35

BRE-JBZ

From: Kaai, Geran
Sent: vrijdag 3 april 2015 15:59
To: Verweij, Ellen
Subject: FW: DIGITALEUROPE on the Risk-Based Approach
Attachments: DIGITALEUROPE_risk based approach_aug 2013.pdf

From: BRE-JUS
Sent: vrijdag 6 september 2013 10:37
To: Kaai, Geran
Subject: FW: DIGITALEUROPE on the Risk-Based Approach

From: [redacted] [mailto:[redacted]]
Sent: vrijdag 6 september 2013 10:34
To: BRE-JUS
Subject: DIGITALEUROPE on the Risk-Based Approach

Dear Mr Kaai,

We would like to share with you DIGITALEUROPE's paper on the Risk-Based Approach on data protection, which is being discussed in the Council right now. We very much welcome the idea of adding flexibility to the draft regulation through a more apt assessment of the risk-obligation scale. We hope our paper will help you in the negotiations.

We would be interested in following up with a meeting, when your agenda permits. If you are amenable to the idea, please feel free to suggest a time slot that would suit you.

In the meantime, please do not hesitate to contact me for any questions you may have.

I look forward to hearing from you.

Kind regards,

[redacted]
Digital Economy Policy Group

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

DIGITALEUROPE

28 Aug 2013

DIGITALEUROPE COMMENTS ON THE RISK-BASED APPROACH

Introduction

The risk-based approach as a means to improve the data protection Regulation has been widely debated in the Council. Moreover, the European Data Protection Supervisor Peter Hustinx spoke out in favour of a risk-based approach as a means to rendering the proposed legislation less prescriptive[1]. DIGITALEUROPE welcomes this discussion as a bold and important step in advancing the debate on data protection.

Concretely, the risk-based approach assesses the risk inherent in data processing operations and incidents when determining the obligations for data controllers and processors. In other words, the risk-based approach would allow for a more nuanced approach to data protection as it recognizes that there are different categories of data processing and incidents, with various degrees of risk involved. Beyond scaling the risk itself, the risk-based approach further encourages measures that reduce the risk involved in data processing. Controllers will strive towards the least risky processing possible if this is rewarded by fewer and more appropriate obligations (scaled and proportionate to the risk involved). When it comes to the protection of personal data such an approach is more effective than prescribing a one-size-fit all solution.

Accordingly, DIGITALEUROPE would like to share below some thoughts regarding the principles underpinning the risk-based approach, as well as how and where a risk-based approach should be visible.

1- WHAT ARE THE PRINCIPLES UNDERPINNING THE RISK-BASED APPROACH?

The notion that personal data needs to be protected adequately is universally accepted. Indeed, the EU has recognised the protection of personal data as a fundamental right. However, no fundamental right is granted without limitations and the significant nuances that exist in the processing of personal data must be taken into consideration.

Risk needs to be the predominant consideration in determining how the fundamental right to the protection of personal data (as specified in the European Charter of Fundamental Rights) may best be safeguarded while ensuring that personal data is adequately protected without imposing inappropriate or disproportionate burdens.

[1] Hustinx, P., "Astroturfing takes root", appeared in FT on 27th June 2013, accessed via: http://presscuttings.ft.com/presscuttings/s/3/articleText/73993966#axzz2XsjJuzad

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

The draft data protection Regulation has been criticized for being too binary in nature, meaning it either applies in full or not at all. In low risk activities such an approach results in unnecessary burdens. The draft has been developed to regulate the facets of consumer interaction with the online world. Consequently, it treats all the different ways of handling personal data of consumers in the online world in the same way. Moreover, it equally applies to industrial or other offline commercial activities and mere B2B relations. If there are no variations in the application of the law, company-internal privacy R&D measures may actually be discouraged since they would not lead to any alleviation of obligations.

Because it is often difficult to determine the level of the risk ex ante, the strength of the risk-based approach lies precisely in the need to evaluate how risk changes dynamically as data processing practices evolve (because of changes in the scale of data processing, or expansions to other fields of business). As practices change (and risk changes), the measures need to ensure compliance will evolve as well. In this way, a risk-based approach stresses and confirms the importance of implementing a data protection culture, rather than meeting one-off compliance formalities.

