BRE-JBZ

From: Kaai, Geran
Sent: vrijdag 3 april 2015 15:57
To: Verweij, Ellen
Subject: FW: DIGITALEUROPE position on Safe Harbour
Attachments: 20140311_DE Safe Harbour position paper_final.pdf

---

From: BRE-JUS
Sent: donderdag 20 maart 2014 16:40
To: Grave, Martijn-de; Ruiter, Mieneke-de; Dam, Caroline-ten; Alink, Marnix; Kaai, Geran; Timmermans, Marieke; Sorel, Alexander; Luijsterburg, Sander; Bos, Nicoline; Zwart, Jan
Subject: FW: DIGITALEUROPE position on Safe Harbour

Van: [redacted]
Verzonden: donderdag 20 maart 2014 16:39:37 (UTC+01:00) Brussels, Copenhagen, Madrid, Paris
Aan: BRE-JUS
Onderwerp: DIGITALEUROPE position on Safe Harbour

Dear Mr Kaai,

I would like to share with you DIGITALEUROPE's position on the revision of Safe Harbour and the specific recommendations by the European Commission on the functioning of Safe Harbour.

Please do not hesitate to contact me for any questions you may have.

Kind regards,

[redacted]
Policy Manager
Digital Economy Policy Group

DIGITALEUROPE >> Rue de la Science, 14 >> B-1040 Brussels
T. +32 2[redacted] >> **M.** +32 [redacted]
http://www.digitaleurope.org

The information in this email is confidential and is intended solely for the addressee. Access to this email by anyone else is unauthorised. If you are not the intended recipient, you must not read, use or disseminate the information. Any views expressed in this message are those of the individual sender, except where the sender specifically states them to be the views of DIGITALEUROPE aisbl.

The information in this email is confidential and is intended solely for the addressee. Access to this email by anyone else is unauthorised. If you are not the intended recipient, you must not read, use or disseminate the information. Any views expressed in this message are those of the individual sender, except where the sender specifically states them to be the views of DIGITALEUROPE aisbl.

[redacted]

DIGITALEUROPE

March 18, 2014

DIGITALEUROPE POSITION ON SAFE HARBOUR REVISION

DIGITALEUROPE welcomes the Communications the European Commission published on 27 November 2013. The EU examination of Safe Harbour has served a useful purpose and we agree that a third review of the Safe Harbour programme, the first formal review in almost 10 years, is appropriate. While maturation of the programme and dialogue between the EU and US has enabled continued improvement over the years, there is room for fresh reflection in order to achieve sustainable improvements. Therefore we appreciate the Commission's efforts to come up with constructive recommendations. We support the large majority of the recommendations, though we have varying levels of concern about three of them and suggest improvements below.

Reform of Safe Harbour

DIGITALEUROPE believes that Safe Harbour is an effective and flexible tool for transfer of data while protecting the privacy of EU citizens. Global business models require transfer of and access to data outside our region. Thousands of companies, both large and small, with and without European or US parentage, rely on Safe Harbour for the transfer of data across borders. Suspending the programme would create for these companies legal and organisational difficulties as it is both extraordinarily costly and, in fact, logistically impossible to instantly amend existing contracts that depend on Safe Harbour.

Safe Harbour permits companies operating in the EU to transfer the data of EU customers to the US based on their declaration of compliance with the Safe Harbour framework1, which includes seven privacy principles similar to those found in the 1995 EU Data Protection Directive. Currently about 3,400 companies have an active certification under the scheme. Membership in the Safe Harbour programme has grown steadily and industry has committed to more stringent data security to stay in compliance with the Safe Harbour's privacy rules, and the U.S. Federal Trade Commission (FTC) has initiated significant enforcement actions. DIGITALEUROPE believes the FTC and third party certification providers have shown both the capacity and the willingness to respond to complaints and to enforce against companies who fail to live up to their Safe Harbour obligations.

We welcome the European Commission's Communication on the Functioning of the Safe Harbour (COM(2013) 847) and many of the recommendations for reform contained within. We are pleased that the Communication notes the self-initiated increase in enforcement cases by the US Federal Trade Commission (FTC), the increase in transatlantic cooperation, the new processes introduced to guard against companies that falsely claim certification, and the tools the US Department of Commerce (DoC) has introduced over the years to address

1 In the case of transfers only for processing purposes a contract is also required between the controller and processor, as it would be if the processing were to take place in the EU.

