European Data Protection Board
Rue Wiertz 60
B-1047 Brussels
edpb@edpb.europa.eu

FEEDBACK

17/10/2020

Dear Sir(s),

Guidelines 07/2020 on the concepts of controller and processor in the GDPR

As a privacy practitioner (and a data subject) I'd like to draw your attention to GDPR Article 4 (16) and (19), the concept of *one-stop-shop mechanism*, as well as *controlling* and *controlled undertakings within groups of undertakings* that seem to go totally unnoticed in the current draft Guidelines.

While I agree with the basic notions about applicable law (items 12 and 13 of the draft Guidelines) and distinctions between controllers and processors, it's worth noting that

a) When first drafted, some of the key objectives of GDPR included enhancing data controllers' responsibility and strengthening the enforcement of data protection principles and rules, but also increasing the legal certainty and reducing the administrative burden for data controllers[1]. One of the issue identified within the area was the adverse effect of the un-coordinated supervision on as well as inconsistent application of the Directive 95/46/EC faced by multinational enterprises based on multiple Member States. These concerns brought up particularly by the European Data Protection Supervisor (EDPS)[2] lead the EU Commission[3], Parliament[4] and Council[5] to introduce a concept of known as *the one-stop-shop mechanism* as well as a number of new Articles and Recitals[6] that seem to support a possibility of controllership by group of undertakings.

[1] See the EU Commission communication COM (2010) 609, sections 2.2.1 – 2.2.4 and 2.5.
[2] See the Opinion of the European Data Protection Supervisor on COM (2010) 609, item 105 and 147, as well as the Opinion of the European Data Protection Supervisor of 7 March 2012, items 79, 106, 107, 208, 211 and 273
[3] See the EU Commission proposal COM (2012) 11, Articles 4 (13), (16), 35 (2), 51 (2), 53 and Recitals 27, 28, 75, 79 and 97, as well as the EU Commission communication COM (2016) 214, page 4
[4] See the Position of the European Parliament adopted at first reading on 12 March 2014 (P7_TC1-COD(2012)0011), Article 4 (13), 35 (2), 51, 53, 54a, 79 and Recitals 97, 98 and 98a.
[5] See the Position (EU) No 6/2016 of the Council at the first reading, Article 4 (16), (19), 37 (2), 56 (1), (6), 60 and 83 (4) – (6), as well as Recitals 22, 36, 37, 122 – 141 and 150. See also the EU Commission communication COM (2016) 214, page 4
[6] See e.g. GDPR Recitals 22, 36, 37 and 150 providing the definition of an establishment and undertaking, confirming that a subsidiary is an establishment, and depending the case, controlled undertaking (vs. a self-standing controller or processor whose processing activities the group of undertakings controls via a controlling undertaking, as well as Articles 4 (16), (19), 37 (2), 56 (1), (6), 58 (2), 60 and 83 (4) – (6) defining the place of central administration (of a group of undertakings) in EU as the main establishment, enabling appointment of a data

Note also that while *the one-stop-shop mechanism* appears to revolve mainly around appointing the lead supervisor, the latter cannot be identified without first identifying the controlling undertaking and ultimately the group as the controller. According to

i. Article 56 (1) "…*the supervisory authority of the main establishment… of the controller*… shall be competent to act as lead supervisory authority for the cross-border processing carried out by *that controller*…";
ii. Recital 22 "Establishment implies the effective and real exercise of activity through stable arrangements. *The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect*." A subsidiary is therefore an establishment.
iii. Article 4 (16) and Recital 36 "'main establishment' means: *as regards a controller with establishments in more than one Member State*, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment" (of the same controller); *The main establishment of a controller* in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements";
iv. Article 4 (7) and Recital 36 "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, *determines the purposes and means of the processing of personal data*; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." "*Where the processing is carried out by a group of undertakings the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings*, except where the purposes and means of processing are determined by another undertaking" (of the same controller).
v. Article 4 (19) and Recital 37 "'group of undertakings' means a controlling undertaking and its controlled undertakings; A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby *the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for*

protection officer, as one of the key accountability related obligation of a controller, on a "consolidated" basis, appointing the supervisor of the main establishment as a sole interlocutor for the group as well as making the group liable for breaches committed by a subsidiary.

example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings."

vi. Article 58 (2) and Recital 150 "Each supervisory authority shall have all of the following corrective powers: to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case; Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes."

b) All legal entities that have revenue are bound to have customers (either intra-group or external) and liabilities of their own among others in contractual, tax etc. terms. The same goes with various regulatory requirements starting from company, book keeping and labour laws. However, should such duties or liabilities automatically constitute a "control stemming from legal provisions" and place the controllership at a subsidiary level, it would effectively undermine not just GDPR's status as *Lex Specialis*[7] and amendments effected as per EDPS's comments, but also reducing the administrative burden, increasing legal certainty and enhancing data controllers' responsibility as some of the key objectives of GDPR[8] by complicating and possibly even multiplying the governance arrangements needed to demonstrate compliance within large group of undertakings, re-exposing them to variations in the various member state laws and allowing them to potentially "box" e.g. some of their higher risk processing activities in smaller undertakings in order to limit their liabilities towards data subjects and authorities.

c) In some cases – as exemplified by Article 109 of Directive 2013/36/EU as amended and the EBA Guidelines for Internal Governance thereof – parent undertakings are obliged to ensure that their policies and procedures designed to meet those statutory duties are applied across the group in uniform manner. The subsidiaries may be maintained also for some specific purpose, or product[9], that the parent company is either legally unable or unwilling to cater, and/or the subsidiaries do not *de facto* have a possibility *not to utilise* the facilities provided by the parent company. Neither way are the subsidiaries governed fully on "sub-consolidated" basis, and the central administration at the parent company assumes the overall decision making power, which should be the *functional* hallmark of controllership.

---

7 The controller role is assigned by general or sector specific laws and not according to the functional and autonomous concepts defined by GDPR. This would contradict among other the Article 62 of Directive 2013/36/EU as amended.
8 See the EU Commission communication COM (2010) 609, sections 2.2.1 – 2.2.4
9 See e.g. the collective investment schemes operated under Directive 2009/65/EC.

> Applying the above to a fictional financial group A seems to indicate that where A AG of Germany is the mother company and consolidating institution of the financial group A, it would be as per Directive 2013/36/EU required to ensure that its policies and procedures designed to meet the statutory duties arising, among others, data protection regulation are applied across the group. A AG would, therefore, have by virtue of ownership, rules which govern it and the power the personal data protection rules implemented across the financial group and thus be singled out as the controlling undertaking of financial group A. Moreover, this would mean that financial group A would be deemed as the controller that controls through A AG the processing of personal data in undertakings affiliated to it. Subsidiaries of A AG would therefore be deemed as controlled undertakings/establishments instead of self-standing controllers or processors. Moreover, financial group A would be held responsible for any wrongdoings of its subsidiaries.

I'd appreciate if you could reflect and clarify the above matter in the Guidelines. I remain at your disposal should you need any further information or clarifications.