Most importantly, it does not statically prescribe obligations, but instead bases them on the context and the risk involved. As a result the risk-based approach allows for an easier and more appropriate adaptation of the rules. Given that the objective is to adopt a Regulation that stands the test of time (i.e. new technological advances) it is crucial to inject a certain degree of flexibility in the text as proposed. The Article 29 Working Party recognises this, e.g. in their 2011 Opinion on location-based data where they cite the so-called 'function creep" as a risk related to the use of location data. "Function creep" delineates the fact that based on the availability of new types of data, new purposes can be developed that were not anticipated at the time of the original collection of the data. An effective risk-based approach addresses such concerns and ensures a more future-proof legislation, fit to deal with technological developments.

2- HOW SHOULD RISK BE UNDERSTOOD?

This section discusses how risks should be measured in order to guarantee that certain obligations are required only for risky specific data processing. Such a proportional approach ensures that riskier processing requires higher security and more checks and balances, while less risky processing should carry fewer burdens. The risk-based approach thus strikes the right balance as it adequately protects data while allowing business to operate.

Determining the risk involved in specific categories or acts of data processing should take into consideration the following criteria:

1. The scale on which personal data is processed –quantitative - (more stringent requirements could be applied to the processing of personal data based on numbers of data subjects involved).

2. The sensitivity of data being processed, and more specifically whether the nature of this data causes it to be more likely to result in harm, considering the full context of data processing – qualitative -(the processing of health related information, racial information, etc.).

3. The field of activity of the data controller, as an indicator for the risk of harm (financial services, health care, legal services).

4. The circumstances in which personal data is handled (personal data of consumers or business related personal data of a data subject in his or her professional capacity or personal data of employees, submission of data to the digital economy of the online world or just along the way in the context of essentially industrial or other offline commercial activities not focused on the use of personal data).

5. The potential for new value creation requires a shift from controlling data collection to focusing on data usage, as also proposed by World Economic Forum report "Unlocking the value of personal data"[2]. Permissions, controls and trustworthy data practices need to be established that enable the value-creating applications of data but prevent the intrusive and damaging ones. In reality, it is the inappropriate use of data that is the main source of potential harm – and what is considered appropriate use of data is contextual and personal. Policy makers need to consider the value that data can deliver throughout its lifecycle, the data governance that is needed to ensure trustworthy data practices by all stakeholders in the data ecosystem, and how technology can enable all of this. For example, if the usage impacts an individual directly it would require different levels of governance than data which is used in an aggregated and de-identified manner.

6. The economical control of data. Although data is exchanged between different legal entities, the risk is considerably smaller, if these entities belong to the same group of companies.

The above criteria are supposed to serve as a starting point to the discussions necessary to clarify how regulation can appropriately consider and address the presence of risk.

3- WHERE SHOULD THE RISK-BASED APPROACH BE VISIBLE?

Adopting a risk-based approach will allow resources to be allocated most efficiently. A one-size-fits-all approach where resources are applied evenly can inadvertently lead to a 'tick box' approach with the focus on meeting regulatory requirements rather than on combating risks and keeping data safe efficiently and effectively. Companies are in the best position to evaluate the risks that their data processing poses to interests of data subjects. The following sections have to be addressed in order to implement a risk-based approach:

---

[2] *"Unlocking the value of personal data: From collection to usage"*, World Economic Forum. Prepared in collaboration with BCG. February 2013. http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf

3- 1- Accountability and administrative burden

DIGITALEUROPE believes all organisations engaged in the processing of personal data, including controllers and processors irrespective of their size, should be held accountable for implementing appropriate, demonstrable and effective technical and organisational measures to ensure compliance with the Regulation.

However, to avoid new types of burdens and modalities on organisations and data protection authorities like those resulting from the detailed and prescriptive proposal, a simpler, and outcome-based organisational accountability obligation should be introduced. To ensure optimal data protection, the Regulation should provide enough flexibility to allow different organisations to implement the most effective technical and organisational measures.

