security (NIS) was given an explicit legal base under Recital 49 as a legitimate interest of the data controller. In reality, such processing relies heavily on automated decision-making. Vectors of attack are becoming increasingly sophisticated, varied and quicker to deploy. At the same time, each device needs to be configured, connected to the network, defined a security policy for and managed on an ongoing basis. Enterprise security teams are moving from a world where a single team member may be responsible for hundreds of devices to potentially hundreds of thousands of devices. Automation, therefore, is an essential part of security.

Ideally, therefore, we would like the guidance to recognize the intention of the policy makers and note that processing for NIS purposes, whether or not it involves automated decision-making, is guided by Recital 49 and the associated grounds for processing of legitimate interest, in accordance with Article 6 (1) (f). This provision would take precedence over the application of Article 22 on the basis of lex specialis.

Should WP29 nevertheless consider NIS processing that involves individual decision-making to be subject to Article 22, the question becomes whether it meets the terms under Article 22(1), the grounds for processing under Article 22(2) or otherwise valid grounds subject to conditions included in Article 22.

One consideration is whether Article 22(1) is a direct prohibition or right to be invoked, as outlined above. If Article 22(1) continues to be considered a prohibition, then the valid grounds for processing would be limited to the 'exceptions' under Article 22(2). As such, legitimate interest would not be valid. If, however, it was to be considered as a right to be invoked, then legitimate interest would remain valid grounds for processing as long as the data subject has not invoked their right not to be subject to automated decision-making either before or after the decision has taken place. In practice, this is workable in part for security practitioners insofar as a malicious actor would be unlikely to raise awareness of their presence by invoking their right. As such, it would be more likely to be used by good actors who are mistakenly subject to a decision. That said, it could also result in objections being made by good actors who are unaware that their device or site is compromised. In such circumstances, security practitioners would be obliged to remove the restrictions regardless of the security implications, which is obviously not good practice. As a result, even if Article 22(1) would be considered to be a right to invoke it presents only a limited solution for NIS processing.

The 'exception' of NIS processing authorized under EU or Member State law also comes into play. Recital 71 specifically mentions this might apply to laws that ensure the security and reliability of the service provided by the controller. Our interpretation is that at least two EU laws may be applicable here: the EU NIS Directive and the proposed ePrivacy Regulation. The NIS Directive requires operators of essential services (OESs) and digital service providers (DSPs) to undertake security measures, whereas the ePrivacy Regulation proposes that providers of publicly available electronic communications services and networks can process electronic communication data in order to maintain or restore security of their services or networks. Aside from the questions as to whether the obligation to undertake security measures is broad enough to cover automated decision-making for NIS purposes or whether all data processed for NIS purposes falls under the definition of electronic communications data, the obvious limitation here is the scope of covered providers. NIS applies only to OESs and DSPs, whereas ePrivacy only covers publicly available electronic communications services and networks. As such, most corporate networks would be excluded. Hence, the legal grounds for processing are not sufficient to address the full range of automated decision-making based on NIS processing.

Other relevant considerations do not have the same broad applicability across different types of NIS processing and are worth examining in relation to individual examples of processing. Three such examples are the use of automated security policies to (1) sandbox compromised devices for observation, restrict their access or ultimately block them from the network; (2) block access to bad web addresses/ domains; and (3) block malicious emails and/or file attachments. Below we consider each of them in turn, without returning to the issues already considered (Recital 49 primacy, Article 22(1) as a right to be invoked and applicability of EU and Member State law).

For contained devices under the first example, we would argue that they would not fall under Article 22(1) on the basis that such action does not amount to a legal effect as it neither impacts legal rights nor rights under a contract. Nor do we see why it would be considered similarly significant. In the 'worst' case, for example, an employee or guest user would be prevented from connecting their device to an enterprise network until the device is remediated. It would not amount to a contract breach, nor would it impact legal rights.