DIGITALEUROPE
Rue de la Science, 14 >> B-1040 Brussels [Belgium]
T. +32 2 609 53 10 >> **F.** +32 2 609 53 39
www.digitaleurope.org
Transparency register member for the Commission: 64270747023-20

concerns raised in the 2004 review. We examine the specific recommendations made by the Commission in more detail below.

Transparency

Transparency is essential if EU citizens are to have the level of accurate information necessary to make decisions about the processing of their personal data. Transparency is enshrined in the right to information in the current Directive (95/46/EC) and acts as the building block for further rights of the data subject.

As such, DIGITALEUROPE supports three of the recommendations made by the Commission related to this transparency. We support the public disclosure of privacy policies (as distinguished from the current requirement to provide summaries of policies to the DoC). While the Communication notes that the vast majority of signatories to the agreement do so, it is nevertheless worth reiterating to the minority that do not. Secondly, DIGITALEUROPE supports the proposal that privacy policies should include a link to the DoC's Safe Harbour website. Not only could this help reduce the possibility of false claims of adherence but it could provide a simple link for citizens to better understand Safe Harbour and what it attempts to achieve. Thirdly, we would support the recommendation that those entities that are not current members of the scheme are clearly flagged. While the 'not current' status option on the Safe Harbour website seems self-explanatory, we would not object to an accompanying warning that such an entity is not meeting the Safe Harbour requirements.

We are, however, concerned about recommendation number 3 that would require companies to publish the privacy provisions of contracts they enter into with subcontractors and notify the DoC. We believe that this requirement to centralise and post the provisions of thousands of individual contracts would impose an excessive administrative burden. We further believe that such a requirement is unnecessary to achieve the goal in mind and may indeed be counterproductive. While the burden primarily would fall on the companies, the DoC would not be immune given they would be expected to do something more with the reams of information sent to them than simply store it. We also question this recommendation from the perspective of competitiveness and business confidentiality, and ask whether it is appropriate to publish individual sections of business-to-business contracts.

An alternative proposal that could achieve the desired result in a more efficient way that would be more understandable and useful for individuals would be to require companies to send to the DoC the templates of the agreement conditions they use in their agreements with subcontractors, with the understanding that these are subject to amendment in individual contract negotiations. Publication of such templates would make it easier to understand the standard approach for handling data and how it meets the Safe Harbour requirements, without raising undue administrative burdens.

Redress

Redress is an important element of data subjects' rights as it is a key means to see that they are upheld. We are pleased to note that the use of Alternate Dispute Resolution (ADR) providers has increased since the last Commission report in 2004 as it is a sign that the system is becoming better established and functioning better. Nevertheless, we believe that the three recommendations in this area are all to be welcomed in order to improve it further.

For each recommendation, we believe it is a case of codifying existing best practice. We agree that public privacy policies should link to the ADR provider and are glad to note the recognition by the Commission that the DoC has been promoting this requirement since early last year. Secondly, we also believe that ADR should be readily available and affordable from the point of view of the citizen making a complaint. The Communication indicates that the ADR providers of four out of five Safe Harbour companies do not require any fee from individuals making a complaint and that fees have been reduced significantly for the remainder. Nevertheless, we support the goal of continuing to reduce costs where they still apply. Finally, we agree that the DoC should oversee ADR providers to check on the information they provide about their procedures and follow up to complaints. This will continue to boost the integrity and credibility of such providers.

Enforcement

Without enforcement there is a potential lack of consequences for those who fail to effectively implement the guarantees they have signed up to on paper. As such, enforcement is essential for the credibility of the system and to ensure that citizens' rights are upheld and companies are treated fairly. Like the Communication, we note that enforcement efforts have increased over the years. Following a lack of referrals by Member States' authorities in the first decade, the FTC took it upon itself to ramp up enforcement cases and has exceeded the activity of the EU's own Data Protection Panel. Moreover, the report rightly notes that in recent years the level of transatlantic cooperation has increased.

We believe that the four recommendations in the Communication on enforcement are sensible measures that would continue to strengthen existing efforts. We support the concept of ex-officio investigations of a proportion of companies to ensure effective compliance if companies are targeted on the basis of reasonable suspicion of non-compliance rather than on random selection. Likewise, follow-up investigation in cases of non-compliance after a period of time is sensible. DIGITALEUROPE also believes that in case of doubts about compliance or pending complaints the DoC should notify the appropriate EU data protection authority. We see this as a natural response in the spirit of international cooperation. Finally, as is the current practice, false claims of Safe Harbour adherence should be investigated.

