March 26, 2018

Attn: Article 29 Working Party

RE: Guidelines on Article 49 of Regulation 2016/679

I. Statement of Interest

ACT | The App Association (App Association) appreciates the opportunity to submit views to the Article 29 Working Party (WP29) on the recently adopted Guidelines on Article 49 of the General Data Protection Regulation (GDPR) 2016/679. The App Association is an international non-profit trade association representing 5,000 small business software application (app) companies and information technology firms in the European Union (EU) and across the digital economy. We advocate for an environment that inspires and rewards innovation, while providing resources to help our members leverage their intellectual assets to raise capital, create jobs, and continue innovating.

Our members take a keen interest in this proceeding because their innovative services are international in nature by virtue of being hosted on major platforms. Our members' business models depend on the free flow of data, and we believe WP29's guidance will play an integral role in untangling the seemingly Gordian knot of confusion surrounding various articles within the GDPR. Considering the hefty maximum penalty[1] imposed on an entity found in violation of the GDPR, the regulation's compliance will depend on clarity in its provisions. This is especially true for small business app companies that cannot bear the financial burden of the regulation's statutory penalties.

[1] GDPR Art. 83(5) (stating that a DPA may impose an administrative fine of €20,000,000 or 4 percent of the company's global annual revenue, whichever is greater, for violating Article 49).

1401 K Street NW Suite 501
Washington, DC 20005

202.331.2130 @ACTonline
ACTonline.org /actonline.org

II. WP29 Must Clarify how the GDPR's Article 49 "Public Interest Derogation will Operate with Article 48

It is crucial for small and medium-sized enterprises (SMEs) facing third-country data transfer requests to understand the delineations of "important reasons of public interest," as it pertains to derogation under Article 49 (1) (d) of the GDPR. Given the international reach of our members, it is difficult to discern which law applies when faced with third-party court orders for data.

The App Association asks the WP29 to clarify the meaning of "important reasons of public interest," because a recent European Commission filing[2] that interprets the Article 49's "public interest" derogation is divergent from prior WP29 guidance on the matter. This disparity creates ambiguity and a potentially serious dilemma. An ongoing case in the U.S. Supreme Court between the U.S. government and Microsoft highlighted this issue. The Court is considering whether a U.S.-based warrant that required Microsoft to provide data stored in Ireland was an extraterritorial application of the U.S.'s Stored Communications Act (SCA)[3].[4] We agree with Microsoft in this case that if the Supreme Court adopts the government's interpretation of Section 2703 of the SCA—in effect making it the U.S. law—it would create potential conflict with Article 48 of the GDPR.[5] This is because the U.S. government is requesting, in effect, to have Microsoft provide data stored in Ireland without using the legal mechanisms articulated in the mutual legal assistance treaty (MLAT) with Irish government.

[2] Brief of the European Commission, United States v. Microsoft, No. 17-2, (Dec. 13, 2017). Available at: https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf.

[3] 18 U.S.C. § 2703.

[4] Brief of EU Data Protection and Privacy Scholars, United States v. Microsoft, No. 17-2, (Jan., 18, 2018)). Available at: https://www.supremecourt.gov/DocketPDF/17/17-2/28272/20180118141249281_17-2%20BSAC%20Brief.pdf.

[5] Brief of Respondent, United States v. Microsoft, No. 17-2 (Jan. 11, 2018). Available at: https://www.supremecourt.gov/DocketPDF/17/17-2/27619/20180111205746909_Brief%20for%20Respondent%202018.01.11.pdf.

EU scholars on data protection and privacy law agreed with our position, writing in an amicus brief that "the Court should adopt a clear rule against applying the SCA to data stored abroad" because any application outside of the United States would violate European data-privacy laws because it does not fall under Article 49's derogations.[6] Specifically, the those scholars opined in their amicus that Article 49(1)(d)'s "public interest" exception must be interpreted narrowly and applied sparingly, otherwise Article 49 would overtake Article 48, allowing "a non-EU country [to] bypass the MLAT process any time protected personal data could aid in criminal prosecution [making it so] Article 48's MLAT requirement would have essentially no effect."[7]

The U.S. Congress recently passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which provides the U.S. law enforcement authorities a framework in the form of bilateral comity agreements to request data that may be stored in foreign sovereign nations.[8] We believe this legislation resolves the issues at bar in the U.S. v. Microsoft case, and we fully expect the data protection agencies of EU member states will negotiate with the United States in good faith to better assist the free flow of data. However, there remain more areas of the Article where the WP29 could provide invaluable guidance to industry.

For example, the language in the Guidelines on Article 49 of Regulation 2016/679 contradicts the EU's staunch position that anything more than limited data transfers would undermine the GDPR ("Recitals 111 and 112 indicate that this derogation is not limited to data transfers that are "occasional"").[9] Recital 111 reduces the standard of derogation from narrowly applied to "not repetitive," which is confusingly defined by what it is not -- a relationship that is not systematic.[10] If the EU government wishes to engage, invest, and bring services into the EU, clarity on this issue will be crucial.

---

[6] Brief of EU Data Protection and Privacy Scholars, United States v. Microsoft, No. 17-2, (Jan., 18, 2018)). Available at: https://www.supremecourt.gov/DocketPDF/17/17-2/28272/20180118141249281_17-2%20BSAC%20Brief.pdf.

[7] Brief of EU Data Protection and Privacy Scholars, United States v. Microsoft, No. 17-2, (Jan., 18, 2018)). Available at: https://www.supremecourt.gov/DocketPDF/17/17-2/28272/20180118141249281_17-2%20BSAC%20Brief.pdf.

[8] See H.R. 4943, S.2383.

[9] Guidelines on Article 49 of Regulation 2016/679 (wp262)

[10] Guidelines on Article 49 of Regulation 2016/679 (wp262)

III. Lack of Clear Guidance of Article 49's Specification Requirement Will Inhibit Valuable Services that Utilise Machine Learning

WP29 provides neither a definition nor an example of the term "specific" within the context of GDPR Article 49 of the GDPR. The example it does provide does not address how a company responds with the appropriate level of specificity if a company uses machine learning (ML) to collect the data subject's information.. As WP29 is aware, it is hard for a company to discern and silo data after it has been incorporated into a system, and given the various levels of collection, it is difficult to articulate what data belongs to the data subject and what would be considered anonymized.

The App Association recommends that WP29 provide further guidance on how companies utilizing ML must comply with this requirement of Article 49 of the GDPR.

Conclusion

The App Association appreciates the opportunity to provide these comments to WP29 and hope it takes our considerations into account when publishing its final guidance.

We hereby consent to the publication of personal data contained in this document.

Sincerely,

Brian Scarpelli
Senior Policy Counsel

Joel Thayer
Policy Counsel

McKenzie Schnell
Associate

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005