In the second example, blocking a user from connecting to a bad website also seems to fail to meet the test of legal or similarly significant effect as it relates to the blocked user. However, it should also be considered whether the owner of the website should also be considered a data subject in the case that they are an individual as opposed to a legal entity. To the extent the traffic to a website is significantly impacted by such a block, which may apply if a website is black-listed across the board by a major supplier of security solutions, it is contestable whether this could or could not amount to a similarly significant effect. Irrespective of that debate, however, we would contend that the blocking of traffic does not amount to processing of data of the website owner under the terms of Article 4(2) as the operation is not actually performed on the website or related data but on the device attempting to contact it. More importantly, we would also not consider the data in question – i.e. the website address – to be personal, regardless of its ultimate owner.

In the third example, automatic decisions to block emails with malicious file attachments or other attack methods should not be considered as amounting to a legal or similarly significant effect from the point of view of the intended recipient, in much the same way as the examples above. It is less clear-cut from the view of the sender of the email. While such emails may not include personal data (e.g. if they are sent from false identities, which may often be the case), from an operational point of view it would be hard to distinguish between ones containing personal data and others that do not. Moreover, blocking such email is a form of processing. If we look at the grounds for processing under Article 22(2), there is no contract in place between the controller and data subject in question, nor is it feasible to obtain their consent. As a result, the legality of blocking such communications and/or files would likely hinge on the interpretation as to whether that amounts to a legal or similarly significant effect. We would argue that in the spirit of the legislation is should not be considered to have such an effect, though recognize that it is not a straightforward determination.

In conclusion, the only clean way to ensure that automated decision-making for network and information security purposes can be conducted with appropriate legal certainty is to recognize the intentions of the policy makers in explicitly providing grounds for such processing in Recital 49 and hence asserting its primacy over and above Article 22. Should the WP29 fail to make such an assertion, neither the interpretation of Article 22(1) as a right to be invoked nor the exception for EU and Member State law under Article 22(2) adequately capture the full range of necessary NIS processing activities. At the very least, the WP29 should clarify the application of Article 22 to examples of NIS processing, in line with the examples given above.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

THE RIGHT TO BE INFORMED

Beyond the specific GDPR provisions on the right to be informed relating to automated decision-making and profiling which are referenced in the guidelines, the GDPR does not require an approach that would result in "ensuring that information about the profiling is not only easily accessible for a data subject but that it is brought to their attention" as specified in the guidelines (page 13). As explained in the guidelines, in relation to profiling the GDPR requires in Recital 60 that "the data subject should be informed of the existence of profiling and the consequences of such profiling".

It is certain that organisations in practice will be looking at the information requirements related to automated decision-making and profiling with special attention given the potential risks and intrusiveness of certain types of such processing. Organisations may also choose to go beyond the minimum legal requirements in this respect to ensure a better consumer experience. But the GDPR does not require organisations to inform data subjects in this respect in a manner that is different from other instances in the sense implied by the guidelines. We are also concerned that such an interpretation by WP29 may lead to excessive notices to data subjects.

Furthermore, it would be helpful to make a clearer distinction in the guidelines as regards the different information provision obligations that relate to automated decision-making and profiling. In addition to the information requirements foreseen in the general rules of the GDPR governing the processing of personal data including Article 12, we would recommend an overview including Recitals 60 and 63, which show more clearly that data subjects have the right to obtain the following information:

- When profiling takes place – The existence and consequences of the profiling;
- When automated decision-making, including profiling, takes place – The logic involved in any automated personal data processing; and
- When specific types of automated decision-making, including profiling, that fall within Article 22(1) and Article 22(4) take place – The existence, the logic involved, the significance, and the envisaged consequences of such processing.

Notably, the end of the example at the beginning of page 18 goes further than GDPR requirements. It reads "The controller must also provide the data subject with information about the collected data, the existence of automated decision-making, the logic involved, and the significance and envisaged consequences of such processing". Given that the activities in the example do not fall under Article 22, information provision on "the significance" should not be required. Also to the extent that there may be no "decision" taken in this example, there should be no obligation to inform about "the logic" involved.

