Industry Coalition for Data Protection

Paper on proposals for a

"New EU legal framework on data protection"

RECOMMENDATIONS

1. **Ensure a flexible legal instrument which outlines rules in a horizontal, technological neutral way but does not lead to additional legal instruments focused on specific sectors, technologies or services.**
2. **Increase harmonisation by moving towards a country of origin approach to establish a well-balanced, harmonised legal framework in all member states.**
3. **Streamline and simplify the international data transfer system.**
4. **Reduce administrative burdens through the abolishment or streamlining of the notification/registration requirements and harmonisation of voluntary DPO requirements.**
5. **Introduce a context-based model of consent to ensure that the concept of consent remains meaningful in light of continued technological evolution.**

INTRODUCTION

The Association for Competitive Technologies (ACT), the American Chamber of Commerce to the EU (AmCham EU), the Business Software Alliance (BSA), DIGITALEUROPE, the European E-Commerce and Mail Order Trade Association (EMOTA), the European Publishers Council (EPC), the European Internet Services Providers Association (EuroISPA), the Federation of European and Direct Marketing (FEDMA), IAB Europe, TechAmerica Europe and the World Federation of Advertisers (WFA) (hereafter referred to as "the Associations") provide jointly a set of concrete recommendations to the European Commission for the revision of the Data Protection framework. The recommendations propose how to achieve the right balance between on the one hand preserving privacy and data protection as a fundamental right in the EU (and globally) while at the same time enabling the free flow of information to allow for a continued development of the Data Single Market and further facilitation of international data transfers.

The revision of the EU legal framework on data protection provides for a great opportunity that will define the competitiveness of the European economy for years to come. We urge the European Commission to balance in a sensible manner the protection of individual rights with the functioning of the Single Market. The ability of the European Information Society to generate innovation and growth, as envisaged in the European Commission's Digital Agenda, depends on creating the necessary trust, but also on the continued use of all kinds of data that are at the heart of the digital economy. Overly strict, static and bureaucratic data protection rules will have a detrimental impact on Europe's digital economy. The Single Market benefits from open competition. Today and in the future data-based business activities are the core instruments to allow any such competition to take place.

The Associations are looking forward to a continued dialogue with all stakeholders to ensure that any new legislative proposal is an overall improvement of the current legal framework within a global context.

1. MORE HARMONISATION IN A SINGLE MARKET

1.1. Better harmonisation and increased legal certainty

Personal data processing is currently regulated in fragmented ways across the EU due to differing implementations and/or interpretations. Each data protection authority has their own interpretation of the broad principles of the cornerstone Data Protection Directive of 1995 (hereafter referred to as "the Directive") and there has been a growing lack of legal certainty regarding the interpretation of its core aspects by Member States. The differences in implementation and/or interpretation of the Directive make it very difficult for businesses to take a European-wide view of data protection compliance. These disjointed regulatory approaches create inefficiencies, unnecessary expense and even business barriers for companies, innovative SMEs in particular, seeking to comply with all applicable laws and regulations and influence negatively the level of protection of data subjects.

In a knowledge-based economy, such obstacles impede the development of the Single Market.

The new EU legal framework should therefore address harmonisation issues and data protection standards in a balanced manner as to enable businesses to take a Europe-wide view of data protection compliance. This would require an adequate balance between the data subject's protection and the interest and needs of European businesses as well as the European society (e.g. freedom of press, access to information, culture...).

Regarding the legal instruments, the Associations support a legal framework which provides the necessary harmonisation at a balanced level. In choosing the legal instrument, we would like to point to the importance of a flexible instrument which should outline the rules in a horizontal and technological neutral way. We would not be supportive of a horizontal instrument supplemented by additional legal instruments focused on specific technologies or services as this would not provide the necessary legal certainty.

1.2. Applicable law

Under the current system, companies that are present in a number of Member States often find that they are subject to several different -- and diverging -- data protection regimes.

These divergent regimes result in uneven protections for users and significant compliance costs for enterprises and SMEs in particular.

In line with the Article 29 Working Parties' Opinion on applicable law (opinion 8/2010), we encourage the Commission to streamline provisions on applicable law by introducing a country of origin principle. This way each data controller would be subject to a single set of rules across the EU. This "country of origin" could be the European Member State where the main establishment of the data controller is located. We acknowledge that this could only be acceptable based on a comprehensive harmonisation of national legislation. However, at the same time this creates an incentive for DPAs to increase further harmonisation and cross border cooperation.

