4

BRE-JBZ

From: Kaai, Geran
Sent: vrijdag 3 april 2015 15:55
To: Verweij, Ellen
Subject: FW: Data Protection: ICDP - Controller/Processor Liability
Attachments: ICDP - General Explanation Liability Controller Processor.pdf

---

From: [redacted] [mailto:[redacted]]
Sent: woensdag 14 januari 2015 15:30
To: Kaai, Geran
Cc: Leenders, Sophie
Subject: Data Protection: ICDP - Controller/Processor Liability

Dear Geran Kaai,

On behalf of the **ICDP – The Industry Coalition for Data Protection**, I would like to wish you a Happy New Year.

Although the issue is not currently on the agenda for DAPIX discussions, we would like to bring to your attention the issue of **shared responsibility between data controllers and processors** as set out in Article 77, which is of particular concern for ICDP.

The article as proposed by the European Commission could seriously undermine established commercial/civil law and business practices while providing no benefit to citizens or businesses.

We have therefore outlined our concerns regarding this issue and provided some suggestions in the attached document. ICDP is currently in the process of putting together specific amendments to the issue which we will also share with you in the near future.

We hope this can be of use to you and would be **happy to discuss the issue further with you in a meeting** at a time that is best suitable for you.

Kind regards,

[redacted]
Manager – Digital Economy Policy

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

[redacted]

EXPECTED BIG OVERHAUL IN CONTROLLER-PROCESSOR RELATIONS

Controllers and processors – who are they?

Today, data protection obligations and responsibilities are governed by a dual concept based on the distinction between "controllers" and "processors". The category under which a data processing operation falls determines who has the primary responsibility for ensuring compliance with data protection rules, who is accountable to individuals and who is liable in case of mishandling of personal data.[1]

Most importantly, **this differentiation between "controllers" and "processors" serves to establish a clear allocation of roles and responsibilities and helps to clarify complex cases, where the data is processed by more than one entity** (e.g. outsourcing of processing).

Why is this important?

According to this model, it is clear that responsibility and liability vis-à-vis the data subject[2] as well as for compliance with the legal requirements **lies with the controller**. The activities of the processor, acting "on behalf of the controller", are determined by the mandate given by the controller to the processor and hence mostly governed by contracts. Should the processor go beyond this mandate, it becomes a (joint) controller, rather than a processor.

This system ensures that the increasingly wide-spread practice of outsourcing does not insert confusion in the system: the consumer knows whom to turn to in case of a problem, and companies have clarity on roles and responsibilities.

When a consumer has a contract, let's say, with an electricity provider, it does not and should not matter whether the company in question processes directly his/her data or outsources it. In case of a data breach, it will be the electricity company who knows the consumer and can therefore notify him/her, and will also be the one who will need to take responsibility for the loss or mishandling of the data. If the processor is the cause of the breach, it should not concern the consumer, the electricity company will be able to take the necessary actions based on its contractual relationship with this processor.

This allocation of liability and responsibility is **grounded in and justified by many practical considerations**. It is the controller that retains a direct relationship with the data subject, determines what information to collect, for what purpose, decides how it is used, whom it is shared with, for how long, etc. The processor, instructed to process the entirety or part of this data, has no direct knowledge of any of the above and relies on the controller to provide the necessary information about what it is expected to do with that data and also about the nature of the data (anonymous data for instance will not be covered by the data protection obligations, whereas personal or sensitive data will have different rules).

[1] A detailed explanation of these can be found in the Article 29 Working Party Opinion (1/2010) on the concepts of "controllers" and "processors"

[2] Whose personal data is being processed.

The processor, hence, has no influence on the essential decisions influencing compliance; its main obligation is to follow the instructions of the controller.

A controller may also use many processors for different purposes, so it is crucial that it remains in control in determining who does what.

Such a clear allocation of roles and liabilities is beneficial to both parties, because it clearly establishes the legal certainty and primacy of the controller in determining the purposes and the substantial means which are essential to the core of lawfulness of processing, such as the data to be processed, length of storage, access, etc. Through a contract it also clarifies the obligations of the respective parties to carry out certain functions as well as consequences related to failures to properly execute such functions and may further specify the required documentation and other factors that are important to inform each party of expectations and obligations.

Why change this clear and useful distinction?

Neither industry nor regulators, including the Article 29 Working Party[3] have found any reason to think that the current distinction between controllers and processors is no longer relevant or workable.