Similarly, on page 20 the guidelines read "In all cases, data subjects should have enough relevant information about the envisaged use and consequences of the processing to ensure that any consent they provide represents an informed choice." The "envisaged use" goes much further than the "existence" required by the GDPR in relation to profiling. Finally, we also note the example on page 23 where the guidelines read "The data subject should also be given information about their profile, for example in which 'segments' or 'categories' they are placed". Given that at this point in the example the processing does not fall under Article 22, the GDPR would not require the level of detail that extends to 'segments' or 'categories' in the general information provision obligation of the controller which relates to the fact that profiling is taking place. This information may indeed be required by the GDPR if the data subject exercises their right to access any generated profile.

ARTICLE 9 - SPECIAL CATEGORIES OF DATA

We recognize that specific attention is required for special categories of data but the guidelines seem to go beyond the GDPR requirements as regards the information provision obligation. Namely on page 22, the guidelines suggest that "The controller should make the data subject aware that not only do they process (non-special category) personal data collected from the data subject or other sources but also that they derive from such data other (and special) categories of personal data relating to them".

The GDPR obligation to provide information relates to the processing of personal data. The outcome of the processing should not be subject to an additional obligation to inform data subjects. If new processing of personal data takes place on the basis of this outcome, the rules on further processing would apply. From a practical point of view, it is often impossible for the controller to inform on what may be "derived" before the processing takes place. And from the point of view of the data subjects, this would result in providing complex information that would not necessarily help their understanding of the processing in the frame of an informed disclosure.

CHILDREN

The WP29 guidance states: "Because children represent a more vulnerable group of society, organisations should, in general, refrain from profiling them for marketing purposes." The WP29 statement references a study on marketing to children aged 6 to 12 yet, as written, it could be interpreted more broadly, to apply that study's findings to anyone under 18. That implies that anyone under 18 should not be exposed to personalized advertising, irrespective of whether consent has been obtained. Such an approach would be inconsistent with the GDPR's existing protections for children, where children of 16 years (or from 13-16, depending on member states' discretion) are deemed mature enough to give consent to the processing of their personal data without parental authorization.

As written, WP29's draft guidance may be interpreted to mean that a 16-year-old cannot lawfully consent to personalized advertising (given that consent is likely to be the lawful basis for much personalized advertising under the GDPR). This position is out of step, given that a 16-year-old in many member states can lawfully consent to sex, marriage or surgical treatment, or join the armed forces. In addition, such a position would have a significantly negative impact on digital advertising for publishers and frustrate the ability of advertisers to reach young, independent consumers.

ARTICLE 5(1) (D) - ACCURACY

On page 19 of the guidelines, the principle of accuracy is very broad as it refers to "a dataset that may not be fully representative or analytics that may contain hidden bias beyond the accuracy of raw data". In addition to GDPR Article 5(1) (d), which requires the accuracy of personal data, in relation to automated decision-making and profiling, we note the GDPR requirements in Recital 71 "[…] the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized […]". We, therefore, suggest that the guidelines should not suggest the extension of the principle of accuracy to "analysing data", "building a profile for an individual" and "applying a profile to make a decision affecting the individual".

ARTICLE 16 - RIGHT TO RECTIFICATION

The guidelines read as follows on page 24 "The right to rectification applies to the 'input personal data' (the personal data used to create the profile) and to the 'output data' (the profile itself or 'score' assigned to the person, which is personal data relating to the person concerned)". This approach is not in line with the GDPR and raises concerns. The right to rectification applies to 'input personal data'. But data subjects cannot request to rectify the 'output data' (we note that the guidelines refer to 'output data' and not to 'output personal data' as opposed to 'input personal data') which can be based on complex algorithms that may include trade secrets or intellectual property. Would it be realistic that every credit score would need to be rectified on a single data subject's request? Similarly, would this process make sense for energy companies that use smart meter data to, for instance, forecast energy demands?