Unresolved issues also remain relating to applicable law with respect to data processors, as well as to data controllers based outside the EU. Resolving uncertainty regarding applicable law is important particularly for facilitating the continued development of cloud computing services. For instance, in a cloud computing scenario, the main establishment of a provider of cloud services in Europe could be in the European Member State where the provider's physical location of its data centre is located in the EU or the location where the main decisions about processing activity in the EU take place, as examples of criteria to solving applicable law difficulties.

1.3. Clarity on essential concepts

a) Personal data definition

Significant legal uncertainty has arisen around the processing of data, which still may be linked to an individual but not by the data controller. For example, in some Member States key coded information (e.g. in pharmaceutical tests) is in some cases still considered personal data even if the key codes are not held by the data controller and there is no realistic chance it could obtain them. Another concern is the definition of IP addresses and whether a website provider should treat them as personal data.

The concept of personal data should be defined following the so-called relative approach, where data is considered personal for someone who can link the data to identified individuals. Getting the response right to the question of where to draw the boundaries of "personal" data is fundamental to the success of Europe's knowledge society. Modern R&D fuelling new businesses and solutions generally relies on the analysis of aggregate information, where it is critical to disambiguate individuals from each other in an anonymous fashion. With this view and having the definition of personal data in mind as

meaning ‘any information relating to an identified or identifiable natural person’, information should only be considered to relate to an “identifiable” natural person when it is likely to be linked to identified individuals taking into consideration the time and manpower that would be required as well as the purposefulness of identifying an individual in the frame of an organisation’s lawful activities. The mere possibility of identification (for example through cross-reference of the available information with other third party sources) should not be sufficient to meet the threshold of the definition. There needs to be a degree of reasonableness and a proximity link between the information available and the identification of the individual in question.

One possibility to deal with these aspects could be to introduce a harmonised definition of indirect or pseudonymous personal data that could benefit from lighter data protection requirements as the processing of such type of data usually present very low risks to privacy.

The definition of personal data could be reformed by adopting a more nuanced and pragmatic approach, including consideration of the context, intent and practices of the data controller. If the data controller does not intend to use the data in a way that requires personal identification of data subjects, or if there is not a reasonable chance that the data controller could actually identify a data subject, that data should not be considered personal data.

b) Anonymisation

Since the personal identity of the data subject is often not what a data controller seeks to establish, data anonymisation techniques can be and are used to safeguard individuals’ rights without compromising the value of the data as a driver of the digital economy. They are instrumental for meeting the key requirement of the Directive that data collection is “adequate, relevant and not excessive in relation to the purposes for which they are collected”.

The importance of anonymisation should therefore be recognised by EU data protection law. In turn, it is critical not to discourage anonymisation by requiring overly complex and burdensome anonymisation processes in relation to data which is unlikely to lead to the identification of the data subject in the first place. In line with Recital 26 of the present Directive, the use of codes of conduct for data anonymisation could be further encouraged.

c) Consent

We share the view that clarification of the concept of consent is needed but changes in the current consent rules need to be carefully considered. Indeed, we have seen that the specific consent rules that were introduced e.g. to limit spam have resulted in increased complexity for businesses but failed to adequately limit spam.

A valid and meaningful form of consent should depend on the context in which it is given. A modern approach to consent should allow for data controllers to choose the most contextually appropriate way of providing information, obtaining consent, and empowering data subjects by offering them control over their data. As data becomes increasingly disseminated and virtually ubiquitous, the moment, the language, the information and the modalities for giving consent are going to be critical to ensure that consent remains meaningful over time and in view of technological developments.

By adding emphasis on the context of consent, a modern EU framework for data protection would move away from the existing binary approach towards a more nuanced and dynamic approach which empowers users.

An overly rigid approach to obtaining consent, focused on requiring the use of particular mechanisms which may ensure meaningful consenting, hardly increases privacy protection while potentially imposes restrictions for business and increases bureaucracy. Depending on the context and execution, more innovative and dynamic mechanisms can provide better and more meaningful protection for consumer privacy (with fewer disruptions for data subjects) than weaker 'opt-in'-like mechanisms. We believe that EU rules should recognise legitimate business purposes for applying different mechanisms for consent, depending on a given context and its specific execution, instead of simplistically favouring one approach over another.

