BISSANTZ

To The European Commission

Comments on the EDPB Guidelines Controller-Processor

Nuremberg, October 9, 2020

Ladies and Gentlemen,

We are a software company and suffer due to the GDPR. We only offer services on the systems of our customers but nevertheless, our customers and our Data Protection Officer wants us to conclude Data Processing Contracts according to Article 28 (3), what we do. You are probably not aware of how much additional bureaucracy you generate by your regulations. Here are my suggestions to make your ideas usable for small companies as ours and to reduce bureaucracy:

1. It is a good German tradition to have clear laws. There is no need to repeat in contracts what is already governed by law. The GDPR is binding, there is no need to assure a Controller that the Processor will respect the law. A contract between the Controller and the Processor should therefore only be necessary, if
   - the purpose of the relationship is at least in part to process personal data, or
   - sensitive personal data is affected.
2. The content of the contract should not repeat Article 28 (3). This article should be modified in a way that letter a) to h) are binding between a Controller and a Processor, whether they have a contract or not. The Contract should only govern the content of the first paragraph of Article 28 (3) in cases of my suggestion 1.

With regards to your Draft of the Guidelines I have a contrary opinion to page 26, number 81. For me, all three examples should not need an additional contract, since everyone must abide by the law. This also applies to some comments in Part II of your draft.

Information and data security is very important to us. We are participating in the TISAX program of the automotive industry, which ensures an up-to-date Information Security Management System (ISMS). A reassessment takes place every three years. You may consider to ease the obligations of closing a contract if the Processor has a certified ISMS.

I published an article in the "Informatik Spektrum" by Springer Verlag. You can find more details there or I can give you more background on my suggestion. We have to conclude the contract because our employees **may** have contact to personal data, and if so, it is basically the name and some company related data of the company the person works for. For me, this is typical in B2B-situations. We are tied to law and the confidentiality agreements anyway and there is no need for an additional contract. The example "IT-consultant fixing a software bug" on page 26 makes it clear.

Please do not hesitate to contact me in case of any questions.

Yours sincerely

BISSANTZ
Bissantz & Company GmbH
Nordring 98 · 90409 Nürnberg
T +49 911 935536-0
F +49 911 935536-10
service@bissantz.de
www.bissantz.de

Dr. Bertram Küppers

CFO

Bissantz & Company GmbH
Nordring 98 90409 Nürnberg
T +49 911 935536 - 0
F +49 911 935536 - 10
service@bissantz.de

Geschäftsführer
Dr. Nicolas Bissantz
Michael Westphal

USt-IdNr. DE181064258
Steuer-Nr. 241/118/25048
Amtsgericht Nürnberg
HRB 15590

www.bissantz.de