Accountability is a well-established principle of data protection, found in existing guidance such as the OECD Guidelines and APEC Privacy Framework and in the laws of for example Canada and Mexico. Regulators, industry and advocacy groups (such as Center for Information Policy Leadership) have further defined the essential elements of accountability.

Essential elements of effective privacy programmes include: sufficient management oversight; policies, processes and practices to make the policies effective; risk assessment and mitigation planning procedures; adequately skilled data protection staff; awareness and training of staff; internal enforcement; issue response and remedies to those whose privacy has been put at risk. Such programmes should be tailored according to the type of the organisation, the nature of the processed personal data and the state of the art of technologies and available methodologies, for example to carry out a data protection impact assessment.

3- 2- Data Protection Impact assessments (DPIA), Data Protection Officers (DPOs), PIAs and prior consultation

The proposed DPIA obligation is problematic. DIGITALEUROPE believes that no specific type of DPIA should be mandated nor should the assessment obligation be reserved to any specific type of processing. DPIAs are one method, among others, to achieve the ultimate objective of ensuring that risks to privacy have been identified and proper mitigation planned in a timely fashion. Today, depending on the size of the organisation, tens, hundreds or even thousands of DPIA's of various kinds are made annually to identify risks and to plan mitigation thereof. Different types of assessments are needed to properly assess different activities. Organisations are constantly searching for best methodologies for such risk identification and mitigation planning. Such methodologies constantly evolve, often in a cooperative, at times in an overlapping way, through efforts by practitioners, academia and various standardisation bodies, and such incremental improvement should not be hindered by mandating any specific type of assessment. Instead, constant development of existing methodologies and adoption of state of the art technologies and methodologies should be encouraged.

Some discussion of the EC proposal has focused on aspects of the Regulation that might increase the compliance burden for data controllers. While elements of the EC proposal adhere to a risk-based approach, others do not, and this inconsistency creates some unnecessary complexity. For example, mandating a DPO for a company just because they have more than 250 employees (Art 35.1 b) appears to fit under a prescriptive approach, rather than a risk-based one.

Similarly, mandatory privacy impact assessments could be justified as part of a precautionary approach provided the criteria that trigger a DPIA are not too broad, and provided there is no automatic link with Article 34 (prior consultation).

Prior consultation should take place when processing is based on either exercise of public authority (Art. 6.1 e) or legitimate interests test (Art. 6.1 f) and the processing in question is likely to present specific significant risks to data subjects. This means e.g. that a prior consultation should not be needed when processing is based on consent or contract. Processing of e.g. location data in itself, even when it is identifiable, should never be seen as presenting specific risks triggering prior consultation or authorisation process.

The supervisory authority's interpretation on what activities are likely to present specific risks requiring prior consultation (art. 34.2. b) needs to be subject to the consistency mechanism to avoid fragmentation across the EU. It is not sufficient to refer to the consistency mechanism only in case of processing related to several member states or in case of impact to free movement of personal data within the union (art 34.5).

Given the nature of the proposed sanctions, organisations are encouraged in turning in massive amounts of DPIAs to data protection authorities for prior consultation or authorisation. It is questionable whether data protection authorities would be capable of assessing such amounts of DPIAs in a timely fashion. It is rather likely to paralyse them and to prevent them from carrying out their duty of overseeing and giving guidance to the market place. The UK's Information Commissioner Christopher Graham has recently pronounced similar concerns in an open letter to the UK's Justice Secretary of State Chris Grayling. Mr. Graham cautions against the prescriptive and box-ticking approach proposed in the current draft by stating that if "we could no longer be selective on the basis of a regulatory risk-based judgment, I fear we would be less effective"[3].

There is a strong possibility that such measures would also lead to delays in the market introduction of new products and services without increasing the protection of individuals.