We also recognise that there are situations where EU citizens should not have to deal with a possibly complex or difficult legal context and having to give her or his consent to the way their data are processed. It should be avoided that the consent-giving-process would become an automatic and unconscious human routine, and thus devalues its importance. It is therefore important to point out that in addition to consent, the Article 8 of the Charter of Fundamental Rights stipulates that data can be processed on some other legitimate basis laid down by law. The 95/46/EC Directive had already established several and very important other "legitimate grounds" for processing personal data, such as the necessity for the performance of an agreement. These "legitimate grounds" have been transposed

into national law. We call upon the lawmaker to provide as much attention to these other "legitimate grounds" as to the consent requirement. We are convinced that these are key legislative solutions both for companies and data subjects in situations where a consent-based processing would neither be adequate nor relevant.

Innovative industry-driven solutions, including at company level and through effective industry-wide self-regulation, have an important role to play[1].

1.4. Reducing administrative burdens

The formalities of some rules as imposed by the current framework result in significant compliance costs and unequal enforcement while not improving the overall level of data protection.

One example is the current registration and notification system which needs to be revised and simplified. Indeed, the registration and notification requirements and processes are often unclear in terms of applicability, and the different approaches to registration and notification create real compliance difficulties when trying to operate on a pan-European basis. The Associations therefore see a strong case for abolishing or considerably easing the registration and notification requirements to high risk scenarios and/or ensuring that they are applied on a more uniform basis across the EU. These mechanisms will need to be set at the right threshold to avoid discouraging SMEs for developing innovative solutions and services. The Associations also see the voluntary appointment of one data protection officer (DPO) for companies as an adequate and voluntary alternative to notification duties. Harmonised requirements for the establishment of a DPO will be essential to ensure an equal implementation across the European Union.

The Associations welcome the Commission's intention to reduce the administrative burden imposed on data controllers by having standardised privacy notices. We agree that transparency is essential to allow users to make informed and meaningful choices about the processing of personal information related to them. The Directive lays down the main elements to be contained in privacy notices. However, because of the leeway afforded to

[1] The online advertising sector offers a useful illustration. It has developed transparency and control tools specifically for behaviourally targeted ads where the user would intuitively expect and understand them – in the ads themselves. By clicking on a standardised icon located in or around the ad, users will be able exercise control over the use of their data for behavioural advertising. This micro-context-sensitive approach departs significantly from the conventional 'opt-in vs. opt-out' dichotomy by giving more contextual information and offering more dynamic, context-specific control.

Member States in implementing the Directive, there are often additional and differing national requirements that create additional administrative burdens especially for SMEs that find it difficult to comply with these rules, and, more broadly, to develop services at the EU level. We would like to caution against standardised compulsory privacy notices drafted without stakeholders' involvement or outside their control. In any case, they should be used as guidance and leave room to companies to adapt them. Any templates developed should be given mutual recognition across all Member States.

1.5. Increasing data controller responsibility and accountability

The Associations support the move from an ex ante regime to an ex post legal system. Legislation should look at establishing clear guidance on what needs to be achieved, instead of narrowly focusing on how to achieve this via prescriptive and administrative processes that do not really accomplish the ultimate objective of increased data protection.

In an ex post system, organisations (public and private) are accountable for their handling of data, wherever that data travels instead of merely seeking legal compliance. It is, however, broader than only focusing on increasing the data controllers' responsibility, as mentioned in the European Commission's Communication of November 2010. It is a concept that underpins the entire legal framework, on how we look at data protection, on how we enforce and supervise it. An optimised legal framework should encourage and give incentives to organisations to be accountable; to have as a recognised corporate objective the protection of the rights of individuals, while at the same time seeking and obtaining legal compliance. This will enable data protection to become a proactive part of their business instead of a reactive compliance function.

Accountability and ex post controls does not mean adding individual new obligations on top of already prescriptive rules, but instead that this term needs to offer a more flexible and effective alternative to the proliferation of complex and potentially conflicting obligations. The Associations also encourage further stakeholder discussion on shaping the accountability concept and how this should be implemented into the new legal framework.

1.6. Privacy Impact assessments (PIAs)

PIAs are a useful tool as part of the accountability measures as mentioned above. Care must be taken, however, to avoid mandating a specific PIA template. Privacy risks are typically contextual and often technology specific. At present, a common and industry

approved privacy threat identification model is missing. Without such a threat identification model a policy based PIA methodology runs the risk of being mere "check list compliance".

