ATOS CONFIDENTIAL

Atos, Burgemeester Rijnderslaan 30, 1185MC Amstelveen

European Data Protection Board (EDPB)

24 June 2022
Ref.: Consultation
Re.: Feedback on Guidelines 04/2022 on the calculation of administrative fines

Dear representative of EDPB,

EDBP has opened the consultation with regards to "Guidelines 04/2022 on the calculation of administrative fines under the GDPR". As our company is dealing with many contracts including the processing of data on behalf of our customers, we often are in the position of data processor in terms of the GDPR. The following input and feedback is based upon both the commercial contracting and public tendering procedure that our company is engaged in on a daily basis.

Over the course of the past years, we repeatedly encounter discussions the topic of penalties when it concerns personal data processing, where our customers blindly want to pass through any penalties, they might receive from a supervisory authority concerning personal data, on through us as their processor. It often includes a broad, unlimited indemnification for these purposes as well. This is an unpleasant and also unreasonable practice, which is experienced throughout the entire sector for companies that are data processors. A contractual clause coming from controllers is not reflecting any form of balance throughout an intended agreement and the current legal and regulatory framework is completely lacking any guidance on how parties should deal with this matter and gives too much freedom for controllers to write off its risks to its processors.

Such a clause, a full and uncapped indemnification including passing through penalties, is not market conform practice. Any penalties, fines, measures etc. imposed by an authority to a controller, are based upon the controller specific circumstances, looking at revenue, size but also track record and cooperation with an investigation as is defined in the GDPR. Passing through such penalties is therefore highly inappropriate. As another example, Dutch Minister has also shown that such practices are unacceptable (https://www.nldigital.nl/news/avg-boetes/).

When negotiating related contractual terms, parties are dealing with contractual liability, where the goal is to reimburse damages, while a penalty is no damage due to the punishing aspect. Something went wrong at the controller's end, else there would have been no investigation at the

controller resulting into a fine/penalty etc. imposed at the controller. Should authorities impose penalties to a controller, the penalty as said is based upon the controller's specific circumstances. The processor has absolutely no influence or say in the process, investigation or anything related. If for example, the controller has received a penalty in the past, this will influence the level of the penalty, or other aspects of its capacity as the investigated data controller.

Due to the administrative law aspects of penalties, there are no possibilities at all for the processor to oppose to the penalty, as the processor is not seen as an interested party, should a penalty be passed through by the controller onto the processor. Hence, the processor is left without any protection and means to defend and influence the situation at hand.

Passing through penalties can also result in the unlawful situation of double penalties for the processor, for example:
1. There is a data breach at the processor, creating a reporting duty to the authorities for both the controller and the processor.
2. The processor duly reports the data breach, the controller does not.
3. As a result thereof, the authorities fine the controller because it did not report the data breach and fines the processor for the data breach.
4. Processor pays its own fine but also gets the controller's penalty for not reporting the data breach despite its obligations.
5. This causes the unacceptable situation when passing through fines/penalties etc. as the processor is paying its own penalty but also needs to pay the penalty that the controller has received, but which is passed through due to the contractual clauses.

Besides the above, should a processor breach its obligations (either under the data processing agreement or GDPR), it would possibly raise general liability as contracted in the services contract. This means that a processor can also be confronter with data processing agreement liabilities ánd general services agreement liabilities. This is another factor why the current guidance and protection in the existing legal framework for data processing is fully lacking. Because without services, there would be no data processing and no service provider should be punished for being a processor and processing data by order of the controller.

Concluding, the current GDPR and the related legal framework is missing its focus on the processing parties of data processing. There is no attention to which party (controller and/or processor) has attributably breached any of the obligations under the agreement and/or GDPR. It also lacks consideration towards the distinction between contractual liabilities and legal liabilities arising out of the GDPR. For any future improvements, there ought to be guidance on how penalties are imposed and creating protection for processors who are being ignored by the current set-up. In our sector, processing of personal data is an inseparable activity of the services we render to our customers, but we shouldn't be sentenced for being a service provider and a processor.

The above is a summary of arguments and experiences that our company has built up during the last couple of years. We urge the European Data Protection Board to engage our feedback as set-out in this letter during its consultation and thank you for offering the opportunity to provide feedback in this phase.

Yours sincerely,

Gigi van Hout
Legal Counsel