DigitalOcean Comments on the Guidelines 9/2022 on personal data breach notification under GDPR

November 29, 2022

DigitalOcean is pleased to provide comments on the European Data Protection Board (EDPB) Guidelines 9/2022 on personal data breach notification under GDPR.

DigitalOcean simplifies cloud computing so small businesses can spend more time creating software that changes the world. With its mission-critical infrastructure and fully managed offerings, DigitalOcean helps developers, startups, and small and medium-sized businesses (SMBs) rapidly build, deploy, and scale applications to accelerate innovation and increase productivity. DigitalOcean combines the power of simplicity, community, open source, and customer support so customers can spend less time managing their infrastructure and more time building innovative applications that drive business growth.

While we appreciate the EDPB's efforts to provide guidance on personal data breach notifications under GDPR, we believe that the guidelines create significant operational and practical challenges for companies not established in the EU that do not ultimately benefit data subjects or EU data protection authorities.

By requiring non-EU companies to report notifiable data breaches to supervisory authorities in **every** Member State where an impacted data subject resides, the proposed guidance creates an unjustified disparity between companies established within the EU and those established elsewhere. Whereas EU-established companies are able to report breaches only to a **single** lead

supervisory authority, non-established companies who have appointed a representative in the EU are not afforded the same opportunity.

The proposed amendment to paragraph 73 would also create additional significant operational burdens for non-EU companies that put good faith efforts into complying with the GDPR. Responding to data breaches is a multi-team effort and includes teams such as Security, Privacy, Legal, Engineering, and Communications. These responses require organizations to invest time, money, and people into ensuring that compliance obligations are met. Managing data protection compliance has become increasingly complex with the enactment of new data protection regulations, especially for companies that must contend with regulations across the globe. The EDPB's proposed revision adds significantly to the challenges and complications facing such companies, particularly due to the lack of harmonized breach reporting forms and processes across the Member States' Data Protection Authorities. Instead of collaborating with and developing solutions with organizations, small and large, this creates more legal and regulatory roadblocks that take away from our ability to focus on quality communications to our customers.

The EDPB's proposed revision will likely create a disproportionate burden on small and medium-sized businesses (SMBs). DigitalOcean's customers are primarily developers, startups, and SMBs. By requiring the same rigor in reporting and compliance for both large and small companies, it unfairly burdens smaller businesses who will struggle to devote additional time and resources to satisfying complex breach notification requirements. SMBs help to create healthy competition and innovation across numerous industries; however, by increasing their compliance burdens, it puts unnecessarily high barriers to entry on SMBs and further allows larger organizations that have significantly more compliance resources to maintain their dominant positions.

The proposed revision is also not necessary because existing notification requirements already ensure that data protection authorities have sufficient information to investigate the breach and that data subjects have sufficient information to take remedial action and exercise their rights. In particular, when

reporting data breaches to the data protection authority in the Member State in which their representative is located, organizations are already required to detail the Member States in which data subjects are likely to have been affected by the breach. Moreover, non-established organizations are also already required to provide notice to individual data subjects under Article 34 of the GDPR. As such, time spent notifying additional data protection authorities is unlikely to provide impacted data subjects or the additional data protection authorities any additional benefit.

In summary, the proposed amendment would create significant operational burdens for SMBs without creating significant benefits for data protection authorities or data subjects. The EDPB's previous guidance established a fair balance between the requirement that non-established businesses to notify EU data protection authorities and the operational considerations of businesses that must contend with multiple cross-border breach notification frameworks. For these reasons, we urge the EDPB to retain its previous guidance at paragraph 73.