In addition to this, compliance with potential mandatory PIA provisions that are implemented in different ways in each Member State would disrupt the Internal Market and dramatically increase the cost of designing and producing ICT products. Indeed, compliance with 27 different sets of rules on PIAs might not be possible for many businesses, particularly SMEs. We therefore do not think mandatory PIAs should be introduced in any new legal framework.

1.7. Privacy by Design and Privacy by Default

Privacy by Design (PbD) is a process that organisations should complete at the start of a project and reassess regularly to ensure that the data privacy and security measures are applied from day one and remain appropriate over time. Further clarity is needed on how it would be defined or implemented before it should be reflected in any new legal framework. In our opinion, it should focus on ensuring that the appropriate process controls are in place when a technological solution is built to guarantee the privacy and security of the data. However, PbD should by no means be a technology-specific requirement to be embedded within products as this would go against technological neutrality. Organisations should remain flexible on how to implement a PbD process within their organisations. Privacy by Design should be understood as the desired objective/outcome. However, the means towards that end should be best determined in each individual case by the data controller. Product specific requirements could dramatically increase the cost of designing and producing ICT products, slow down the innovation cycle and may exclude SMEs from participating in the development of new services.

In the same vein, it would be undesirable for privacy rules to dictate specific technological outcomes – including 'Privacy by Default' – which will only impede the development of new technologies without guaranteeing stronger privacy protections.

Additionally, Privacy by Design could also encourage greater take up and use of Privacy Enhancing Technologies (PETs) as means of supporting compliance with the Privacy by Design procedural requirement. However, PETs should not become legal requirements: depending on the information they process and the business model they follow, organisations across different sectors should be afforded sufficient flexibility to determine

how best to comply with data protection rules, thereby ensuring the most effective protection for data subjects.

2. INTERNATIONAL DATA TRANSFERS

With increasing globalisation and the advent of new technologies such as cloud computing, companies and citizens are able to benefit from doing business globally. This does, however, require the routine movement of large amounts of personal data across borders, including between the EU and third countries. To stimulate innovation and allow the EU to deliver on the promises of growth and jobs, the transfer of data on a worldwide basis should not be restricted as long as robust safeguards for the processing of that data are in place. We therefore support the recently approved ICT principle on global data flows by the EU and US which points towards the need to avoid obstacles to such flows[2].

While we welcome the Commission's plans to improve and streamline procedures for transferring data out of the EU, we would like to caution against an overly burdensome or prescriptive framework. Therefore we encourage the Commission to explore firstly the continued relevance of the adequacy principle as a basis for international transfers and then to investigate the possibility of streamlining this procedure by focusing the analysis on the outcomes sought by a particular country's legislation.

Alongside such reform, streamlining and harmonising the notification and approval requirements for Binding Corporate Rules (BCRs) and Model Contractual Clauses (MCCs) mechanisms could help reduce the bureaucracy and burden on companies while offering adequate levels of data protection.
BCRs are currently too narrow in scope (applying only to intra-group transfers and to controllers) and too long and costly in its implementation to be of a clear added value to facilitate data transfers. Same, the MCCs reviewed in February 2010 by the European Commission need to be revised and improved.

At the same time**,** we call upon European policymakers to pursue bilateral or multilateral international agreements on minimum protection levels for the privacy and security of

[2] Principle #3. Cross-Border Information Flows: Governments should not prevent service suppliers of other countries, or customers of those suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in other countries.

transferred data. Achieving a better understanding of jurisdictional issues is critical and should be tackled through enhanced dialogue.

3. USERS' RIGHTS – AN INCREASED TRUST ENVIRONMENT

3.1. Right to be Forgotten and data portability

The creation of a '**Right to be Forgotten'** is redundant with the already existing provisions on data protection. The current Directive already provides data subjects with the right to object to the processing of their personal data and to access, correct and/or delete their information. In addition, the requirement to store personal data for no longer than necessary and for a specified purpose only already provides adequate limits to storage and retention periods of personal data. We are open in working with all stakeholders to identify the problem that the introduction of a 'Right to be Forgotten' would attempt to tackle and to explore possible solutions. We also would like to introduce a distinction between data the data subject directly inputs and are retained by the service provider such as emails and photos, and other data generated in the operation of a service.