3- 3- Consent

In order for consent to be meaningful, data subjects must be clearly informed about how their data is used. But consent need not always be given "explicitly". Instead, data subjects should be allowed to give consent in any manner that is appropriate within the context of the product or

[3] Open letter from Information Commissioner Christopher Graham to Secretary of State (Justice) Chris Grayling, 24th May 2013, accessed via: http://www.ico.org.uk/news/~/media/documents/library/Corporate/Notices/rt-hon-chris-grayling-ministry-of-justice-20130603.ashx

service that they are using. Consent for the processing of personal data is contextual in nature. Companies relying on consent to process data should be required to ensure that consent is informed and meaningful – and this the Regulation does. But the Regulation should also permit innovators to use different mechanisms to obtain consent that reflect how and in what contexts consent is obtained and data will be used. The term "unambiguous" leaves more scope and is apt for usage in a risk-based approach context.

3- 4- Definition of personal data

The definitions in Art. 4 of the proposed Regulation (concerning personal data, data subject and location) are over-inclusive and fail to reflect many of the risk-based approach considerations highlighted above. Not all identifiers are used to distinguish users in the online context. Some identifiers also exist, for example, in various independent and non-related numbering spaces or as hardware serial numbers before, after and independently from any use of such identifiers to identify a person. The current proposal means that if anyone in the world holds a key to identifying a person, the data is personal data, and must be protected fully as defined in the Regulation. Yet, it would be meaningless, for example, and not at all in line with the actual risk involved, to require manufacturers to treat their production serial numbers as personal data even though some one in the future may independently use the same identifiers to identify individuals.

Consideration of location data provides another important example of where the risk-based approach is extremely relevant and should be taken into greater account. Location data is privacy sensitive only when it reveals an identifiable person's actual location at a given time or when it can be used to establish, through reasonable efforts, the identity of an individual. A mere latitude/longitude or other presentation of a geographical location presents no privacy issues as long as it is not directly linked to an individual. Moreover, at some point location becomes so inaccurate that its sensitivity as location data diminishes (note the difference between e.g. Notre Dame, Paris, France and Europe), while it in some instances could still be sensitive without being "location data". Through privacy by design, actual granular location data originating from individuals can also be used for various purposes without there being any reasonable means to identify any individuals. The currently overly broad definition of 'data subject' should as such be reduced to encompassing those identifiers to cases where – in combination with other specific information - they can be used to identify a natural person.

3- 5- Definition of processing: clear roles between controllers and processors

The current Directive actually already adopts a risk-based approach to the relationship between a data controller and a data processor by clearly demarcating their roles and liabilities. The draft Regulation would fundamentally change this concept – and inject confusion into well-settled contractual relations -- by establishing joint liability between all data controllers and data processors. The proposed Regulation therefore adopts a precautionary approach which seeks to extend obligations and liabilities as widely as possible, allegedly to ensure maximum protection for the data subjects. However, where obligations are directly imposed on the processor by law (as opposed to by contract with a controller) the processor can no longer rely on the controller's

instructions alone, and will thus have a need to "know" the data subject and the context of the data processing in which they are involved in order to understand their obligations to secure the data. Conversely though, because the controller is no longer fully and exclusively in charge of complying with the legal requirements on processing, its own ability to properly assess, understand and manage the risk involved in the processing is damaged. Last but not least, the risk to the privacy of the data subject is also increased, both because documentation and information requirements are duplicated in breach of the data minimisation principle, and because the data subject loses the certainty of having to deal with one single entity, the data controller, when seeking remedy. This blurring of lines between the two parties' roles in every case, without consideration of the context or risk, creates unnecessary compliance burdens, impinges on companies' freedom to contract, and is likely to confuse established consumer relationships.

For example, the documentation requirements may increase the administrative burden on organisations rather than lead to a reduction as envisaged by the European Commission in its proposal. It is unfortunate that there is no requirement to assess the risks of data processing when determining the administrative requirements applied to the data controller and processors in particular situations.