However, the European Commission noted that new technologies are enabling ever smaller and less experienced controllers to engage in a wide range of online commercial activities. This has raised two types of concerns. First, that controllers may not be able to carry out their obligations due to lack of knowledge, skills or resources. Secondly, that small controllers may not be able to impose the correct contractual provisions on processors due to a knowledge gap or lack of leverage when negotiating the agreement. In the European Commission's opinion, this second issue may be even more prominent in the context of cloud computing.

To address these, the European Commission argued that the definitions and concepts of "controllers" and "processors" need to be clarified and detailed in specific provisions. In fact, it suggested that "harmonized rules" on the responsibilities and liability of both controllers and processors are needed to foster legal certainty.

In January 2012, the European Commission put forward a proposal for a General Data Protection Regulation, in which it suggested to introduce the concept of "joint" liability, allowing data subjects to seek redress from both the controller and the processor. This would in practice erase one of the main pillars of the current distinction, making processors directly liable.

[3] An advisory committee composed of the representatives of Data Protection Authorities of the EU.

Challenges resulting from blurring the roles and responsibilities

As mentioned above, one of the core reasons for distinguishing between controllers and processors is to ensure the workable and practical allocation of responsibilities and liability. Creating joint and equal liability goes counter to this and creates significant and negative unintended consequences.

It undermines controller/processor relationships. Under the current system, processors can rely on the controllers' assertions as to the nature of the data, as well as on the instructions on what processing to carry out, how long to keep it, whom to share it with, etc. If the processor has independent obligations, then each instruction given will need to be evaluated (and possibly changed) based on how the processor interprets its compliance obligation. The controller loses control over its instructions and there will likely be both delays and misunderstandings related to the interpretation of obligations.

It also creates an unjustified compliance burden, as it duplicates compliance efforts and generally increases the cost and complexity of processing. It is impossible to assume that a processor can learn the business model of all of its customers and be fully aware of how they collect and use the information. Making processors responsible for understanding a range of these services at a minimum will dramatically increase costs, if at all possible. This would create an effective barrier to SMEs to enter the market as processors.

It also undermines some of the fundamental privacy principles, like data minimization. This is because, under the current system, the processor has no need or benefit from knowing detailed information about the data subject. With a direct obligation placed on the processor, they will need to have direct knowledge of the data subject and much more information about the data and its broader use. This would trigger more collection and dissemination of information, rather than less.

Finally, joint controllers must be allowed to contractually allocate their respective liability, thereby reflecting their respective roles and direct or indirect relationships with data subjects. This is crucial, as joint controllers do not necessarily have a direct relationship with the data subject and they do not control the same kind and amount of personal data. Should this option not be available or restricted, there is a risk, in line with the above, that a joint controller may have to gather additional information on the data subject to be able to respond to that data subject's query or complaint, which would run counter to the principle of data minimization. The joint and several liability should thus only apply to joint controllers where they have not determined their responsibilities and liabilities in a written arrangement, as required by Article 24.

Potential solutions for consideration

The core element and reason for the distinction between controllers and processors, namely to allow for easy allocation of roles and responsibilities, needs to be preserved.

However, the current debate has demonstrated the need to explain and assist both controllers and processors to better comply with data protection requirements. Such solutions could include the following:

- Material and guidance for SME controllers to better inform them of their obligations and their rights when outsourcing.
- Fact sheets, which SME controllers can provide to processors related to the nature and important aspects of the personal data in question to help both processors and controllers agree on the appropriate level of security and service.
- Guidance that helps appropriately define the roles of processors and controllers in specific engagements and in this way ensure that each party undertakes appropriate responsibility.

Many processors already provide their customers with such information and guidance, so the above mentioned materials could be developed together with industry within a foreseeable timeframe.

Many processors also adhere to internationally recognized standards. Raising awareness around these and explain their benefits could also help SME controllers to make appropriate choice when entrusting data on a third party.

Yours sincerely,

Members of Industry Coalition for Data Protection (ICDP)

ICDP is comprised of 20 associations representing thousands of European and international companies who are building, delivering, and advancing the digital experience. Members of ICDP include: ACT | The App Association, American Chamber of Commerce to the EU (AmCham EU), BSA | The Software Alliance (BSA), Computer and Communications Industry Association (CCIA), European coordination committee of the radiological, electromedical and healthcare IT industry (COCIR), DIGITALEUROPE, European Association of Communications Agencies (EACA), E-Commerce Europe, European Digital Media Association (EDiMA), European Multi-channel and Online Trade Association (EMOTA), European Publishers Council (EPC), European Internet Services Providers Association (EuroISPA), Federation of European Direct and Interactive Marketing (FEDMA), GS1, IAB Europe, Interactive Software, Federation of Europe (ISFE), Japan Business Council in Europe (JBCE), TechAmerica Europe and the World Federation of Advertisers (WFA)