The introduction of a principle of data portability should not be the subject of discussions on the EU legal framework on data protection. In addition, it would bring serious competition issues with regards to the commercial added value created by companies over these data. Moreover, in many cases such a right would require the creation of technical means to transfer data which would have detrimental impacts on businesses and likewise on data security.

Finally, a 'Right to be Forgotten' and data portability would bring contradiction with already existing laws, as in a lot of cases a copy of any given data must be retained by the original controller for a given time period to comply with specific accounting, tax and similar laws.

3.2 Collective redress

With regards to a European instrument for collective redress, we feel that the Commission should not pre-empt the ongoing work on this issue. A public consultation on the working document 'Towards a Coherent European Approach on Collective Redress' is currently

being carried out. In any case, we do not believe that a specific collective redress instrument for the data protection sector is needed or justified.

Moreover, the instrument of collective redress is not compatible to fundamentals of our West-European law traditions. Our societies and legal systems are based on the rights of the individual, not on the rights of a "collective". Chapter VI of the Charter of Fundamental rights postulates the freedoms related to the justice system as the freedoms of the individual. If the Commission feels a need to improve the legal systems in the Member States, it should always address the individual's position. Introducing a class action instrument in the spirit of the American law tradition would devalue the position the individual should and must have according to our European legal traditions and understanding of the fundamental rights. Besides, a collective redress instrument would decrease the necessity to maintain and strengthen the individual's position as we know it, possibly leading to or even facilitating an "unbalanced system". The EU should rather strive to make our existing legal systems more effective, giving the Member States advice on such areas as improving the administrative side of the court systems, avoiding bureaucratic legal procedures, legal aid, assigned counsels, etc.

3.3. Privacy seals/EU certification schemes

We welcome private sector efforts to develop useful tools such as privacy seals or certification schemes for aiding consumers in identifying online businesses and services that maintain high privacy standards. We would also welcome Commission efforts to support voluntary, industry-led efforts in this area with reasonable cost structures that will not disadvantage SMEs. Mandatory certification schemes will, in contrast, create barriers to innovation and impose additional, unreasonable costs on organisations that are required to accredit their products under such schemes. Any scheme, if introduced, must be a competitive advantage, not a new burden. It should be structured in a way that avoids unduly burdening companies – and particularly SMEs – with costly and bureaucratic obligations which discourage participation. Specifically, the scheme should be voluntary, affordable (undue costs create barriers to entry for SMEs), neutral and recognised globally. We also encourage the Commission to take a more active role in promoting self-regulation mechanisms.

CONCLUSION

The Associations are committed to ensuring the free flow of information to further shape the Single Market while at the same time ensuring a strong and harmonised level of protection for data subjects not only across Europe but also globally.

We are looking forward to continuing our dialogue with all stakeholders as to ensure a new legal framework which stands the test of time.

The Association for Competitive Technology (ACT AIBSL) is an international non-profit association based in Brussels. ACT is an international advocacy and education organisation representing more than 4,000 innovative small and medium-sized enterprises (SMEs) in the information communication technology (ICT) sector from around the world, including some 1,000 members in the European Economic Area (EEA). ACT advocates an environment that inspires and rewards innovation. Its mission is to help members leverage their intellectual assets to raise capital, create jobs, and continue innovating.

Contact: Greg Polad, Greg.Polad@fticonsulting.com

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate U.S. investment in Europe totalled €1.4 trillion in 2009 and currently supports more than 4.5 million jobs in Europe.

Contact: Roger Coelho, RCO@amchameu.eu

The Business Software Alliance (www.bsa.org) is the world's foremost advocate for the software industry, working in 80 countries to expand software markets and create conditions for innovation and growth. Governments and industry partners look to BSA for thoughtful approaches to key policy and legal issues, recognizing that software plays a critical role in driving economic and social progress in all nations. BSA's member companies invest billions of dollars a year in local economies, good jobs, and next-generation solutions that will help people around the world be more productive, connected, and secure. BSA members include Adobe, Altium, Apple, Asseco Poland S.A., Attachmate, Autodesk, Autoform, AVEVA, AVG, Bentley Systems, CA Technologies, Cadence, Cisco, CNC/Mastercam, Corel, Dassault Systèmes SolidWorks Corporation, DBA Lab S.p.A., Dell, HP, Intel, Intuit, Kaspersky Lab, Mamut, McAfee, Microsoft, Minitab, NedGraphics, O&O Software, PTC, Progress Software, Quark, Quest, Rosetta Stone, SAP, Scalable Software, Siemens, Sybase, Symantec, Synopsys, Tekla, and The MathWorks.