All together, these changes – based on a precautionary rather than the current risk-based approach – will oblige companies to invest in compliance with unnecessary precautionary instructions, potentially diverting resources away from innovation and value creation, with a corresponding impact on jobs and growth. It remains a source of on-going frustration to industry of all kinds that this issue is not well understood, and that the potential impacts of such a change to the status quo are routinely downplayed.

3- 6- Breach notification

The Regulation's personal data breach notification regime should be flexible enough to address the different levels of risk different breaches pose to the data subjects affected. Further, obligations imposed on companies which suffer a breach should take into account any risk-mitigating measures companies took before or after the breach took place.

More specifically, notifying DPAs and data subjects should be required only when a breach is material - for instance when it is likely to severely affect the rights and freedoms of the data subject. A blanket obligation to notify all breaches would not only drain the resources of companies and DPAs, but would also keep both sides from focusing on grave breaches which pose high risks. A similar argument has been put forward by the UK's Information Commissioner Christopher Graham who warns that the stringent obligations put on companies to comply with the Regulation will unnecessarily flood DPAs, forcing them to move towards a process-driven approach as opposed to advising and guiding companies based on the inherent risk in their processing[4]. Furthermore, notifications should not be required if, prior to the breach, the data controller had applied appropriate technological protection measures to the data: for instance, if

[4] Graham, Christopher, Information Commissioner, letter to Rt Hon Chris Grayling MP, 24th May 2013, accessed via http://www.ico.org.uk/news/~/media/documents/library/Corporate/Notices/rt-hon-chris-grayling-ministry-of-justice-20130603.ashx

the data had been encrypted or pseudonymised, the risk posed to the data subjects concerned will be minimal. Last but not least, notification should not be required if, after the breach, the controller took measures which ensured the data subject's rights and freedoms are no longer likely to be affected.

3- 7- Sanctions

The draft data protection Regulation imposes penalties and sanctions which are significantly more onerous than those applicable under the existing rules in the various Member States. In addition, the Regulation will centralise the rather fragmented enforcement powers and practices that are currently exercised across Europe.

Depending on the breach, fines are intended to be allocated in three layers of either 0,5%, 1% or 2% of annual worldwide turnover. The lower level of 0,5% would be applicable for example to breaches relating to subject access requests. The middle level of 1% would be applicable in a range of specified circumstances, for example failure to comply with the right to be forgotten; and failure to maintain documentation relating to processing operations. The highest level, which attracts a fine of up to 2% of annual worldwide turnover, is applicable to more serious breaches, for example processing data without a sufficient legal basis; failure to notify a personal data breach; and failure to appoint a Data Protection Officer.

The level of fines is far beyond what currently applies in any EU member state and could be seen as unduly onerous and disproportionate for several reasons:

First, in some cases the fines envisaged are disproportionate to the possible damage suffered. For example, failure to appoint a Data Protection Officer would trigger the highest level of fine, yet it is not necessarily clear exactly what level of harm such a failure would cause.

Whilst the administrative sanctions proposed have been closely focused upon, the Regulation provides data protection regulators with other key powers of sanction. This includes the power to serve enforcement notices; impose temporary or definitive bans on processing; suspend data flows to third countries; and through new investigative powers, the ability to effectively audit companies by requesting access to certain information or access to company premises. The Regulation also entitles data subjects to go to Court where their rights have been infringed and seek compensation from the controller or processor if they suffer damage as a result of unlawful processing. In relation to compensation where more than one controller or processor are involved in the processing, each shall be jointly and severally liable for the entire amount of the damage. This is likely to focus both the controller's and processor's attention on the contractual protection offered by warranties and indemnities. In view of the fact that the Regulation envisages not only fines but also other, non-pecuniary, types of sanctions and provides for joint controller-processor liability, one could argue that the scope and height of fines should be restricted. For instance, the Regulation could provide that fines should be meted out only after other measures (e.g. enforcement notices or processing bans) have been imposed and failed to force a company to fulfill its obligations under the Regulation.