The rectification of 'input personal data' may well result in the automatic rectification of output data to some extent. The scope of the right to rectification does not extend to 'output data' – as opposed to the right of access which does apply to 'output data'. To reinforce this analysis, it is useful to look at the right to data portability in relation to which WP29 guidelines clarify that inferred or derived data (i.e. the profile itself or the score in the example above) are not included in the scope of the obligation. The relevant WP29 guidelines read on page 8 "In contrast, inferred data and derived data are created by the data controller on the basis of the data 'provided by the data subject'. These personal data do not fall within the scope of the right to data portability. For example, a credit score or the outcome of an assessment regarding the health of a user is a typical example of inferred data. Even though such data may be part of a profile kept by a data controller and are inferred or derived from the analysis of data provided by the data subject (through his actions for example), these data will typically not be considered as 'provided by the data subject' and thus will not be within scope of this new right".

ARTICLE 17 – RIGHT TO ERASURE

The guidelines suggest on page 25 that "similarly the right to erasure (Article 17) will apply to both the input and the output data". Following the same thinking as outlined above in relation to the right to rectification, the 'output data', i.e., the profile itself, should not automatically be subject to the right to erasure. To the extent that the profile relates to an identified or identifiable individual, it should be erased when the right is exercised. But often such profiles are used in organisations in ways that no longer identify the individual. Therefore, the profile itself would need to be erased only in the cases where it qualifies as personal data under the GDPR.

DATA PROTECTION IMPACT ASSESSMENTS

The guidelines read on page 27: "Article 35(3) (a) refers to evaluations including profiling and decisions that are 'based' on automated processing, rather than 'solely' automated processing. We take this to mean that Article 35(3) (a) will apply in the case of decision-making including profiling with legal or similarly significant effects that is not wholly automated, as well as solely automated decision-making defined in Article 22(1)."

We agree that the provision includes decision-making that is not wholly automated. But we would like a clarification that Article 35(3) (a) only covers automated decision-making including profiling that otherwise falls within the scope of Article 22. This is clear in Article 35(3) (a) of the GDPR which reads "[…] which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person".

AUTOMATED DECISION-MAKING AND PROFILING IN VARIOUS SECTORS

It is useful that the "Introduction" of the guidelines aims to provide an overview of how automated decision-making and profiling are used in practice. However, it is difficult to fully understand and describe the enormous breadth of uses of automated decision-making and profiling in the various sectors. In order to assist WP29 in its understanding of how complex it can be to apply the general legal provisions to many different uses, we note here a few examples on how automated decision-making and profiling are used today in various sectors:

- In the **banking sector**, credit card fraud detection and prevention as well as creation of predictive models to analyse risk and create a single view of the risk and exposure across all entities of a banking group.
- Detection of medical conditions and trends by **pharmaceutical companies**.
- Service improvement, product supply management, product placement improvement and warranty management in the **retail sector**.
- Determination of effectiveness of website architecture, services improvement, customer relationship management and personalisation of services in **e-commerce**.
- Decision support analytics systems in the **airline sector** to ensure efficiency and competitiveness.
- In the **telecommunications sector**, improvement of marketing campaigns and customer retention programs.
- Detection and prevention of discrimination in **employment, housing or academic decisions** (such decisions may otherwise be influenced by human nature either intentionally or unintentionally.
- In the Internet-enabled world, **machine learning and artificial intelligence** to e.g., create better spell checkers, improve translation services, enable traffic prediction, ensure content availability, design and deploy disaster recovery programs, enable connected cars.
- Management of smart meters, consumption and demand forecasting in the **energy sector**.

--

For more information please contact:
Iva Tasheva, DIGITALEUROPE's Policy Manager
+32 493 40 56 12 or iva.tasheva@digitaleurope.org

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's members include in total 25,000 ICT Companies in Europe represented by 61 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: ANITEC-ASSINFORM
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK