

Data Protection – Joint Controller

By Carmen Lupșan

In Romania, there is a lack of awareness about liability when jointly processing personal data, both on the side of data controllers and advisers. Frequently, all parties involved in a case of data processing are classified as data controllers, “just to be on the safe side” so they must all observe their rights and obligations.

For the reasons presented below, that is not recommendable.

Regulation

There is nothing new about joint responsibility when it comes to data protection. Although it was not expressly regulated by law, it has been a recurrent subject in practice¹. It is regulated in art. 26 of the General Data Protection Regulation (GDPR) as follows:

‘Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.’

In practice, it is difficult to draw a clear line in determining the position of the parties involved. For the time being, there is no guidance in this regard from the data protection authorities (except in Belgium and Norway), which makes the analysis of the case facts more difficult.

The European Court of Justice gives a broad meaning to the term ‘joint responsibility’. According to its jurisprudence, even Facebook and the operators of a Facebook page can be under circumstances joint controllers.²

Why is the classification important?

Controllers are liable for personal data that they process. A joint controller is also liable for the processing activity of the other joint controllers. The data subject can exercise its rights – including compensation for damages resulting from the data processing – against each and every joint controller. This makes it even clearer that joint controllers should have agreements about the distribution of their rights and obligations, although not necessarily in form of a contract (other than in case of a data processor).

Especially relevant is the liability issue in this context. If third parties file claims, each joint controller will be, in principle, liable to the full extent. Often one of them runs a higher risk of facing claims (e.g. because he is closer to the data subject, having a direct contractual relationship). If the rights and obligations of every joint controller are stipulated in a contract, their liabilities will also be easier determined internally between the respective joint controllers, to facilitate any claim for damages between them.

Determining obligations is also crucial between joint controllers regarding the allocation of the significant fines³.

¹ In its opinion of 1/2010, on the concepts of ‘responsible’ and ‘processors’ WP 29 has, among other things, named the joint controller and has given several examples.

² Economic Academy Schleswig Holstein, C 210/16

How can a company determine whether it is a joint controller?

The determination is difficult to make in practice, especially when the joint controllers are involved in a project to a different extent and at different moments in time. Furthermore, the processing of the same personal data does not necessarily mean that the processors are jointly liable.

Considering the accountability principle, a controller should check, based on the actual situation, to what extent purposes and means truly prove to be jointly determined with another controller, and should document the result accordingly (data protection impact assessment). Of great importance is the influence exercised by every party to the data processing in each case. It is thus to be determined, why (scope) and how (means) the data processing is carried out, respectively who can actually influence these two aspects.

- **Why?**

What result will the data processing have, and to what extent can a controller determine or at least influence this purpose? An important role in answering this question might also be the beneficiary of the processing.

- **How?**

What technical and organizational means are used in data processing and who might have an impact on it?

Conclusion

Determining joint responsibility is of high importance, considering the liability towards the aggrieved party and the significant fines as per GDPR. In the absence of express guidance by the Romanian Data Protection Authority, the joint controllers must agree upon the exact delineation of their rights and obligations.

Contact and further information:



STALFORT Legal. Tax. Audit.
Bucharest – Bistrița – Sibiu

Office Bucharest:

T.: +40 – 21 – 301 03 53

F: +40 – 21 – 315 78 36

M: bukarest@stalfort.ro

www.stalfort.ro

³ As per art. 83 paragraph. 4 lit. a (for companies up to 2% of worldwide annual turnover) in the case of infringements against art. 26 GDPR