From:	EDPS Website <no-reply@edps.europa.eu>
To:	European Data Protection Supervisor <EDPS@edps.europa.eu>
Sent at:	11/12/19 16:32:11
Subject:	EDPS Website: Contact form

YOUR EU REPRESENTATIVE

European Data Protection Supervisor (EDPS)
Rue Wiertz 60
1047 Brussels
Belgium

Brussels, 11 December 2019

Submitted via the EDPS contact form (https://edps.europa.eu/node/759)

Subject: GDPR issue in the context of the data breach notification procedure applicable to non-EU/EEA companies without an establishment in the EU/EEA

Dear Madam, Dear Sir,

We are writing to you in the hope of obtaining clarification regarding the procedure applicable for data breach notifications by non-EU/EEA companies without an establishment in the EU/EEA.

We act as EU representative appointed pursuant to article 27 of the GDPR and we are confronted with an issue that is crucial to the services that we provide to non-EU/EEA companies. We would therefore greatly appreciate your guidance on this matter.

Indeed, there appears to be a contradiction between the three following texts:

i. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)
ii. Guidelines WP 250 on Personal data breach notification and
iii. Guidelines WP 244 for identifying a controller or processor's lead supervisory authority.

i) Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)

These Guidelines state the following: "*in the absence of an establishment in the Union, a controller or processor* ***cannot benefit from the one-stop-shop mechanism*** *provided for in Article 56 of the GDPR*" (Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Adopted on 12 November 2019 p. 13).

Based on that statement, it appears that a non-EU/EEA company without an establishment in the Union that experiences a data breach does not benefit from the one-stop-shop mechanism and must therefore notify the data breach to all data protection authorities ("DPA's") in the EU/EEA where concerned data subjects are located (which means a potential of 46 DPA's).

This point of view was verbally confirmed during the IAPP Congress in Brussels a few weeks ago by members of the EDPB, the EU Commission and the CNIL.

ii) Guidelines WP 250 on Personal data breach notification

The Guidelines WP250 on Personal data breach notification under Regulation 2016/679 Adopted on 3 October 2017 as last Revised and Adopted on 6 February 2018, state : "*Where a controller not established in the EU is subject to Article 3(2) or Article 3(3) and experiences a breach, it is therefore still bound by the notification obligations under Articles 33 and 34. Article 27 requires a controller (and processor) to designate a representative in the EU where Article 3(2) applies. In such cases, WP29 recommends that* ***notification should be made to the supervisory authority in the Member State where the controller's representative in the EU is established****. Similarly, where a processor is subject to Article 3(2), it will be bound by the obligations on processors, of particular relevance here, the duty to notify a breach to the controller under Article 33(2)*" (p. 18)

iii) Guidelines WP 244 for identifying a controller or processor's lead supervisory authority

The Guidelines WP 244 for identifying a controller or processor's lead supervisory authority Adopted on 13 December 2016 as last Revised and Adopted on 5 April 2017 state that "*The GDPR's cooperation and consistency mechanism only applies to controllers with an establishment, or establishments, within the European Union. If the company does not have an establishment in the EU,* ***the mere presence of a representative in a Member State does not trigger the one-stop-shop system****.* ***This means that controllers without any establishment in the EU must deal with local supervisory authorities in every Member State they are active in, through their local representative***" (p. 10)

Our question

Should non-EU/EEA companies that do not have an establishment in the EU/EEA and that experience a data breach notify all DPA's where concerned data subjects are located (which means a potential of 46 DPA's) or should they only notify the DPA in the Member State where the company's Article 27 representative is established?

We thank you in advance for your time and consideration regarding this very important GDPR matter.

Kind regards,

[redacted]

Founder and Chair Account Manager