Potential sanctions are a crucial factor for companies to consider when taking a risk-based approach to data processing. The draft Regulation does state that an administrative sanction

shall be effective, proportionate and dissuasive. It also states that the amount of the fine will take into account such things as the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the technical and organisational measures in place and the degree of cooperation with the supervisory authority in order to remedy the breach. However, the draft rules also provide prescriptive situations where certain levels of fines should be imposed on a company. Moving away from this prescriptive drafting and towards a risk-based approach would improve these rules and provide flexibility for regulators to impose fines in proportion to the damage caused. It will allow regulators to focus on factors such as the scale of processing and the actual harm caused to the individual when assessing the appropriate level of fines.

4- BENEFIT-BASED APPROACH AS COUNTERPART OF THE CONSIDERATION OF RISK

The binary character of the draft is also visible within the indistinct assumption that every right granted to a data subject would benefit him/her. The right to be forgotten or the right to transfer personal data (Art. 17, 18) should be thoroughly analysed with regard to the vast variety of the thinkable scope of these rights. This becomes especially obvious comparing the handling of data within the online world of the digital economy with handling such data in the context of essentially industrial or other offline commercial activity not focused on the use of personal data. The benefit of a data subject to be entitled to transfer his or her personal data processed by the family owned local business around the corner in the course of a customer rewards program may therefore be reconsidered. The same applies to the employee file of an employer that is very unlikely to be handed over to the next employer by the data subject and is of rather limited use for himself. On the other hand, both examples require an immense effort of the data processor to transfer the respective personal data into a generally conferrable data format.

5- FOCUSING ON PREVENTION

A risk-based approach is focusing its efforts on prevention e.g. avoidance of high risk data breaches to occur in the first place. Hence, this approach presumes a regulatory environment that is focused on high risk data processing, the fostering of trust between regulator and regulated, promoting accountability e.g. rise to the top of well-intended and well informed companies and a restrictive use of punitive sanctions (last resort). Such an approach holds the potential to go beyond "best-practice" promotion and creates an environment where anonymised "bad-practices" are mediated by regulator but willingly shared in the industry and safe procedures for whistle-blowing reporting are developed. Knowledge sharing of effective preventive measures and solutions are promoted and contribute to the creation and accumulation of an experience base that can be reused across sectors and members states.

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 57 global corporations and 34 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, Bang & Olufsen, BenQ Europa BV, Bose, Brother, Canon, Cassidian, Cisco, Dell, Epson, Ericsson, Fujitsu, Hitachi, HP, Huawei, IBM, Ingram Micro, Intel, JVC Kenwood Group, Kyora Document Solutions, Kodak, Konica Minolta, Kyocera Mita, Lexmark, LG, Loewe, Microsoft, Mitsubishi Electric, Motorola Mobility, Motorola Solutions, NEC, Nokia, Nokia Siemens Networks, Océ, Oki, Oracle, Panasonic, Philips, Pioneer, Qualcomm, Research In Motion, Ricoh International, Samsung, SAP, Sharp, Siemens, Sony, Swatch Group, Technicolor, TP Vision Texas Instruments, Toshiba, Xerox, ZTE Corporation.

NATIONAL TRADE ASSOCIATIONS:

Belgium: AGORIA; **Bulgaria:** BAIT; **Cyprus:** CITEA; **Denmark:** DI ITEK, IT-BRANCHEN; **Estonia:** ITL; **Finland:** FFTI; **France:** Force numerique, SIMAVELEC; **Germany:** BITKOM, ZVEI; **Greece:** SEPE; **Hungary:** IVSZ; **Ireland:** ICT IRELAND; **Italy**: ANITEC; **Lithuania**: INFOBALT; **Netherlands:** ICT OFFICE, FIAR; **Poland:** KIGEIT, PIIT; **Portugal:** AGEFE; **Romania:** APDETIC; **Slovakia:** ITAS; **Slovenia:** GZS; **Spain:** AMETIC, **Sweden:** IT&Telekomföretagen; **United Kingdom:** INTELLECT
Belarus: INFOPARK; **Norway:** IKT NORGE; **Switzerland:** SWICO; **Turkey:** ECID, TESID, TÜBISAD; **Ukraine:** IT UKRAINE.