

Public consultation: Comments on the “Guidance – Addendum (Annex to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation)

Certification criteria assessment

Adopted on 06 April 2021”

This paper exclusively reflects the views of its author.

“Par. 3 Submitting a Certification Scheme TP a SA point 9 “What types of organization will ask for a certification? E.g.: is the scheme aimed at a specific sector, or at a specific type of organization like associations or SMEs?”

Regarding this fundamental question representing a propaedeutic point for the whole certification mechanism, it will be desirable and at the same time beneficial to have certification mechanism also specifically related to multinational groups. Indeed, the current global market requires mechanisms able to certificate processes of personal data and / or the security of products and services on a global dimension. Often, for example, the product is produced in a third country and thus it will be advantage for everyone (data subjects – market - Institutions) to have specific certification mechanisms on this. At the same time, it would be important to have additional guidance and specific certification mechanisms in relation to the processes in the context of data transfer. It would be also useful to have more certification mechanisms and certification bodies able to act and issue certificates at EU level with the same validity in each EU Member State.

A concrete example, it could be the case of HR management in multinational group with subsidiaries on different countries. In this kind of scenarios, it would be possible that each subsidiary is a controller of its local employees and at the same time is in a joint controller relationship with a holding. For example, it is possible a scenario where in the same group:

Country A , Company A is a controller in joint relationship with Holding X

Country B, Company B is a controller in joint relationship with Holding X

Country C, Company C is a controller in joint relationship with Holding X

As described in par. **“10.4 Scenario 4: How to handle certification in a joint controllership scenario?”**, responsibility should be clarified in the joint controllership arrangement. In addition to this, anyway, it could be beneficial to have also the possibility to carry out a kind of “joint application” for group of companies for the same ToE. Instead, this would be efficient in terms of coordination and would cover by one mechanism several subsidiaries of the same group. Otherwise, as in the example above, it would be necessary to carry out three different applications.

Marco Costantini

Data Protection Officer