Contact: Thomas Boué, thomasb@bsa.org

DIGITALEUROPE is the voice of the European digital economy including information and communication technologies and consumer electronics. DIGITALEUROPE is dedicated to improving the business environment for the European digital technology industry and to promoting our sector's contribution to economic growth and social progress in the European Union. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 57 global corporations and 37 national trade associations from across Europe. In total, 10,000 companies employing two million citizens and generating €1 trillion in revenues.

Contact: Anna-Verena Naether, Annaverena.Naether@digitaleurope.org

EMOTA, the European E-Commerce and Mail Order Trade Association, represents 20 national associations in the European Union and beyond, which in turn represent about 2600 traders. As the association representing e-commerce and distance selling in the European Union the goals of EMOTA are to support the removal of any barriers for trade in the Single Market and to support the efforts towards increasing consumer trust in the Single Market, online and offline.

Contact: Susanne Czech, suczech@emota.eu

The European Publishers Council (EPC) is a high level group of Chairmen and CEOs of Europe's leading media groups actively involved in multimedia markets spanning newspapers, magazines, online publishing, journals, databases, books and broadcasting. We have been communicating with Europe's legislators since 1991 on issues that affect freedom of expression, media diversity, democracy and the health and viability of media in the European Union. The overall objective has always been to encourage good law-making for the media industry.

Contact: Nikolas Moschakis, nikolas.moschakis@europe-analytica.com

EuroISPA is the world's largest association of Internet Services Providers (ISPs) representing the interests of more than 1800 ISPs across the EU and the EFTA countries. EuroISPA is a major voice of the Internet industry on information society subjects such as cybercrime, data protection, e-commerce regulation, EU telecommunications law and safe use of the Internet (www.euroispa.org).

Contact: Andrea D'Incecco, andrea@euroispa.org

FEDERATION OF EUROPEAN DIRECT AND INTERACTIVE MARKETING

The Federation of European Direct Marketing (FEDMA) represents the direct marketing sector at European level. Its national members are the Direct Marketing Associations (DMAs) representing users, service providers, and media/carriers of direct marketing. FEDMA also has 200 company members in direct membership. The direct marketing sector represents an expenditure of over 30 billion Euro and employs over 1.5 million people directly, and many more indirectly, within the EU.

Contact: Mathilde Fiquet, mfiquet@fedma.org

IAB Europe is the voice of the online advertising sector through its 29 national associations representing more than 5,000 company members, as well as corporate members including Adconion, Adobe, ADTECH, Alcatel-Lucent, AudienceScience, BBC, CNN, comScore Europe, CPX Interactive, Criteo, e-Bay, Ernst & Young, Expedia Inc, Fox Interactive Media, Gemius, Goldbach Media Group, Google, GroupM, Hi-media, InSites Consulting, Koan, Microsoft Europe, MTV, Netlog, News Corporation, nugg.ad, Nielsen Online, Orange Advertising Network, Prisa, Publicitas Europe, Sanoma Digital, Selligent, Smartclip, Specific Media, Tradedoubler, Truvo, United Internet Media, ValueClick, White&Case, Yahoo! and zanox. Supported by every major media group, agency, portal, technology and service provider, IAB Europe coordinates activities across the region including public affairs, benchmarking, research, standards settings, and best practices.

Contact: Kimon Zorbas, vp@iabeurope.eu

TechAmerica Europe (established in 1989) represents leading US high-tech companies with significant presence in Europe (Euro 100bn investment in 27 Member States and 500,000 employees). TechAmerica Europe is the EU office of TechAmerica, the oldest and largest high-tech Association in the US, which represents approximately 1,200 member companies of all sizes and from all sectors of the industry.

Contact: Aneta Podsiadla, Aneta.Podsiadla@techamerica.org

WFA is the only global organization representing the common interests of marketers.
It brings together the biggest markets and marketers worldwide, representing roughly 90% of global marketing communications spend, almost US$ 700 billion annually.
WFA champions responsible and effective marketing communications.

Contact: Malte Lohan, M.Lohan@wfanet.org