Access by US authorities

We understand that the European Union's desire to better safeguard EU citizens' data in light of the revelations about surveillance programmes in the US and beyond. It is essential for a well-functioning digital single market that consumers can trust that their data is protected and their human rights are not infringed. Nevertheless, we are not convinced that an agreement designed for the commercial transfer of data, in which processing for national security, public interest and law enforcement is specifically removed from the scope, is the right place to try to address this issue.

Of the two recommendations relating to this topic, we understand the intention behind insisting that the national security exception is used proportionately. However, this issue applies more broadly than within the narrow confines of the Safe Harbour scheme and should be resolved in direct government-to-government negotiations on the norms in cyber

surveillance and access by authorities. It cannot be resolved in a commercial agreement that is not a prerequisite for such surveillance to take place. Attempting to do so would only deflect attention from the real discussions that need to occur.

The second recommendation is an example of how the debate can be unhelpfully deflected. It requires that companies explain in their privacy policies when they apply exceptions to the Safe Harbour Principles to meet national security, law enforcement or public interest requirements. Whatever the rights and wrongs of the government-to-government dispute, this requirement unnecessarily would put companies in the middle of a jurisdictional conflict they cannot themselves resolve.

Additional reform

Above and beyond the recommendations of the Commission, one additional area we have identified for reform is the level of compatibility between Safe Harbour and the Standard Contractual Clauses (Model Clauses) under the Data Protection Directive. It makes sense that the mechanisms established for transfer of data outside of the EU should be interoperable.

A key point would be for the obligations and contractual clauses stemming from the two mechanisms to be interchangeable as data flows from controllers to processors and sub-processors. For example, a controller could derive terms from Safe Harbour obligations in its contract with a processor, which the processor chooses to implement via model clauses in its contract with sub-processors, or vice versa.

Conclusion

In conclusion, DIGITALEUROPE supports the review of the Safe Harbour agreement. While we believe the instrument has been a practical and effective method for enabling global data flows that meet the expectations of the EU, renewed assessment should be used to improve it further.

We support recommendations made by the Commission in the area of transparency, redress and enforcement. We do not, however, believe this is the best place to address questions related to access to data by US authorities. We also propose an alternative recommendation to the proposal on the publication of subcontractors' contractual clauses. Finally, we ask for an additional reform that would improve the interoperability of Safe Harbour and Model Clauses.

DIGITALEUROPE looks forward to be a constructive partner for policy-makers in this debate and is ready to contribute to ongoing work.

DIGITALEUROPE

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 58 global corporations and 35 national trade associations from across Europe. In total, 10,000 companies employing two million citizens and generating €1 trillion in revenues. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

THE MEMBERSHIP OF DIGITALEUROPE

COMPANY MEMBERS:

Acer, Alcatel-Lucent, AMD, APC by Schneider Electric, Apple, BenQ, Bose, Brother, Canon, Cassidian, Cisco, Dell, Epson, Ericsson, Fujitsu, Hitachi, HP, Huawei, IBM, Ingram Micro, Intel, Jabil, JVC Kenwood Group, Kodak, Konica Minolta, Kyocera, Lexmark, LG, Loewe, Microsoft, Mitsubishi Electric, Motorola Mobility, Motorola Solutions, NEC, Nokia, Nokia Siemens Networks, Nvidia, Océ, Oki, Oracle, Panasonic, Philips, Pioneer, Qualcomm, Research In Motion-Blackberry, Ricoh International, Samsung, SAP, Sharp, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, Xerox, ZTE Corporation.

NATIONAL TRADE ASSOCIATIONS:

Belgium: AGORIA; **Bulgaria:** BAIT; **Cyprus:** CITEA; **Denmark:** DI ITEK, IT-BRANCHEN; **Estonia:** ITL; **Finland:** FFTI; **France:** Force NUMérique, SIMAVELEC; **Germany:** BITKOM, ZVEI; **Greece:** SEPE; **Hungary:** IVSZ; **Ireland:** ICT IRELAND; **Italy**: ANITEC; **Lithuania**: INFOBALT; **Netherlands:** Nederland ICT, FIAR; **Poland:** KIGEIT, PIIT; **Portugal:** AGEFE; **Romania:** APDETIC; **Slovakia:** ITAS; **Slovenia:** GZS; **Spain:** AMETIC, **Sweden:** Foreningen Teknikföretagen, IT&Telekomföretagen; **United Kingdom:** INTELLECT

Belarus: INFOPARK; **Norway:** IKT NORGE; **Switzerland:** SWICO; **Turkey:** ECID, TESID, TÜBISAD; **Ukraine:** IT UKRAINE.